Buď pánem svého prostoru

Jak chránit sebe a své věci, když jste online

Editovaly Linda McCarthy
a Denise Weldon-Siviy

Edice CZ.NIC

Buď pánem svého prostoru
Jak sebe a své věci chránit, když jste online
Editovaly Linda McCarthy a Denise Weldon-Siviy

Vydal CZ.NIC, z. s. p. o.
Americká 23, 120 00 Praha 2
www.nic.cz

ISBN: 978-80-904248-6-9
Edice CZ.NIC

CZ.NIC | SPRÁVCE DOMÉNY CZ

Hlavní editor: Denise Weldon-Siviy
Řídící editor: Linda McCarthy
Ilustrace: Heather Dixon
Sazba: Lucie Derzsiová

Přeložila agentura Šupito ve spolupráci s týmem Smith Language Services.

– Věnování

Tato kniha je věnována všem dospívajícím, kteří si udělají čas na to, aby se něco dozvěděli o bezpečnosti a o tom, jak se chránit a chovat se chytře při pohybu na Internetu. Také chceme poděkovat všem dospívajícím, kteří se do tohoto projektu zapojili, a dospívajícím, kteří vznik této knihy inspirovali – Ericu a Douglasovi.

– Editovaly Linda McCarthy
– a Denise Weldon-Siviy

Buď pánem svého prostoru

Jak chránit sebe a své věci, když jste online

– Edice CZ.NIC

Předmluva vydavatele

Vážení čtenáři,

dostává se vám do ruky kniha, která vznikla jako reakce na stále častější útoky zaměřené proti domácím uživatelům a jejich počítačům, mobilním telefonům, tabletům a dalším zařízením připojeným k síti sítí, tedy k Internetu. Kniha není jen suchým technickým povídáním o jakýchsi virtuálních hrozbách, ale přináší konkrétní příklady skutečných mladých lidí, kteří se v určité chvíli stali obětí počítačové kriminality či se na počítačové kriminalitě dokonce podíleli. Zde se ostatně nalézá velmi důležitá informace, která by měla být pro všechny uživatele středobodem úvah o vlastním přístupu k zabezpečení jejich křemíkového miláčka. Když totiž pomineme uživatele, kteří se rozhodli vstoupit na dráhu zločinu dobrovolně, jsou zde stále ti, kteří se stali nedobrovolnými pomocníky počítačového zločinu a to kvůli svému laxnímu postoji k vlastní bezpečnosti. Je potřeba mít stále na paměti, že i počítač, který neobsahuje žádná citlivá data a který není používán k přístupu k takovým datům, může být po jeho ovládnutí útočníkem zneužit k páchání další trestné činnosti. Ta však již může být, minimálně na počátku vyšetřování, připisována na vrub uživateli, který prostě jen opominul obranu před možnými riziky. Proto si každé zařízení se síťovou konektivitou zaslouží pravidelnou péči a pečlivé nastavení bezpečnostních opatření. My, kteří se počítačovou bezpečností zabýváme každý den, si dobře uvědomujeme, že pro mnohé uživatele mohou být otázky spojené s počítačovou bezpečností na první pohled komplikované. I proto vítám český překlad této knihy, která k vám přichází prostřednictvím Edice CZ.NIC, jako skvělou příležitost seznámit mladé uživatele Internetu a jejich rodiče s důležitými bezpečnostními pravidly jednoduchou, srozumitelnou a názornou formou.

Pro českého čtenáře má kniha ještě jedno, možná nechtěné, kouzlo. Vzhledem k jejímu zaměření na americký právní systém, normy a místní reálie, najde čtenář při čtení knihy pasáže, které jej pravděpodobně pobaví. Stejně jako se lidé baví historkami o starší dámě, která sušila svého psa v mikrovlnce a pak žalovala výrobce mikrovlnky, neboť v návodu nebylo uvedeno, že mikrovlnka není určena k sušení psů, tak možná čtenáře této knihy pobaví právní důsledky některých nepromyšlených činů náctiletých, které jsou v knize zmíněny. Těžko si například představit, že by u nás byla dospívající děvčata potahována za šíření dětské pornografie kvůli pořízení vlastních fotografií ve sportovních podprsenkách.

Zrovna tak je potřeba upozornit na rozdílný přístup amerického práva k problematice stahování audiovizuálních děl, než jaký platí u nás v České republice. Samotné stahování audio-

vizuálních děl není u nás na rozdíl od USA nelegální, zato zpřístupňování autorských děl na Internetu bez souhlasu autora není ani naším právním řádem tolerováno. Při čtení kapitoly o pirátství si pak přemýšlivý čtenář může zároveň udělat představu o schopnosti amerického záznamového průmyslu prosazovat pouze jeden správný názor. Ať už je to způsobeno schopností prosadit v americké společnosti celospolečenský konsenzus, který zpětně pronikl do knihy, či zda za tím byl lobbing přímo u autorů této publikace, v uvedené kapitole zcela chybí jakýkoliv oponentní názor.

Tyto skutečnosti však nemají vliv na odbornou stránku knihy, která je obsáhlým a kvalitním zdrojem informací o počítačové bezpečnosti a rizicích spojených s používáním Internetu, jak pro náctileté uživatele, tak pro jejich rodiče. Nevím o žádné jiné knize dostupné v českém jazyce, která by takto názorně a přitom nekomplikovaně seznamovala uživatele s riziky, na která by měli být při používání Internetu připraveni. Závěrem bych chtěl čtenářům této ojedinělé knihy popřát, aby jim pomohla „projíždět" informační dálnicí bez nehod a s pocitem bezpečí.

Pavel Bašta

bezpečnostní analytik, CZ.NIC
Praha, 5. prosince 2013

Obsah

Předmluva vydavatele – 9
Předmluva – 23
Komu je tato knížka určena – 25

1. Chraň si svůj prostor – 31
1.1 Výzkum malwaru – 32
1.2 Nachystej si prkno, než začneš surfovat! – 34

2. Poznej své přátele – 39
2.1 Proč malware existuje? – 39
2.2 Viry – 41
2.2.1 Jak se viry replikují – 43
2.2.2 Škodlivé payloady – 43
2.2.3 Nechvalně známé viry – 45
2.3 Červi – 47
2.3.1 Obzvláště zlí červi – 49
2.3.2 Variace a mutace – 51
2.4 Trojské koně – 52
2.5 Botnety – 54
2.6 Sociální inženýrství – 56
2.7 Jak se vyhnout malwaru – 58

3. Škodlivý „ware" – 63
3.1 Spyware – 64
3.2 Adware – 65
3.2.1 Licence pro koncové uživatele (EULA) – 66
3.2.2 Sítě Peer to Peer (P2P) – 67
3.2.3 Bezpečné stahování – 68
3.3 Keyloggery – 68
3.4 Falešné programy a scareware – 69
3.5 Ransomware – 74
3.6 Black Hat optimalizace pro vyhledávače – 75
3.7 Současné a budoucí hrozby – 77

4. Hackeři a crackeři – 81
4.1 Hackeři – 81
4.1.1 Kdo je to hacker? – 82
4.1.2 Černé, bílé a šedé klobouky – 84
4.2 Hackeři chtějí váš počítač – 86
4.3 Nástroje hackerů – 86
4.3.1 Skenovací nástroje – 87
4.3.2 Prolamování hesel – 88
4.3.3 Rootkit – 90
4.4 Voláme bílé klobouky! – 92

5. Jak poslat SPAM na věčnost – 99
5.1 E-mail a SPAM – 100
5.1.1 Co je to SPAM? – 100
5.1.2 Není SPAM protizákonný? – 101
5.2 Spoofing – 103
5.2.1 Falešné adresy – 103
5.2.2 SPAM proxy a relay – 105
5.3 Ťuk ťuk – jak spammeři poznají, že jste doma – 106
5.3.1 Skryté sledování – 107
5.3.2 Scavengery a crawlery – 108
5.3.3 Je vaše e-mailová adresa na prodej? – 109
5.4 Sociální inženýrství – 109
5.5 Aby se SPAM do příchozích zpráv nedostal – 110
5.6 SPIM – 111

6. Kyberšikana – 115
6.1 Šikana se přesouvá do digitálního světa – 116
6.2 Útoky na online reputaci – 117
6.2.1 Frontální útoky – 117
6.2.2 Útoky na identitu – 118
6.3 Ochrana reputace – 119
6.3.1 Vygooglujte se – 119
6.3.2 Pokud potřebujete, obraťte se na odborníky. – 120

6.4 Jak se chránit před kyberšikanou – 121

7. Rhybaření pro peníze – 127
7.1 Co je to phishing? – 127
7.1.1 Jak běžné jsou phishingové útoky? – 130
7.1.2 Kdo se stává obětí phishingu? – 130
7.2 Jak poznat, že na vás útočí rhybáři – 133
7.2.1 Jak dobré podvody jsou? – 133
7.2.2 Jak poznám phishingový podvod? – 134
7.3 Phisheři vašich přátel – 138
7.4 Podfuk s katastrofou – 139
7.5 Nenechte se ulovit phishery – 140

8. Bezpečné nákupy v kyberprostoru – 143
8.1 Základy online nakupování – 144
8.1.1 Co si kupují? – 146
8.2 Potíže s nakupováním – 147
8.2.1 Sběrači dat – 148
8.2.2 Únosci – 150
8.2.3 Online podvod (Fraud) – 152
8.3 Jak nakupovat bezpečně – 155
8.3.1 Šifrování – 156
8.3.2 Secure Socket Layer (SSL) – 158
8.3.3 Digitální podpisy, certifikáty a hašování – 159
8.3.4 Bezpečnostní tokeny – 161

9. Prohlížeč přeje připraveným – 165
9.1 Aby soubory cookies pracovaly PRO vás – 165
9.1.1 Škodí mi soubory cookies? – 166
9.1.2 A co když nechci sdílet? – 168
9.1.3 Sbírání drobků – 169
9.2 Výběr prohlížeče – 169
9.3 Rozhodnutí pro Internet Explorer – 170
9.3.1 Mazání seznamu v panelu adresy – 171

9.3.2 Čištění dočasných souborů, historie Internetu a souborů cookie – 172
9.3.3 Nastavení způsobu zacházení se soubory cookies – 173
9.3.4 Uchovávání citlivých dat – 174
9.3.5 Používání procházení a filtrování InPrivate – 175
9.3.6 Provádění antiphishingových kontrol – 176
9.4 Rozhodnutí pro Firefox – 176
9.4.1 Detekce zastaralých funkcí plug-in – 178
9.4.2 Vypnutí pokročilých možností JavaScriptu – 178
9.4.3 Vypnutí Javy – 181
9.4.4 Používání hlavního hesla – 181
9.4.5 Funkce add-on pro Firefox, které usnadňují život – 183
9.5 Rozhodnutí pro Google Chrome – 185
9.6 Pochopení problému s funkcemi plug-in – 186

10. Soukromé blogy ve veřejném prostoru – 191
10.1 Co je tedy blog? – 192
10.2 Blogy letí vzhůru – 193
10.3 To myslíš vážně?!!! – 194
10.4 Trvanlivost výrobku – 196
10.5 Bloggeři se požírají navzájem – 197
10.5.1 Útočné blogy – 197
10.5.2 Právní důsledky – 199
10.6 Myslet dopředu – 199
10.7 Jak správně blogovat – 200

11. Socializace – 205
11.1 Kde jsou přátelé – 206
11.2 Přátelé: skuteční a virtuální – 207
11.3 Skupiny – 208
11.4 Aplikace třetích stran – 209
11.5 Rhybáři přátel – 209
11.6 Zveřejňování příliš mnoha informací. – 210
11.6.1 Pochybné fotografie – 211
11.6.2 Nebezpečné webkamery – 211

11.6.3 YouTube – 212
11.7 Online rozchod – 213
11.8 Zapípej, ptáčku – 213
11.9 Tipy k zachovávání bezpečí na sociálních sítích – 214

12. Přátelé, slizouni a piráti – 219
12.1 Seznamování se na síti – 220
12.1.1 Kde se slizouni na síti zdržují – 221
12.1.2 Jak se chránit před slizouny – 221
12.2 Lháři, slizouni a kyberstalkeři – 223
12.2.1 Lháři – 224
12.2.2 Slizouni – 224
12.2.3 Kyberstalkeři – 225
12.3 Monitorování Internetu – 226
12.3.1 Monitorovací programy – 226
12.3.2 Bezplatné e-mailové účty – 227
12.4 Pirátství na informační dálnici – 228
12.4.1 Jste pirátem? – 229
12.4.2 Ohrožujete své rodiče? – 230

13. Sportování s porty – 235
13.1 Co je to tedy síť? – 235
13.2 Jak sítě komunikují – TCP/IP – 238
13.2.1 Adresy IP – 238
13.2.2 Datové pakety – 241
13.2.3 Potvrzení – 242
13.3 Volaný port – 242
13.4 Trochu více o šířce pásma – 244
13.5 Požární stěna – 244
13.5.1 Co je to tedy firewall? – 246
13.5.2 Překlad síťové adresy – 247
13.5.3 Jak mě firewally chrání? – 248
13.5.4 Nastavení firewallu – 249
13.5.5 Firewally zdarma – 250

14. Zkuste to bez drátů! – 253
14.1 Už žádné dráty – 253
14.2 Co je to bezdrátové připojení? – 254
14.3 Nejste sami – 256
14.4 Zamknutí sítě WLAN – 259
14.4.1 Stahování nejaktuálnějšího firmwaru – 260
14.4.2 Změna hesla a uživatelského jména k routeru – 261
14.4.3 Změna výchozího názvu sítě – 262
14.4.4 Aktivace šifrování – 262
14.4.5 Další kroky – 264
14.5 Veřejné hot spoty – 265
14.6 Mobilní zařízení – 266
14.6.1 Útoky na mobilní zařízení – 266
14.6.2 Sexting – 269
14.7 Stručně řečeno – 270

15. Jak získat pomoc – 275
15.1 Nezbytné bezpečnostní prvky – 276
15.2 Další vychytávky – 277
15.3 Souhrnná bezpečnostní řešení – 279
15.4 Zálohovací produkty a postupy – 280
15.5 Nástroje pro odstraňování škodlivého kódu – 281
15.6 Dodavatelé bezpečnostních programů – 282
15.7 Aktualizování programu – 283
15.7.1 Nastavení automatických aktualizací – 283
15.7.2 Kupte si novou verzi – 284
15.8 Buďte v obraze, co se týče bezpečnost – 284

16. Vyladění – 289
16.1 Přednostní nastavení firewallu – 289
16.2 Záplatování bezpečnostních děr – 291
16.2.1 Kdo hledá díry? – 292
16.2.2 Proč je dobré aktualizovat v úterý? – 293
16.3 Používání automatických aktualizací – 294

16.4 Vytváření uživatelských účtů – 295
16.4.1 Co je administrátorský účet? – 296
16.4.2 Proč jsou standardní uživatelské účty dobré? – 297
16.4.3 Jak se vytváří nový uživatelský účet? – 298
16.5 Ochrana účtů heslem – 299
16.6 Vytvoření možnosti pro resetování hesla – 300
16.7 Testování bezpečnosti, kterou jste nastavili – 302

Poznámka pro rodiče – 307
Poděkování – 311
Přispěvatelé – 312

Předmluva

Linda McCarthy byla inspirována k sepsání prvního vydání knihy ***Buď pánem svého prostoru***, když dva dospívající členové její domácnosti zničili domácí počítačovou síť, kterou do té doby považovala za docela bezpečnou. Další inspirací bylo pro Lindu zjištění, že Douglas s Ericem se nesnažili nic zničit ani na ni udělat dojem, když domácí síť vyřadili z provozu. Prostě používali Internet tak, jak to dělají normální dospívající.

Od té doby se tato knížka stala společným projektem poskytujícím bezplatné vzdělání o bezpečnosti na Internetu dospívajícím a jejich rodinám. Do vydání z roku 2010 přispěla mimo jiné Denise Weldon-Siviy, matka čtyř dětí, učitelka a spisovatelka. K dalším odborníkům, o které se náš tým rozrůstá, patří specialisté na firewally, a klasické i bezdrátové sítě, stejně jako pokročilí uživatelé operačního systému Mac OS X a prohlížeče Firefox. Naši designéři a animátoři tyto koncepty spojují a dávají jim formu vhodnou pro dospívající čtenáře. Projektu se také účastní několik dospívajících a nové dospívající průběžně přidáváme, aby byl projekt neustále aktuální a svěží. Bez zapojení dospívajících by tato kniha ani tento projekt nemohly existovat.

Na teď a na později. Stejně jako malware, který se mění každý den, i my plánujeme aktualizovat tyto online verze podle potřeby, aby byli naši čtenáři chráněni. Počítačová bezpečnost je pohyblivým cílem. Formát elektronické knížky nám umožňuje pohybovat se spolu s ním.

Velmi nám záleží na tom, aby byla tato kniha k dispozici pro VŠECHNY dospívající a všechny rodiny, které se potřebují něco dozvědět o bezpečnosti. Z tohoto důvodu je tato kniha zdarma k dispozici online podle licence Creative Commons Licensing (creativecommons.org). Tento projekt by nemohl vzniknout bez sponzorských společností a jejich podpory.

Komu je tato knížka určena

Tato knížka je určena všem dospívajícím a je důležitým zdrojem informací pro všechny rodiče a učitele. Obzvláště je však určena těm dospívajícím, kteří si rozumí s počítačem, umí zacházet s klávesnicí, Internet používají každý den a chtějí vědět, jak zabezpečit své systémy, uchovat si svůj internetový životní styl a chránit svá data. Tato kniha poskytuje důležité podrobnosti umožňující těmto dospívajícím uchovat své soukromí, identitu a reputaci v kybersvětě v bezpečí.

Zkrátka, je to knížka pro normální dospívající, jako jsi ty. Uvědomujeme si, že toho o počítačích hodně víš, pravděpodobně o hodně víc než tvoji rodiče. Také od svých dospívajících víme, v čem mohou spočívat tvé mezery ve znalosti počítačů. Tuto knížku jsme napsali, abychom tyto mezery pomohli zaplnit.

Protože víme, že nemáš moc času, píšeme stručně a snažíme se soustředit na důležité aspekty bezpečnosti při používání Internetu. Taky jsme se snažili, aby to bylo čtení zajímavé, proto jsme zahrnuli příklady ze skutečného života a případové studie skutečných dospívajících, jako jsi ty.

Tato knížka je ti určena, i když jsi expert na počítače! Mnoho z toho, čím se zde zabýváme, budeš určitě znát. Přesto se rádi vsadíme, že zde najdeš mnoho informací, které jsi dosud nevěděl. A určitě najdeš hodně podrobných informací, které můžeš sdílet s přáteli, sourozenci nebo rodiči, kteří toho nevědí tolik, co ty.

Komu je tato kniha také určena, i když ne na 100 %

I když je tato knížka plná podrobností, neobsahuje očíslované pokyny. Chtěli jsme napsat knížku, se kterou by sis chtěl sednout a přečíst si ji, a ne další 400stránkový technický manuál. Všem uživatelům Mac OS se omlouváme, že uvádíme jen snímky obrazovek z operačního systému Microsoft Windows 7. Ačkoli bychom rádi zahrnuli všechny varianty, v tomto vydání to nebylo z praktických důvodů možné. Brzy však přidáme dodatek určený jen uživatelům Mac OS. Přesto se většina této knihy vztahuje stejně tak na uživatele Mac OS, jako na všechny ostatní.

Při čtení mějte na paměti, že hackeři neútočí na Mac OS tak často, jako na osobní počítače na platformě Windows, ale pokud k útoku dojde, je zrovna tak otravný a potenciálně nebezpečný. Proto musí uživatelé Mac OS zachovávat stejné bezpečnostní postupy – instalovat firewally, aktualizovat antivirový program a podobně. Musíte jen používat programy určené pro Mac OS a ne programy pro jiné operační systémy, o kterých zde bude řeč.

Co se dozvíte

Tato kniha je určena všem dospívajícím, kteří

- se bojí nechtěného stažení adwaru, spywaru a virů
- mají strach ze scarewaru a ransomwaru (viz dále)
- chtějí zůstat v bezpečí na sociálních sítích
- mají obavy z online útočníků a zlodějů identity
- vytrubují své důvěrné informace do světa na oblíbených hot spotech
- při online nákupech nehledí na svou bezpečnost
- nejsou si vědomi rizik spojených s používáním webové kamery či provozování sextingu
- nevědí, jak se vypořádat s kyberšikanou doma nebo ve škole
- blogují o samotě a v šeru.

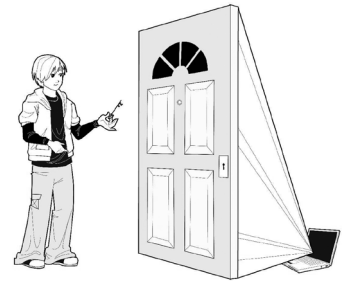
Napadlo vás něco? Moc rádi se dozvíme, co si o této knížce myslíte. Pošlete nám svůj názor na adresu lindamccarth@gmail.com.

Pomozte chránit lesy a zároveň poučit všechny ve své škole. Dejte svým přátelům, rodině a spolužákům vědět, že je tato kniha k dispozici zdarma na mnoha stránkách sponzorských společností, stejně jako na sítích MySpace (myspace.com/ownyourspace), Facebook (facebook.com/ownyourspace) a na adrese Buď pánem svého prostoru (ownyourspace.org). Český překlad naleznete na webové stránce - knihy.nic.cz

1. Chraň si svůj prostor

– Obsah kapitoly

1. Chraň si svůj prostor – 31
1.1 Výzkum malwaru – 32
1.2 Nachystej si prkno, než začneš surfovat! – 34



1. Chraň si svůj prostor

Braden je typický 14letý kluk. Posledních 6 měsíců se vytáhl o 10 centimetrů, noha se mu zvětšila o dvě čísla a snědl skoro tunu pizzy. A taky už přesně 12krát neúmyslně zaviroval rodinný počítač. Napřed si stáhl nějaké cool emotikony, které chtěl používat v IM zprávách. Ty emotikony však bohužel obsahovaly i adware, který ho zahrnul vyskakovacími okny a zpomalil výkon celého počítače. Potom si Braden nainstaloval „bezplatnou" hru, která obsahovala trojského koně, program, který spammerům z Ruska umožnil převzít kontrolu nad jeho počítačem a používat ho k posílání nevyžádané pošty. O několik týdnů později Braden odpověděl na e-mail, který vypadal jako pravý, a žádal jej o potvrzení přihlašovacích údajů na Facebook. Tento phisher potom pomocí Bradenových přihlašovacích údajů posílal Bradenovým přátelům na Facebooku adware. Nedlouho poté Braden klikl na Ano pro instalaci bezpečnostního programu, když mu vyskakovací okno oznámilo, že je jeho počítač infikován adwarem. Jak asi tušíte, tento program instaloval další adware. Bradenova máma vyplýtvala tolik času a peněz na opravu rodinného počítače, že si začínala říkat, jestli za to Internet doopravdy stojí. Jistá si je tím, že internetová bezpečnost je nyní MNOHEM komplikovanější, než tomu bývalo…

Od vzniku Internetu koncem 70. let se počet jeho uživatelů každých 9 až 14 měsíců zdvojnásobil. Když si to spočítáte, vyjde vám graf neuvěřitelného růstu – z 281 počítače na Internetu v roce 1981 k oslňujícím 400 milionům v roce 2000. Do roku 2009 překročil počet **netizenů** 1,5 bilionu. Internetu v USA používají již téměř všechny domácnosti.

Netizen Občan kyberprostoru (tj. Internetu) (z anglického „Net" – síť a „Citizen" – Občan). Netizen je každá osoba používající Internet k účasti v online sociálních komunitách. Když přijmete nového přátele na Facebooku, rozšiřujete si svou sociální skupinu. Jste dobrý netizen!

I když používání Internetu mezi dospělými neustále roste, mezi mladými se jedná doslova o boom. V červnu 2009 žilo 90 % dospívajících Američanů v domácnostech s internetovým připojením. Pokud jste součástí těchto 90 %, je opravdu důležité, abyste se naučili chránit svůj počítač před škodlivými kódy.

Jak se dozvíte později, hrozí vašemu počítači zvláštní nebezpečí. Stránky s adwarem se soustředí na dospívající, jako jste vy, zneužíváním stránek, které obvykle navštěvujete. Na online fórech se pohybují pedofilové předstírající, že jsou dospívající. Dokonce i krádež

identity, což je jiný potenciální následek škodlivého kódu, může být obzvláště závažná pro dospívající, kteří si svou finanční a obchodní identitu teprve budují. Pokud používáte počítač svých rodičů, můžete ohrozit i jejich finanční a osobní informace.

Prozatím si pamatujte, že bezpečnost na Internetu vyžaduje daleko více než jen zapnutý antivirový program. A je také mnohem důležitější, než si patrně uvědomujete. V následujících několika kapitolách budeme hovořit o tom, co potřebujete vědět a dělat, abyste sebe, svůj počítač a možná dokonce i své rodiče lépe chránili při používání Internetu.

1.1 Výzkum malwaru

Malware je obecný název pro škodlivý kód. Jedná se o programový kód speciálně vyvinutý k tomu, aby poškodil počítač nebo data v něm. Pokud se učíte španělsky (nebo latinsky), asi víte, že „mal" znamená „špatný" – jako malfunkce (selhání funkce) nebo Darth Maul v Epizodě I hvězdných válek (ten zjevně záporný chlapík v červeném a s rohy na hlavě). Předponou „mal" nikdy nezačíná nic dobrého. Malware je doslova špatný software.

> **Malware** Programový kód vyvinutý k tomu, aby poškodil počítač nebo data v něm.

Protože „škodlivý kód" a „malware" znamenají totéž, pro zjednodušení v celé knížce používáme výraz „malware".

Ve světě malwaru existuje několik standardních typů záporných hrdinů. Všemi se budeme v této knížce zabývat, ale hlavními kategoriemi jsou:

- viry
- červi
- trojské koně
- botnety
- keyloggery
- spyware

- adware
- scareware
- ransomware.

Některé z těchto kategorií již pravděpodobně znáte. Například počítačové viry jsou v populární kultuře tak známé, že představují velké finále sci-fi thrilleru z roku 1996 *Den nezávislosti.* Pokud se pamatujete, Will Smith zachránil svět tím, že pomohl Jeffu Goldblumovi (který je známější jako Ian Malcolm z Jurského parku) nahrát počítačový virus na „mateřskou loď" a tak vypnul silové pole vesmírného plavidla mimozemšťanů. Ve skutečném životě mají viry a červi na svědomí útoky na celé nechráněné sítě. V srpnu 2009 útočníci způsobili odstávku Twitteru na téměř tři hodiny a nechali tak 44 milionů tweetujících osob na celém světě mimo dosah. Zkuste si představit, že by celé odpoledne nefungovaly servery CNN a Fox News.

Samozřejmě znáte také antivirový program. Většina nových počítačů (avšak ne všechny) je nyní přímo z továrny vybavena alespoň zkušební verzí jednoho z hlavních antivirových programů. Obvykle se jedná o Norton AntiVirus, Trend Micro, McAfee nebo Webroot. Co se týče ochrany proti virům, jsou všechny z nich vynikající produkty.

Možná však nevíte, že vás antivirový program nemůže chránit před *všemi* typy útoků. Řada lidí se domnívá, že když mají nainstalovaný antivirový program, jsou chráněni. Tak tomu není, protože k ochraně potřebujete několik bezpečnostních vrstev. Antivirový program je jen jednou z nich.

Než se podíváme na další vrstvy bezpečnosti, je důležité pochopit, co antivirový program může a nemůže dělat. Představte si svůj antivirový program jako sérii očkování. Očkování proti obrně vás nechrání před žloutenkou. Stejně tak antivirový program nemusí nutně váš počítač chránit proti spywaru a adwaru. Pokud svůj antivirový program pravidelně neaktualizujete, nemusí vás chránit ani před novými typy virů. Obdobně jako jejich biologičtí bratranci, i počítačové viry mutují. Stejně jako potřebujete nové očkování proti chřipce každou zimu, abyste byli chránění před novými kmeny virů, musíte také průběžně aktualizovat svůj antivirový program. Proti dalším typům malwaru můžete potřebovat jiné typy ochrany. To si vysvětlíme, až budeme mluvit o konkrétních typech malwaru.

1.2 Nachystej si prkno, než začneš surfovat!

Když si koupíte počítač, není bezpečný. Nikdy byste neměli vybalit počítač z krabice a připojit jej k Internetu, aniž byste podnikli kroky k jeho ochraně. Představte si svůj počítač jako světového cestovatele, který potřebuje očkování, aby na cestách neonemocněl.

Ve skutečnosti je váš počítač zřejmě zamořen mnoha **bezpečnostními dírami,** což jsou chyby ve způsobu napsání počítačových programů, které by mohly způsobit zranitelnost počítače vůči útokům. Míra závažnosti těchto chyb v kódu definuje míru přístupu, kterou může útočník nebo jeho malware získat.

Varování!
Nevzdělaní programátoři + chyby v programování = bezpečnostní díry!

Pokud si říkáte, proč má váš počítač bezpečnostní díry ještě před tím, než jste ho začali používat, odpověď je následující: počítačové systémy běží na programech – doslova desítkách milionů řádků kódu, který počítači říká, jak interpretovat to, co chcete jako uživatel říci. Tyto řádky počítači říkají co dělat, když přetáhnete nežádoucí soubor do Koše nebo udělíte programu Microsoft Outlook pokyn přihlásit se na Internet a podívat se, zda vám někdo neposlal e-mail. Všechny tyto řádky kódu naprogramovali lidé. Když tito programátoři udělají chybu, mohou ji hackeři využít k získání neautorizovaného přístupu do vašeho počítače. Možná to zní divě, ale většinu programátorů nikdo neučil, jak psát bezpečné kódy. Navíc programátoři neuvažují jako zločinci. Neříkáme to často, ale když někdo záměrně krade nebo poškozuje data někoho druhého – je to zločinec. Normální programátor si nikdy neřekl: „Jů, tyhle řádky kódu bych mohl použít k tomu, abych se někomu vloupal do počítače" – protože se ve skutečnosti NECHCE nikomu do počítače vloupávat.

Bezpečnostní díra Jakákoli chyba ve způsobu, jakým je počítačový program napsán nebo používán, kvůli které je počítač zranitelný při útoku. Odborníci na počítačovou bezpečnost jim také říkají bezpečnostní zranitelnost.

Nedostatečné zaměření na bezpečnost v rámci vývoje se začíná měnit. Více programátorů začíná auditovat (dvojitě kontrolovat) své kódy speciálními nástroji, které hledají chyby v progra-

mu, jež mohou vést k neautorizovanému přístupu k systému či datům. Než to začne dělat celá komunita programátorů, bude to ještě chvíli trvat. Už však vznikly miliony řádků kódu, které vytvořili programátoři programující s dobrým úmyslem, ale malou schopností programovat bezpečně. Protože všechny počítačové systémy mají bezpečnostní díry, musíte se chránit a zalepit tyto díry před tím, než začnete surfovat po Internetu, stahovat hudbu nebo hrát hry.

Varování!
Nechráněný počítač připojený do sítě může podlehnout útoku již za 15 vteřin! Než začnete surfovat, chraňte svůj počítač!

Proč tak rychle? Jakmile jste online, může trvat pouze 15 vteřin, než se někdo pokusí na váš počítač zaútočit. Pokud napřed nenainstalujete bezpečnostní program, tento první útočník může získat přístup na váš počítač, aniž byste o tom věděli! V nejhorším případě může útočník získat dostatek vašich osobních údajů, aby vám mohl ukrást identitu.

Pokud používáte internetové bankovnictví ke sledování účtu, mějte na paměti, že vaše data nejsou jen informace. Může se jednat o Vaše finance. A aby to bylo ještě zajímavější, hacker může váš počítač použít i k útokům na jiné počítače! Z těchto důvodů (a z mnoha dalších, které si řekneme později) nikdy nesurfujte po Internetu bez bezpečnostních záplat, antivirového programu a instalovaného firewallu.

Když jste si počítač kupovali, asi jste si dali dohromady seznam požadavků: velikost operační paměti a pevného disku, jakou grafiku budete potřebovat pro své oblíbené hry, jestli chcete DVD i vypalovat, nebo se na ně jen dívat. Než se poprvé připojíte k Internetu, potřebujete také seznam kroků, potřebných k zajištění počítačové bezpečnosti. Tento seznam představuje úplný základ. Neměli byste z něj vynechat žádný bod. Na seznamu musí být ochrana proti virům. Musíte si ji nainstalovat a nastavit tak, aby počítač tento program pravidelně aktualizoval. Musíte také nainstalovat veškeré bezpečnostní záplaty, které byly vydány pro operační systém a programy, který chcete používat.

Bezpečnostní záplata **Oprava programu uzavírající bezpečnostní díru. Záplaty se pravidelně vydávají pro operační systémy (jako Windows 7) a internetové prohlížeče (jako je Internet Explorer a Firefox), stejně jako pro další softwarové aplikace.**

1. Chraň si svůj prostor

Internet je úplně super místo, ale je to také královský soud upírů z Volterry. Myslíme si, že by bylo skvělé se tam podívat, ale museli bychom znát zákony Volturiů, předem vědět o schopnostech Ara a Jane a také přivést naše vlastní nesmrtelné. Internet je přesně takový! Dějí se tam úžasné, nové a vzrušující věci – ale opravdu byste tam neměli chodit, aniž poznáte rizika, pochopíte, jak se chránit a ozbrojíte se správnou ochranou.

Seznam pro bezpečnost na Internetu:

Antivirus
Antispyware
Osobní firewall
Bezpečnostní záplaty

2. Poznej své nepřátele

– Obsah kapitoly

2. Poznej své přátele – 39

2.1 Proč malware existuje? – 39

2.2 Viry – 41

2.2.1 Jak se viry replikují – 43

2.2.2 Škodlivé payloady – 43

2.2.3 Nechvalně známé viry – 45

2.3 Červi – 47

2.3.1 Obzvláště zlí červi – 49

2.3.2 Variace a mutace – 51

2.4 Trojské koně – 52

2.5 Botnety – 54

2.6 Sociální inženýrství – 56

2.7 Jak se vyhnout malwaru – 58

2. Poznej své přátele

Seznamte se s Ericem z města Novato v Kalifornii. Je to normální dospívající, který rád vytváří webové stránky pro své přátele. Eric tráví spoustu času na Internetu. Hodně hraje počítačové hry, chodí na hodně různých stránek, kde hledá nové nápady a také rád stahuje bezplatné programy. Než si Eric pořídil svůj vlastní notebook, používal k surfování po Internetu a stahování bezplatných programů počítač své mámy. Počítač Ericovy mámy se nakonec tak zpomalil, že stahování čehokoli trvalo věčnost. Tak se Eric zeptal kamaráda, co má dělat. Tehdy také Eric zjistil, že měl mít firewall a stažené záplaty, aby do jeho systému nemohli hackeři nainstalovat spyware. Eric si myslel, že potřebuje jen antivirový program a nikdy neslyšel o drive-by malwaru.

Eric se draze poučil o tom, že se mu do systému dostal hacker a bere si z něj důvěrné informace. Tedy, ne z Ericova systému. Byl to systém Ericovy mámy a její důvěrné informace. Oops...promiň, mami. Teď má Eric vlastní notebook s firewallem, aktuálními záplatami, antivirovým program a ochranou proti spywaru.

Co se stalo Ericovi? Prostě neměl dostatečnou ochranu pro to, aby udržel nepřátele venku a nepustil malware dovnitř. Jako většina dospívajících potřeboval o bezpečnosti vědět mnohem víc, než věděl. I když je ochrana proti virům důležitá, není to všepokrývající a všemocná složka bezpečnosti. Malware se vám do systému může dostat mnoha způsoby. Možná jste jen navštívili webovou stránku vytvořenou speciálně pro stahování malwaru.

2.1 Proč malware existuje?

Když vezmete v úvahu, kolik práce stojí napsání programu, musíte se ptát, proč by se někdo tak moc snažil dostat se do počítače někoho, koho ani nezná. Abyste pochopili, proč lidé píší malware, je dobré podívat se nejdřív na to, KDO ho píše.

Malware píše překvapivý počet dospívajících. Podle výzkumnice Sarah Gordonové mají tito dospívající společného hlavně to, že toho moc společného nemají. Její výzkum ukazuje, že autoři malwaru „se liší věkem, mírou příjmů, lokalitou, sociální interakcí/kontaktem s vrstevníky, úrovní vzdělání, tím, co se jim líbí a nelíbí, i komunikačními způsoby."

Zatímco někteří dospívající píší malware prostě proto, že to chtějí zkusit, jiný trpí falešným pocitem, že budou slavní. Sláva byla určitě cílem Svena Jaschana, 18letého dospívajícího z Německa odsouzeného v roce 2005 za vytvoření Sasser.e – variace staršího červa známého jako Netsky. Sasser doslova zaplavil počítače po celém světě miliony nevyžádaných zpráv. Jaschanovým cílem nebylo ani tak způsobit škody na internetovém obchodování , jako vybudovat si jméno. Po svém uvěznění řekl policistům, že chtěl jen vidět, jak se o programu, který vytvořil, píše v novinách na celém světě. Jaschan reportérům řekl: „Bylo skvělé, jak se Netsky začal šířit a já se stal ve své třídě hrdinou."

Je takový obdiv oprávněný? Stěží. Vezměte si případ Jeffreyho Lee Parsona z Minnesoty, 18letého chlapce zavřeného za rozšíření varianty viru Blaster. Ačkoli to na jeho přátele a sousedy udělalo alespoň částečně dojem, svět počítačových profesionálů to nechalo chladným. Parson prostě jen zkopíroval existující vir Blaster, vytvořil jeho jednoduchou variantu (k tomu nebylo zapotřebí moc velkých schopností) a poté ho téměř okamžitě chytili, když ji rozšířil. Na tom není co obdivovat.

Povaha tvůrců malwaru se změnila s technologií, kterou zneužívají. Úplně první programy, které se samy replikovaly, vznikaly hlavně jako technické cvičení. Většinou je tvořili vysokoškolští programátoři, často v rámci výzkumu na doktorátu. Velmi brzy se toto pole rozšířilo o dospívající, kteří hledali technickou výzvu, stejně jako o stereotypní osamělé geeky – dospívající s malými společenskými schopnostmi, kteří malware psali, aby si udělali jméno. Tito autoři nejen že své viry nijak dobře neskrývali, mnozí je neskrývali vůbec. Jejich cílem bylo, aby co nejvíce lidí vědělo, co udělali.

Není překvapivé, že mnoho z těchto autorů malwaru chytili. I dnes některé malwary obsahují informace o autorovi. V některých případech se skutečně jedná o jména autorů malwaru nebo názvy skupin, které představují. V jiných případech jsou uvedení autoři sami oběťmi.

V poslední době se do smyčky přidali i profesionálové. Mikko Hypponen z finské bezpečnostní firmy F-Secure říká: „Dřív jsme bojovali s dětmi a dospívajícími, kteří psali viry jen pro zábavu. Nyní je většina nalezených virů profesionální akcí." Jde jim o peníze, ne o slávu.

Lidé pořád píší malware jako výzvu nebo proto, aby se stali slavnými, ale také je to způsob, jak ukrást duševní vlastnictví různých společností, zničit podniková data, podpořit podvodnou

činnost, špehovat jiné země, vytvořit sítě kompromitovaných systémů a podobně. Autoři malwaru vědí, že miliony počítačových systému jsou zranitelné a jsou odhodláni těchto zranitelností zneužít. Znamená to, že se ze všech dospívajících uživatelů Internetu stávají počítačoví kriminálníci? Ne. Prostě to znamená, že díky širokému rozšíření Internetu více lidí Internet používá k páchání zločinů.

Mrtví nebo živí!

Některé z obětí malwaru podobně jako na divokém západě nabídly velké odměny těm, kdo chytí a usvědčí autory červů a virů. Trend zahájila společnost Microsoft, která nabídla odměnu 250 000 USD (v přepočtu přibližně 5 milionů Kč) a později dokonce 500 000 USD (v přepočtu přibližně 10 milionů Kč) za dopadení autorů virů Blaster a SoBig. V rámci přípravy na budoucí útoky založila společnost Microsoft 5. listopadu 2003 Program antivirové odměny s počátečním vkladem 5 milionů USD, aby pomohla oficiálním úřadům dopadnout autory malwaru. Stejný přístup pokračuje i dnes. V únoru 2009 nabídla společnost Microsoft odměnu 250 000 USD za informace vedoucí k dopadení a usvědčení osob zodpovědných za červa Conficker.

Na počítačích se dnes skladuje více informací než kdykoli dříve, a tyto informace mají velkou cenu. Možná si to neuvědomujete, ale váš počítač a vaše data jsou ohroženější než kdykoli před tím. I kdybyste na počítači neměli ŽÁDNÉ osobní informace, ŽÁDNÉ finanční údaje a nic, co by někoho mohlo jakkoli zajímat, váš počítač stejně mohou zneužít k útoku na někoho jiného. Jak řekl 16letý Justin z Kalifornie: „To fakt není dobrý, že si někdo může převzít kontrolu nad cizím počítačem a používat ho“.

2.2 Viry

Počítačový virus je sada počítačových pokynů, které se samy replikují. Virus může být úplný program (samostatný soubor) nebo část kódu – pouze součást souboru s počítačovým programem. Ve své základní podobě virus vytváří své vlastní kopie. Některé viry jsou vyvinuty tak, aby se šířily jen za určitých okolností, například v určitém datu, nebo pokud počítač patří k určité doméně. Některé viry s sebou také nesou tzv. „payload“ (náklad). Ten virům říká, že mají způsobit škodu, jako je vymazání souborů nebo útok na jiné systémy. Payloady budeme podrobněji probírat v další části. I virus bez payloadu může způsobit velké potíže. Jen tím, že se kopíruje, může virus rychle zabrat všechnu dostupnou operační paměť počítače.

Počítačový virus je hodně podobný viru biologickému. Chřipka je dobrým příkladem viru, který se může šířit od jedné osoby k druhé. Do jaké míry onemocníte, záleží na typu chřipky a na tom, zda jste očkovaní. Jakmile jste infikováni chřipkou, můžete virus také šířit na všechny osoby, se kterými přijdete do styku.

V nejhorším případě se z vás může stát nová Tyfová Mary. Jak možná víte, imigrantka Mary Mallonová byla kuchařkou, která na přelomu 19. a 20. století pracovala v New Yorku. I když byla sama zdravá, od roku 1900 do roku 1915 šířila po městě spolu se svými slavnými broskvovými zákusky i břišní tyfus. Záznamy říkají, že nakazila 25 až 30 lidí a pravděpodobně způsobila nejméně 3 úmrtí. Po 3. úmrtí byla „Tyfová Mary" umístěna do konce svého života do karantény. V počítačovém světě mají přenašeči daleko větší dosah. Zatímco Tyfová Mary nakazila pouhých 50 lidí za 15 let, počítačové viry a červi mohou nakazit tisíce systémů za minutu. Když byl v roce 2001 vypuštěn do světa virus Code Red, infikoval více než 250 000 systémů za pouhých 9 hodin.

Virus je kód, který se sám kopíruje. Viry v sobě také někdy nesou ničivý payload.

Jakmile je virem infikován jediný počítač, může infikovat tisíce dalších počítačů. Jak velká škoda vznikne, záleží na dvou okolnostech: (1) Zda je každý počítač v síti chráněn aktuálním antivirovým programem a (2) zda virus obsahuje payload. Pokud virus obsahuje payload, může vykonávat škodlivé příkazy, jako například mazat všechna vaše data; pokud to udělá, nemůže se nadále replikovat, protože už nejsou žádné programy, které by mohl infikovat. Většina virů payload neobsahuje, prostě se jen replikují. I když to zní poměrně neškodně, proces kopírování využívá operační paměť a místo na disku. Proto zasažené počítače pracují pomalu a někdy vůbec.

Virus číslo 1

Fred Cohen, který byl tehdy doktorandem na univerzitě v Jižní Kalifornii, napsal první zdokumentovaný počítačový virus v roce 1983 jako experiment při studiu počítačové bezpečnosti. Úřady z něj měly takové obavy, že podobné projekty zakázaly.

2.2.1 Jak se viry replikují

Většina virů vyžaduje k zahájení replikace lidský zásah. Replikaci viru můžete nevědomky spustit, když kliknete na přílohu nakaženého e-mailu. Jakmile je virus aktivován, může vytvářet a přenášet své vlastní kopie pomocí e-mailu nebo dalších programů.

Váš počítač se může viry nakazit, pokud:

- sdílíte nakažená CD
- stahujete a spouštíte infikované programy z Internetu
- otevřete přílohy nakažených e-mailů
- otevřete nakažené soubory na disku USB.

Stejně jako se chřipka vrací každou zimu v jiné formě, takže je loňské očkování proti chřipce neúčinné, i počítačové viry se vrací v nových variantách. Často jen několik jednoduchých úprav kódu vytvoří novou variantu viru. Čím více variant vznikne, tím více příležitostí k proniknutí do vašeho systému virus má. McAfee udává, že se každý den objeví více než 200 nových virů, trójských koní a jiných hrozeb.

Když lékař zjišťuje, zda máte v těle virus, sleduje soubor příznaků, které společně přítomnosti virů napovídají. Antivirový program stejným způsobem používá k identifikaci známých virů signaturu (podpis). Tu si můžete představit jako otisk prstu. Když chtějí vyšetřovatelé na místě činu zjistit, zda byl na místě nějaký konkrétní zločinec, hledají jeho otisky prstů. Když chce antivirový program zjistit, zda nebyl váš počítač nakažen konkrétním virem, hledá **signaturu** tohoto viru.

Signatura Jedinečný bitový řetězec, který antivirový program používá k identifikaci viru.

2.2.2 Škodlivé payloady

Všechny viry jsou otravné. Některé také nesou ničící payload. Payload je sada pokynů, které obvykle vašemu počítačovému systému – nebo někomu jinému – provedou něco nepříjemné-

ho. Payload může zničit nebo změnit vaše data, změnit nastavení systému nebo odeslat vaše důvěrné informace. Škody mohou být obrovské.

Odkud se viry berou?

Geograficky jsou viry nesmírně rozdílné. Některé ze známějších malwarů dokonce vznikly na docela nečekaných místech:

- Brain vznikl v Pákistánu.
- Černobyl, ačkoli svým názvem odkazuje na ukrajinské město, vznikl na Tchaj-wanu.
- Michelangelo začal ve Švédsku, nikoli v Itálii.
- Tequilla zní mexicky, ale tento virus vznikl ve Švýcarsku.
- Yankee Doodle je překvapivě opravdu americký virus!

Když byl v roce 1999 poprvé spuštěn payload viru Černobyl, jen v Koreji byl postižen téměř milion počítačů, což korejské uživatele stálo odhadem miliardu dolarů!

Dnes obvykle používané payloady zahajují takzvané DoS útoky (Denial of Service, odmítnutí služby). Tento typ útoku obvykle míří na webové stránky třetích stran a pokouší se zabránit běžným uživatelům v přístupu na tuto stránku tím, že stránku doslova zahltí hromadou požadavků z infikovaných počítačů. MyDoom.F je dobrým příkladem malwaru s ničivým payloadem. MyDoom.F přenáší payload, který zahájí DoS útok A ZÁROVEŇ smaže soubory s obrázky a dokumenty z vašeho PC. Ničivější payloady mohou nepozorovaně měnit data. Když je payload odhalený, už je zkrátka příliš pozdě.

I když si viry obvykle představujeme jako útočící programy, nejčastěji infikují dokumenty nebo soubory dat. Na rozdíl od programů, které uživatelé zřídka neomezeně šíří, dokumenty cestují často a daleko. Při psaní této knížky cestoval dokument obsahující tuto kapitolu mezi Lindou, Denisem, vydavatelem, korektory a sazeči. Jiné dokumenty cestují MNOHEM dál. Žadatelé o práci mohou při hledání dokonalého pracovního místa šířit stovky životopisů e-mailem nebo je nahrávat na síť.

2.2.3 Nechvalně známé viry

Existují doslova desítky tisíc počítačových virů. Některé jsou škodlivé, jiné zábavné, ale stále obtěžují. Z této oblasti stojí za zmínku tyto viry:

Známé viry

Název viru	Datum uvedení	Významnost
Stoned	1987	Kdyby byl kategorií virů politický aktivismus, virus Stoned (Zhu lený, pozn. překladatele) by byl jejím prvním členem. Obvykle nebyl škodlivý, jen zobrazoval nápis: „Tvůj počítač je teď zhulený! LEGALIZUJTE MARIHUANU!"
Yankee Doodle	1989	Tento virus každý den v 5 odpoledne přehrál svým obětem přes reproduktory systému část písničky „Yankee Doodle".
Michelangelo	1991	Byla to katastrofa, která se nikdy nestala. Virus byl napsán tak, aby ve stanovený den (6. března, v den narození Michelangela) smazal všechna data uživatelů. Protože se mu v médiích věnovala OBROVSKÁ pozornost, pesimisté svět připravovali na 5 milionů zasažených počítačů. Když nastal 6. březen, odehrálo se méně než 10 000 incidentů. Virus Michelangelo ve skutečnosti dokázal jen to, že si průměrní uživatelé počítačů všimli existence virů a raketově se zvýšil prodej antivirových programů.
Concept	1995	Tento virus se šířil přes dokumenty aplikace Microsoft Word. Byl jedním z prvních, které fungovaly na různých operačních systé mech.
Marburg	1998	Tento virus byl pojmenovaný podle krvácivé horečky, což je závažná forma viru Ebola způsobující krvácení z očí a jiných tělesných otvorů. Virus Marburg se spustil (na hodinu přesně)

		3 měsíce poté, co byl počítač infikován. Následovaly náhodné chyby operačního systému. Marburg také poškozoval antivirové produkty, takže oběti hrozilo riziko od dalších virů.
CH1	1998	Ačkoli byla tato rodina virů pojmenována podle jaderného reak toru na Ukrajině, který vybuchl v roce 1986, ve skutečnosti pocha zela z jihovýchodní Asie. Když byl virus 26. dne v měsíci spuštěn, způsobil, že nebylo možné počítač spustit A NAVÍC přepsal pevný disk náhodnými znaky.
Waledec	2009	Známý také jako virus Valentine's Day. Oběti obdrží e-mail od „tajného obdivovatele" s odkazem na „valentýnskou" stránku. Tato stránka ve skutečnosti stahuje program, který nejen že využívá adresář oběti, ale také instaluje falešný antivirový pro gram, který si říká MS AntiSpyware 2009. Tento záškodnický antivirový program vydává opakovaná varování o tom, že je počítač uživatele používán k odesílání SPAMu, a poté požaduje, aby se uživatel zaregistroval a koupil si jeho nejnovější verzi pro odstranění „viru".

Možná jste si všimli, že mnoho z těchto virů je staršího data. Jestli si říkáte, zda jsou už viry překonané, odpověď zní: Zdaleka ne! Stalo se to, že technologie malwaru pokročila. Staré viry se vyvíjí v nové (kterým se říká varianty nebo mutace) a nové viry vznikají každý den. Mnohé z těchto virů nyní zahrnují prvky červů, trójských koní a jiných forem pokročilejšího malwaru. Viry jsou tu stále – jen si hrají se zákeřnějšími přáteli.

Všimli jste si také, že větší část poslední tabulky je psána v minulém čase. O těchto virech mluvíme, jako by už neexistovaly. To není technicky pravda. Viry jsou trochu jako ponožky, které se ztrácí v pračce. Často se znovu objeví, když je čekáte nejméně. Většina těchto virů stále existuje někde v divokých koutech kyberprostoru. Pouze již nejsou velkými hrozbami. Částečně je tomu tak proto, že jsou tyto viry zaměřené na technologie, které se už nepoužívají. Důležitějším faktorem je však to, že je nyní všechny antivirové programy rutinně vyhledávají. Ty momentálně nejnebezpečnější viry jsou takové, o kterých ještě nevíme.

2.3 Červi

Většina lidí používá výrazy virus a červ, jako by se jednalo o totéž. Existují však mezi nimi dva hlavní rozdíly: schopnost cestovat o samotě a schopnost existovat samostatně jako oddělené programy.

K zahájení replikace viru je zapotřebí lidského zásahu. To u červů NEPLATÍ. **Červ** může vytvářet své vlastní kopie na síti nebo se přesouvat pomocí e-mailu bez lidského zásahu.

Červ Malwarový program, který se v sítích sám kopíruje.

Červ je také obvykle samostatným programem. Červ se *sám přenáší* mezi počítači v síti. Virus *se připojuje* k souborům. Když se virus kopíruje, kopíruje se do dalších souborů na stejném počítači. (Virus se šíří na jiné počítače, když je některý z infikovaných souborů přenesen na jiný počítač, nejčastěji uživatelem, který si není vědom infekce svých souborů.) Červ se kopíruje spíše na jiné počítače než do jiného souboru na stejném počítači.

Konečným výsledkem všeho tohoto kopírování je nakonec odmítnutí služby. Kdosi chce kdesi použít síťový zdroj a nemůže, protože červ zabírá příliš mnoho místa na disku nebo šířky pásma. Červi také často zahajují DoS útoky proti konkrétním webovým stránkám. Virus Code Red byl zaměřen na webovou stránku Bílého domu. Virus Blaster útočil na webovou stránku s aktualizacemi společnosti Microsoft.

Jiní červi odesílají tolik dat bez významu, že velké části Internetu přestanou odpovídat. To může být finančně zničující. Když virus Slammer položil Internet na kolena, letecká společnost Continental Airlines musela zrušit lety z Newarku v New Jersey, protože nemohla zpracovávat letenky. Slammer způsobil také výpadek tísňových linek. V okolí Seattlu ztratili operátoři nouzové telefonní linky 911 přístup ke svým telefonickým střediskům. I když s tímto výpadkem nebyla přímo spojena žádná úmrtí, mohlo to také dopadnout jinak.

Červ číslo 1

Na počátku 80. let vytvořili výzkumníci společnosti Xerox John Shoch a Jon Hupp aplikaci k automatizaci instalace a aktualizace programů napříč místní sítí. Když aplikace narazila na „bug" (chybu), distribuovala ji také.

Shoch a Hupp poznamenali: „Trapný výsledek viděli všichni: 100 mrtvých počítačů v celé budově." Neúmyslně vytvořili prvního síťového červa.

Naše společnost spoléhá na počítačové sítě v mnoha dalších ohledech, než je bankovnictví a vzdělání. Propuknutí infekce virem Sasser podle obecného názoru způsobilo výpadek vlakové radiové sítě a 300 000 cestujících tak zůstalo vězet v australském městě Sydney. Počítačové sítě samozřejmě spojují více než jen přepravní systémy. Spojují také naše nemocnice a sanitky. Mnoho semaforů je také ovládáno počítačem. Může být jen otázkou času, než bude mít jeden z těchto žertíků fatální následky.

Červi se mohou do vašeho systému dostat bez vašeho vědomí mnoha způsoby. Mohou do vašeho počítače proniknout z Internetu kvůli bezpečnostní chybě. Možná máte na počítači spuštěnou cool hru, ale ve skutečnosti vás jen červ přiměl k jejímu spuštění tím, že vás přesvědčil, že se jedná jen o hru. Někdy nemusíte udělat nic. Některé z pokročilejších virů, Code Red a Slammer, se rozšířily, aniž by uživatel musel COKOLI udělat.

Červi jsou také navrženi tak, aby byli rychlí. Rychlost, se kterou se uvolňují po zjištění bezpečnostní chyby, ale před tím, než je vydaná záplata, je ohromující. Aby to bylo ještě horší, začínají tak zvaní **script kiddies** šířit varianty červů.

> **Script kiddie** Málo talentovaný hacker (často nezralý dospívající), který používá jednoduché a dobře známé techniky ke zneužívání zranitelných míst internetové bezpečnosti. V hackerské komunitě je označení „script kiddie" velkou urážkou.

Jedním nechvalně známým málo talentovaným hackerem byl Jeffrey Lee Parson. Když byl ještě na střední, umístil do oběhu variantu viru Blaster. Skutečný tvůrce toho malwaru – osoba, která napsala původního červa Blaster – nebyl nikdy odhalen. Parson byl jenom imitátor. Tak jako Parson, téměř kdokoli může provést drobné úpravy kódu. Nejsou k tomu zapotřebí stejné znalosti a kreativita, jaké potřebujete k vytvoření skutečného viru nebo červa. Výsledky drobných změn mohou být i tak zničující. Pouhé týdny poté, co Parson vypustil do světa svou variantu červa Blaster, odborníci odhadli, že červ infikoval 500 000 počítačů na celém světě. Ani to ale nebyla jen jeho práce. Parsonova varianta Blasteru infikovala pouze 7 000 počítačů. Pak se přidaly varianty jeho varianty, které vytvořili další script kiddies.

Jak se červi stávají stále složitější a rozvinutější, nezrychluje se jen vytváření jejich variantale dramaticky vzrostly i rychlosti infekce. Během útoku červa Code Red v roce 2001 se počet nakažených počítačů zdvojnásoboval každých 37 minut. Na vrcholu útoku červa Slammer se tento počet zdvojnásoboval každých 8,5 vteřiny!

2.3.1 Obzvláště zlí červi

Tak jako viry, i červi existují v mnoha tvarech a formách. Zde jsou jedny z nejvýznamnějších.

Známí červi

Název červa	Datum uvedení do oběhu	Významnost
Morris	1988	Robert Morris Jr., absolvent Cornellovy univerzity, je zodpovědný za všeobecně uznávaného prvního červa, který byl uvolněn na Internet. Tento červ zasáhl 6 000 až 9 000 důležitých Unixových počítačů a způsobil odstávku velké části Internetu, která tehdy existovala. Morris sám se stal prvním autorem červa, který byl za svou činnost uvězněn.
Melissa	1999	Mellisa byla smíšená hrozba zahrnující virus, který útočil na dokumenty aplikace Word. Když uživatelé otevřeli infikovaný dokument, Mellisa se dostala k jejich sezna mu kontaktů a poslala se mailem až dalším 50 lidem.
I Love You	2000	Červ „I Love You" se dostavil ve formě e-mailů s předmětem: „I Love You" (Miluju tě) a přílohou Love-Letter-For-You.txt.vbs. Čtenářům, kteří tuto přílohu otevřeli, byl prohledán počítač a nalezená hesla se po slala zpět na webovou stránku na Filipínách. Červ se potom velice rychle poslal na všechny kontakty, které našel v adresáři aplikace Outlook Express. Tento červ

		se na náš seznam dostal kvůli používání sociálního inženýrství při vytvoření zprávy, kterou si MUSELI přečíst i jinak zkušení čtenáři.
Code Red	2001	Červ Code Red útočil na webové stránky, nikoli na počítače. Nejprve změnil obsah zasažených stránek na tuto zprávu: Ahoj! Vítej na http://www.worm.com! Hacknul Číňan! V předem nastavený den, 19. července, infikované servery přestaly infikovat další servery a zahájily masivní útok na webovou stránku Bílého domu. Tento útok selhal jen proto, že odborníci odhalili jeho cíl (18. července) a přesunuli webové stránky Bílého domu na jinou internetovou adresu.
Slammer	2003	Známý také jako „červ, který za 15 minut položil Inter net". Slammer do Internetu vrazil doslova plnou rychlostí. Do 10 minut infikoval tento červ 90 % svých cílů. Do 15 minut nebyli přístupné některé důležité části Internetu.
Sasser	2004	Na rozdíl od mnoha jiných červů Sasser NEBYL šířen hromadnou poštou. Namísto toho útočil skrze bezpečnostní díry operačního systému a šířil se bez zásahu uživatele.
Conficker	2008	Conficker používal celou škálu malwarových technik k převzetí kontroly nad vzdálenými infikovanými systémy. Poprvé byl zjištěn v listopadu 2008 a do ledna 2009 získal kontrolu nad 9 až 15 miliony počítačů v téměř 200 zemích.
SillyFDC	2009	Do konce roku 2010 získal tento červ značnou moc narušením infikovaných počítačů, které stahovaly a instalovaly další bezpečnostní hrozby.

2.3.2 Variace a mutace

I když jeden červ nebo virus stačí na zadělání problémů, jen málo malwarů zůstane delší dobu ve svém původním stavu. Původní autoři, stejně jako další tvůrci malwaru, neustále produkují nové varianty starých útoků. Červ MyTob se stal zdrojem 12 dalších verzí do konce měsíce. Červ Netsky se během prvních 6 měsíců vyvinul do 29 variant.

Máte minutku?

Při své nejvyšší rychlosti infikoval červ Code Red více než 2 000 serverů za minutu!

U biologického viru může jedna malá mutace způsobit, že očkování již neúčinkuje. U počítačového viru může drobná úprava kódu způsobit, že antivirový program virus nepozná. Autoři virů vědí, že jakmile někdo vytvoří nový virus, mohou prostě jen přidat několik změn a způsobit, že se jejich varianta dostane přes antivirové programy. Některé viry jsou dokonce polymorfní a mohou se měnit samy.

Antivirový program může naštěstí detekovat nové varianty virů nebo červů pomocí heuristiky. Přesto varianty a mutace nadále způsobují problémy. Proto je nutné, aby byl váš antivirový systém aktuální. Pokud jste svůj antivirový systém od minulého týdne neaktualizovali, nemáte nové signatury. A signatury z minulého týdne mohou identifikovat viry z minulého týdne, avšak nikoliv nové viry a mutace z tohoto týdne. Většina mutací je změněna jen natolik, aby nebyla poslední virová signatura platná.

Varianta Změněná forma viru nebo červa. Varianty jsou obvykle jen natolik odlišné, aby původní signatura viru již neodpovídala.

Aby na vás nezaútočily novinky z minulého týdne, mějte vždy antivirový systém nastavený tak, aby stahoval aktualizace od antivirového dodavatele automaticky. Nezapomínejte – antivirový program je pouze jedním kouskem bezpečnostní skládačky. Firewally a bezpečnostní programy pro detekci/prevenci narušení mohou také detekovat různé červy a je možné je použít k prevenci nechtěných připojení. Systém prevence narušení je často součástí firewallu , který vám umožňuje detekovat a někdy také blokovat útoky, při kterých se útočníci snaží dostat do vaší sítě.

2.4 Trojské koně

Název „Trojský kůň" pochází z řecké mytologie. V hrdinském činu, o kterém pojednává epický básník Vergilius ve své knize Aeneis, získali Řekové přístup do města Troja tak, že Trojanům darovali obrovského dřevěného koně. Potěšení Trojané vzali darovaného koně za městskou bránu do města. V noci se z koně vynořily hordy Řeků, kteří se v něm skrývali. Trojany podřezali ve spánku a otevřeli městské brány.

V počítačové terminologii má trojský kůň podobný cíl: zakamuflovat se jako něco neškodného nebo žádoucího, poté otevřít dveře a pustit dovnitř útočníky. Tak jako se naši předkové naučili „Bát se Danajských, i když nesou dary", i vy byste se měli vždycky ptát na motivy a skutečný důvod bezplatného programu.

Princip trojského koně spočívá v tom, že musí být dostatečně lákavý, aby jej chtěl uživatel používat. Ve skutečnosti je pravým účelem mnoha trojských koní otevřít „zadní vrátka" k vašemu počítači, která umožňují snadný návrat. Tato zadní vrátka umožňují cizím osobám ovládat váš počítačový systém nebo přistupovat k vašim souborům bez vašeho svolení či vědomí. Tak se mohou autoři malwaru později vrátit a ukrást vaše důvěrné informace nebo dokonce použít váš počítač k útoku na někoho jiného.

Metody používané k přesvědčení uživatelů, aby si trojského koně instalovali, se liší. Jedním ze lstivých způsobů byl v roce 2009 trojský kůň Swine Flu (Prasečí chřipka). Při tomto útoku uživatelé obdrželi e-mail tvářící se jako by pocházel od Centra pro kontrolu a prevenci onemocnění. E-maily, jejichž předměty byly podobné jako „Vládní registrace k vakcinaci proti H1N1" nebo „Váš osobní vakcinační profil" nabádaly uživatele k vytvoření online profilu v očkovacím programu proti H1N1 v jejich státě. Uživatelé, kteří na odkaz klikli, si místo toho nainstalovali trojského koně.

Trojského koně můžete spustit, aniž byste si toho byli vědomi. Nezjištěné trojské koně jsou smrtelné, a když se spojí s útoky **nultého dne**, mají potenciál způsobit masové škody.

Útok nultého dne („zero day attack") je útok založený na bezpečnostní díře, které si tvůrci nejsou vědomi nebo na ní nestihli zareagovat. Proto není pro odražení útoku k dispozici žádná ochrana. Útok Aurora byl útok nultého dne spojený s trojským koněm, který se používal

k vytažení důvěrných informací. Když společnost McAfee Labs útok 14. ledna 2010objevila, škodu již utrpěla společnost Google a dalších udávaných 34 společností. Ve skutečnosti mohlo být zasaženo mnohem více společností. Především počítačové společnosti nerady přiznávají, že jejich stránky narušili hackeři.

Útok nultého dne Útok zneužívající bezpečnostní díru, pro kterou dosud neexistuje záplata.

Na první poslech to možná zní divně. Nejsou snad VŠECHNY útoky založeny na bezpečnostních dírách, o kterých nevíme? Překvapivě nikoli. Většina útoků zneužívá zranitelnosti, která je poměrně dobře známa. Tyto útoky jsou úspěšné především proto, že uživatelé neodvedou dobrou práci při aplikaci aktualizací a záplat řešících tato zranitelná místa.

Útoky nultého dne jsou problematické, protože v podstatě neexistuje jednoduchý způsob, jak se chránit před problémem, o kterém odborníci zatím neví. Má se za to, že útok Aurora začal koncem roku 2009 a většina obětí si jej nevšimla do poloviny ledna 2010. Útok Aurora byl neuvěřitelně sofistikovaný. Používal kombinaci malwarových programů, z nichž některé používaly několik vrstev šifrování k zakrytí svých činností. Útok byl zamířen proti mailu společnosti Google (Gmail), stejně jako tuctu jiných společností pracujících v oblasti technologií, médií, chemikálií a obrany. Protože se útok na Gmail soustředil na účty čínských disidentů, někteří komentátoři naznačují možnou účast čínské vlády.

Zatímco trojský kůň Aurora byl použit především ke krádeži zdrojového kódu a jiných duševních vlastnictví různých společností, jiné trojské koně jsou vytvářeny speciálně pro získávání informací od dospívajících a spotřebitelů. Například trojský kůň WIN32/PSW se zaměřuje na hráče online her. Tento trojský kůň nainstaluje keylogger, který zachycuje přihlašovací údaje hráče. Zloději použijí tyto přihlašovací údaje ke krádeži herních avatarů, virtuální hotovosti a pokladů.

Spuštění trojského koně může také někdy aktivovat počítačový vir nebo červa. Této kombinaci škodlivého kódu pracujícího společně se říká blended threat. Útokem několika různými způsoby zároveň se mohou smíšené hrozby – i ty, které nejsou útoky nultého dne – velmi rychle šířit a napáchat velké škody.

Blended threat (smíšená hrozba) Forma malwaru zahrnující více než jeden útok. Smíšená hrozba může zahrnovat virus, červa, trójského koně i DoS útok v jednom jediném útoku.

2.5 Botnety

Zombie počítač

Tabitha, studentka prvního ročníku střední školy v Gettysburgu vystoupila ze školního autobusu a utíkala domů přečíst si e-maily. Protože má přátele (skutečné i virtuální) téměř na celém světě, poštu si kontrolovala alespoň třikrát denně. Když Tabitha dorazila domu, zapla počítač a zjistila, že jí nefunguje Internet. O tři hodiny později byla situace stejná a ani večer jí stále Internet nefungoval.

Protože se domnívala, že je problém na straně poskytovatele připojení, donutila svého otce, aby vydržel několik kol automatických telefonických odpovědí a nahraných reklam, a nakonec se skutečně dovolal živému operátorovi kabelové společnosti. Dozvěděli se něco nečekaného a docela děsivého. Ten samý den ráno kabelová společnost zjistila, že z Tabithina připojení odchází stovky e-mailů. Kvůli masivnímu toku e-mailů kabelová společnost její připojení vypnula. To jí ale bohužel neřekli.

Tabitha byla bezradná. Stejně jako čím dál větší počet uživatelů, Tabithini rodiče si pořídili domácí síť. Jednoduchý router (k dostání v obchodě Staples (Autocont) za 50 USD, v přepočtu přibližně 1 000 Kč) rozdělil internetový kabel a umožnil připojení jak jejího počítače, tak přístroje jejích rodičů.

Její počítač byl infikován malwarem, a z jejího počítače se tak stal tzv. zombie. Někdo jiný převzal nad jejím počítačem kontrolu a používal jej ke spuštění útoků na jiné počítače.

Počítač této dospívající dívky se stal součástí botnetu. Síť **botů (botnet)** je soubor infikovaných počítačů, kterým se často říká zombie. Každý **zombie** počítač ovládá a kontroluje autor malwaru nebo hacker – téměř vždy bez vědomí plnoprávného vlastníka počítače. Majitel botnetu může vydávat povely z centrálního místa a všechny zombie tyto povely splní – obvykle se jedná o útok na další hostitele. Tabitha opravdu netušila, že se její počítač stal součástí botnetu. Neměla také ani ponětí, kdo převzal kontrolu nad jejím počítačem. Neznala ani webovou stránku, na kterou se pokoušeli zaútočit. Kdyby její otec nezavolal kabelové společnosti, nikdy

by možná nevěděla, že byl její počítač zneužit. Věděla jen, že ztrácí, i když jen dočasně, své připojení, a že ji to nesmírně frustruje. Představa, že někdo cizí ovládá její počítač, jí připadala prostě nechutná.

Zombie nebo bot Počítač, který byl infikován škodlivým kódem umožňujícím jeho vzdálené ovládání bez vědomí vlastníka počítače.

Botnet je soubor počítačů, které byly infikovány červem nebo trójským koněm instalujícím kód (známý jako bot). Ten útočníkovi umožňuje spouštět vzdálené příkazy a používat systémy pro budoucí útoky. Kód malwaru otvírá zadní vrátka, která hackerovi umožňují ovládat stroj a vzdáleně provádět příkazy.

Botnet Soubor vzdáleně ovládaných botů. Hackeři často používají sítě botů ke spouštění útoků proti jiným počítačům.

Jakmile hacker sesbírá dostatek infikovaných počítačů, má k dispozici doslova armádu „zombie", které je možné použít k útoku na jiné počítače. Tyto zombie často provádí DoS útok, při kterém se mnoho poškozených počítačů snaží připojit k jediné webové stránce tak dlouho, než stránka spadne. Při tomto typu útoků je účelem zaplavit cílový stroj velkým množstvím dat. Vysílaná data jsou sama o sobě obvykle neškodná, ale velká míra vytíženosti spotřebuje šířku pásma napadeného počítače. Spotřebovává internetové zdroje, které má napadený počítač k dispozici, a neumožňuje mu řádně komunikovat.

Výsledek je ve všech případech stejný. Právoplatným uživatelům je odmítnuta služba kvůli velkému vytížení.

DoS útok „Denial of Service" – odmítnutí služby. Při DoS útoku je oběť tak zavalena automaticky generovanými požadavky, že se k ní nemohou řádní uživatelé vůbec dostat.

V nedávných letech byly botnety použity k útoku na některé z největších jmen počítačového a podnikového světa. Microsoft, Amazon, Yahoo! a dokonce CNN.com se ocitli na mušce DoS útoků. Protože jsou botnety náhodně sestaveny z počítačů na celé světové síti, jediný příkaz může spustit DoS útok botnetu kdykoli, z jakéhokoli místa na světě. Nebo dokonce

z několika míst na světě zároveň. V březnu 2009 jsme byli svědky identifikace velkého botnetu překřtěného na „Ghostnet“ (síť duchů), která zahrnovala více než 1 200 infikovaných strojů ve 103 zemích.

Většina strojů, které jsou součástí botnetu leží mimo území Spojených států. V polovině roku 2009 se jen 18 % všech infikovaných počítačů nacházelo v USA. Přesto je to obrovský počet infikovaných počítačů. Od poloviny roku 2008 do roku 2009 vzrostl počet infikovaných počítačů o 50 %. Společnost MacAfee Avert Labs našla 12 milionů nových Zombie jen v prvním čtvrtletí roku 2009.

Jestliže jsou hrozby stále děsivější, pak útoky také. V jediném útoku v červnu 2004 se obrovskému botnetu sestávajícímu z domácích počítačů podařilo způsobit výpadek stránek společností Apple Computer, Microsoft a Yahoo! na celé dvě hodiny. Jak mohl jediný útok sundat webové stránky čtyř největších počítačových firem současnosti? V tomto případě soustředěním na pátou společnost, Akamai. Akamai provozuje jmenné servery, které překládají názvy domén, jako je www.microsoft.com, do číselných podob používaných Internetem. Společnost Akamai tak v podstatě spravuje adresář, který uživatele Internetu přesměrovává na určité webové stránky. Jak se ukázalo, společnosti Apple Computer, Google, Microsoft i Yahoo! byly klienty společnosti Akamai.

Co tedy můžete udělat, aby se váš počítač nestal cílem útoku jiných počítačů? Logickým řešením je záplatování počítače. Musíte se ujistit, že jste použili všechny aktuální záplaty pro svůj operační systém a prohlížeč. Skutečnou otázkou však je, jak se chránit před malwarem který může z Vašeho počítače udělat Zombie. Prvním krokem je, jako v oblasti počítačové bezpečnosti téměř vždy, mít instalovaný a VŽDY aktuální antivirový program. Musí zahrnovat detekci spywaru a adwaru a musí mít schopnost podezřelé soubory odstraňovat. A měli byste si být jistí, že je váš počítač chráněn velmi dobře nastaveným firewallem.

2.6 Sociální inženýrství

Škodlivé kódy jsou na světě již více než 20 let. Všichni víme, že otevírání příloh je nebezpečné a sdílení souborů může způsobit, že nebudete mít vlastní platné soubory. Přesto se každý rok stanou oběťmi malwaru miliony uživatelů.

Obvyklým důvodem je sociální inženýrství. Sociální inženýrství zahrnuje porozumění lidské povaze a používání tohoto pochopení ke zneužívání uživatelů. Autorům malwaru umožňuje ošálit uživatele, aby porušili vlastní bezpečnostní pravidla. Sarah Granger, která píše pro časopis Security Focus, to dobře vyjádřila definicí sociálního inženýrství jako „hackerova chytrá manipulace s lidskou přirozenou tendencí důvěřovat".

Sociální inženýrství Používání obecné znalosti lidského chování k přesvědčení uživatelů, aby porušili svá vlastní bezpečnostní pravidla.

Dobrý příklad použití sociálního inženýrství k šíření malwaru jsme viděli při útoku viru Love Bug. Většina lidí, kteří tento e-mail otevřeli, tak učinili z jedné ze tří možných příčin – z nichž všechny se týkaly základní lidské psychologie:

1. E-mail přišel od někoho, koho znali a věřili mu – kolegy, chotě nebo starého přítele. Někdo, kdo je možná opravdu miluje.

2. Mysleli si, že daný e-mail je jen vtip. Internetem kolují denně miliony vtipů (z nichž některé jsou mnohem horší než jiné). U domácích uživatelů se tyto vtipné anekdoty ve velké míře podílí na celkovém používání e-mailu.

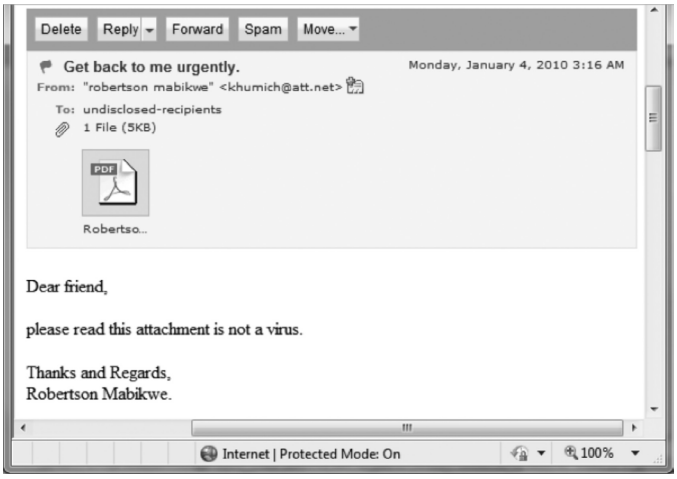
3. Prostě si nemohli pomoct. Zpráva „Miluji tě" od vzdáleného kolegy, bez ohledu na to, jak nepravděpodobná a zvláštní, prostě vzbudila zvědavost příjemce.

Sociální inženýrství se samozřejmě týká i jiných věcí, než je citový život uživatelů. Některá běžná použití sociálního inženýrství v malwaru zahrnují hádání hesel, falšování e-mailů tak, aby vypadaly jako příchozí pošta od přátel, maskování se za úřední osobu a nepodceňování lidské chamtivosti.

Neznáme se?

Lidé velmi rádi zůstávají v kontaktu. Spammeři na to spoléhají, když vytváří předmět zprávy s textem, který uživatele vede k přesvědčení, že odesílatele mohou znát. Virus Love Bug na tento faktor do velké míry spoléhal, když uživatele vábil k otevření přílohy. Jak snadné je přesvědčit vás k otevření infikovaného PDF souboru, který vám někdo poslal?

Skočili byste na tento?



Text zobrazeného dopisu: Milý příteli, přečti si prosím tuto přílohu. Není to virus. Díky a zdravím.

Tento příklad, stejně jako mnoho útoků v posledním čtvrtletí roku 2009, zneužívá zranitelnosti programu Adobe Acrobat, který váš počítač potřebuje k zobrazování souborů PDF. Jako u většiny útoků, ani zde se nejedná o útok nultého dne. Bezpečnostní díra, na kterou je útok zaměřen, byla identifikována a zazáplatována již dávno. Přesto mají tyto typy útoků úspěch, protože mnoho uživatelů nemá nainstalované novější verze programu Adobe Acrobat, nebo neaplikovali bezpečnostní záplaty.

2.7 Jak se vyhnout malwaru

Vyhnout se malwaru začíná být mnohem komplikovanější, než tomu bývalo. V minulosti se mohli uživatelé chránit poměrně jednoduše nesdílením dokumentů a neotevíráním e-mailů od osob, které neznají. To už dnes nestačí. Dnešní uživatelé potřebují vědět, co dělat, stejně jako to, čemu se vyhnout.

Prvním krokem k ochraně před škodlivými kódy je provádět prevenci, stejně jako reagovat na vzniklé situace. Zaprvé nezapomeňte na základy:

• Nainstalujte si jeden z nejlépe hodnocených antivirových programů. Zde neplatí žádné výmluvy o tom, že si ho nemůžete dovolit. Microsoft a AVG nabízejí bezplatné verze svých antivirů. McAfee a Symantec také nabízejí bezplatné verze (McAfee jen pro zákazníky operátora Verizon, Symantec pro zákazníky poskytovatele připojení Comcast).

• Používejte možnost automatické aktualizace antivirového programu. Mějte na paměti, že se neustále objevují nové mutace malwaru. Automatické aktualizace pomáhají udržovat aktuálnost vašich signatur.

• Instalujte záplaty na VŠECHNY programy, které používáte. To zahrnuje prohlížeče, plug-iny (jako Flash) a aplikace jako Adobe Acrobat a Acrobat Reader.

• Stahujte pouze programy z oficiálních zdrojů. Když potřebujete novou verzi programu Acrobat Flash, běžte na stránku společnosti Adobe. Neklikejte na odkazy ve vyskakovacích oknech.

• Buďte velmi opatrní u každého stahování „bezplatných" programů. Pamatujte si, že malware se často maskuje jako freeware.

• Mějte se na pozoru před emaily od neznámých lidí. Nikdy neotvírejte přílohy emailů, jejichž původ neznáte.

• Dávejte pozor i na emaily od lidí, které znáte. Některé útoky vypadají, jako by je prováděla osoba, kterou znáte. Mnoho červů se také samo posílá všem osobám v adresáři oběti. Než otevřete přílohu neočekávaného emailu, pořádně si to promyslete. Abyste měli jistotu, můžete odesílateli nejprve zavolat nebo poslat email.

3. Škodlivý „ware“

– Obsah kapitoly

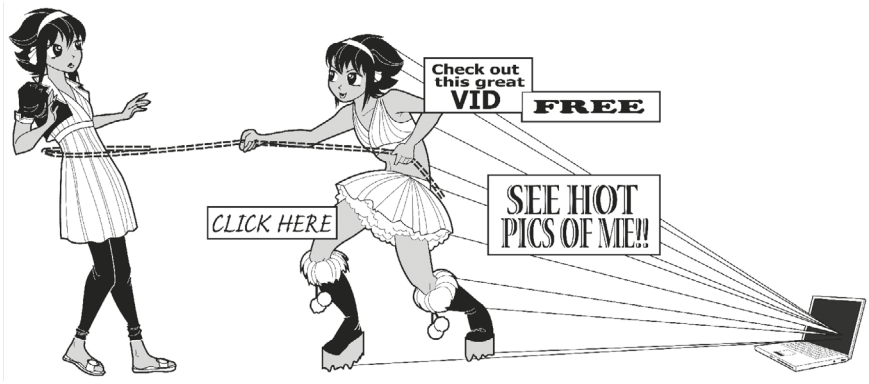
3. Škodlivý „ware" – 63
3.1 Spyware – 64
3.2 Adware – 65
3.2.1 Licence pro koncové uživatele (EULA) – 66
3.2.2 Sítě Peer to Peer (P2P) – 67
3.2.3 Bezpečné stahování – 68
3.3 Keyloggery – 68
3.4 Falešné programy a scareware – 69
3.5 Ransomware – 74
3.6 Black Hat optimalizace pro vyhledávače – 75
3.7 Současné a budoucí hrozby – 77

3. Škodlivý „ware“

Seznamte se s dívkou Stef z města Camden v americkém státě Maine. Stef miluje hudbu a ráda si na svůj iPod stahuje nejnovější hity.

Když dostala e-mail nabízející deset písniček zdarma, neváhala a klikla na odkaz uvnitř mailu, kde se měla dozvědět podrobnosti. Teď její počítač bombardují reklamní společnosti a je neustále zamořen vyskakovacími okny.

Stef si myslela, že dostane jen pár písniček. Netušila, že „zdarma“ není vždy „zadarmo“.



Stef se stala obětí adwaru – jednoho z mnoha otravných problémů, jejichž název končí na „ware“. Stejně jako spyware, falešné bezpečnostní programy a ransomware, i adware představuje pro uživatele zásadní problém. Ačkoli si Stef myslela, že ji od takových problémů ochrání antivirový program, ochrana je mnohem složitější, než se zdá. Adware a spyware jsou opravdu samostatná kategorie. Program McAfee tyto programy označuje jako **PUP** (potentially unwanted programs, potenciálně nežádoucí programy). To je poněkud přehnaně slušný výraz, protože většina spywaru je nežádoucí a ještě jsme nepotkali nikoho, kdo by opravdu stál o adware. A i když se bezpečnostní programy, jako je antivirus, pokouší PUP zastavit, nebo vás na ně alespoň upozornit, autoři adwaru své programy neustále mění, aby zabránili jejich nalezení.

PUP Potenciálně nežádoucí programy (Potentially Unwanted Programs). Politicky korektní termín pro nechtěný adware a spyware.

Programy PUP neustále útočí na počítačové systémy a některé sbírají data o vás. Tyto data grabbery často bez vašeho vědomí sbírají informace a posílají je někomu jinému, či je ukládají do zvláštního souboru pro pozdější použití (až se to bude hackerovi hodit). Někdy tyto údaje použije třetí strana k cílené reklamě. V podstatě hledají lepší způsoby, jak vám něco prodat. Jindy se tyto informace použijí ke krádeži vaší identity nebo ovládnutí vašeho počítače.

Data grabbery Softwarové programy, které sbírají informace o vás a odesílají je třetí straně. Data grabbery zahrnují adware, spyware a keyloggery.

3.1 Spyware

Některé společnosti prodávají legální „spywarové“ (špionážní) programy. Mnohé programy rodičovské kontroly uživatele v podstatě špehují. Stejně si počínají programy sledující zaměstnance. Když mluvíme o spywaru, nemáme na mysli tyto programy. V této knize se věnujeme zlovolnému spywaru. To jest programům instalovaným bez vašeho vědomí, které mohou spotřebovávat systémové zdroje, ovlivňovat výkon a krást důvěrné informace. Jak již anglický název napovídá, spyware vás při používání počítače doslova špehuje. Mimo jiné může sledovat, jaké stránky navštěvujete a co tam děláte. Spyware může také zahrnovat keyloggery sbírající uživatelská jména a hesla, která zadáváte na různých internetových stránkách.

Spyware Softwarový program monitorující využití počítače bez vašeho vědomí.

Spyware se od červů a virů liší tím, že jeho primárním účelem je vás špehovat. Sám se nereplikuje. Přesto je stejně nebezpečný, jako červy a viry. Pokud vám záleží na soukromí, musíte pochopit, jak se spyware na váš počítač dostane, a zda vám či vašim rodičům hrozí nebezpečí.

Pokud se váš systém bez zjevné příčiny zpomalil, možná již v počítači spyware máte, protože jste navštívili škodlivou nebo poškozenou webovou stránku a program se bez vašeho vědomí nainstaloval. Tento typ vnucování kódu se nazývá **drive-by download.** Některý spyware se dokonce nainstaluje i poté, co při dotazu na jeho instalaci zvolíte možno „Ne“.

Drive-by download Program, který se bez vašeho vědomí nainstaluje, když navštívíte škodlivou nebo zneužitou webovou stránku.

3.2 Adware

Podle toho, koho se zeptáte, adware může být buď legální komerční program, nebo je to malware, který přistane v systémech uživatelů bez jejich vědomí, nebo bez skutečně informovaného souhlasu. Někteří lidé mluví o adwaru a spywaru, jako by šlo o jedno a totéž, tak tomu ale není.

Adware je typ programu, který do vašeho webového prohlížeče dodává reklamu. Inzerenti také adware používají k tomu, čemu říkají behaviorální zacílení (zacílení podle chování uživatele). To jim umožňuje směřovat reklamy na spotřebitele, kteří si daný produkt s nejvyšší pravděpodobností koupí, na základě jejich dalších online aktivit. Adware má ve skutečnosti určité oprávněné využití a většina výrobců adwaru se snaží zůstávat v mezích zákona tím, že od uživatelů vyžadují souhlas s instalací programu.

Adware Program, který uživatelům poskytuje cílený reklamní obsah, často tak, že v počítači shromažďuje informace o tom, co uživatel na síti dělá, a které stránky navštěvuje.

Adware je někdy neuvěřitelně otravný. Může vám změnit domovskou stránku, zaplavit obrazovku mnoha vyskakovacími reklamami, nainstalovat do prohlížeče nástrojové lišty a přečíst soubory cookies, které máte na počítači nainstalovány. Může se také do počítače dostat, aniž byste o tom věděli.

Dospívajícím, kteří Internet hodně využívají, může adware do počítače proniknout bez jejich vědomí. Tyto programy se mohou svézt se stahovanými bezplatnými nástroji, jako jsou spořiče

obrazovky, nebo se mohou stáhnout, když navštívíte škodlivou webovou stránku. Dospívající si také adware často stáhnou spolu s oblíbenými programy, hudbou nebo filmy.

I když je adware obvykle nežádoucí, někdy jde o situaci „něco za něco“. Některé webové stránky vám často umožní stáhnout si „bezplatný“ program, pokud spolu s ním přijmete i adware. Tento program samozřejmě není bezplatný. Výměnou za program prodáváte svůj čas, který strávíte sledováním (zavíráním nebo snahou o zavření) všech vyskakovacích oken. Taková dohoda nemusí být vždy nevýhodná. Přemýšlejte o tom. Kdyby vám vaše kabelová společnost dala zdarma kabelovou TV, pokud budete používat systém zabraňující filtrování reklam z vysílání, možná by vám pořád připadalo, že jste uzavřeli výhodný obchod. Podobnou dohodu uzavíráte, když používáte některé z populárních programů na sdílení souborů. Důležité je uvědomit si, na jakou dohodu přistupujte.

3.2.1 Licence pro koncové uživatele (EULA)

Mnozí z nás si neuvědomují, že jsme souhlasili s instalací adwaru, protože při instalaci nového programu nebo přihlašování k novým internetovým službám nečteme **licenci pro koncové uživatele (End User Licensing Agreement, EULA).** To je pochopitelné. Licence pro koncové uživatele jsou obvykle dlouhé, nudné a psané nesrozumitelným právnickým jazykem. Často jsou napsané malým písmem a matoucím jazykem a většina uživatelů mylně předpokládá, že v nich není nic až tak důležitého. Některé společnosti vydávají licence pro koncové uživatele napsané tak zdlouhavě a komplikovaně, že by se jejich význam pokusil rozšifrovat jen ten nejodhodlanější vědátor. Adwarová aplikace TinkoPal nabízí licenci pro koncové uživatele obsahující více než 5 000 slov umně uspořádaných do pouhých 145 vět, z nichž každá obsahuje téměř 40 slov.

EULA End User Licensing Agreement, licence pro koncové uživatele. Jedná se o podrobný, právnickým jazykem psaný dokument, se kterým musíte souhlasit, než si můžete nainstalovat většinu programů.

I když není lehké vyhnout se používání záměrně zavádějících licencí pro koncové uživatele, pravdou je, že většina společností se to ani nepokouší, protože předpokládají, že si licenci stejně nepřečtete. Dost z nich je naprosto otevřených a skutečně adwarovou funkci uvedou.

Při tomto typu stahování zůstává adwarová společnost v mezích zákona, protože může argumentovat tím, že jste na začátku při instalaci se vším souhlasili, i když se můžete cítit podvedeni.

3.2.2 Sítě Peer to Peer (P2P)

Sítě Peer-to-Peer (rovný s rovným, P2P) jsou místa, která dospívající často navštěvují a sdílejí zde zdroje, jakými jsou hudba, filmy, software, hry a jiné programy. I když už je dnes server Napster hodně komerční, začínal jako populární síť P2P. V síti P2P můžete online hledat soubory a sdílet je s jinými lidmi, kteří používají stejný program na sdílení souborů. K obvyklým programům na sdílení souborů patří Kaaza, LimeWire, iMesh a Bit Torrent.

Stahování ze sítí P2P je z mnoha důvodů velmi populární. Najdete zde obsah, který je in, nový nebo moderní. Pokud hledáte indie retro techno-punk, asi jej najdete na stránce P2P. Stahování ze stránek P2P je také často bezplatné. A nebezpečné.

Proč nebezpečné? Komerční stránky si obvykle nesmírně opatrně hlídají, co poskytnou ke stahování. Pokud tomu tak není, lidé je budou patrně žalovat za stažené soubory, které jim zničily počítač. Umělci je zřejmě budou žalovat za porušení autorských práv. Když se jedná o peníze, lidé obecně dost často podávají žaloby. I když tyto soudní pře (nebo strach z nich) zvyšují ceny, zvyšují také motivaci operátorů zajistit, aby byly jejich stahované soubory bezpečné a v mezích zákona.

Když začnete stahovat z neznámých stránek a stránek, které spoléhají na individuální příspěvky, jako jsou sítě P2P, je to nebezpečné. Stahováním her, filmů a hudby z neznámých stránek se můžete dostat do problémů hned na několika úrovních. Můžete si stáhnout škodlivý kód, adware, spyware, trojské koně nebo keylogger. Můžete také porušit autorská práva a čelit pokutám za pirátství. I když je materiál, který stahujete, bezpečný, můžete si toho stáhnout víc, než jste čekali. Když jste si instalovali program potřebný ke sdílení souborů na síti P2P, možná jste souhlasili s přijetím adwaru.

Teď si možná říkáte: „Ale já stahování zadarmo *potřebuju*! Je to jeden z hlavních důvodů, proč jsem vůbec chtěl počítač.“ Nezoufejte. Ať už stahování bezplatných souborů *potřebujete* nebo ne, určitě si je *nemusíte* stahovat pomocí adwarové verze programu. Mnoho služeb P2P posky-

tuje komerční stahovací balíček, který adware neobsahuje. Háček je samozřejmě v tom, že je komerční – to znamená, že za něj budete muset zaplatit. Pokud se vám při pohledu na cenovku protáčejí panenky, vzpomeňte si, že za bezplatné stahování PLATÍTE. Prodáváte svůj čas (ke sledování reklam) a podrobnosti o svých osobních zvycích při surfování. Pro mnoho lidí je tato cena prostě příliš vysoká.

3.2.3 Bezpečné stahování

Do počítače si toho můžete stáhnout hodně – písničku, film, nový spořič obrazovky, hru nebo jiný typ softwarového programu. Než ale cokoli stáhnete, položte si tyto otázky:

1. Můžete stránce, ze které stahujete, důvěřovat?

2. Je to, co stahujete, legální kopie, nebo se pravděpodobně jedná o pirátskou kopii? Porušujete zákony na ochranu autorských práv?

3. Zahltí váš počítač adware? (Nejste si jistí? Pořádně si přečtěte licenci pro koncového uživatele!)

4. Je program ke sdílení souborů, který používáte ke stažení této položky, opravdu bezpečný? Nebo za něj platíte prodejem svého času na sledování reklam? Pokud ano, nevadí vám to?

5. Je soubor, který si chcete stáhnout, bezpečný? Může obsahovat malware, například trojského koně? Chcete to riskovat?

3.3 Keyloggery

Keyloggery (odposlechy klávesnice) jsou nedílnými součástmi některých adwarových a spywarových programů. Jiné keyloggery se instalují odděleně jako samostatné programy a jsou propagovány jako systémy pro rodičovský nebo zaměstnanecký dohled.

Keylogger je přesně tím, čím se podle anglického názvu (key = klávesa, logger = záznamník) zdá být – programem, který zaznamenává každý úhoz klávesy, při psaní na počítači. To může být neuvěřitelně nebezpečné. Jen si představte co všechno píšete. Když používáte online bankovnictví, zadáváte své uživatelské jméno a heslo k bankovnímu účtu, možná dokonce i čísla účtů. Pokud si po síti objednáváte hry nebo oblečení, zadáváte čísla platebních karet svých rodičů. Posíláte-li po síti žádosti o platební karty nebo o zaměstnání, zadáváte rodné číslo a další osobní údaje – vše, co zloděj potřebuje ke krádeži vaší identity.

Keylogger Program zaznamenávající každý úhoz klávesy při psaní na počítači.

Hackeři instalují keyloggery do osobních počítačů bez vědomí jejich uživatelů již mnoho let. Když pomineme postavení keyloggerů mimo zákon, což by pravděpodobně stejně nepomohlo, je jediným řešením tohoto problému odpovídající ochrana počítače. Postavit keyloggery mimo zákon stejně není možné. Jsou běžnou součástí palety všech nástrojů pro bezpečnostní odborníky. Odborníci tyto nástroje využívají při vyšetřování k dopadení zloduchů při činu.

Není bez zajímavosti, že se některé z těchto keyloggerů prodávají rodičům ke sledování aktivit jejich dospívajících na síti! Jestli si myslíte, že se vás to netýká, trochu se nad tím zamyslete. Výzkumná studie organice Pew Internet & American Life Project v roce 2007 ukázala, že 53 % rodičů s domácím přístupem k Internetu používá monitorovací programy. Kromě toho 45 % rodičů používá filtrovací program k úplnému zablokování určitých webových stránek nebo typů materiálu. Někdy samozřejmě monitorování provádí sami dospívající. V polovině roku 2008 byl student vyššího ročníku známé kalifornské střední školy uvězněn za to, že na počítač školní sekretářky nainstaloval program sledující hesla, a pomocí ukradených hesel si potom změnil známky.

3.4 Falešné programy a scareware

Je krutou ironií, že některé „spywary“ existují jen proto, aby se lépe prodávaly programy určené k potírání spywaru. Těmto podvodům se říká **falešné antivirové programy** nebo také **scareware.** Falešný antivirový program předstírá, že je pravým bezpečnostním programem. Některé z těchto programů jsou docela sofistikované a skutečně vypadají, že JSOU vaším vlastním bezpečnostním programem informujícím vás o zjištěném problému.

Falešný antivirový program Známý také jako scareware. Aplikace používající neetické marketingové praktiky k tomu, aby uživatele svedla k zaplacení a stažení bezcenného nebo škodlivého programu maskujícího se jako bezpečnostní počítačový program.

Nejběžnější falešný antivirový program zobrazuje poplašnou zprávu oznamující, že je váš počítač infikovaný spywarem. Formát této zprávy často vypadá tak, jakoby ji zobrazoval váš vlastní bezpečnostní program. Tyto zprávy často zobrazují logo společnosti Microsoft nebo podobné logo a používají stejný styl vyskakovacích oken, jaké byste viděli, kdyby byl váš počítač malwarem skutečně infikován.

Podvodník se vám poté pokusí prodat program pro odstranění „nalezeného“ spywaru. Aby byl dojem z opravdovosti ještě vyšší, většina falešných antivirových programů používá názvy, které znějí důvěryhodně a povědomě. Nejlépe se v roce 2009 prodávaly tyto: SpywareGuard 2008, AntiVirus 2009, SpywareSecure a XP AntiVirus. Stejná webová stránka, která vytváří vyskakovací okno prohlašující, že je váš počítač infikovaný, často ve skutečnosti opravdu infikuje váš počítač malwarem, který neustále přesměrovává váš prohlížeč k reklamám na jejich programy. Naivní uživatelé zjistí, že koupí programu za průměrnou cenu okolo 49,95 USD (v přepočtu asi 1 000 Kč) jen instalují nový a jiný spyware, a oběti obvykle skončí s počítačem, který není možné používat.

Jedná se o starou hru v novém kabátě. V říjnu 2004 Americká federální obchodní komora zažalovala tři společnosti, Seismic Entertainment Productions, Smartbot.Net a Sanford Wallace, za skutky rovnající se spywarovému vydírání. Tyto tři společnosti nejprve infikovaly osobní počítače spywarem, který uživatele zahltil nežádoucími vyskakovacími okny s reklamou, poté se jim pokoušely prodat antispywarové programy řešící problém, který právě samy způsobily.

I když je to stará hra, taktiky jsou nové a neustále se vyvíjejí. Scarewarové inzeráty se nyní pravidelně objevují tam, kde je uživatelé nečekají – například na první stránce výsledků hledání v hlavních vyhledávačích. Jak? Zaprvé je důležitý objem. Bezplatný nástroj LinkScanner, který uživatelům pomáhá neklikat na škodlivé webové odkazy, na jaře roku 2009 detekoval 30 000 webových stránek obsahující reklamy na scarware denně.

Aby podvodníci zvýšili počet kliknutí, zahrnují také fráze, které budou lidé patrně často vyhledávat, jako je *Vítěz soutěže American Idol (Česko hledá Superstar)* nebo *Rozpis závodů NASCAR (Utkání Sparty a Slávie)*. (O tomto procesu, kterému se říká black hat optimalizace pro vyhledávače, hovoříme dále v této kapitole). Podvodníci také čím dál častěji vkládají odkazy na sociální sítě, do příspěvků na Twitteru a dokonce i do komentářů u videí na YouTube. Díky praktice v angličtině zvané **malvertising** (zkratka pro „malicious advertising“, škodlivá reklama) se reklamy na falešné bezpečnostní programy objevily na renomovaných stránkách (včetně stránek Newsweek, Fox News a New York Times). Cílem je zneužít důvěru uživatelů k renomované stránce.

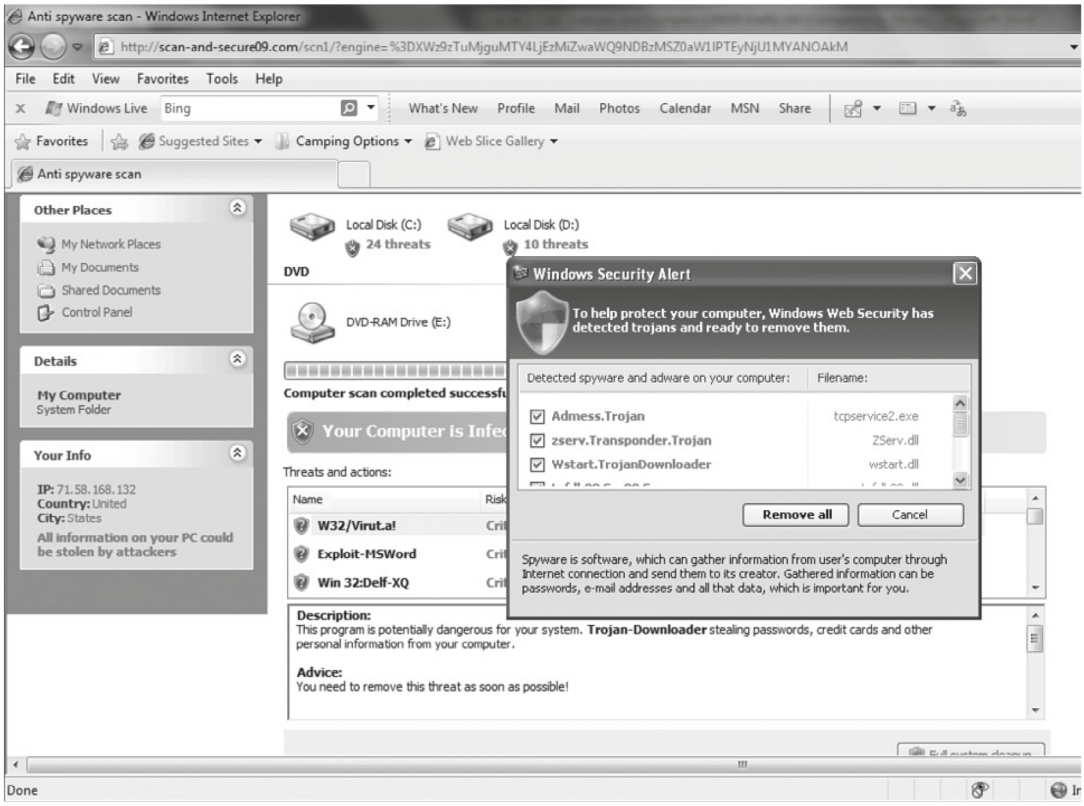
Malvertising Praktika propagování falešného bezpečnostního programu na renomovaných webových stránkách zneužívající důvěru uživatelů v tyto stránky.

Tyto podvody jsou velmi obvyklé. Zde je jeden, na který jsme narazili při aktualizaci této knihy. Na první pohled to vypadá důvěryhodně, že?

Text hlášení: *Tento počítač je ohrožen z malwaru! Může dojít k vážnému poškození vašich soukromých údajů nebo souborů a je třeba okamžitě přijmout opatření. Vraťte se do antivirového programu Personal Security a stažením souboru svůj počítač ochraňte.*

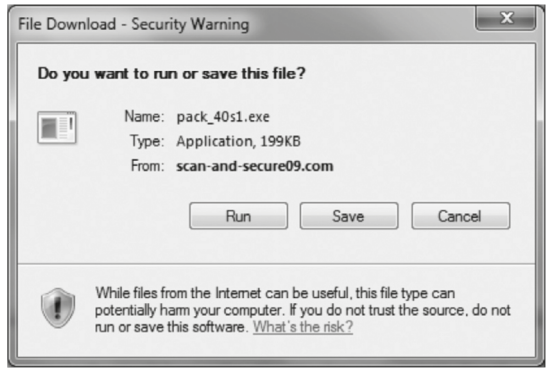
Varováním pro nás bylo to, že se bezpečnostní program našeho počítače nejmenuje Personal Security, a lidé, kteří ho napsali, umí anglicky natolik dobře, že by nenapsali doslova: „Tento počítač je ohrožen z malwaru!“ Po pravdě řečeno, většina falešných bezpečnostních programů je napsaná profesionálněji.

Na další úrovni si s podvodem dali daleko víc práce. Všimněte se, že následující webová stránka vůbec nevypadá jako webová stránka, dokud se nepodíváte nahoru na lištu s adresou. Místo toho vypadá jako varovné hlášení operačního systému Windows.



Všimněte si, že ve vyskakovacím okně je také logo operačního systému Windows identifikujícího údajný malware.

Ať už na této stránce kliknete na cokoli, začne stahování.



Ještě jednou opakujeme, že nezáleží na tom, na co kliknete. Většina scarewarů pokračuje se stahováním a nakažením vašeho počítače, ať už si v tento okamžik vyberete jakoukoli možnost – **Run** (Spustit), **Save** (Uložit) nebo **Cancel** (Zrušit). Pokud nemáte před tím, než se dostanete do tohoto bodu, spuštěný dobrý antimalwarový program, dostali jste se do velkých potíží.

Tato stará hra jen tak neskončí. Deník Wall Street Journal v dubnu 2009 uvedl, že se počet scarewarových programů od července do prosince 2008 ztrojnásobil. Před koncem roku 2008 identifikovala Pracovní skupina pro potírání phishingu (Anti-Phishing Working Group, APWG) více než 9 000 samostatných scarewarových programů kolujících po Internetu. V první polovině roku 2009 skupina APWG identifikovala nárůst scarewarových programů o 583 %. Tyto podvody se objevují téměř všude včetně zneužitých e-mailů a dokonce i uvnitř komentářů obsahujících odkazy na opravdové stránky, jako je YouTube nebo Twitter.

3.5 Ransomware

U tzv. **ransomwaru** jdou zločinci ještě dále a drží váš počítač jako rukojmí, dokud nezaplatíte výkupné (anglicky „ransom“). Ransomware se od obecného scarewaru a falešného bezpečnostního programu liší tím, že autoři ransomwaru vyřadí váš počítač z provozu, nebo jeho odstavením pohrozí, pokud nezaplatíte výkupné. Někdy se jedná o planou výhrůžku, ale to uživatel jen těžko pozná.

Nejobvyklejší formou ransomwaru je nástavba falešného bezpečnostního programu. V tomto scénáři malware, který jste si neúmyslně nainstalovali v reakci na falešnou zprávu o spywaru nebo viru, ve skutečnosti odstaví vaše soubory nebo kriticky důležité programy, dokud si nekoupíte program, který se pokoušejí prodat. Někdy se však podvodníci neobtěžují předstírat, že prodávají produkt, a otevřeně vydírají.

Ransomware Forma malwaru, při které jsou soubory na počítači uživatele zašifrovány nebo je systém (či mobilní zařízení připojené na Internet) vyřazen z provozu, dokud není zaplaceno výkupné.

Ransomware je forma malwaru, která je často zaměřena na mobilní zařízení. „Výkupné“ často spočívá v odeslání placené textové (SMS) zprávy. Při jedné z nedávných infekcí požadoval ransomware Trj/SMSlock.A, aby infikovaný uživatel odeslal placenou textovou zprávu, a uvedl v ní údajně unikátní číslo, aby mohl obdržet deaktivační kód. Autoři tohoto kódu naštěstí nebyli z nejchytřejších a bezpečnostním expertům se podařilo publikovat bezplatný nástroj generující deaktivační kódy. Když říkáme, že nebyli z nejchytřejších, myslíme to vážně: požadavky na výkupné zveřejňovali pouze По-русски (v ruštině).

Většinou jsou autoři ransomwaru chytřejší, i když stejně slizcí. Jeden exemplář malwaru, který se rozšířil v květnu 2009 prostřednictvím nakažených odkazů na Twitteru, vypnul a vyřadil z provozu všechny ostatní programové aplikace, dokud si oběti nekoupily dvouletou licenci na falešný bezpečnostní balíček za přibližně 49,95 USD (v přepočtu přibližně 1 000 Kč).

Gauneři také často nezamknou celý váš počítač – pouze soubory, které budete s nejvyšší pravděpodobností používat. Ransomware LoroBot, identifikovaný v říjnu 2009, zašifroval všechny textové soubory uživatele, dokumenty aplikace Word, soubory PDF a JPG, a poté požadoval 100,00 USD (v přepočtu přibližně 2 000 Kč) za dešifrovací program.

3.6 Black Hat optimalizace pro vyhledávače

Pokud často používáte vyhledávač, víte, že i to nejpečlivěji zadané vyhledávané heslo vede ke stovkám či tisícům výsledků. I když to vypadá jako skvělá věc pro všechny nalezené webové stránky, pravdou je, že se nepodíváte na víc než několik prvních stránek žádného z výsledků vyhledávání. Ve skutečnosti je dost pravděpodobné, že se nepodíváte na víc než prvních 20 výsledků. Společnosti to vědí a hodně se snaží, aby se jejich webové stránky objevovaly mezi těmito prvními dvaceti nalezenými stránkami. Zajišťování toho, aby se webová stránka objevila co nejvýše na seznamu výsledků hledání, se nazývá optimalizace pro vyhledávače (Search Engine Optimisation, SEO).

Jak se to dělá? Pořadí přidělené jakémukoli výsledku vyhledávání závisí na celé řadě faktorů. I když většina lidí předpokládá, že se na předních místech umístí nejpopulárnější stránky, popularita není jediným zvažovaným faktorem. Společnost Google tvrdí, že při seřazování webových stránek používá více než 200 různých kritérií. Ačkoli společnost Google používané faktory nezveřejňuje, aby zmátla spammery, většina technik, které používají velké vyhledávače, je dobře známa. Ve vyhledávacím algoritmu se spolu s dalšími faktory ke stanovení pořadí stránky používají popularita stránky, obsah a počet stránek, které obsahují odkazy na tuto stránku. SEO tyto známé faktory používá ke zlepšení pořadí stránky.

Pořadí je velmi důležité. Čím vyšší pozice stránky ve výsledcích vyhledávání, tím více lidí tuto stránku najde. Většina provozovatelů webových stránek chce, aby se jejich stránky umístily na první stránce výsledků vyhledávání – čím výše, tím lépe.

Jak tedy stránka získá lepší pořadí? Primárním faktorem je obsah. Čím lepší je obsah, tím více odkazů na něj míří. Avšak kvalita obsahu není jediným faktorem. Webová stránka s kvalitním obsahem ve skutečnosti nemusí zaznamenat mnoho nových návštěvníků, protože se ve vyhledávání umisťuje na nižších pozicích. Tuto stránku nikdo nenajde. Zde přicházejí na řadu konzultanti, obzvláště konzultanti pro optimalizaci pro vyhledávače. Optimalizace je honosný způsob, jak říct, že webová stránka bude používat algoritmus vyhledávače ve svůj prospěch, aby získala vyšší pořadí ve výsledcích vyhledávání. Techniky a konzultanti SEO upravují obsah a další data webových stránek, aby zlepšili pořadí stránky. Většina hlavních provozovatelů vyhledávačů dokonce pro webmastery zveřejňuje informace o tom, jak mají své stránky strukturovat, aby si vedly dobře.

Technika SEO je sama o sobě naprosto zákonnou obchodní praktikou. Problém začíná, když se používá zákeřně. Stalo se vám, že jste něco hledali, a našli jste výsledky, které vůbec nesouvisely s hledaným výrazem? Všimli jste si odkazů na něco, co vypadalo jako falešný bezpečnostní program, když jste hledali heslo, které s bezpečností vůbec nesouviselo? Některé techniky SEO totiž manipulují algoritmy vyhledávačů pomocí klamných, nezákonných a neschválených prostředků. Těmto technikám se říká **black hat SEO**. K některým z podvodných technik patří krádež legitimního obsahu oblíbené stránky a jeho zveřejnění na stránce se SPAMem. Vyhledávačům se tak nabídne legitimně vyhlížející obsah kvůli vytvoření pořadí, ale normální uživatelé na webu najdou pouze stránky se SPAMem. Jinou technikou je zaplnění webové stránky opakovanými slovy, aby se zvýšil počet použití klíčových slov pro vyhledávače. Hlavní vyhledávače tyto techniky neschvalují a upravily své algoritmy tak, aby snižovaly pořadí webových stránek, které se o tyto techniky pokoušejí. Tedy, udělají to, když je najdou.

Black hat SEO Používání podvodu, aby webová stránka skončila v pořadí výsledků vyhledávání na vyšší příčce, než si zaslouží. Často se používá k přesměrování nic netušících vyhledávajících na stránky naplněné malwarem (například falešným bezpečnostním programem).

Kromě SPAMu se techniky black hat SEO používají k ještě nebezpečnějším účelům. Hlavním důvodem, proč se techniky SEO používají, je zvýšení počtu návštěvníků na konkrétní webové stránce. Když chce hacker vyzkoušet svůj nejnovější škodlivý program, jaký je lepší způsob, jak

získat zájemce? Když vytvoří webovou stránku a použije techniky black hat SEO, aby na ni přitáhl více lidí, bude mít velký počet osob, které pro něj kód otestují. Hacker musí na zvednutí pořadí své stránky vynaložit opravdu málo energie.

Podle toho, jaká klíčová slova hacker zvolí, může si dokonce vybrat specifickou skupinu osob, na které se zaměří. Děti s větší pravděpodobností hledají slova jako „pomoc s úlohou z matematiky“ nebo „jonas brothers“ než hesla „důchod“ či „zubní protézy“. Pomocí techniky black hat SEO může podvodník přesměrovat dospívající hledající určitou herní stránku na falešnou herní stránku, kde si místo her stáhnou malware. Když procházíte výsledky vyhledávání, buďte vždy opatrní. Jen proto, že se nějaká stránka umístila na horních příčkách, ještě nemusí být relevantní ani bezpečná. Když je možné ošálit vyhledávače, je možné ošálit i vás.

3.7 Současné a budoucí hrozby

Bitva mezi uživateli a hackery je obvykle o prsa. Obě strany se pokouší zůstat o krok napřed před druhou stranou. V poslední době se tento boj stal pro uživatele mnohem složitějším. V minulosti jsme se museli obávat pouze o domácí počítače, a ty jsme mohli obvykle dost dobře ochránit standardním balíčkem antivirových programů.

Doba se změnila. Dnešní uživatelé tráví víc času na síti a na cestách. Naše počítače se teď vejdou do kapsy a spojují nás s kýmkoli, kdekoli a kdykoli. Se známými se spojujeme nejen prostřednictvím e-mailu, ale také tweetů, SMSek a aktualizací stavu v reálném čase na stránkách sítí Facebook nebo MySpace.

Očekáváme – a dostáváme – okamžitou komunikaci. Stojíme ve frontě na lístek do kina? Najdeme si jeho recenze na iPhonu, zkontrolujeme tweety od kamarádů, kteří už film viděli.

Zatímco komunikujeme se světem, hackeři zneužívají našeho propojení a naší důvěřivosti. V našich chytrých telefonech hledají slabá místa, podvodem nás lákají k instalacím malwaru, narušují výsledky vyhledávání, zveřejňují falešné webové stránky, které se tváří jako pravé, a používají naše trvale připojené počítače v botnetech k doručování SPAMu, k útokům na jiné počítače a k pokusům o změny výsledků vyhledávání.

A těsný závod pokračuje. Hackeři jsou neustále pokoušeni k hledání nových slabých míst, obcházení bezpečnostních programů a klamání uživatele. Uživatelé se musí mít neustále na pozoru a instalovat a aktualizovat legitimní bezpečnostní program, aktualizovat ho, když se najdou slabá místa, a vyhýbat se minovému poli phishingových podvodů, útoků falešných programů a podvodných webových stránek rozšiřujících malware.

Co nás čeká v budoucnu? Hackery zřejmě stále to samé. Budou nadále zneužívat veškeré slabiny, které najdou, k získání přístupu do našich osobních počítačů, k našim soukromým účtům a osobním informacím. Také patrně své snahy rozšíří a uvidíme více útoků na mobilní zařízení. Naše mobilní zařízení jsou v mnoha směrech lákavými cíli. Obsahují více osobních informací a jsou vždy připojené, mají také méně metod ochrany před útoky. Uživatele v budoucnu čeká větší zodpovědnost a vzdělání. Pochopení důležitosti bezpečnosti informací, především zabezpečení osobních informací, bude mít nebývalý význam. A zdatným uživatelům, jako jste vy, bude záležet na tom, aby se naučili, jak a kdy svá data chránit před hackery.

4. Hackeři a crackeři

– Obsah kapitoly

4. Hackeři a crackeři – 81

4.1 Hackeři – 81

4.1.1 Kdo je to hacker? – 82

4.1.2 Černé, bílé a šedé klobouky – 84

4.2 Hackeři chtějí váš počítač – 86

4.3 Nástroje hackerů – 86

4.3.1 Skenovací nástroje – 87

4.3.2 Prolamování hesel – 88

4.3.3 Rootkit – 90

4.4 Voláme bílé klobouky! – 92

4. Hackeři a crackeři

Adrian Lamo začal brzy. Svůj první „hack" (obzvláště chytré využití počítače) provedl na základní škole – jednalo se o obtížnou techniku dvojitého zápisu na starý disk počítače, který vlastnil v 8 letech. (Dvojitý zápis byl užitečný fígl, který uživateli umožňoval uložit dvakrát tolik informací.) Když Adrian dosáhl 18 let, pracoval na vlastní pěst a v hackerské komunitě si vybudoval celkem slušné jméno.

Adrianovou specialitou bylo pronikání do počítačových sítí špičkových amerických společností – America Online, Microsoft, Excite@Home, Yahoo!, WorldCom atd. Média mu přezdívala „užitečný hacker", protože těchto proniknutí nezneužíval. Místo toho svůj čin oznámil správcům sítě napadených společností a často také tisku.

Když bylo Adrianovi v roce 2001 pouhých 20 let, svěřil se reportérovi magazínu Security Focus s tím, co je jeho hlavním problémem: „Dochází mi významné americké společnosti." To bohužel ve skutečnosti nebyl jeho jediný problém.

Když se obětí jeho schopností stal deník New York Times, nepoděkovali mu. Podali na něj žalobu. Nakonec byl Adrian odsouzen ke 2 letům podmínečného trestu a bylo mu nařízeno zaplatit odškodné ve výši 64 000 USD (v přepočtu přibližně 1 280 000 Kč). Na to, že mu hrozilo 5 let za mřížemi, ještě dopadl dobře.

Stejně jako Adrian, spousta hackerů vůbec nečeká, že budou soudně stíhaní. Jiní ani nepředpokládají, že je chytí. Typy hackerů, stejně jako jejich záměry, se poslední dobou mění. V minulosti hackeři poškozovali webové stránky jednoduše proto, že to bylo považováno za „cool". V současnosti jsou hackeři motivováni finančně a dokonce politicky. V této kapitole se dozvíte o různých typech hackerů a nástrojích, které používají. Probereme také, jak se můžete dovědět více o bezpečnostní problematice a o kariéře v oblasti počítačové bezpečnosti.

4.1 Hackeři

Spousta teenagerů využívá své počítačové dovednosti k hackování her – prohlíží Internet a vyhledávají zkratky a způsoby, jak „přelstít" (s použitím cheatů) své oblíbené počítačové hry.

Přestože lidé používají stejný výraz, hackování počítačů je VELMI odlišné od hackování her. Hackování hry pomocí podvodu je znakem nedostatečného smyslu pro sportovní chování. Hackování počítače bez povolení vlastníka je trestný čin. Nemyslete si, že je hackerství skvělé jen kvůli tomu, že je Hollywood ukazuje v atraktivním světle. Vezměte si případ Jeffrey Lee Parsona, 18letého mladíka z Minnesoty, který byl zatčen za to, že do oběhu uvedl variantu červa Blaster. Zatímco si Parson chtěl vybudovat jméno jakožto programátor, získal pouze záznam v rejstříku a 18 měsíců ve vězení. Juju Jiang z Queensu v New Yorku byl odsouzen na 27 měsíců za instalaci keyloggerů v kopírovacím centru Kinko's a použití získaných hesel k přístupu do bankovních účtů obětí. Případů usvědčení z hackerství přibývá a tresty se zpřísňují. Brian Salcedo byl teenager, když pronikl do počítačů společnosti Lowe a nainstaloval tam program ke zcizení čísel kreditních karet zákazníků. Přesto dostal 9 let.

Zatímco dříve hackeři (obzvláště dospívající) vyvázli poměrně snadno, tento trend se mění spolu s tím, jak si veřejnost uvědomuje skutečnou cenu za počítačové zločiny. Zákonodárci také zpřísňují předpisy tak, aby zahrnovaly počítačové zločiny. Jak řekl americký státní zástupce John McKay: „Nedovolme pochyby o tom, že kyberhackování je zločin."

4.1.1 Kdo je to hacker?

Všeobecně lze říci, že **hacker** je někdo, kdo bez povolení proniká do počítačového systému nebo osobních souborů jiné osoby.

> **Hacker** Programátor, který bez povolení proniká do počítačového systému nebo dat jiné osoby.

Někteří odborníci používají raději termín „cracker" (z anglického výrazu „safe cracker" označujícího lupiče prolamující kódy bezpečnostních sejfů), protože výraz hacker může mít i jiné významy. Hrstka programátorů se ráda nazývá hackery a tvrdí, že hackování je pouze vynalézání obzvláště chytrých programovacích technik. Je na tom něco pravdy, ale když už jednou Hollywood pojem hacker uchopil, jen tak se ho nepustí.

Dokud široká veřejnost považuje hackery za počítačové vandaly a zločince, je poměrně zbytečné snažit se význam tohoto slova změnit. Proto v této knize nazýváme osoby, které pronikají

do počítačových systémů, hackeři – nikoli crackeři.
Zpočátku pocházela většina hackerů z řad počítačových nadšenců – obvykle studentů informatiky – a často odpovídali profilu geniálních samotářů toužících po slávě. Nezapomínejme však, že ne všichni hackeři mají talent. Script kiddies jsou málo talentovaní hackeři (často nezralí dospívající), kteří používají jednoduché a dobře známé techniky ke zneužívání zranitelných míst na Internetu. Hackeři jsou osoby ze všech sociálních vrstev. Někteří jsou i dnes studenty informatiky. Jiní jsou bývalí zaměstnanci s touhou pomstít se společnosti, která jim podle jejich názoru ukřivdila. A jiní jsou součástí organizovaných zločineckých skupin.

V současnosti se vládní agentury pro dodržování zákonů nejvíce obávají **kyberterorismu**. Ve světě po 11. září si vlády začínají uvědomovat, kolik škody může být napácháno na světové ekonomice, pokud by jedna či více nezákonných skupin dostaly svůj technologický ekvivalent letadla na informační dálnici. To byla hlavní obava v prvních hodinách po vypuknutí infekce virem Code Red, který byl zaměřen na oficiální webové stránky Bílého domu. Teoreticky by kyberterorista mohl způsobit značnou škodu zastavením celosvětové ekonomiky (doslova zničením počítačů, které řídí celosvětovou burzu), nebo – pravděpodobněji – útokem na infrastrukturu napadením počítačů, které řídí naše topné systémy, elektrárny, nemocnice, zařízení na čištění vody atd. Když si uvědomíte, jak je většina předních světových národů závislá na technologii, katastrofické scénáře jsou téměř nekonečné.

Kyberterorista Hacker nebo autor malwaru, který používá virus, červa nebo koordinovaný počítačový útok ke spáchání teroristického činu proti politickému protivníkovi.

I když Internet dosud velkému teroristickému útoku nečelil, možné škody jsou ohromující. Ministerstvo vnitřní bezpečnosti (DHS) i Federální agentura pro zvládání krizí (FEMA) si tuto hrozbu uvědomují. V současné době FEMA i DHS spolupracují na projektu Cyberterrorism Defence Initiative (CDI, Iniciativa ochrany proti terorismu), který zdarma nabízí protiteroristické školení pro osoby, které poskytují a chrání národní infrastrukturu. Kurzy jsou zdarma pro kvalifikované pracovníky z řad vlády, bezpečnostních složek, hasičů, veřejné služby, veřejné bezpečnosti a zdraví, zdravotnické záchranné služby, vysokých škol a univerzit. Je zřejmé, že kyberterorismus zůstane v dohledné budoucnosti závažnou hrozbou.

4.1.2 Černé, bílé a šedé klobouky

Pokud jde o bezpečnost, můžeme rozlišovat hodné hochy, zloduchy a další skupinu žijící na pomezí mezi těmito dvěma póly. Obvykle jsou nazýváni Black Hats (černé klobouky), White Hats (bílé klobouky) a Gray Hats (šedé klobouky) Vzhledem k tomu, že existuje nesmírně mnoho odstínů šedé, odlišení těchto skupin není vždy tak snadné, jak by se mohlo zdát.

White hats

Označení „bílé klobouky" se používá pro bezpečnostní experty. Přestože často používají stejné nástroje a techniky jako černé klobouky, dělají to se záměrem odhalit zloduchy. To znamená, že tyto nástroje používají pro etické hackování a forenzní informatiku. Etické hackování je proces, kdy se bezpečnostní nástroje používají k testování a vylepšování bezpečnosti (nikoli k jejímu narušování!). Forenzní informatika je proces shromažďování důkazů potřebných k odhalení a usvědčení počítačových zločinců.

Black hats

„Černé klobouky" jsou samozřejmě zloduši. Jsou to lidé, kteří vytvářejí a rozesílají viry a červy, pronikají do počítačových systémů, kradou data, vyřazují z provozu sítě a prostě páchají elektronické zločiny. O černých kloboucích v této knize hovoříme na několika místech. Černé klobouky a autoři malwaru nejsou v rámci bezpečnostní komunity považováni za totéž – přestože obě skupiny porušují zákon.

Etické hackování **Využití bezpečnostních nástrojů k objevování bezpečnostních děr a k testování a zlepšování bezpečnosti.**

Některé bílé klobouky pracují pro firmy, které se zabývají počítačovou bezpečností. Mezi ně lze zařadit firmy, které chrání společnosti před počítačovými útoky, stejně jako společnosti, které obětem počítačových zločinů pomáhají pachatele úspěšně pohnat k zodpovědnosti. Jedna z těchto společností, American Data Recovery (ADR), dokonce poskytuje služby soudního znalce. Společnost Computer Evidence, Ltd. zaujímá mezinárodní přístup k potírání zločinů a má své kanceláře v Evropě, USA, Asii, Jižní Americe a na Středním východě. Vzhledem k nárůstu počítačové kriminality se forenzní informatika stává rychle se rozvíjející možností uplatnění pro seriózní programátory. Ostatní bílé klobouky jsou specializovaní programátoři,

které zaměstnávají velké společnosti a organizace. Úkolem těchto bílých klobouků je uzavírat bezpečnostní díry, aby ochránili své zaměstnavatele před černými klobouky.

Forenzní informatika Proces shromažďování digitálních důkazů, které jsou zapotřebí k identifikaci a usvědčení počítačových zločinců.

Gray hats

Šedé klobouky stojí někde uprostřed, protože etickou hranici občas překročí (nebo – častěji – ji prostě jinak definují). Šedé klobouky například proniknou do počítačových systémů společnosti jen proto, aby se tam prošly a porozhlédly. Jednoduše si myslí, že pokud nezničí žádná data, nepáchají zločin. Potom si jdou zažádat o pracovní místo jako bezpečnostní konzultanti velkých korporací. Své předchozí nabourání do systému společnosti si ospravedlňují jako určitý trénink v oblasti počítačové bezpečnosti. Spousta z nich opravdu věří, že veřejnosti slouží tím, že společnosti informují o riziku hrozícím jejich počítačům.

Klobouky pro všechny!

Chtěli byste vidět všechny klobouky na jednom místě? Zkuste DEFCON. Každý červenec se hackeři všech druhů a velikostí vypravují do Las Vegas na setkání, které se samo propaguje jako „největší neoficiální hackerská událost na světě."

Na události, kterou časopis PC World překřtil na „Školu pro hackery" – přehlídce hackerských tipů, novinek, autogramiád a dalších akcí, jsou vítáni i dospívající, kteří schrastí registrační poplatek. Samozřejmě se objeví i hodní hoši. Tak často, že se oblíbenou konferenční hrou stalo „Najdi federála"!

Problém je, že ať už se na to díváte, jak chcete, vloupání je stále vloupání. Jak byste se cítili, kdyby se nějaké děti od sousedů vloupaly do vašeho domu a prohrabaly se všemi vašimi věcmi jen proto, aby vám ukázaly, že váš dům nebyl zabezpečený? Necítili byste se poškození i v případě, že by nic nerozbily ani neukradly? A co je ještě důležitější, najali byste si tyto děti, aby vám dům hlídaly? Nebo byste si řekli, že zřejmě nemají moc smyslu pro etiku?

4.2 Hackeři chtějí váš počítač

Můžete si myslet, že se hackeři o váš počítač nezajímají, ale opak je pravdou. Hackeři chtějí přístup do vašeho systému z mnoha různých důvodů. V kapitole 2, Poznej své nepřátele jsme hovořili o botnetech a armádách botů. Jakmile je váš systém jednou zneužit a zařazen do jedné z těchto armád, někteří hackeři prodají název vašeho systému na seznamu zneužitých počítačů. Pamatujte si, že jakmile se hacker jednou dostane dovnitř a nastraží trojského koně, otevře komukoliv dveře k případnému návratu. Hackeři to vědí a vydělávají na tom peníze. Jsou si vědomi, že když už se jednou vašeho počítače zmocní, snadno se skryjí a je velmi obtížné je vysledovat.

Celkově lze říct, že se na Internetu dá snadno skrýt. Zneužité počítače na celém světě pomáhají ukrývání zjednodušit. Je velmi snadné nalézt poslední **adresu IP,** ze které byl zahájen útok, ale hackeři před zahájením útoku přeskakují mezi mnoha nezajištěnými systémy, aby utajili svou polohu.

> **Adresa IP** Jedinečná adresa, která identifikuje, kde je počítač připojen k Internetu. Adresu IP má každý počítač, i ten váš, pokud používáte širokopásmové připojení.

V průběhu posledních čtyř let byla většina kyberútoků započata z počítačů v USA. Nicméně to neznamená, že systémy ve Spojených státech jsou původním zdrojem útoku. Hacker z Ruska může váš počítač klidně použít k zahájení útoku odmítnutí služby (DoS). Pro celý svět to pak může vypadat, jako byste útok začali vy, protože hacker skryl své stopy tak, aby bylo možné dohledat jen poslední „skok".

4.3 Nástroje hackerů

Za starých časů kolovaly nástroje hackerů v podsvětí. Dnes nabízí hackeři nástroje volně po celém Internetu. Pokud se chcete přesvědčit, zkuste vyhledat Googlem heslo „free hacker tools" (bezplatné hackerské nástroje).

Je pravda, že všechny z těchto více než 55 milionů výsledků hledání nejsou nutně skutečné nástroje, ale víc než dost jich existuje jen proto, aby dělaly problémy. Jejich počet také narůstá. Když jsme tuto knihu v roce 2007 vydali poprvé, stejný způsob vyhledávání volně dostupných hackerských nástrojů nám nabídl pouze 20 milionů výsledků.

Poznávání těchto nástrojů je důležité, ale stejně tak důležitý je i způsob, jakým je poznáváte. Vyzkoušet si je pod dohledem v počítačové učebně nebo na hodině informatiky je v pořádku, ale nepokoušejte se testovat je na Internetu na vlastní pěst. Pamatujte si, že hackování počítačů je protizákonné.

Může to být také nebezpečné. Dříve než použijete nějaký hackerský nástroj z Internetu, zeptejte se sami sebe: „Můžu věřit hackerským nástrojům?“ Opravdu si to promyslete. Mohlo by se jednat o nástroj, který vám skutečně umožní otevřít zadní vrátka do něčího systému. Nebo to také může být nástroj, který pohodlně otevře zadní vrátka do vašeho systému. Možná i obojí. A pokud bude napaden váš systém místo systému někoho jiného, komu přesně byste si chtěli stěžovat?

4.3.1 Skenovací nástroje

Bílé klobouky používají skenovací nástroje k testování zabezpečení systému. Dobrý skenovací nástroj prohledá počítač připojený k Internetu a prověří širokou škálu zranitelných míst. Může pomocí „klepání na porty“ zjišťovat, zda jsou body připojení k Internetu ve vašem

počítači dobře chráněny. Zkontroluje také operační systém, který používáte, a zjistí, jestli jste použili záplaty na již známé bezpečnostní díry systému. A samozřejmě zkontroluje váš firewall a otestuje, zda je váš přístroj chráněn před širokou škálou útoků zvenčí.

Bílé klobouky nejsou jediní lidé, kteří mohou použít skenovací nástroje. Pro kontrolu vlastního systému můžete vyzkoušet bezplatný skenovací nástroj Shields UP od společnosti Gibson Research Company, dostupný na webové stránce www.grc.com. Podívejte se také na spoustu dalších skenovacích nástrojů, které společnost GRC nabízí.

4.3.2 Prolamování hesel

Programy prolamující hesla jsou nejběžnějšími a nejzákladnějšími nástroji hackerské výbavy. Jsou k dispozici již nějaký čas a poměrně efektivně „uhodnou" většinu uživatelských hesel, alespoň částečně proto, že většina uživatelů si s vybíráním bezpečných hesel nedá moc práce.

Prvním krokem při prolamování hesla je často jednoduše hádání. To je jednoduché díky sociálnímu inženýrství. Hackeři vědí, že většina uživatelů si vybírá jednoduchá hesla, která se dají snadno zapamatovat. Nejčastějšími volbami jsou téměř vždy jména, která mají pro uživatele osobní význam – na vrcholu seznamu jsou křestní jména nejbližších členů rodin, těsně následována jmény domácích mazlíčků a oblíbených sportovních týmů. Crackeři hesel můžou například nahrát celý anglický (a často španělský) slovník, ale spoustu hesel mohou odhalit také pomocí obsahu jakékoli oblíbené knížky s dětskými jmény. Další výběr slabých hesel zahrnuje obvyklá čísla a čísla v běžném formátu, jako jsou telefonní čísla a čísla sociálního pojištění.

Celou situaci ještě zhoršuje fakt, že spousta uživatelů si nastaví stejné uživatelské jméno a heslo pro všechny účty, čímž hackerům nabídnou celou sklizeň při odhalení jediného hesla.

To je věc, kterou je nutné uvážit, než na síti Facebook použijete stejné heslo, jako používáte ve škole či v práci.

Zapomněli jste heslo?

Vítejte v klubu. Stejně dopadne 8 z 10 uživatelů počítače!

Spousta uživatelů nevyvine při vytváření slušného hesla vůbec ŽÁDNÉ úsilí. V prosinci 2009

došlo k napadení webové stránky RockYou a byla zveřejněna hesla 32 milionů uživatelů. V souvislosti s následky útoku analyzovala tato hesla firma pro datovou bezpečnost Imperva. Jako je tomu u většiny účtů, které to nezakazují, jedním z nejoblíbenějších hesel bylo slovo „heslo". Není také překvapující, že spousta uživatelů zvolila pro stránky RockYou heslo „rockyou". Obzvláště ubohá však byla číselná hesla. Polovina z desítky nejčastějších hesel byla vytvořena uživateli, kteří byli buď velkými fanoušky pořadu „Počítáme s Matějem", nebo šíleně pyšní na to, že se naučili počítat. Jejich hesla? 12345, 123456, 1234567, 12345678 a 123456789. Ostatní uživatelé z desítky nejčastějších hesel zjevně měli předchozí zkušenost se stránkami, které vyžadovaly kombinaci číslic a písmen. Svá hesla nastavili jako „123abc" nebo „abc123". Již dříve jsme zmínili, že spousta počítačových zločinců nebývá příliš chytrá. S takovými hesly to ani nepotřebují.

Klíčem k vytvoření *dobrého* hesla je vymyslet něco, co nemůže kdokoliv uhodnout, ani jednoduše prolomit. Použití jména vašeho domácího mazlíčka tudíž *není* dobrou metodou. Použití přihlašovacího jména je také špatnou cestou, protože ten, kdo zná vaše přihlašovací jméno (nebo jméno, vzhledem k tomu, že spousta přihlašovacích jmen je jednoduchou obměnou vašeho příjmení), se do vašeho systému jednoduše naboural.

Chcete také heslo, které jednoduše nerozlousknou nástroje hackerů. Automatické nástroje pro zjišťování hesel existují již desítky let. Tyto nástroje vyhledávají běžná jména, slova a kombinace slov. Z toho důvodu je nejlepší metoda pro vytvoření hesla použití neslovních hesel s využitím speciálních znaků. Spousta aplikací vyžaduje sedm nebo osm znaků. K vytvoření ideálního hesla použijte minimálně 7 znaků, využijte číslice i písmena, alespoň jedno z písmen napište velké (protože většina hesel rozlišuje velká a malá písmena) a přidejte zvláštní symbol jako *, $ nebo #. Část písmen můžete zkombinovat ze slov, která pro vás něco znamenají, ale bude obtížné je uhodnout. Například číslo Lindina domu je 18, její domácí mazlíček se jmenuje Flash a ráda v noci pozoruje hvězdy. Takže dobré heslo, které si lehce zapamatuje (ale pro hackery bude obtížné je rozlousknout) by mohlo být Flash18*. Nebuďte líní a nepropadněte zvyku užívání slabých hesel.

Další důležité pravidlo je NEPOUŽÍVAT stejné heslo pro více účtů. Pro časté uživatele počítače může být dodržování tohoto pravidla náročné.

Dobrá hesla Jedná se o neslovní hesla vytvořená kombinací věcí, které si můžete snadno zapamatovat, jako např. jméno domácího mazlíčka, název ulice a nějaký znak.

Vzhledem k tomu, že hlavní problém s nastavením hesla je neschopnost uživatelů pamatovat si bezpečná hesla, je nepravděpodobné, že by se tento problém vyřešil, dokud nebudou hesla nahrazena jednoduššími formami technologií, jako je **biometrika.** Biometrika využívá k identifikaci zabezpečených biologických dat. Běžně biometrické systémy využívají otisků prstů, rozpoznání hlasu a snímků sítnice (oka). Obrovskou výhodou těchto systémů je, že uživatel je nemůže zapomenout, je téměř nemožné tyto systémy náhodně (nebo záměrně) předat jiné osobě a je neuvěřitelně obtížné je zfalšovat.

Biometrika Využití biologických dat, jako jsou otisky prstů či snímky oční sítnice, k identifikaci.

4.3.3 Rootkit

Nejvyšším cílem hackerů je získat úplnou kontrolu nad vaším systémem bez vašeho vědomí. **Rootkit** je typ zákeřného kódu, jehož pomocí toho mohou dosáhnout. Přesněji řečeno, rootkit je souborem nástrojů, které hacker používá k dosažení dvou cílů:

1. Získat plný přístup k zneužitému počítači nebo počítačové síti
2. Zamaskovat skutečnost, že tento přístroj či síť byly zneužity

První rootkity byly vytvořeny na počátku 90. let. Od té doby byly dost propracovány. Dnešní rootkity otvírají nová zadní vrátka pro další přístup, shromažďují jména a hesla uživatele, instalují a monitorují keyloggery, a dokonce napadají další přístroje nebo sítě. Rootkity dokonce mění i logovací soubory (aby skryly skutečnost, že došlo ke zneužití) a deaktivují bezpečnostní programy. S použitím těchto nástrojů rootkity pracují, jako by bylo možné jim plně důvěřovat. Mohou se skrývat za jinými programy běžícími v systému. A mohou unikat vyhledávání programů, které sledují chování systému.

Rootkit Soubor nástrojů, které hackerovi umožňují získat plný přístup k nezabezpečenému počítači a zamést za sebou stopy.

Jak se tedy rootkit na počítač dostane? Nejběžnější cestou je otevřená bezpečnostní díra (jako je operační systém bez záplatované bezpečnostní zranitelnosti), která hackerovi vůbec umožní proniknout do vybraného přístroje. Rootkity se také mohou do počítače dostat pomocí červů.

Pomocí rootkitů byly provedeny některé z velmi vážných počítačových útoků. Jednou museli úředníci z univerzity v Connecticutu přiznat, že objevili rootkit, který byl nainstalovaný – a běžel nepozorovaně – na jednom z jejich **serverů** po dobu jednoho roku. „Napadený" server obsahoval osobní údaje spousty studentů, zaměstnanců a členů fakulty. Přestože neexistoval žádný důkaz, že by toto narušení vedlo ke konkrétním krádežím identity, zanechalo to univerzitu v nezáviděníhodném postavení, kdy musela 72 000 osob oznámit, že jejich jména, rodná čísla, data narození a telefonní čísla možná byla zcizena. Jak řekl Mark Russinovich, spoluzakladatel webových stránek s bezpečnostními nástroji www.Sysinternals.com, magazínu eWeek: „Odhaduji, že došlo i k jiným nálezům na dalších místech, jen jsme se o nich nedozvěděli."

Server Počítač, který obsluhuje velký systém (jako střediskový počítač), tím, že zajišťuje vysokorychlostní přístup ke specifickému typu dat, jako jsou osobní soubory nebo e-mailové účty. Není pochyb, že stejně tvrdě byly zasaženy další servery, a rovněž i některé domácí počítače. Rootkity jsou typ malwaru, který spousta internetových bezpečnostních balíčků běžně nehledá. Naštěstí existují snadno dostupné bezplatné nástroje, které to zvládnou. Společnost Sysinternals, kterou v roce 2006 získala společnost Microsoft, stále provozuje webové stránky poskytující řadu bezplatných bezpečnostních nástrojů včetně programu RootkitRevealer. Ve skutečnosti byla celá sada Russinovichových nástrojů Sysinternals – včetně programu RootkitRevealer – zakomponována do balíku Sysisternals Suite, který je zdarma dostupný ke stažení na stránkách Microsoft TechnNet (http://technet.microsoft.com/en-us/sysinternals/).

Rootkit válčí ve světě WOW

Přestože jsou rootkity často používány k odcizení finanční identity, někdy se krade virtuální majetek. Podívejte se na tento skutečný příspěvek z diskuzního fóra hry World of Warcraft:

0. Keylogger a rootkit.TDSS pomoc 12/16/2009 07:20:15 AM PST

Toto je můj příběh. Nechal jsem své předplatné WoW 16. listopadu 2009 zmrazit a 13. prosince 2009 jsem se rozhodl vrátit zpět a obnovit je. Když jsem si však kontroloval stav účtu, zjistil jsem, že byl toho rána obnoven za použití neznámé kreditní karty. Přihlásil jsem se do hry a zjistil, že můj bojovník 80. úrovně byl přesunut na jiný server a byla mu odebrána všechna výzbroj. Následně jsem byl zabanován, protože se hacker za použití mého účtu účastnil nelegální činnosti.

Nakonec jsem si změnil heslo, spustil několik antivirů a odstranil všechen malware, který jsem dokázal objevit. Ban byl zrušen a včera jsem znovu začal hrát. Zkoušel jsem se dnes ráno přihlásit a zjistil jsem, že mi bylo změněno heslo a s mými postavami někdo opět neoprávněně manipuloval. Změnil jsem tedy opět heslo z jiného počítače, než na kterém hraji.

Mám podezření, že jsem napoprvé nenašel keylogger. Spustil jsem ještě několik dalších kontrol pomocí různých programů a zjistil, že je můj počítač infikován malwarem Rootkit.TDSS a trojským koněm Trojan.Agent ....

4.4 Voláme bílé klobouky!

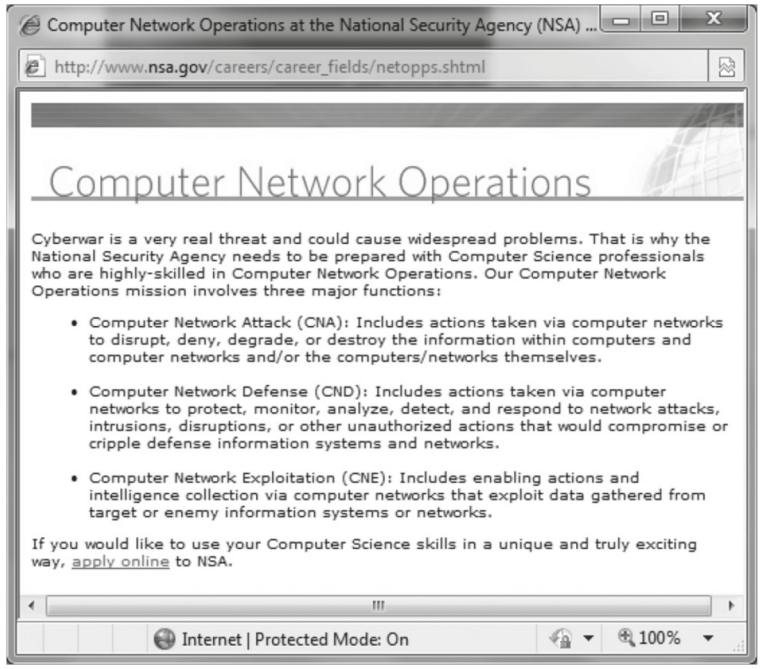
S nárůstem počtu počítačových zločinů v poslední době a rozhodnutím policejních orgánů postihovat počítačové zločiny přísněji se zvýšil nedostatek bílých klobouků. Jelikož cenu určuje nabídka a poptávka, platy rostou. Podle průzkumu institutu SANS provedeného v roce 2008 přes 98 % odborníků v oblasti počítačové bezpečnosti vydělává více než 40 000 dolarů ročně (v přepočtu přibližně 800 000 Kč). Celých 38 % z nich vydělává přes 100 000 dolarů ročně (v přepočtu přibližně 2 000 000 Kč).

Ještě lepší je výhled na zaměstnanost. Dokonce i s nástupem celosvětové ekonomické krize na konci roku 2008, kdy společnosti napříč zemí začaly propouštět, si 79 % z nich vytvořilo plán k udržení zaměstnanců z oblasti počítačové bezpečnosti. Válka s terorismem také zvýšila vládní potřebu bezpečnostních expertů.

Janet Napolitano, sekretářka Ministerstva vnitřní bezpečnosti (DHS), v září 2009 oznámila, že DHS do roku 2012 najme 1 000 odborníků v oblasti kyberbezpečnosti.

Být bílým kloboukem má něco do sebe. Kromě možnosti dobrého zaměstnání a platu je zde jako bonus vědomí, že pomáháte přetvářet Internet v lepší a bezpečnější místo.

Jestliže zvažujete kariéru v oblasti počítačové bezpečnosti, porozhlédněte se po vysokých školách a univerzitách, které nabízejí počítačovou bezpečnost jako součást osnov informatiky. Konkrétně Purdue University v Indianě se může pochlubit několika významnými bílými klobouky, které absolvovaly její studijní program. To je ale jen jedna z možností. Pokud je pro vás zásadní otázkou financování (a popravdě, pro koho není?!), můžete také zvážit nabídku stipendií, které nabízí Národní bezpečnostní agentura (NSA).



Text zprávy:
Provoz počítačových sítí
Kybernetická válka je velmi reálnou hrozbou a může způsobit celosvětové potíže. Proto musí být Národní bezpečnostní agentura připravená a mít k dispozici počítačové odborníky, kteří jsou velmi zkušení v operacích s počítačovými sítěmi. Naše mise zahrnující operace s počítačovými sítěmi spočívá ve třech hlavních funkcích:

• *Útok na počítačovou síť (CNA): zahrnuje činnosti provedené prostřednictvím počítačových sítí se záměrem přerušit, odmítnout, zhoršit nebo zničit informace v počítačích a na počítačových sítích, případně samotné počítače a počítačové sítě.*

• *Obrana počítačových sítí (CND): zahrnuje činnosti provedené prostřednictvím počítačových sítí s cílem chránit, monitorovat, analyzovat, detekovat a reagovat na síťové útoky, narušení nebo jiné neautorizované akce, které by poškodily nebo vyřadily z provozu obranné informační systémy a sítě.*

• *Využívání počítačových sítí (CNE): spočívá v umožňování činností a špionážním sběru dat prostřednictvím počítačových sítí s využitím dat získaných z informačních systémů nebo sítí patřících cílům nebo nepřátelům.*

Chcete-li se o kariéře v oblasti počítačové bezpečnosti, etickém hackování a bezpečnostních nástrojích dovědět více, podívejte se na některou z těchto stránek, které se zaměřují na bezpečnost:

• **http://securityfocus.com/ SecurityFocus** je nezávislá stránka, která není spojená s žádným konkrétním bezpečnostním produktem; poskytuje rozsáhlé aktuální informace o počítačové bezpečnosti splňující potřeby uživatelů počítačů a odborníků v oblasti informačních technologií.

• **http://searchsecurity.techtarget.com/ SearchSecurity.com** je stránka, která nabízí kompletní služby se zaměřením na odborníky v oblasti počítačové bezpečnosti. Tato stránka poskytuje specifické bezpečnostní vyhledávací nástroje, každodenní novinky z oblasti bezpečnosti, možnost zasílání informačních bulletinů zaměřených na bezpečnost a více než tisícovku odkazů na další stránky s bezpečnostní tématikou.

• **http://www.sans.org/ SANS.org** je oficiální stránkou institutu SANS (SysAdmin, Audit, Network, Security), který má celosvětově vedoucí postavení v poskytování školení z oblasti počítačové bezpečnosti. Institut SANS poskytuje zdarma řadu prostředků včetně týdenního přehledu bezpečnostních rizik (@RISK) a všeobecných bezpečnostních novinek (NewsBites), stejně jako více než 1000 odborných dokumentů zaměřených na počítačovou bezpečnost.

• **http://www.cerias.purdue.edu/ CERIAS** je zkratka pro Center for Education and Research in Information Assurance and Security (Centrum pro vzdělávání a výzkum v oblasti informační bezpečnosti a soukromí). Webové stránky centra CERIAS poskytují širokou škálu informací zaměřených na problematiku počítačové bezpečnosti.

5. Jak poslat SPAM na věčnost

– Obsah kapitoly

5. Jak poslat SPAM na věčnost – 99

5.1 E-mail a SPAM – 100

5.1.1 Co je to SPAM? – 100

5.1.2 Není SPAM protizákonný? – 101

5.2 Spoofing – 103

5.2.1 Falešné adresy – 103

5.2.2 SPAM proxy a relay – 105

5.3 Ťuk ťuk – jak spammeři poznají, že jste doma – 106

5.3.1 Skryté sledování – 107

5.3.2 Scavengery a crawlery – 108

5.3.3 Je vaše e-mailová adresa na prodej? – 109

5.4 Sociální inženýrství – 109

5.5 Aby se SPAM do příchozích zpráv nedostal – 110

5.6 SPIM – 111

5. Jak poslat SPAM na věčnost

Tessa byla nesmírně nadšená, když její táta o velikonočních prázdninách konečně ustoupil a dovolil jí založit si vlastní e-mailový účet. Kontrolovala jej 4x až 5x denně – nemohla se dočkat, až bude mít vlastní poštu. Vypadalo to, jako by svou novou adresu dávala každý den někomu – kamarádům ve škole, dětem z církevního společenství mladých, dokonce i novým přátelům, které poznala na Internetu. Aby měla jistotu, že ji každý může najít, přidávala své jméno do online adresářů a dokonce umístila svou novou adresu na rodinný web.

Zhruba první měsíc bylo všechno perfektní. Tessa pociťovala spojení se světem. Potom se začala dovídat o některých jeho temných obyvatelích.

Napřed Tessu začaly nudit hloupé e-maily určené pro dospělé. Bláhoví lidé se jí pokoušeli prodat věci, které si ve 13 letech vážně nemohla přát. Někteří z nich ji dokonce zkoušeli přesvědčit, aby podepsala smlouvu na kreditní karty. Tessa se zkoušela těchto e-mailů zbavit posíláním odpovědí na odkazy, které ji měly odstranit z databází pro odesílání e-mailů. Ale počet e-mailů se jen zvyšoval.

Brzy začal Tesse z některých e-mailů běhat mráz po zádech. Spoustu věcí, které se jí lidé pokoušeli prodat, ani nechápala, ale hodně jí připomínaly ten den, kdy místo hodiny zdravovědy zkoušela raději zůstat doma. A počet e-mailů stále narůstal.

Před posledním týdnem ve škole dostávala Tessa tolik nevyžádané pošty, že v té hromadě nebyla schopná najít vzkaz od svých přátel. Vzdala to a přestala svůj e-mail používat. Když začalo léto, Tessin táta pro ni založil nový e-mailový účet. Tentokrát nastavil filtry, aby automaticky odstraňovaly zprávy, které nebude chtít. Nyní je Tessa již velmi opatrná na to, komu svou novou e-mailovou adresu dá.

Spousta dospívajících je stejně jako Tessa zahlcena e-maily, které nechtějí, a ve skutečnosti by ani neměli být nuceni je vidět. Obrovský počet nevyžádaných e-mailových zpráv také zabírá ohromné množství počítačových zdrojů. Společnost Microsoft v bezpečnostní zprávě z roku 2009 uvedla, že 97 % všech e-mailů jsou SPAMy. Jak je to vůbec možné? Naštěstí se ne všechny z těchto SPAMů dostanou do příchozí pošty.

Na každý SPAM, který zahodíte, váš poskytovatel internetového připojení (Internet Service Provider, ISP) zablokuje několik dalších, než do vaší e-mailové schránky dorazí. Bohužel se i tak velké množství SPAMů dostává do oběhu.

5.1 E-mail a SPAM

SPAM je elektronický ekvivalent reklamních letáků. Je to e-mail, o který jste nežádali (nebo nevědomky souhlasili s jeho přijetím) a téměř nikdy o něj nestojíte. Některé SPAMy jsou nevyžádaná pošta z legitimních společností, které se vám pokoušejí prodat své výrobky. Jiné jsou nevyžádané e-maily z dosti pochybných společností, které se snaží o totéž. Když se to sečte, všichni tito spammeři pohltí obrovský podíl pásmového připojení.

5.1.1 Co je to SPAM?

Jestli to chcete vědět, SPAM je anglický název konzervovaného masného výrobku. Pokud jste jej nikdy nezkusili, chutná jako něco mezi šunkou a hovězím masem v konzervě. Do počítačové terminologie se výraz SPAM dostal na počátku 70. let z komediální parodie Monty Python. V této scéně se dvojice herců pokouší objednat si snídani bez SPAMU v restauraci, kde každé jídlo SPAM v nějaké podobě obsahuje. Máte z toho celkově pocit, že SPAM je všude, ve všem a vy mu nemůžete uniknout. Nevyžádané e-maily rozhodně vyvolávají podobné pocity.

Spam Nechtěné e-mailové zprávy, nazývané také elektronickou nevyžádanou poštou.

Překvapující množství SPAMů je zaměřeno na výrobky, které jsou buď zcela ilegální, nebo se pohybují na dost nejisté půdě. Obvyklým zdrojem SPAMů jsou například reklamy na online studijní programy. Pravdou je, že existuje mnoho online studijních programů, které jsou vynikající a vysoce uznávané – obzvláště na úrovni magisterského studia. Nicméně většina těchto škol nezahlcuje Internet SPAMem inzerujícím své programy. Školy, které to obvykle dělají, jsou – jak jste již uhodli – „neakreditované" univerzity. Při hodnocení jakéhokoliv předmětu nebo služby, které naleznete inzerované v nevyžádané poště, mějte na paměti heslo „Caveat Emptor" („bez záruky"). Jedná se o latinský výraz upozorňující kupující, aby byli na pozoru. Je samozřejmě naprosto jasné, že získat jakékoliv vysokoškolské vzdělání přes Internet, bez účasti na výuce a bez jakéhokoliv zkoušení, asi nebude úplně normální. Tento typ

společnosti se nazývá „továrna na diplomy“ (diploma mill). Diplom vydaný takovou školou není skutečným vysokoškolským vzděláním. Co je ale důležitější, používání takového padělku diplomu k získání zaměstnání nebo povýšení je nezákonné.

5.1.2 Není SPAM protizákonný?

To je velmi dobrá otázka, na kterou nelze jednoduše odpovědět. Pravdou je, že některé SPAMy jsou ilegální. Některé ne. Velmi obtížné je i vymezení rozdílu. Protože SPAM opravdu obtěžuje, Kongres USA se mu zvláště věnoval v zákoně CAN-SPAM z roku 2003. Tento zákon byl přezkoumán a rozšířen v roce 2005. Zákon CAN-SPAM je tedy stále platný (a stále neúčinný).

Jako většina amerických vládních iniciativ, i tato nese název odvozený ze zkratky – CAN-SPAM znamená „Controlling the Assault of Non-Solicited Pornography And Marketing“ (Kontrola napadání nevyžádanou pornografií a marketingem). Jejím cílem bylo omezit množství SPAMu tím, že odesílatele učiní právně odpovědnými. Ve skutečnosti definice tohoto zákona velkou část SPAMu zlegalizovaly a odpůrci mu proto začali říkat „I Can SPAM“ („Můžu spamovat“). Tento zákon definoval jako ilegální všechny nevyžádané elektronické zprávy, které neobsahovaly platný předmět a nadpis, skutečnou poštovní adresu odesílatele, jasné označení obsahu pouze pro dospělé, pokud je toto označení zapotřebí, a nějaký mechanismus umožňující odhlášení. Nefungovalo to. Tři roky po přijetí tohoto zákona se SPAM rozšířil tak, že tvořil 75 % všech e-mailových zpráv a jen méně než polovina procenta těchto zpráv ve skutečnosti splňovala podmínky zákona CAN-SPAM.

První zločin

Jeremy Jaynes byl v roce 2004 prvním člověkem, který byl odsouzen za spamování. V době své vrcholné aktivity Jaynes odeslal více než 10 milionů zpráv denně. Většina obsahovala nabídku rychlého zbohatnutí a různé falešné zboží a služby.

Bohužel virginský zákon, díky němuž byl odsouzen, později zrušili – změna, kterou v březnu 2009 potvrdil americký nejvyšší soud tím, že zákon odmítl obnovit.

A co je zajímavé, prvním člověkem zatčeným podle zákona CAN-SPAM byl dospívající, 18letý Anthony Greco z města Cheektowaga ve státě New York. Celkově ale bylo podle zá-

kona CAN-SPAM zatčeno velmi málo osob a ještě méně jich bylo úspěšně odsouzeno.

Velký problém zákona CAN-SPAM je mechanismus umožňující odhlášení. Mechanismus odhlášení je způsob, jak se může příjemce odhlásit z mail listu. To jste bezpochyby viděli v nevyžádaných e-mailech, které jste obdrželi. Všeobecný formát je:

```
Jestliže si nepřejete dostávat další informace od (dosaď spammera), odpovězte prosím na tuto zprávu a jako předmět zprávy uveďte Odhlásit.
```

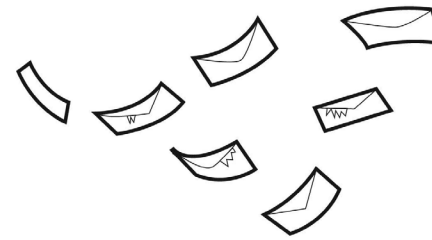
Mohli jste se také setkat s tímto formátem:

```
Pokud si přejete zrušit zasílání našich inzerátů nebo jste přesvědčeni, že vám tato zpráva byla zaslána omylem, můžete navštívit oddělení předplatného na našich webových stránkách.
```

Aby spammeři dodali svým prohlášením o legitimitě na věrohodnosti, často zákon CAN-SPAM ve svých odhlašovacích doložkách citují:

```
Tento e-mail je komerčním inzerátem a byl poslán v souladu se zákonem CAN-SPAM. Nechceme vám posílat informace, o které nestojíte, pokud si proto přejete být odhlášeni z dalšího rozesílání zpráv, použijte prosím odkaz umístěný na této stránce dole.
```

Cíl je v těchto případech vždy stejný. Pro odhlášení z databáze musíte navštívit webové stránky spammera, nebo mu poslat e-mail. Problém je, že jakmile tak učiníte, potvrdíte, že mají vaši skutečnou, platnou adresu, a že se k vám jejich zprávy dostávají. Pokud spammeři hrají podle pravidel, bude to fungovat bez problémů. Pokud podle pravidel nehrají, jednoduše jste jim dali najevo, že vaše e-mailová adresa stojí za prodej. Vzhledem k tomu, že spousta spammerů podle pravidel nehraje, odborníci silně doporučují NIKDY neodpovídat na nevyžádané e-maily a nenavštěvovat odkazy uvedené ve SPAMech. Pokud byste tak učinili, může se stát, že počet SPAMů, které obdržíte v budoucnosti, spíše závratně poroste, než aby se snižoval.



5.2 Spoofing

Spoofing (falšování) je parodování něčeho dobře známého. Ve své čisté podobě je falzifikát obvykle docela dobrý vtip. Komik Weird Al Yankovic si vybudoval kariéru psaním hudebních parodií na populární písně. Jednou z jeho nejlepších písní byla v roce 1983 parodie na hit Michaela Jacksona *Beat it (Poraz to)* s názvem *Eat it (Sněz to)*. Obzvlášť vtipný byl související videoklip.

Spoofing (neboli falšování) e-mailů už tak zábavný není. K **falšování e-mailů** dochází, když osoba, která vám posílá e-mail – téměř vždy se jedná o SPAM – předstírá, že je někým jiným. Spammeři jsou schopní zfalšovat zprávy vytvořením nepravých záhlaví, která obsahují nepravdivé směrovací informace. Pravé směrovací informace jsou součástí e-mailu určující internetovou adresu vašeho e-mailového účtu. Jde o číslice, které e-mailovým serverům umožní doručit váš mail. Definici přesměrování si můžete představit velmi podobně jako poštovní adresu. Není-li adresa platná, e-mail není doručen. Nepravdivá informace o přesměrování vlastně skrývá skutečnou adresu člověka, který e-mailovou zprávu posílá.

5.2.1 Falešné adresy

Když někomu odešlete e-mailovou zprávu, odeslaná zpráva vždycky začíná záhlavím, které obsahuje vaše jméno a e-mailovou adresu. Tyto položky jsou ve vašem e-mailovém programu definovány jako „Zobrazované jméno“ a „Zobrazovaná e-mailová adresa“. Změnou těchto položek můžete vlastně zobrazit, cokoliv si přejete. Dohledání takto jednoduše zfalšovaného e-mailu bude samozřejmě velmi snadné. Spammeři také vkládají nepravé směrovací informace; e-mail tak vypadá, jako by byl odeslaný přes jeden nebo více systémů, které s ním s největší pravděpodobností nepřišly do styku. Vysledování zpráv zfalšovaných pomocí nepravdivých směrovacích informací je MNOHEM obtížnější, a někdy nemožné.

Falešný e-mail E-mailová zpráva obsahující nepravou adresu odesílatele, což znemožňuje určit, odkud vlastně byla odeslána.

Falšování e-mailů je mimo jiné tak snadné proto, že je jejich záhlaví tvořeno pomocí **SMTP (Simple Mail Transfer Protocol**, **protokol jednoduchého přenosu pošty)**, a protokol SMTP

nemá autentikaci. Jednou z možností, jak spoofing omezit, je používat v e-mailu digitální podpisy. O digitálních podpisech budeme hovořit v ***kapitole 8, Bezpečné nákupy v kyberprostoru.***

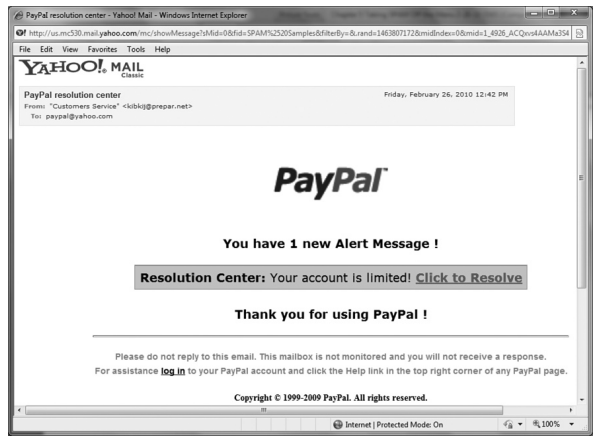
SMTP (Simple Mail Transfer Protocol) internetový protokol, který se používá k posílání a vytváření e-mailových zpráv.

V některých případech mohou být falešné e-maily zábavné. Před několika lety vtipálci šířili velmi zábavnou volební parodii, která vypadala, jakoby přišla z Národního vedení americké Demokratické strany. Bylo zřejmé, že se jedná o vtip, a falšování (i když nevhodné) nebylo provedeno se zlým úmyslem. U spousty falšovaných e-mailů je tomu však naopak.

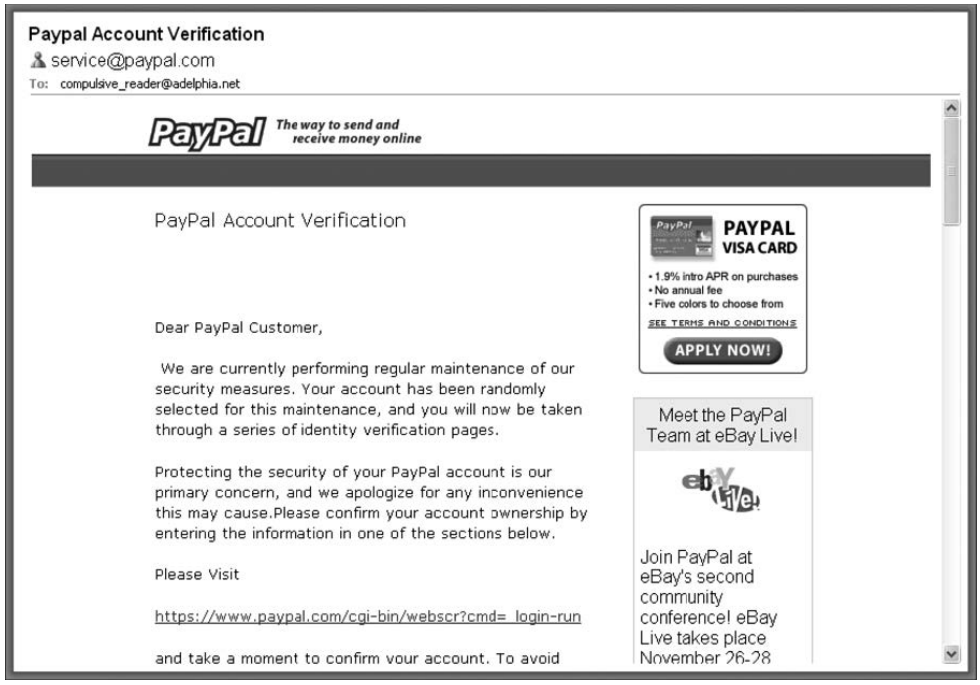
Falešné adresy jsou obvyklým námětem při pokusech o phishing. **Phishing** (vyslovujte stejně jako „fishing" – rybaření) je podvodná technika k získávání informací. Phisher (osoba provádějící phishing) odesílá e-mail vypadající jako e-mail od společnosti, kterou znáte a věříte jí, a žádá po vás informace, které byste pravděpodobně chtěli dané společnosti dát. V současnosti se phisheři často zaměřují na uživatele online služeb jako je eBay, Amazon a PayPal. Pokud jste si například vy nebo vaši rodiče oblíbili nakupování předmětů přes aukce na serveru eBay, máte pravděpodobně účet PayPal. Služba PayPal vám umožňuje vytvořit si online bankovní účet a používat jej k nakupování předmětů na serveru eBay, aniž byste jeho prodejcům dávali číslo své kreditní karty.

Phishing Podvodná technika přesvědčování obětí k poskytnutí osobních a finančních informací.

Pokud máte účet PayPal, pravděpodobně jste již obdrželi e-mail podobného znění:



Nebo podrobnější verzi:



V čem je problém? Tyto e-maily *nebyly* odeslány ze serveru PayPal. Pokud kliknete na obsažený odkaz a vložíte požadované informace, doslova předáte zlodějům informace o kreditních kartách svých rodičů.

O phishingu budeme více hovořit v ***kapitole 7, Rhybaření pro peníze***. Pro teď si jen uvědomte, že pokud jde o záhlaví e-mailů, není dobré dát na první dojem.

5.2.2 SPAM proxy a relay

Jak už víte, velká část vypuštěného SPAMu ve skutečnosti nepochází z adres, které jsou v e-mailech uvedeny. Co nevíte, je, že část ho možná pochází přímo z vašeho počítače.

Jak se to může stát? V kapitole 2 jsme mluvili o botnetech a o tom, jak mohou autoři malwaru infikovat váš počítač trojským koněm, který z něj udělá zombie. Hodně těchto zombií

se používá k posílání SPAMu. Jedním z virů, které to dělají, je virus SoBig.F. Virus SoBig také falšuje adresy v e-mailech, které posílá, takže to vypadá, jako by e-maily pocházely od někoho, jehož adresa je uvedena ve vašem e-mailovém adresáři.

Když dojde ke zneužití zombie počítače, který je pak použit k posílání SPAMu, říká se tomu SPAM relay. Počítač prostě předává (anglicky „relay") dál SPAMové zprávy, které vznikly jinde. Dochází k tomu velmi často. Nechráněné domácí počítače jsou v boji se SPAMem velkou překážkou.

SPAM relay Zneužitý počítač, který je používán k odesílání SPAMu bez vědomí majitele počítače.

I když jsou hlavním problémem domácí počítače, někdy činí potíže také poštovní servery, které používají poskytovatelé internetového připojení (ISP). I když servery bývají unášeny méně často, než jednotlivé počítače, jejich velké databáze e-mailových adres z jejich únosů činí zásadní problém. Když je unesen poštovní server a používá se k posílání SPAMu, říká se tomu SPAM proxy.

SPAM proxy E-mailový server zneužitý k posílání SPAMu.

ISP dnes pečlivě dbají na to, aby jejich poštovní servery zneužity nebyly. Většina domácích uživatelů počítačů to však bohužel nedělá. Kroky potřebné k ochraně vašeho počítače před tím, aby se z něj stal SPAM relay, jsou naštěstí stejné, jako kroky nutné k ochraně před počítačovými viry, červy a trojskými koni.

5.3 Ťuk ťuk – jak spammeři poznají, že jste doma

Když předpokládáme, že svou e-mailovou adresu nezveřejňujete po celém Internetu, možná si říkáte, jak vás spammeři našli a proč vám posílají TOLIK e-mailových zpráv. To je dobrá otázka a existuje na ni několik dobrých odpovědí.

5.3.1 Skryté sledování

Panuje oblíbená představa, že v případě jaderného útoku přežijí dvě skupiny zvířat: krysy a švábi. To platí i pro Internet. Pokud dojde k jeho úplnému vypnutí, první skupiny, které se opět objeví, budou pravděpodobně spammeři a web bugy.

Pokud jste ještě **web bug** neviděli ani o něm neslyšeli, jste na tom stejně jako většina ostatních lidí. Web bug (někdy také „web beacon“) je skrytý obrázek, který spammeři používají ke sledování e-mailových zpráv. Technicky řečeno je většina webových bugů definována jako transparentní GIF – soubor obrázku o velikosti pouhý 1x1 pixel – proto je příliš malý na to, abyste jej v e-mailu viděli.

Web bug Skrytý obrázek používaný spammery k ověření toho, že skutečně čtete SPAM, který vám posílají. (Říká se mu také web beacon (webový maják) nebo transparentní GIF).

Když si přečtete e-mailovou zprávu, grafické nebo obrázkové prvky v e-mailu se zobrazí stažením ze samostatné webové stránky. V minulosti byla většina e-mailových programů nastavena tak, že automaticky stahovaly grafiku, takže čtenáři netušili, že si stahují informace z jiné stránky. Dnes je výchozí nastavení takové, že často uvidíte nefunkční obrázky, jako je tento:

Jeden po druhém...

Když se díváte na obrázek na monitoru svého počítače, vidíte kvalitní grafický obrázek – podobný fotografii nebo kresbě. Ve skutečnosti se každý počítačový obrázek skládá z tisíců malých teček zvaných pixely.

Pojem „pixel“ je odvozen ze zkratky anglických slov „picture element“ – obrázkový prvek. Na tom, kolik pixelů v určitém obrázku je, závisí jeho rozlišení – jak „kvalitní“ nebo čistý obrázek vypadá.

Pokud používáte digitální fotoaparát, již tento pojem znáte. Fotografie vysoké kvality obsahuje oprav-

du hodně pixelů. Například fotoaparát Kodak Easy Share P880 poskytuje snímač na 8 megapixelů. To je asi tak osmkrát 1 milion pixelů v jediné fotografii.

Zkuste si představit obrázek obsahující pouze 1 krát 1 pixel. Ten nevidíte, což je samozřejmě u web bugů účelem.

Když kliknete na stažení grafiky, spammer ví, že je vaše e-mailová adresa platná, a že jeho e-mailovou zprávu opravdu vidíte. Nebuďte překvapení, když budete SPAM dostávat i nadále!

5.3.2 Scavengery a crawlery

Před chvílí jsme žertovali o tom, že vás možná překvapuje množství SPAMu, které dostáváte, když svou e-mailovou adresu nezveřejňujete po celém Internetu. Neskutečné je, že přesně tohle lidé dělají! Používají své e-mailové adresy jako uživatelská jména v online komunitách, uvádějí své e-mailové adresy na svých webových stránkách a dokonce používají své pravé adresy při posílání vzkazů v online uživatelských skupinách. Všechny tyto kroky jsou dobrým způsobem, jak začít dostávat SPAM.

Toto je také oblast, kde je důležité uzamykat informace, které sdílíte na sociálních sítích. Kontaktní informace, jako je e-mailová adresa, by se měly zobrazovat pouze přátelům, pokud je vůbec chcete uvádět. Popravdě řečeno nikomu na sociálních sítích svoji e-mailovou adresu dávat nepotřebujete. Každý, kdo vás najde na sítích Facebook nebo MySpace, vás může kontaktovat pomocí zprávy nebo e-mailu PŘÍMO na těchto sítích, takže nepotřebuje znát vaši osobní adresu. Celou e-mailovou adresu samozřejmě nikdy neuvádějte ve zprávách, které posíláte na něčí stránku nebo zeď.

E-mailový scavenger Typ webového crawleru, který prohledává Internet a sbírá (sklízí) všechny e-mailové adresy, které najde uvedené na webových stránkách.

Zveřejnění e-mailové adresy online může způsobit potíže, protože někteří spammeři používají programy zvané crawlery, které se kradou (anglicky „crawl“) webovými stránkami

(tj. prohledávají je) na Internetu a hledají známé znaménko @, objevující se ve všech e-mailových adresách. Některé společnosti mají z této činnosti docela slušný zisk.

5.3.3 Je vaše e-mailová adresa na prodej?

Pokud byla vaše e-mailová adresa zveřejněna na Internetu, je možné, že ji právě teď někdo prodává. Protože Internet je veřejné místo, sklízení adres na prodej (ačkoli je otravné) je naprosto legálním počinem. Pokud zkusíte zběžně vyhledat hesla jako „e-mail harvester" (sběratel e-mailů) nebo „e-mail spider" (e-mailový pavouk), najdete velké množství produktů sklízejících e-mailové adresy. Většina z těchto produktů stojí méně než 100 USD (v přepočtu přibližně 2 000 Kč).

Někdy prodávající nemusí e-mailové adresy „sklízet". Prostě použijí vlastní zákaznické nebo členské záznamy. Hudební služba SpiralFrog v roce 2009 prodala adresy 2,5 milionu svých zákazníků několika spammerům doslova pár dní před tím, než věřitelé převzali kontrolu nad firmou, která už byla v té době mrtvá. Jeden z těchto spammerů za adresy zaplatil 8 500 USD (v přepočtu přibližně 170 000 Kč). I když se jednalo, jak poznamenal jeden z bývalých zákazníků služby SpiralFrog, o „nechutný" počin, pravděpodobně nebyl nelegální. Mnoho bezplatných (a placených) služeb si vyhrazuje právo sdílet, distribuovat nebo prodávat informace, které jim poskytnete. Proto je důležité, abyste četli pravidla poskytování služby na každé webové stránce před tím, než jí tyto informace poskytnete.

5.4 Sociální inženýrství

Ačkoli je to zvláštní, někteří podvodníci se soustředí na SPAM, protože lidé jako vy začínají být příliš chytří a chrání své počítače aplikacemi, které hackerům nedovolí útočit na slabá místa programů.

Většina SPAMových zpráv při přesvědčování uživatele k tomu, aby si je přečetl, spoléhá na sociální inženýrství. Jsou to podobné triky, které používají autoři virů, aby vás přiměli otevřít přílohy e-mailu, i když víte, že byste to dělat neměli.

Co se týče sociálního inženýrství, spammeři do velké míry spoléhají na políčka „Od:" a „Předmět:" v e-mailových zprávách. Políčko „Od": je často zfalšované tak, aby vypadalo, jako

by odesílatelem byly velké společnosti nebo organizace, které znáte a věříte jim. Řádky „Předmět:“ jsou psány tak, aby vás překvapily nepřipravené nebo zneužily zvědavosti či chamtivosti.

Zde jsou některé z běžných údajů v políčku „Předmět:“, které spammeři používají:

```
Předmět: RE: Váš e-mail
```

Tento přístup se snaží vás nachytat a přesvědčit vás, že je zpráva odpovědí na vámi poslaný e-mail. Nepředpokládejte, že každý e-mail, který začíná písmeny RE, je skutečně odpovědí. Vždy se podívejte na políčko „Odesílatel“.

```
Předmět: Xbox hry na 30 dní zdarma
Předmět: Oznámení o VÝHŘE v loterii – VYHRÁLI JSTE!!!!
```

Dostat něco zadarmo je vždycky super, ne? Protože se mnoho dospívajících účastní online loterií a soutěží, je tento přístup velmi účinný. Když dostanete podobný e-mail, zeptejte se sami sebe, zda cena odpovídá některé loterii, které jste se skutečně zúčastnili. S účastí v těchto loteriích byste také měli být opatrní. Mnoho z nich existuje jen proto, aby sbíraly e-mailové adresy.

```
Předmět: Zhubněte až 30 kg za měsíc!
```

SPAMy nabízející diety jsou u dospívajících kupodivu velmi účinné. Studie zveřejněná v roce 2009 v časopise Southern Medical Journal zjistila, že téměř 20 % vysokoškolských studentů s nadváhou si opravdu koupilo produkty na snížení hmotnosti propagované e-mailovým SPAMem. Většina produktů propagovaná pomocí SPAMu bohužel sníží leda tak objem vaší peněženky. O pomoc se snížením hmotnosti byste měli požádat svého lékaře, ne spammera ze sousedství.

5.5 Aby se SPAM do příchozích zpráv nedostal

Když spammeři začínali, dobrých nástrojů na obranu před nimi nebylo mnoho. Dnes je k dispozici řada sofistikovaných nástrojů a technik k blokování SPAMu. Při obraně proti SPAMu hraje důležitou roli způsob, jakým používáte svou e-mailovou adresu, stejně jako činnosti, které se SPAMem provádíte.

I když se technologie pro blokování SPAMu zlepšuje, spammeři neustále zkoušejí, jak ji obejít. Žádná metoda vás před SPAMem neochrání na 100 %. První obrannou linií jsou přesto tyto zásady:

• Podezřelé e-maily mažte bez čtení!
Tak se vyhnete virům a červům, stejně jako dalšímu SPAMu.

• Neklikejte na odkazy v e-mailech.
Pamatujete si na web bugy? Nenechte je,
aby vám vlezly do počítače!

• Neodpovídejte na SPAM. I když jsou některé možnosti
odhlášení z mail listu opravdové, většina z nich bohužel není.
Z dlouhodobého hlediska budete dostávat méně SPAMu,
když jej budete prostě mazat, než když budete žádat o vynětí z mail listu.

• Dávejte pozor na to, kde svou e-mailovou adresu zveřejňujete.
Aby vás nechytly webové crawlery, které sklidí vaši e-mailovou adresu,
neuvádějte svou plnou e-mailovou adresu na žádné veřejně
přístupné webové stránce.

• Pokud máte filtry, používejte je, ale nečekejte,
že se postarají o všechno.

Filtry mohou být velmi užitečné při zachycování některých typů SPAMu. Spammeři však neustále mění obsah políčka „Předmět“, aby jejich zprávy filtry nezachytily. Obsah zprávy je často uveden ve formě grafického souboru nebo obrázku. Protože filtry prohlížejí text, všechna klíčová slova nebo fráze uvedené v grafice jim uniknou.

5.6 SPIM

SPIM je verze SPAMu šířená programy pro odesílání IM zpráv. Tak jako SPAM, i SPIM se hojně rozšiřuje a své příjemce nesmírně rozčiluje.

Distribuce **SPIMu** vzrostla, když se začaly IM zprávy více využívat. V roce 2007 používalo IM zprávy 50 % dospívajících Američanů. V roce 2009 toto číslo raketově vzrostlo, když členové sociálních sítí začali využívat IM zpráv na sítích Facebook a MySpace.

SPIM Nevyžádané IM zprávy. SPIM je verze SPAMu šířená IM zprávami.

Dospívající používají IM zprávy ještě více, než dospělí. Proto je pravděpodobnější, že budou dostávat SPIM. Někdy je SPIM záměrně určen dospívajícím. V únoru roku 2005 se stal 18letý obyvatel New Yorku, Anthony Greco, první osobou uvězněnou za posílání SPIMu poté, co zaplavil stránky MySpace.com přibližně 1,5 milionem SPIM zpráv. Anthony uživatele doslova zahltil SPIM reklamami na refinancování hypoték a nevhodnými stránkami pro dospělé. Pokud si myslíte, že na reklamy na hypotéky asi moc lidí nekliklo, uniká vám pointa. Anthonyho skutečným cílem nebylo prodávat služby propagované SPIMem, šlo mu o vydírání společnosti MySpace. Kontaktoval ji a nabídl jí, že její uživatele před SPIMem ochrání za pouhých 150 USD (v přepočtu přibližně 3 000 Kč) denně. Jak se ukázalo, nebyl to právě chytrý tah. Greco byl zatčen na letišti v Los Angeles, když si myslel, že letí na schůzku s Tomem Andersonem, prezidentem společnosti MySpace, kvůli podpisu dohody o výplatě výkupného. Někteří zločinci si prostě věci nepromyslí.

SPIM, stejně jako SPAM, také často existuje proto, aby uživatele přesměroval na malwarové stránky. V květnu 2009 byli uživatelé sítě Facebook zahlceni zprávami žádajícími je, aby se „podívali na mygener.im." Uživatelé, kteří na odkaz klikli, byli přesměrování na webovou stránku s adwarem.

Protože jsou sociální sítě častými cíli SPIMu i SPAMu, začínají se bránit pomocí právníků i bezpečnostních aktualizací. Společnost Facebook nedávno vysoudila 711 milionů USD (v přepočtu přibližně 14 220 000 000 Kč) na tak zvaném „králi SPAMu" Sanfordu Wallacovi

za jeho útoky na uživatele sítě Facebook. I když je nepravděpodobné, že by Wallace tolik hotovosti někdy schrastil, je tento občanský spor projevem nového agresivního postoje sociálních sítí vůči spammerům.

6. Kyberšikana

– Obsah kapitoly

6. Kyberšikana – 115

6.1 Šikana se přesouvá do digitálního světa – 116

6.2 Útoky na online reputaci – 117

6.2.1 Frontální útoky – 117

6.2.2 Útoky na identitu – 118

6.3 Ochrana reputace – 119

6.3.1 Vygooglujte se – 119

6.3.2 Pokud potřebujete, obraťte se na odborníky. – 120

6.4 Jak se chránit před kyberšikanou – 121

6. Kyberšikana

Megan Meier, 13letá dívka z města Dardenne Prairie ve státě Missouri, se s 16letým Joshem Evansem setkala online na síti MySpace. Za několik týdnů se z nich stali dobří přátelé, i když se nikdy ve skutečném životě nesetkali. Josh tvrdil, že se nedávno přestěhoval do blízkého města O'Fallon, kde se vzdělával doma a ještě neměl telefon. Přesto si online často psali a Meganina rodina později uvedla, že Megan mívala dobrou náladu. Po několika týdnech se ale tento online flirt začal zvrhávat. Josh údajně slyšel, že se Megan nechová dobře ke svým přátelům. Přeposlal její zprávy, aniž by mu k tomu dala svolení. Na síti se objevily zraňující poznámky o Megan. Potom jí Josh poslal poslední zprávu: „Všichni v O'Fallon ví, co jsi zač. Jsi špatná a všichni tě nenávidí… Svět by byl lepší, kdybys tu nebyla." Krátce poté Megan spáchala sebevraždu.

Meganina zkušenost byla tragická – obzvlášť proto, že Josh Evans vůbec neexistoval. Účet na stránkách MySpace s jeho jménem si založila 49letá Lori Drew, matka bývalé Meganiny kamarádky, která žila jen čtyři domy od Megan. Prokurátoři zjistili, že zraňující zprávy posílala paní Drew spolu se svou tehdy 18letou dočasnou zaměstnankyní, Ashley Grills. Lori Drew si navíc byla před zahájením hoaxu plně vědoma toho, že se Megan léčila s depresí.

V reakci na Meganinu smrt se problému kyberšikany začala v celé Americe věnovat pozornost. Společnost WiredSafety zahájila program povzbuzující dospívající, aby složili **Meganinu přísahu** a také se zavázali, že nebudou „používat technologii jako zbraň ke zraňování druhých".

Megan bohužel není jediným dospívajícím, kterého osoby dopouštějící se kyberšikany trápily za hranice únosnosti. A síť MySpace také není jediným místem, kde k útokům dochází. 14. ledna 2010 spáchala 15letá Phoebe Prince z města South Hadley ve státě Massachusetts sebevraždu poté, co na ni skupina děvčat ze školy rok útočila prostřednictvím textových zpráv a sítě Facebook. Pokud si myslíte, že jsou terčem kyberšikany jen děvčata, nenechte se mýlit. Riziko hrozí i chlapcům, jak dokazuje sebevražda 13letého Ryana Patricka Halligana z Vermontu, který měsíce trpěl kyberšikanou útočníků zpochybňujících jeho sexuální orientaci. V roce 2008 jeden 16letý chlapec z Brightonu sotva přežil pokus o sebevraždu po dlouhotrvajícím „vztahu" s – jak se později ukázalo – smyšleným chlapcem jménem Callum na stránkách sítě Bebo.

Všichni tito dospívající mají společné to, že byli zranitelní vůči zradě a ponížení od online přátel, kteří nebyli tím, za koho se vydávali.

6.1 Šikana se přesouvá do digitálního světa

Šikana na školním dvorku je problémem už od zavedení prvních malotřídek. Dnešní šikanující mají jednoduše větší prostor a mnohou si vybírat z mnohem větší nabídky obětí. Pojem **kyberšikana** pokrývá široký rozsah obtěžujícího chování. Kyberšikana často spočívá v posílání nenávistných zpráv na sociálních sítích. Zprávy se tak dostanou ke stovkám místních dětí. V minulosti jste mohli mít dojem, že strůjci šikany zničí vaši pověst před celou školou. Dnes, když mají děti stovky online přátel, útočníci skutečně mohou oslovit všechny žáky jedné školy.

A kyberšikana se netýká jen počítačů. Může k ní patřit také posílání obtěžujících textových zpráv a nevhodných fotografií mobilním telefonem. Někdy děti tyto zprávy nahrají z telefonu na webové stránky, rozšíří si tak publikum a zhorší napáchané škody.

Kyberšikana Forma zastrašování a obtěžování pomocí elektronických prostředků jako jsou e-maily, textové zprávy, chatovací místnosti a stránky se sociálními sítěmi.

Kyberšikana může mít mnoho podob. Někteří lidé šikanují posíláním urážlivých nebo výhružných e-mailů nebo textových zpráv přes mobilní telefony. Jiní útočí na stránkách sociálních sítí vytvářením nenávistných skupin. A hrstka jich útočí hned v několika formátech, takže si jejich oběti připadají jako pod nepřetržitou palbou. Jedna dospívající dívka udává, že ji bývalý přítel šikanoval na stránkách Facebook, MySpace a Bebo, e-mailem, na Twitteru, ve videích na serveru YouTube, která neschválila, a dokonce i textovými zprávami. Nakonec se bála zapnout počítač nebo zvednout telefon.

Jiní šikanující nejsou tak vytrvalí, ale jsou neuvěřitelně podlí. Někteří používají stránky s hlasováním k vytvoření soutěže o netlustější nebo nejošklivější osobu na své škole. Dnešní technologie bohužel poskytuje nespočet příležitostí k anonymní krutosti.

Jak špatné to je? Více než polovina středoškoláků se alespoň jednou stala terčem online šikany. A téměř všichni dospívající, se kterými jsme mluvili, znají někoho, kdo byl terčem šikany, nebo byli sami šikanováni.

Nenávidím tě, všichni tě nenávidí... chcípni.
–Anonymní zpráva na webové stránce jednoho teenagera

6.2 Útoky na online reputaci

Nejobvyklejší formu kyberšikany představují útoky na online reputaci. Vaše online reputace je důležitá. Pokud se nehodláte naprosto stáhnout z 21. století, značná část vašeho života bude strávena, diskutována a zaznamenána online. V určitém okamžiku možná budete mít více přátel na síti Facebook než v reálném životě. Když už nic jiného, reálný a virtuální život se vám budou velmi silně prolínat. Špatná reputace v jednom z nich bude mít následky i ve druhém. Proto strůjci kyberšikany používají útoky na online reputaci jako hlavní způsob útoků.

6.2.1 Frontální útoky

Většina online útoků na reputaci při kyberšikaně je dost přímočará. Obvyklým útokem je nenávistná skupina na sociálních sítích. Tím myslíme skupinu na sociálních sítích nebo na jiné webové stránce, která má doslova název „Nenávidím Honzu Nováka". Není to úplně originální, ale už jsme si řekli, že osoby dopouštějící se kyberšikany rozumu příliš nepobrali.

Rychlá prohlídka skupin na sociálních sítích nám odhalila doslova tisíce nenávistných skupin. Jedna skupina představující typický příklad tohoto konceptu se jmenuje prostě „Nenávidím Jeremyho_____" Snažíme se samozřejmě chovat ohleduplně. Skutečná skupina uváděla Jeremyho celé jméno a příjmení. Taky tam byla Jeremyho fotografie, název jeho střední školy a příspěvky jako: „Nenávidím Jeremyho, co ty?"

Jeremyho nenávistná skupina je jednoznačným případem kyberšikany. Jak to poznáme? Zaprvé je zde zjevné schéma vyjádřené slovy „Nenávidím". Další klíčem je, že administrátoři a téměř všichni členové skupiny chodí na stejnou střední školu. Zajímavé je, že profily těch, kdo nenávidí Jeremyho, vypadaly dost uboze. Naproti tomu Jeremy vypadá jako inteligentní, dobře vychovaný kluk.

Za dvacet let mohou tito strůjci kyberšikany nosit Jeremymu kávu nebo mu připravovat hamburgery. To však samozřejmě nemá vliv na to, jak zle se Jeremy cítí dnes.

Nenávistné skupiny nejsou samozřejmě technicky povoleny. Doslova všechny stránky se sociálními sítěmi tento typ skupin výslovně zakazují. Jeremyho nenávistná skupina ve skutečnosti porušuje tři pravidla použití služby Facebook, ve kterých uživatelé souhlasí s tím, že nebudou obtěžovat ostatní uživatele, nebudou sdílet nenávistný obsah a nebudou druhé povzbuzovat k porušování pravidel používání služby.

Proč tedy síť Facebook nenávistné skupiny automaticky nemaže? Překvapivě to není tak lehké, jak se zdá. Existuje mnoho lidí, míst a věcí, které můžete online klidně nenávidět. Mnoho dlouhodobých členů má například skupina „Nenávidím růžičkovou kapustu". Je také v pořádku nesnášet televizní pořady, filmy a hudební skupiny. Podle počtu fanouškovských skupin a nenávistných skupin jsou uživatelé sítě Facebook zjevně rozpolceni mezi láskou a nenávistí k filmům *Svítání*. Je také v pořádku nesnášet jednotlivce, POKUD se jedná o veřejné osoby. To zahrnuje politiky, i když zde byste měli při posílání obsahu uplatňovat zdravý rozum. Ačkoli vám první dodatek ústavy zaručuje právo nenávidět jakéhokoli voleného představitele, pokud jen pomyslíte na prázdné výhrůžky, pamatujte, že členové FBI, CIA, tajné služby i NSA prohlížejí Internet a hledají hrozby národní bezpečnosti.

6.2.2 Útoky na identitu

K útokům na identitu, stejně jako ke krádežím identity, dochází, když se za vás někdo vydává. Rozdíl je v tom, proč to daná osoba dělá. Při krádeži identity se za vás zločinci vydávají, aby pro sebe něco získali. To může být kreditní karta, za kterou nemusejí platit (protože účet přijde vám). Nebo to může být rodné číslo, které mohou prodat dělníkovi bez platných dokladů. Důležité je, že zlodějům identity vůbec nejde O VÁS. Chtějí vaši identitu, aby získali něco PRO SEBE. Při útocích na identitu jde naopak POUZE o vás.

Při útoku na identitu se za vás strůjce kyberšikany vydává, aby zničil vaši online reputaci. Šikanující často jménem svých obětí vytvářejí webové stránky, které naplní nenávistnými řečmi a obsahem. Cílem je přesvědčit kohokoli, kdo si tuto webovou stránku přečte, o tom, že jste naprosto příšerní. Obětí takového útoku na identitu se stal jeden městský soudce z Ohia, když zločinec, kterého před tím odsoudil, vytvořil webovou stránku se jménem soudce

a představil ho jako rasistického pedofila. Šikanující si ani nemusí vytvářet webové stránky. Stačí mu použít vaše skutečné jméno a adresu k registraci na stránkách propagujících drogy, pornografii nebo jiné téma, kvůli kterému by vás nemuseli chtít přijmout na vysokou, do budoucího zaměstnání nebo do armády, když si vás osoby zodpovědné za přijímání nových zaměstnanců vyhledají online.

Většina strůjců kyberšikany si vystačí s tím, že své oběti urážejí a vyhrožují jim. Menší část z nich však jménem svých obětí páchá zločiny. V roce 2007 byla skupina bojující proti internetovému zločinu z názvem CastleCops napadena kýmsi, kdo zahltil jejich paypalový účet dotacemi z podvodně používaných paypalových účtů. Oběti používající PayPal o prostředníkovi nic nevěděly. Viděly jen, že jejich účty byly vybrané a peníze se posílaly na účet skupiny CastleCops. Reputace této skupiny tak byla velmi poškozena.

6.3 Ochrana reputace

Vaše online reputace je důležitější, než si možná myslíte. Většina zaměstnavatelů rutinně kontroluje online příspěvky žadatelů o místo. Reputace poskvrněná na střední škole může za 10 let ovlivnit výši vaší výplaty. Abyste se vyhnuli problémům, uděláte nejlépe, když budete svou online reputaci sledovat, a na případné problémy rychle zareagujete.

6.3.1 Vygooglujte se

Abyste chránili svou online reputaci, musíte vědět, co o vás lidé online říkají. Jedním ze způsobů, jak to zjistit, je vyhledat své jméno na vyhledávači Google. (Nebo Yahoo!. Nebo Bing. Můžete použít kterýkoli z velkých vyhledávačů. Protože obvykle nehledají na stejných místech, může být dobré vyhledat své jméno v několika vyhledávačích.)

Zádrhel vyhledávání na Googlu spočívá v tom, že moc dobře nefunguje u lidí s velmi běžnými jmény. Vyhledáváním jména John Smith dostanete 100 000 000 výsledků. Pokud nemáte neuvěřitelně neobvyklé jméno nebo příjmení, je pravděpodobné, že budete muset vyhledat více než jen své jméno. Výhodou obvyklého jména je, že nikdo nebude předpokládat, že John Smith registrovaný jako nastávající neonacista jste vy, a ne nějaký jiný John Smith.

Pokud máte poměrně obvyklé jméno, musíte hledat své jméno PLUS město, nebo své jméno PLUS telefonní číslo a podobně. Vyhledejte také svou e-mailovou adresu.

6.3.2 Pokud potřebujete, obraťte se na odborníky.

Pokud zjistíte, že byla vaše online reputace poškozena, co nejdříve s tím něco udělejte. I kdyby se vám to teď nezdálo důležité, za několik let, až budete hledat první práci, to může být velmi důležité. Podle zprávy organizace Cross-Tab 70 % osob zodpovědných za přijímání zaměstnanců odmítlo kandidáty kvůli informacím, které našly online. Pokud vás odmítnou kvůli něčemu, co najdou online, alespoň by to mělo být něco, co jste *skutečně* udělali nebo řekli, a ne práce nějakého strůjce kyberšikany, který se vám snaží uškodit.

Vaší první reakcí by měla být stížnost přímo na stránce, kde jste našli informace poškozující vaši reputaci. Většina stránek neprodleně odstraňuje veškeré příspěvky, které by mohly být vykládány jako obtěžování.

Pokud to nebude stačit, zvažte, zda se neobrátit na odborníka. Očišťováním reputace se ve skutečnosti zabývá mnoho společností. Patří k nim mimo jiné společnosti Defendmyname, Naymzma a ReputationDefender. Nečekejte však zázraky – a čekejte, že vás to bude něco stát. Monitorovací služby, které prohledávají Internet a hledají potenciálně poškozující příspěvky od vás a o vás, jsou poměrně levné a stojí asi 10–15 USD (v přepočtu přibližně 200–300 Kč) za měsíc. To však obnáší jen NALEZENÍ informací o vás. Skutečné odstranění těchto informací stojí 30 USD (přibližně 600 Kč) a více za každou položku.

Když budete informovat odborníky, nezapomeňte v případě potřeby uvědomit i policii. Jinak byste mohli dopadnout jako dospívající, který poslal tento příspěvek na stránkách Ask.com na serveru Yahoo!.


Resolved Question

Show me another »

I know I already asked a similar question but how do I tell my parents the FBI is coming?

I already asked how to tell them I'm going to jail but now I the FBI may be coming. On facebook I harassed some people with some death threats and they said they were calling the police. So how do I tell my parents and how do I keep them from yelling me?

4 weeks ago

Report Abuse

Text zprávy:
Vyřešená otázka

Vím, že už jsem se na něco podobného ptal, ale jak mám říct rodičům, že si pro mě přijde FBI?

Už jsem se ptal, jak jim mám říct, že půjdu do vězení, ale teď po mě možná jde FBI. Na facebooku jsem pár lidem vyhrožoval, že je zabiju, a oni řekli, že na mě zavolají policii. Jak to mám teda říct rodičům a jak to mám udělat, aby mě neseřvali?

6.4 Jak se chránit před kyberšikanou

I když je reputaci možné očistit, je to obvykle složité a nákladné. Je mnohem lepší se od začátku před kyberšikanou chránit, než zkoušet zvrátit škody, které může napáchat. Tak jako u většiny počítačových zločinů však není ochrana jednoduchá.

Když byl zveřejněn příběh „Sebevraždy na MySpace kvůli mámě", pozornost veřejnosti se okamžitě zaměřila na problém kyberšikany. Od té doby tento případ slouží jako ilustrace toho, jak je obtížné legálně bránit děti před online obtěžováním, dokonce i před otevřeně zraňujícím obtěžováním, jako v tomto případě. Počáteční reakce veřejnosti na Meganinu sebevraždu byla do roka následována rozsudkem. V listopadu 2008 byla 49letá Lori Drew odsouzena v procesu, kteří právníci považují za první oficiální rozsudek nad kyberšikanou. Rozsudek vycházel z toho, že Drew porušila pravidla použití služby MySpace, která vyžadují, aby uživatelé poskytovali pravdivé informace o sobě, a souhlasili s tím, že nebudou „obtěžovat ani poškozovat druhé". V červenci 2009 byl však rozsudek zrušen na základě toho, že strany sporu ve skutečnosti nikdy pravidla používání služby nečetly, jen je kliknutím na tlačítko odsouhlasily. (Dříve už jsme mluvili o tom, jak autoři malwaru spoléhají na to, že uživatelé nečtou licence EULA, a tak je mohou „legálně" zavalit adwarem. Zdá se, že uživateli udělený souhlas s podmínkami, které nečetli, chrání i strůjce kyberšikany.)

Případ Drew také vedl k přijetí Zákona Megan Meier o prevenci kyberšikany. V roce 2009 však tento zákon uvázl před výborem. Několik mediálních příspěvků poukazovalo na závažné problémy s tím, že tento zákon porušuje práva plynoucí z prvního dodatku Ústavy. Tento problém bude patrně souviset se všemi zákony týkajícími se kyberšikany. Je téměř nemožné chránit svobodu slova, jak se o to naše společnost snaží, aniž bychom alespoň někdy nechránili

také nenávistné řeči.

Jak tedy můžete pomoci? Pokud víte o případu kyberšikany ve škole, nahlaste ho – i kdybyste cílem šikany nebyli vy. Vydejte se na válečné tažení proti kyberšikaně. Nezapomeňte, že tažení může začít kdokoli a kdekoli. Po Meganině sebevraždě zahájila skupina dospívajících tažení pro zastavení kyberšikany, aby tak uctili Meganinu památku. Vytvořili Meganinu přísahu, závazek dospívajících, že budou bojovat proti kyberšikaně. Zvažte, zda by se tažení nemohla zúčastnit i vaše škola.

Co ještě můžete dělat, abyste sebe a své přátele chránili před kyberšikanou? Buďte ostražití a pamatujte na 10 hlavních kroků prevence kyberšikany:

1. Znejte své přátele. Někteří dospívající vystavují sebe a své informace riziku přijímáním žádostí o přátelství od osob, které ve skutečnosti neznají. Věří zřejmě tomu, že to dělá každý. Není tomu tak. Studie uživatelů sociálních sítí pro dospívající, kterou v roce 2008 provedli výzkumníci z Univerzity státu Kalifornie, ukázala, že pouze 5 % dospívajících má mezi online přáteli osoby, které mimo Internet neznají. Takže buďte klidní, až budete příště ignorovat žádost o přátelství od někoho, koho nepoznáváte.

2. Podepište Meganinu přísahu a požádejte vaši školu, aby ji podepsali všichni studenti. Nezapomeňte, že útoky kyberšikany jsou úspěšné, protože děti se raději přidají k davu a stanou se útočníky, než aby se proti útočníkům postavily. Znění přísahy si můžete stáhnout ze stránky stopcyberbullying.org.

3. Omezte informace, které zveřejňujete. Nikdy neuvádějte informace, které by vás mohly osobně identifikovat, jako je domácí adresa nebo telefonní číslo. Tím se můžete chránit proti útoku na identitu.

4. Pečlivě nastavte své soukromí. Stránky se sociálními sítěmi vám umožňují upravit nastavení soukromí doslova u všeho, co sdílíte – aktualizace stavu, fotografie, členství ve skupinách – když tento obsah sdílíte. Pečlivě zvažte, jak moc chcete svůj soukromý život zveřejňovat. Nemyslete si, že jen proto, že jste si stránku nastavili jako soukromou, k ní nikdo nemá přístup.

5. Zjistěte si, co o vás zveřejňují vaši přátelé – na fotografiích stejně jako slovy. Vaši přátelé nemusejí brát ochranu vašeho soukromí tak vážně, jako vy. Často se googlujte.

6. Věřte svým instinktům. Když máte z nového přítele husí kůži, přátelství zrušte. Okamžitě.

7. Myslete před tím, než kliknete. Nezapomeňte, že jakmile něco pošlete nebo zveřejníte, nemůžete to vzít zpět. Pokud si nejste jisti, jestli je něco vhodné, pak to patrně vhodné není. Buďte obzvlášť opatrní při sdílení čehokoli v okamžiku, kdy jste naštvaní nebo rozrušení. Pokud zuříte kvůli něčemu, co jste si přečetli online, udělejte si v používání počítače přestávku a teprve poté odpovězte.

8. Nahlaste zneužívání. Činnosti na síti mohou způsobit i horší věci, než jen zraněné city. Nahlášením šikany můžete zabránit sebevraždě. Jak by vám bylo, kdybyste o šikaně věděli, a neudělali jste NIC? Chcete si to nést po celý život?

9. Nešikanujte sami sebe. Před každým příspěvkem dostatečně přemýšlejte. Příliš často dochází k poškození online reputace tím, že lidé napřed sdílejí a poté přemýšlejí.

10. Nešikanujte druhé. Vždy je dobré jednat s druhými tak, jak bychom chtěli, aby oni jednali s námi. Také vás to ochrání před odvetnými kyberútoky.

7. Rhybaření pro peníze

– Obsah kapitoly

7. Rhybaření pro peníze – 127

7.1 Co je to phishing? – 127

7.1.1 Jak běžné jsou phishingové útoky? – 130

7.1.2 Kdo se stává obětí phishingu? – 130

7.2 Jak poznat, že na vás útočí rhybáři – 133

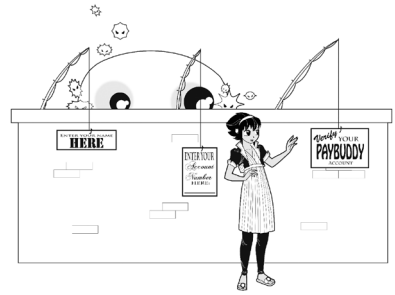
7.2.1 Jak dobré podvody jsou? – 133

7.2.2 Jak poznám phishingový podvod? – 134

7.3 Phisheři vašich přátel – 138

7.4 Podfuk s katastrofou – 139

7.5 Nenechte se ulovit phishery – 140



7. Rhybaření pro peníze

V květnu 2006 se 14letý Takumi ze čtvrti Nagoya v Tokiu stal prvním japonským nezletilým obviněným z internetového zločinu zvaného phishing. Takumi vylákal z uživatelů osobní informace tím, že vytvořil webovou stránku maskovanou jako oblíbená stránka s internetovými hrami. Touto léčkou ukradl Takumi identitu 94 osob. Dospívající děvčata, kterým ukradl osobní informace, se dokonce pokusil vydíráním přimět k tomu, aby mu poslala svoje nahé fotografie.

Jediná neobvyklá věc na Takumim byl jeho věk. Protože je v sázce tolik peněz, phisheři (kyberzločinci používající podvodné techniky k vylákání citlivých dat) jsou dnes obvykle profesionálními zloději. Ruská mafie a jiné organizované kriminální skupiny berou phishing vážně. A vy byste měli také.

V této kapitole probereme phishingové podvody podrobně. Řekneme vám, jak poznat, že na vás chystají léčku, a jak nepadnout do pasti. Tyto zásady byste měli naučit i své rodiče, je to pro jejich dobro.

7.1 Co je to phishing?

Phishing (vyslov „fišing“) se v angličtině vyslovuje stejně jako „fishing“, rybaření, a má s ním také mnoho společného. Podvodníci jen místo ryb loví informace. Phishingový útok obvykle začíná falešným e-mailem. Ten se tváří, jako by jej poslala společnost, kterou znáte a věříte jí, a možná s ní už obchodujete. V e-mailu se dočtete, že došlo k problému s vaším účtem, může se jednat o nezákonné použití nebo poplatky, nebo vás jednoduše žádají o ověření informací kvůli zlepšení vaší ochrany. Tohle je vlastně docela pěkná ukázka sociálního inženýrství – profesionální podvodník vám nabízí ochranu před bezpečnostními riziky.

Phishing Pokus vylákat z uživatelů osobní informace nebo finanční údaje.

Pravděpodobně jedním z nejlépe známých pokusů o phishing je podvod s PayPalem.

Pokud už jste na Internetu něco kupovali, zejména ze zahraničí, asi PayPal znáte. PayPal je online služba, pomocí které lidé platí za předměty koupené na stránkách, jako je eBay. I když PayPal není technicky vzato banka, funguje hodně podobně – umožňuje vám snadno převádět peníze na jiný paypalový účet pouhým odesláním e-mailu. Tyto typy transferů jsou možné díky tomu, že když jste si vy nebo vaši rodiče paypalový účet zřizovali, museli jste jej spojit se skutečným bankovním účtem nebo kreditní kartou.

Lidé nakupující online mají službu PayPal rádi, protože jim dává pocit většího bezpečí než předávání čísel platební karty neznámým osobám. Takže v čem je problém? V posledních letech se PayPal stal také velkým cílem hackerů a phisherů. A nejsou sami. I když jsme mluvili o DoS útocích a červech zaměřených na přerušení provozu komerčních webových stránek, největším problémem, který může potkat většinu velkých online hráčů – jako jsou společnosti PayPal, eBay a Amazon – nejsou bezpečnostní problémy s jejich internetovými stránkami. Největším problémem jsou phisheři lákající z jejich zákazníků finanční údaje.

Jestli jste někdy PayPal použili, asi už jste se s podobným podvodem setkali. Dokonce i pokud jste PayPal nikdy nepoužili a nemáte ani PayPal účet, pravděpodobně jste už tento typ podvodů viděli. To proto, že phisheři toho mají hodně společného se spammery. Jde jim o kvantitu, ne o kvalitu. PayPal má více než 202 milionů uživatelů operujících ve 190 zemích a regionech, takže existuje slušná šance, že značný podíl e-mailových adres, na které phisheři posílají SPAM, patří majitelům účtů PayPal. Ověřují si to? Vůbec se neobtěžují.

Podvod s PayPalem

```
Vážený uživateli služeb PayPal,
momentálně provádíme pravidelnou údržbu našich bezpečnostních opatření. Váš
účet byl pro tuto údržbu náhodně vybrán a nyní Vás provedeme sérií stránek
ověřujících Vaši identitu.

Ochrana bezpečí vašeho účtu PayPal je naší prioritou a omlouváme se za zdržení,
které Vám tato opatření mohou způsobit. Potvrďte prosím, že vlastníte tento
účet, zadáním informací do jedné z níže uvedených částí.

Navštivte prosím adresu https://www.paypal.com/cgi-bin/webscr?cmd=_login-run
```

```
a věnujte chvíli potvrzení Vašeho účtu. Aby nedošlo k přerušení služby, je
nutné, abyste svůj účet potvrdili co nejdříve. Váš účet bude v našem systému
aktualizován a služby PayPal můžete nadále používat bez přerušení.

Pokud svůj účet neaktualizujete, bude jeho status změněn na „omezený".

Děkujeme, personál společnosti PayPal

Děkujeme, že používáte PayPal!

CHRAŇTE SVÉ HESLO
NIKDY heslo nikomu nedávejte a přihlašujte se pouze na stránce https://www.
paypal.com/cgi-bin/webscr?cmd=_login-run Chraňte se před podvodnými webovými
stránkami tím, že vždy zkontrolujete lištu s URL/adresou, než se přihlásíte.
```

To také vysvětluje, jak mohli vaši rodiče dostat požadavek na „aktualizaci informací" o kreditních kartách, které nikdy neměli. Phisheři, stejně jako spammeři, prostě spoléhají na vysoký počet pokusů. Pokud návnadu spolkne byť jen malý podíl spotřebitelů, dotáhnou věc do konce.

Všimněte si, že náš příkladový paypalový podvodný e-mail vás žádá o návštěvu konkrétní webové stránky, https://www.paypal.com/cgi-bin/webscr?cmd=_login-run. To je obvyklá součást všech pokusů o phishing, vložený odkaz. V určité chvíli vás všechny phishingové e-maily požádají o kliknutí na uvedené odkazy, abyste se přihlásili ke svému účtu a aktualizovali nebo ověřili informace o něm. Problémem je samozřejmě to, že vás tento odkaz nepřesměruje na váš skutečný účet. Namísto toho vás odvede na falešnou obrazovku – často sérii obrazovek – vypadající stejně jako skutečná webová stránka příslušné společnosti.

Když na odkaz kliknete, všechno, co od toho okamžiku napíšete, se posílá přímo podvodníkovi, který tento pokus o phishing nastražil. Pokud zadáte uživatelské jméno a heslo, dáváte tomuto podvodníkovi vše, co potřebuje, aby vaším jménem na příslušné stránce vystupoval. Když je cílem phishingu banka nebo podobná instituce, jako je PayPal, dáváte zločinci všechny podrobnosti nutné k tomu, aby vám doslova vysál účty. Pokud zadáte informace o platební kartě, můžete v krátké době na účtu očekávat neočekávané operace. I když je možné, že si s vaším účtem podvodník pořádně užije při nákupech, pravděpodobnější je, že vaši platební

kartu prodá někomu jinému. V roce 2009 se čísla platných platebních karet na černém trhu prodávala za 300 USD za kus (v přepočtu přibližně 6 000 Kč).

Můžete dokonce poskytnout všechny údaje, které zločinec potřebuje k úspěšné krádeži vaší identity. Pokud se tak stane, nové pohyby na vašem účtu mohou být tím nejmenším z vašich problémů. Zkušený zloděj si může vaším jménem pořídit NOVÉ platební karty a poskvrnit tak informace o vaší úvěruschopnosti nesplacenými účty, které mohou vaši finanční historii zničit ještě dříve, než začala.

E-mail není jedinou metodou používanou k phishingu. Základní phishingový podvod už ve skutečnosti útočí na počítače desítky let. Velkou změnou je to, že se mohou podvodníci díky počítačům daleko lépe skrývat. Na rozdíl od phishingu po telefonu, který se dá snadno sledovat, je při e-mailovém phishingu mnohem snadnější se skrývat, protože e-mail používající smyšlenou adresu a falešné přesměrovávací informace je téměř nemožné sledovat.

7.1.1 Jak běžné jsou phishingové útoky?

Neuvěřitelně obvyklé. Jen v první polovině roku 2009 došlo k 56 000 samostatných phishingových útoků. Některé byly zaměřeny na finanční údaje – častými cíli jsou banky, platební karty a služba PayPal. Jiné byly zaměřeny na zdánlivě nedůležité stránky, jako jsou fotogalerie, herní stránky, Twitter nebo Facebook. Proč? U nefinančních stránek phisheři ve skutečnosti hledají hesla. I když někteří phisheři mohou skutečně chtít ukrást vaši hru World of Warcraft, většina z nich předpokládá, že jste, stejně jako mnoho dalších lidí, zahlceni mnoha účty a tak používáte na všech stránkách stejné přihlašovací údaje. Uživatelské jméno a heslo ke zdánlivě nedůležitému účtu může docela dobře fungovat i s vaším bankovním účtem.

Proč jsou tyto útoky tak obvyklé? Z pohledu phisherů tato taktika funguje. I když se lidé stávají poněkud zkušenějšími (nebo se prostě jen víc bojí), pořád se jich příliš mnoho nechá zlákat vábničkou phishingu.

7.1.2 Kdo se stává obětí phishingu?

Ačkoli podvodníkům naletí jednotliví zákazníci, oběťmi phishingu jsou také společnosti, jejichž zákazníci ztratí důvěru v jejich online služby a v některých případech je dokonce pře-

stanou používat. To se týká podniků všech typů a velikostí, ale hlavními oběťmi jsou online služby a finanční skupiny.

Banky

Hlavními cíli phishingových podvodů jsou ze zjevných důvodů banky. David Jevans, předseda pracovní skupiny pro potírání phishingu APWG, v prosinci 2009 udával: „V poslední době jsme byli v USA svědky pokusů kyberzločinců o krádeže 100 milionů dolarů (v přepočtu asi 2 miliardy korun) z podnikových účtů. 40 milionů z nich není možné získat zpět.“ Těchto v přepočtu 600 milionů korun se ztratilo z podnikových účtů hlídaných vyškolenými finančními odborníky. Jen si představte celkovou škodu, které mohou čelit spotřebitelé nevyškolení v odhalování podvodů.


Notice From Wachovia!
From: "Customer Service" <iwbgon@accouts.net>
To: admin@info.org

WACHOVIA
A Wells Fargo Company

We recently have determined that different computers have logged onto your Online Banking account, and multiple password failures were present before the logons. We now need you to re-confirm your account information to us.

If this is not completed by January 27, 2010, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner.

To confirm your Online Banking records click on the following link:
https://onlineservices.wachovia.com/auth/AuthService

Thank you for your patience in this matter.

Text zprávy:
WACHOVIA

V nedávné době jsme zjistili, že se na váš online bankovní účet přihlašovalo několik počítačů a před přihlášením byla opakovaně zadávána neúspěšná hesla. Nyní potřebujeme, abyste nám svůj účet potvrdili.

Pokud tak neučiníte do 27. ledna 2010, budeme nuceni váš účet na neurčito uzavřít, protože mohl být použit k podvodným účelům. Děkujeme za Vaši spolupráci v této záležitosti.

Své bankovní záznamy potvrdíte kliknutím na tento odkaz:
hhtps://onlineservices.wachovia.com/auth/AuthService

Děkujeme za Váš čas!

Bankovní podvody jsou jiným phishingovým výpadům podobné v tom, že jejich cílem je přesvědčit vás k zadání přihlašovacích údajů. Běžná je výhrůžka zablokováním přístupu k vašemu účtu, pokud téměř okamžitě neodpovíte. Zloději nechtějí, abyste se před kliknutím zastavili a chvíli přemýšleli. E-mail od banky Wachovia, který zde uvádíme, byl odeslán 26. ledna a vyhrožoval odpojením služby všem, kteří neodpovědí do následujícího dne. Skutečná banka by vám nikdy na odpověď nedala jen 24 hodin. Kdykoli uvidíte požadavek na neuvěřitelně rychlou odpověď, předpokládejte, že čtete podvodnou zprávu. V tomto případě nemohla žena, která e-mail obdržela, nikam kliknout, protože ani neměla u banky Wachovia otevřený účet. Wachovia je však opravdu velká banka a mnoho lidí u ní účet má.

Protože příjemce v tomto případě poznal podvod, tato konkrétní rybářská expedice selhala. Úspěšné podvody stojí banky celé jmění v nákladech nutných k rušení účtů a opakovanému vydávání platebních karet. Jako gesto dobré vůle dostávají zákazníci novou kartu zdarma. Nakonec to však všichni platíme prostřednictvím vyšších bankovních poplatků.

Online společnosti

Protože online podniky často závisejí na e-mailech jako jediném způsobu komunikace se zákazníky, phishingové pokusy tyto společnosti zasahují nejbolestněji. Nejčastějšími cíli jsou největší online společnosti, jako je eBay, PayPal nebo Amazon.

Nezaměstnaní

Někteří z podvodníků neznají ani strach, ani soucit. Když se v roce 2009 ekonomika dotkla dna, phisheři se zaměřili na nezaměstnané. Tabitha, 22letá čerstvá absolventka střední školy hledající práci, podala inzerát se žádostí o zaměstnání na velkém inzertním serveru Craig's List a začala se stávat cílem jednoho pokusu o phishing za druhým. Tyto e-maily tvrdily, že žádosti o pracovní místa je nejprve nutné „ověřit", než budou podstoupeny dále, a uváděly odkaz na službu „screeningu kreditní situace" žádající nezaměstnané o zadání všech údajů, které by podvodník potřeboval ke krádeži jejich identity.

Pravděpodobně i vy

Není důvod se domnívat, že byste zrovna vy nemohli být v krátké budoucnosti na seznamu cílů internetových podvodníků. Jste jedním ze 125 milionů uživatelů, kteří používali službu MySpace? Pokud ano, už jste se možná obětí phishingu stali a ani o tom nevíte. Začátkem června 2006 byla v Kalifornii objevena a odstraněna nastražená stránka lovící přihlašovací údaje

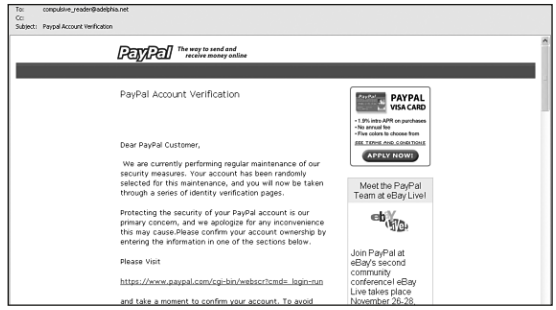
ke službě MySpace. Jednalo se o obzvláště lstivý útok, při kterém hacker zval prostřednictvím IM zpráv uživatele k zobrazení fotek, které vypadaly, jako by pocházely od jednoho z online „přátel“ oběti útoku. Když se cíl chytil a použil uvedený odkaz, ve skutečnosti zadával své přihlašovací údaje podvodné stránce, která zachytila jeho přihlašovací údaje, předala je dál a poté je skutečně použila k přihlášení na MySpace. Časová prodleva byla minimální a uživatel se skutečně dostal až na svou MySpace stránku, takže si většina obětí ani neuvědomila, že jim byly informace ukradeny.

7.2 Jak poznat, že na vás útočí rhybáři

Nikdo nemá rád, když ho vodí za nos. Abyste se nestali nedobrovolnými účastníky rybářského výletu, měli byste pochopit dvě věci. Zaprvé si musíte uvědomit, jak dobré a přesvědčivé ty podvody jsou. Zadruhé se musíte naučit, jak herce odhalit.

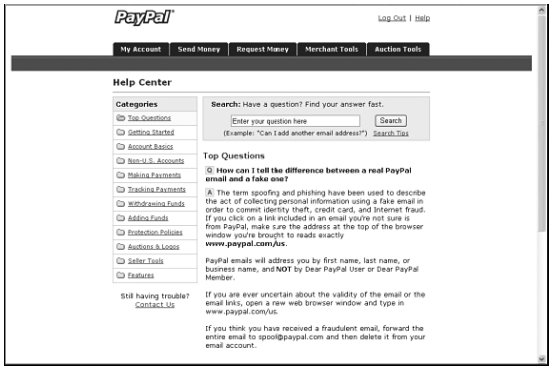
7.2.1 Jak dobré podvody jsou?

Falešné obrazovky mohou být velice přesvědčivé. Podívejte se na tento phishingový pokus přimět uživatele služby PayPal k odhalení uživatelského jména a hesla.



Falešná obrazovka služby PayPal hrající roli v pokusu o phishing

Tato falešná obrazovka je docela přesvědčivá, že? Všimněte si reklam na PayPal Visa a eBay. Nyní ji srovnejte se SKUTEČNOU obrazovkou služby PayPal (zde velmi případně uvádíme obrazovku nápovědy vysvětlující uživatelům, jak poznat falešné e-maily od PayPalu a nenechat se oklamat).



Skutečná obrazovka služby PayPal

Falešné zprávy samy o sobě jsou tak přesvědčivé, že na ně odpoví až 20 % respondentů. To je hodně lidí vystavujících své osobní a finanční údaje velkému riziku. Kvůli značné četnosti těchto útoků mnoho produktů pro internetovou bezpečnost phishingové útoky vyhledává. Mezi novým způsobem útoku a odpovídající novou bezpečnostní ochranou však vždy existuje krátká prodleva. Abyste se během této prodlevy chránili, musíte vědět, jak rozpoznat phishingové úroky, a preventivně chránit své osobní informace.

7.2.2 Jak poznám phishingový podvod?

V knize *Harry Potter a vězeň z Azkabanu* J. K. Rowlingová představuje úžasné zařízení nazývané lotroskop. I když je vyladěné tak, aby hledalo především temnou magii, obecně se lotroskop zapne vždy, když se v jeho blízkosti objeví osoba nebo předmět s nekalými úmysly.

Když víte, na co se dívat, je snadnější podvod rozpoznat. Podvody prozradí poměrně široká škála vlastností. Patří k nim generické názvy, logo, které tak docela neodpovídá, špatná gramatika, požadavky na ověření a maskovaná webová adresa. Když narazíte na JAKOUKOLI z těchto vlastností, měl by se váš vnitřní lotroskop zapnout.

Známe se?

Jak elegantně vyjádřil Shakespeare v *Romeovi a Julii:* „Copak je po jméně? Co růží zvou, i zváno jinak, vonělo by stejně." Tak to je možná pravda u květin, ale u e-mailu platí, že to, jak vás odesílatel oslovuje, mnoho prozrazuje o tom, s kým skutečně mluvíte.

U phishingových podvodů začíná SPAMový e-mail téměř vždy eufemismem v místě, kde by mělo být vaše jméno.

Vážený uživateli online služeb:
Vážený zákazníku naší banky:
Vážený držiteli bankovního účtu:
Vážený člene osobního klubu:

Někdy se podvodníci snaží oslovení zamaskovat tak, že slovo „Vážený" vypustí a začnou pozdravem, který obvykle nebývá spojen se jménem:

Zdravíme Vás!
Vítejte!
Varování!
Bezpečnostní upozornění!

Až na několik málo výjimek platí, že jakýkoli skutečný e-mail, který obdržíte a který vyžaduje další informace, bude pocházet od společnosti, která vás zná stejně dobře, jako vy znáte ji. Vaše banka opravdu zná vaše jméno i příjmení. Společnost, která vašim rodičům vydala kreditní kartu, rovněž.

Kvůli vysokému počtu pokusů o phishing nyní mnoho společností přidává jména i k dopisům, které by jinak měly jen jednoduchou formu. Když jedna naše přítelkyně, která online prodává a kupuje knížky, obdržela od služby eBay dopis v obecné formě s oslovením „Vážený uživateli stránky Half.com", věděla, že se skutečně jedná o e-mail ze serveru eBay, protože nad pozdravem obsahoval také tento řádek:

```
eBay posílá tuto zprávu Melindě J Smith (missy_bookseller). Vaše registrované uživatelské jméno je uvedeno jako důkaz, že tato zpráva vznikla na serveru eBay.
```

Používání pořádné gramatiky

Pokud je vaše máma stejná jako většina ostatních, určitě vám často připomínala, že máte

používat správnou gramatiku, abyste nezněli jako povrchní nebo nevzdělaní lidé. Možná dodala, že nemáte mluvit jako kriminálník.

Z důvodů, které lze v době mnoha dostupných a snadných nástrojů ověřujících správnost anglické gramatiky jen těžko pochopit, většina phishingových e-mailů používá špatnou nebo přímo příšernou gramatiku. Podívejme se na překlad části e-mailu posílaného uživatelům obchodu Amazon:

```
Pozdravy!
Kvůli souběžným podvodným pokusům jsme obdrželi. Pravidelně aktualizujeme
a ověřujeme naše zákazníky. Během náhodné kontroly naše oddělení byl problém
s vaším účtem, který jsme nemohli ověřit informace o váš účet. Buď se vaše
informace změnily, nebo jsou neúplné.
```

Co je na tomto odstavci špatného? Tak zaprvé, první odstavec je fragment. „Kvůli souběžným podvodným pokusům jsme obdrželi." Zatímco první věta končí příliš brzy, třetí je moc dlouhá a na konci přestává dávat smysl. Docela ironické je, že cílem tohoto podvodu je právě server Amazon. Opravdu si myslíte, že by největší prodejce knih na světě nedal dohromady souvislou větu? To je dobrý příklad toho, proč musíte v hodinách jazyka dávat pozor!

Ďábel tkví v detailech

Téměř stálicí všech pokusů o phishing je požadavek, abyste „ověřili svůj účet" nebo „potvrdili informace o svém účtu". Strůjce podvodu v podstatě chce, abyste mu poskytli své údaje, a on tak mohl používat váš účet.

Kvůli předpisům na ochranu soukromí, bezpečnostním potížím a zdravému selskému rozumu vás důvěryhodné společnosti NIKDY nepožádají o potvrzení následujícího typu informací:

- Kódy PIN.
- Uživatelská jména.
- Hesla.
- Čísla bankovních účtů.
- Čísla platebních karet.

Víte, kam jdete?

Dalším jasným důkazem toho, že budete přesměrováni na falešnou webovou stránku, je neodpovídající adresa **URL.**

> **URL** Lokátor uniformních zdrojů (Uniform Resource Locator). URL je slovní adresa používaná k lokalizaci specifických webových stránek na Internetu.

V případě pokusů o phishing, které vás chtějí podvodně přimět k použití falešných webových stránek, někdy zjistíte, že adresa URL uvedená v e-mailové zprávě neodpovídá skutečné URL. Falešná adresa URL často obsahuje písmena navíc, nebo slova, která nejsou součástí skutečné adresy. Tohle je dostatečný důvod k tomu, abyste ze zásady NIKDY neklikali na odkazy uvedené v nevyžádané poště.

V některých případech může adresa vypadat jako oficiální, ale nemusí být správná. Například podvod s PayPalem, o kterém jsme již v této kapitole mluvili, posílá oběti na adresu URL www.paypal-transactions.com.I když tato adresa zní věrohodně, NENÍ stejná jako www.paypal.com. Je nanejvýš pravděpodobné, že tuto pozměněnou adresu služba PayPal vůbec nevlastní.

Jinou běžnou technikou je vynechat nebo přehodit několik písmen. Tak se z adresy www.amazon.com stává www.amzaon.com nebo www.amzon.com. Tyto adresy jsou tak podobné, že lidé, kteří text čtou jen povrchně – a nečekají žádné chytáky – se skutečně nechají ošálit. Několik takových adres jste již možná viděli a ani si neuvědomili, že všechno není úplně v pořádku. Výzkum, který provedli odborníci zabývající se čtením, odhalil, že náš mozek automaticky doplní chybějící písmena a slova, aniž by si toho většina čtenářů všimla. Stejně jako mnoho jiných částí phishingu, i zde se jedná o sociální inženýrství.

Chytří kyberzločinci používají také služeb zkracování URL, aby se skryli za odkazem, který vypadá jako skutečný. Služby zkracování URL už jsou známé poměrně dlouho. Služba TinyURL zahájila činnost v roce 2002. Dnes je k dispozici více než 100 různých zkracovacích služeb. Služba zkracování URL dělá přesně to, co byste podle jejího názvu řekli. Umožňuje uživatelům zkrátit dlouhou adresu URL vytvořením krátkého hesla, v podstatě přezdívky. Když se služby zkracování URL používají počestně, je to skvělá pomoc pro všechny uživatele

s průměrnou schopností psát na klávesnici. Při nečestném používání mohou být zkrácené adresy URL použity k přesměrování uživatelů ze zdánlivě důvěryhodné nebo spolehlivé webové stránky na stránku s nesouvisejícími reklamami, nevhodným obsahem nebo malwarem. Protože se zkrácené adresy URL v internetovém podvodnictví používají stále častěji, některé aplikace automaticky rozšíří zkrácenou URL tak, abyste přesně viděli, kam míříte. Aplikace na plochu, jako je např. Tweetdeck, zobrazují okno ukazující jak zkrácenou, tak plnou adresu URL. Webová stránka Twitteru také prodlužuje zkrácené adresy URL, když přes ně přejíždíte myší, dokonce i u tweetů s vloženým JavaScriptem.

I když si zkrácenou adresu URL rozbalíte, není tak jednoduché říct, zda se jedná o škodlivou stránku. Některé webové stránky používají názvy domén určené k oklamání uživatele zahrnutím části (nebo celé) adresy URL pravé a důvěryhodné webové stránky. Například www.facebook.com.badguy.com ve skutečnosti NENÍ součástí Facebooku, ačkoli byste to podle adresy URL určitě čekali.

Lepším řešením problému škodlivých odkazů je špatné odkazy ve skutečnosti filtrovat. Přesně to začínají dělat stránky se sociálními sítěmi, protože se tolik jejich uživatelů stává terčem phisherů používajících klamné adresy URL a odkazy na škodlivé webové stránky. Služba Twitter v březnu 2010 oznámila, že bude automaticky směrovat všechny odkazy poslané na Twitteru přes službu kontrolující škodlivé adresy URL. Ostatní sociální sítě budou nade vší pochybnost následovat její příklad a lumpové si začnou hledat nové způsoby, jak na uživatele útočit.

Mezitím je dobré vědět, že si nikdy nemůžete být naprosto jisti, kam vás daná adresa URL zavede. Abyste na cestě zůstali v bezpečí, ujistěte se, že máte aktuální antivirový program a ochranu proti spywaru.

7.3 Phisheři vašich přátel

V poslední době se ve světě phishingu rozšířil fenomén útoků na stránkách sociálních sítí. Ty často začínají jako odkaz na zdi nebo aktualizace stavu obsahující odkazy, stejně jako techniky sociálního inženýrství přesvědčující uživatele ke kliknutí. Jeden z populárních podvodů z roku 2008 popsal Michael Arrington ze společnosti TechCrunch. Jednalo se o příspěvek na zdi v této podobě:

```
lol nemůžu uvěřit, že tyhle fotky zveřejnili.... až to uvidí její kluk, tak
to bude ZLÝ – http://www.facebook.com.profile.php.id.371233.cn
```

Uživatelé, kteří na tento odkaz klikli, byli přesměrováni na stránku vypadající přesně jako přihlašovací stránka na Facebook. Cílem samozřejmě bylo získat přihlašovací jména a hesla uživatelů sítě Facebook. Proč? Tak zaprvé je to jednoduché. Když získáte přihlašovací údaje jednoho uživatele, můžete tuto zprávu poslat všem jeho přátelům na síti Facebook a přitom získat přihlašovací údaje alespoň některých z nich. Pak to pošlete jejich přátelům, a tak dál. Jakmile phisher získá dostatečné množství přihlašovacích údajů na síť Facebook, může je prodat spammerovi.

V reakci na opakované phishingové útoky v roce 2009 mluvčí sítě Facebook Barry Schnitt doporučil uživatelům před přihlášením zkontrolovat, že je na liště adresy nápis www.facebook.com. Schnitt také poznamenal: „Lidé by měli být zdravě podezřívaví a sami sebe se ptát: proč mě to odhlásilo?“

7.4 Podfuk s katastrofou

Phisheři a další podvodníci často zneužívají lidské touhy pomáhat. Jennifer Perry, správní ředitel společnosti E-Victims, poznamenal: „Jakmile někde dojde ke katastrofě, jako je cholera v Zimbabwe nebo konflikt v Gaze, během několika hodin se vyrojí podvody, s jejichž pomocí se kriminálníci snaží získat peníze darované na tyto účely.“

V roce 2005 se v USA vyrojilo tolik podvodných stránek, že se FBI spojila s ministerstvem spravedlnosti a jinými skupinami a vytvořili Jednotku pro odhalování podvodů v souvislosti s hurikánem Katrina. Při zemětřesení na Haiti v roce 2007 se podvody děly na mezinárodní úrovni. Během čtyř dnů po zemětřesení bylo zaregistrováno více než 400 webových stránek souvisejících s Haiti. I když některé z nich byly opravdové, mnoho bylo vytvořeno jen proto, aby mohly shromažďovat informace o platebních kartách ochotných dárců.

Během dvou týdnů od katastrofy obdržela federální policie 170 stížností týkajících se podvodných sbírek. Podle Kevina Haleyho, ředitele střediska Symantec Security Reponse, „… kyberpodvodníci také manipulují s online hledáním, aby výsledky hledání hesel jako je „Fond na pomoc Haiti“ nebo „Dary Haiti“ směrovaly uživatele na phishingové stránky nebo stránky

nacpané malwarem“. Abyste se této konkrétní formě phishingu vyhnuli, odborníci radí nevyhledávat a jít přímo na webovou stránku důvěryhodné a dobře známé neziskové organizace. Pečlivě si zkontrolujte adresu, nepoužívejte adresy obsahující především čísla (běžná technika, kterou podvodníci používají). Mějte také na paměti, že většina legitimních neziskových organizací vlastní webové stránky s koncovkou .org nebo .com.

7.5 Nenechte se ulovit phishery

Legitimní stránky bank a elektronických podniků nikdy neposílají e-maily požadující čísla účtu, hesla, rodná čísla ani jiné osobní informace. Problém však spočívá v tom, že e-maily, ve kterých phisheři žádají o tyto informace, vypadají tak opravdově, že se mnoho lidí nechalo napálit a poskytlo phisherům to, co hledali.

Nikdy neaktualizujte ani nezadávejte číslo bankovního účtu, přihlašovací údaje, rodné číslo, přihlašovací jméno a heslo k IM zprávám, ani jiné osobní informace, ať už stránka vypadá sebevíc opravdově. Vaši rodiče si nemusí být vědomi tohoto typu podvodů, proto jim o něm řekněte, aby se nestali kořistí phisherů.

8. Bezpečné nákupy v kyberprostoru

8. Bezpečné nákupy v kyberprostoru – 143
8.1 Základy online nakupování – 144
8.1.1 Co si kupují? – 146
8.2 Potíže s nakupováním – 147
8.2.1 Sběrači dat – 148
8.2.2 Únosci – 150
8.2.3 Online podvod (Fraud) – 152
8.3 Jak nakupovat bezpečně – 155
8.3.1 Šifrování – 156
8.3.2 Secure Socket Layer (SSL) – 158
8.3.3 Digitální podpisy, certifikáty a hašování – 159
8.3.4 Bezpečnostní tokeny – 161

8. Bezpečné nákupy v kyberprostoru

Seznamte se s Frankem Wongem, 15letým klukem z Clevelandu v Ohiu, který nakupuje na Internetu. Frank zahájil své zkušenosti s online nakupováním, když použil platební kartu své matky Sally k otevření vlastního účtu Xbox 360. O několik týdnů později byla Sally ohromená, když se Frank zeptal, jestli by si nemohl na Internetu kupovat trička. V místním nákupním centru neměli ta cool trička, která Frank chtěl. Nakupování triček na Internetu Sally ušetřilo cesty do nákupního centra a byla šťastná, že si Frank kupuje svá trička, knihy a další věci online. Sally nákupní centra nesnáší.

Frank si pořád nemůže zapamatovat kód svého zámku ve školní šatně. Ale číslo Sallyiny Visa karty se naučil nazpaměť, včetně data platnosti a ověřovacího kódu! Sally není z jeho schopnosti zapamatovat si informace o její platební kartě tak nadšená, ale nakupování online miluje.

Letos nebude Sally ani zdaleka jedinou mámou (nebo tátou), kteří se vyhnou nakupování v nákupním centru díky pohodlným online nákupům. **eKomerce** se stala zásadní součástí života amerických spotřebitelů.

eKomerce Elektronická komerce (obchod). Nakupování a prodávání zboží online.

Před pouhými deseti lety se zdálo, že je online nakupování doménou špičkových profesionálů a technologické elity. Již tomu tak není. Dnes už hledají na Amazonu nebo v obchodě eToys dokonalé dárky stejně tak babičky, jako programátoři. Počet uživatelů portálu eBay se také rozrostl o velký podíl zákazníků nakupujících dovolené.

Na první pohled se online nakupování zdá jednou z mála oblastí, ve které využívání Internetu nevévodí dospívající. Na Internetu ve skutečnosti nejvíc nakupují generace, které demografové nazývají Generace X a Millennials. Generace X zahrnuje osoby narozené od roku 1965 do roku 1976, z nichž 80 % nakupuje online. Generace Millennials se skládá z lidí narozených v letech 1977 až 1990. Online nakupuje 71 % z nich. Naproti tomu online nakupuje pouze 38 % uživatelů mladších 18 let. Tedy, ne tak docela. Největším rozdílem mezi dospívajícími a jejich rodiči z generací X nebo Millennials ve skutečnosti spočívá v tom, kdo je držitelem platební karty. Dospívající nakupující online tak samozřejmě činí s platební kartou někoho jiného. Když započítáte počet dospívajících, kteří jsou příjemci zboží zakoupeného online, jež

si sami vybrali, ale objednal je za ně jejich rodič, získáte mnohem vyšší podíl zákazníků online obchodů.

Jak se stávalo online nakupování stále populárnějším, veřejnost si začala být více vědoma problematiky soukromí a bezpečnosti. Při odesílání čísla platebních karet a eŠeků jsou někteří lidé tak trochu paranoidní. eŠek je elektronickou verzí bankovního šeku. Na rozdíl od peněžní poukázky (což je kousek papíru podobný šeku, který si může za hotovost koupit kdokoli, i když nemá šekový účet), **eŠek** je spojen s konkrétním bankovním účtem, právě tak jako obyčejný šek. Prostě jen existuje pouze v elektronické podobě, ne v papírové.

eŠek Elektronická verze bankovního šeku.

Z eKomerce by lidé měli být trochu nervózní, ale v rozumných mezích. Ačkoli se spolu s eKomercí rozšířily i online podvody, online paranoia se rozšířila ještě rychleji. Měli byste být opatrní při předávání čísel platební karty vašich rodičů naprosto neznámým lidem? Samozřejmě! Je to opravdu nebezpečnější než předat platební kartu pokladní při nakupování v nákupním centru? Nemusí být.

S použitím možností placení na Internetu jsou samozřejmě spojena reálná rizika. Ale je důležité se na ně dívat ze správné perspektivy. V této kapitole se budeme zabývat skutečnými riziky online komerce a budeme otevřeně mluvit o tom, jak tato rizika minimalizovat a přitom využít zázraků a svobod, které nám přináší možnost mít všechna nákupní centra na dosah ruky píšící na klávesnici.

8.1 Základy online nakupování

Když se většině Američanů stalo dostupné širokopásmové připojení k Internetu, počet osob nakupujících online se raketově zvýšil. Kyber pondělí (pondělí se zvláštními slevami na online nákupy) se nyní v Americe stalo stejně důležitou součástí vánočního období jako Černý pátek (pátek po Díkůvzdání), a získává nad svým předchůdcem náskok. V roce 2009 se online prodeje v Kyber pondělí vyšplhaly na 887 milionů dolarů (v přepočtu přibližně 17,7 miliard korun). A kupodivu ani to nebyl rekord v online prodejích za jediný den. Tento rekord

v současné době představuje 913 milionů dolarů (v přepočtu přibližně 18,3 miliardy korun). To je prodej za téměř miliardu dolarů v jediný den!

Online zákazníky jsou dnes osoby téměř každého věku a většiny socioekonomických skupin. Samozřejmě že nejchudší nakupující se na online nákupech podílí nejméně. Pochopitelně se také podílí na mnohem menším počtu veškerých nákupů obecně. Překvapující ale je, že největší část prodeje mají na svědomí osoby ze středních vrstev, nikoli ti nejmajetnější nakupující. Netizeni citliví na cenu oceňují online nakupování nejvíce, protože používají vyhledávače a stránky srovnávající obchody, aby za svoje peníze při online nakupování dostali co nejvíce.

Rozšíření rychlejšího širokopásmového připojení mělo také na online nákupy vliv. Protože uživatelé širokopásmového připojení už nemusí dlouho čekat na načtení podrobných fotografií nebo webových stránek, představují naprostou většinu nakupujících na síti.

Rozdíly mezi pohlavím

Co se týče využívání Internetu, existuje opravdu značný genderový rozdíl (rozdíl mezi oběma pohlavími) – ale asi jiný, než byste čekali. Zdaleka nejvíce všech internetových služeb využívají starší dospívající děvčata.

Patnácti- až sedmnáctiletá děvčata online komunikují mnohem více, než jakákoli jiná skupina, zasílání IM zpráv používá 97 % z nich – zatímco u chlapců ve stejném věku je to jen 87 %. A děvčata si také zdaleka nejvíc hledají online informace o čemkoli, od středních škol po náboženství až k oblíbeným hercům.

Počet osob nakupujících online bude pravděpodobně vzrůstat. Několik studií zjistilo, že když uživatel získá s nákupem online dobrou zkušenost, pravděpodobně bude online nakupovat čím dál více. A navzdory obavám z online podvodů a krádeží identity je většinová zkušenost s online nákupy skutečně dobrá. Se svým posledním nákupem online bylo spokojeno plných 80 % nakupujících. Online obchodování je neuvěřitelně pohodlné – zejména tehdy, když vám nepřeje Matka Příroda. Když bylo východní pobřeží USA v prosinci 2009 zasaženo bouřemi, online prodeje dosáhly 4,8 miliard dolarů (v přepočtu přibližně 96 miliard korun) za jediný týden.

8.1.1 Co si kupují?

Když zmíníte online nakupování průměrnému nováčkovi, asi se dočkáte poznámky o službě eBay. I když je tento obr online aukcí stále tím nejlepším místem, kde hledat vzácné čajové šálky a sběratelské položky všeho druhu, eBay už není hlavním kohoutem na dvorku online prodejů. V roce 2010 patřily k nejžhavějším trhům nabídky za pevnou cenu, a to jak na stránkách vyhrazených pouze eKomerci, tak v online verzích tradičních obchodních řetězců.
Takže co online zákazníci kupují? Téměř všechno:

Elektroniku a počítačové zboží
Jak se dá očekávat, elektronické zboží se online prodává neuvěřitelně rychle. Přeci jen se jedná o zboží zaměřené konkrétně na online uživatele, kteří jsou technologicky nejzdatnější.

Oblečení
Když začal oděvní řetězec LL Bean and Lands' End nabízet online nákupy tradičním katalogovým zákazníkům, zahájil trend, který dosud nevykazuje žádné známky ústupu. I když tomuto trhu řetězec LL Bean and Lands' End stále dominuje, připojily se již i firmy Old Navy, Gap, Hot Topic, Forever 21, Delia's, Hollister, Pac Sun a Victoria's Secret.

Hledáte lepší nabídku?

Nákupy se snadným srovnáním jsou jednou z mnoha oblastí, kde online nákupy poráží tradiční provozovny z betonu a cihel na hlavu. Když si chcete srovnat ceny plánovaných nákupů, můžete použít některou z nejpopulárnějších stránek pro srovnání cen:

- NexTag
- PriceGrabber
- PriceRunner
- Pronto.com
- Shopping.com
- Shopzilla
- StreetPrices.com
- Yahoo Shopping

Knihy

Prodeje nových i použitých knih online také strmě vzrostly. V čele stojí server Amazon, ale v patách mu kráčí mnoho konkurentů s velkými prodeji (Barnes and Noble, Borders, Abe Books apod.). Amazon samozřejmě vykazuje astronomická čísla, která není snadné následovat. V roce 2009 se na Amazonu prodala média za více než 12 miliard dolarů (v přepočtu přibližně 240 miliard korun). Ačkoli se nejedná jen o knihy („média" zahrnují knihy, hudbu a DVD), stejně je to pěkná řádka šťastných čtenářů!

Skoro všechno ostatní

Co se týče neobvyklých předmětů v téměř jakékoli kategorii, stojí v čele trhu aukční síň eBay. Ačkoli je v populární kultuře postavení serveru eBay nafouknuto do téměř mystických rozměrů, i jeho skutečná pozice je dost obdivuhodná. Jen za poslední čtvrtletí roku 2009 se zde prodalo zboží za více než 2 miliardy dolarů (v přepočtu přibližně 40 miliard korun). Celkem si všech 90 milionů registrovaných uživatelů na serveru eBay koupilo každou vteřinu roku 2009 zboží za 2 000 dolarů (v přepočtu přibližně 40 000 korun). Ačkoli je to neuvěřitelné, byl to oproti roku 2008 propad odrážející všeobecné zpomalení ekonomiky.

Konkurentem serveru eBay se stala služba craigslist poskytující zdarma inzeráty potenciálním prodávajícím a obchodníkům.

Co se týče obvyklejších položek, nezapomeňme na americký obchodní řetězec Walmart. Online nabízí širokou škálu běžného, obvyklého zboží. V červenci 2009 navštívilo adresu Walmart.com více než třicet dva a půl milionu návštěvníků.

8.2 Potíže s nakupováním

Ačkoli 80 % osob nakupujících online je se svými nákupy spokojeno, stále je zde mnoho ostrých zatáček, kterými je třeba při navigaci komerčními kouty kyberprostoru bezpečně projet. Pro většinu uživatelů je nejdůležitější pochopit sběr dat (a vyhnout se mu) a chránit se jak před online podvody, tak před krádeží identity.

8.2.1 Sběrači dat

Sběr dat (data pharming) je jedním z rizik online nakupování, nebo i jen prohlížení stránek. Jednoduše řečeno, sběračem dat je ten, kdo na Internetu sklízí informace o jeho uživatelích a buduje si sbírky (databáze) těchto informací.

To není vždy špatná věc. Někteří z největších hráčů v online maloobchodě sbírají značné množství informací o svých zákaznících. Tito uživatelé dodržující zákon nikdy nepoužívají pojem „sběr dat". Místo toho „sledují preference". Vezměte si Amazon. Pokud na serveru Amazon nakupujete, je pravděpodobné, že toho o vás a vašich nákupních zvycích docela hodně vědí. Sledují, na co se díváte, i co kupujete. Sledují vaše koupě a dokonce tyto údaje používají k tomu, aby vám navrhli jiné položky, o které byste mohli mít zájem. Pokud si koupíte jednu knížku z nějaké série, Amazon vás informuje, když přijde na trh následující díl.

Stejně postupuje i online půjčovna filmů Netflix. Když na jejích stránkách ohodnotíte filmy, shromažďují vaše hodnocení a používají je k tomu, aby vám navrhli podobné filmy, které by se vám mohly líbit.

Toto sledování preferencí pro vás může být často výhodné. Zjistili jsme, že více než 75 % filmů, o kterých si Neflix myslel, že by se nám mohly líbit, představují filmy, které jsme už viděli, nebo

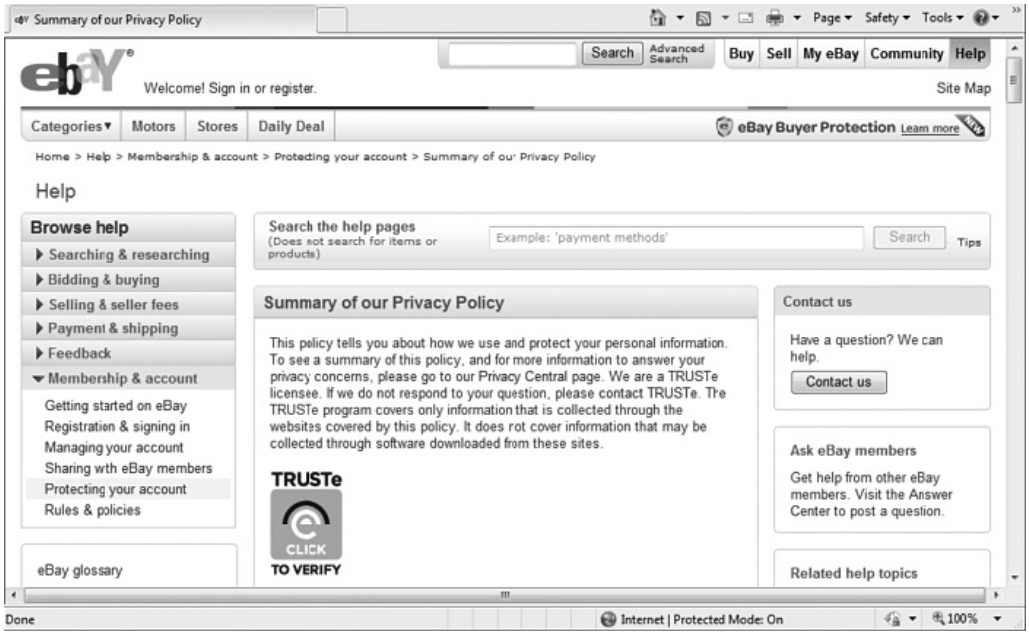
jsme jejich zhlédnutí plánovali. Stejně tak jsme si objednali alespoň tucet předmětů, které navrhoval Amazon, a byli jsme s nimi docela spokojení.

Sledování preferencí se stává problémem, když nevíte, že jsou vaše preference sledovány, nebo vám nikdo neřekne, komu se tyto údaje prodávají, či dokonce že se vůbec prodávají. Pokud jste si vědomi toho, že jsou vaše online nákupy sledovány, nezapomeňte se sami sebe zeptat: „Jak bezpečné jsou systémy sledující, co kupuji?"

Když zvažujete nějakou koupi prostřednictvím nové online stránky, je nejdůležitější zjistit, jaké jsou jejich předpisy na ochranu soukromí. Důvěryhodné stránky mají na domovské stránce (a většině dalších stránek) odkazy, které vás přesměrují přímo na předpisy na ochranu soukromí.

Odkaz na informace o ochraně soukromí společnosti Amazon se objevuje v dolní části každé stránky na serveru Amazon

Tyto předpisy vám řeknou, zda jsou informace o vás a vašich koupích prodávány. Nemyslete si, že když jsou předpisy na ochranu soukromí jasné a zřetelné, znamená to, že je vaše soukromí chráněno. Velký podíl eKomerčních stránek informace PRODÁVÁ. Prochází jim to, protože většina uživatelů se nikdy neobtěžuje přečíst si vystavené předpisy na ochranu soukromí. Nezůstávejte v nevědomosti o tom, co se s vašimi informacemi děje. Předpisy na ochranu soukromí si vždy přečtěte. Že daná stránka neposkytuje žádné předpisy na ochranu soukromí? Pak pravděpodobně neposkytuje ani žádné soukromí. Důrazně vám doporučujeme nakupovat jinde.



Předpisy na ochranu soukromí portálu eBay

8.2.2 Únosci

Na rozdíl od sběru informací, což může být někdy dobré a jindy špatné, být **unesený** není dobré nikdy. Únosce vás pošle na jinou stránku, než na kterou chcete jít. Můžete si myslet, že nakupujete na stránce eToys.com, a přitom se díváte na dobře zfalšovanou stránku a předáváte číslo platební karty svých rodičů nějakému mistrovskému podvodníkovi na Ukrajině.

> **Únos** Přesměrování uživatele z webové stránky, kterou chtěl otevřít, na jinou (často podvrženou) stránku bez jeho vědomí.

Spoofing (falšování)

Uživatele lze oklamat několika způsoby. Už víte, že podvodníci často vytvářejí podvržené verze dobře známých stránek, které do značné míry vypadají jako skutečná stránka, ale nacházejí

se na jiné internetové adrese (URL). Útočníci posílají e-mail a odkazy na falešnou stránku a doufají, že tam nic netušící uživatelé zadají své osobní a finanční informace. Už jsme o tom mluvili v ***kapitole 7, Rhybaření pro peníze.*** Tento problém je čím dál častější, protože phishingová schémata se neustále rozšiřují, ale dá se mu naštěstí snadno vyhnout. Prostě NIKDY neotvírejte stránku kliknutím na odkaz uvedený v nevyžádané poště. Namísto toho napište adresu URL, kterou znáte, do adresového řádku prohlížeče. A je po problému.

Obvykle. Někdy však problémem není phishingový e-mail, ale uživatel, který nezná správný pravopis nebo neumí pořádně psát na klávesnici. Adresu URL sám napíše, ale nenapíše ji správně. Autoři podvrhů si vybírají adresy URL, které odpovídají běžným překlepům v názvech adres komerčních webových stránek. Většina internetových bezpečnostních balíčků dnes naštěstí kontroluje tento typ přesměrování v rámci standardní ochrany před podvody. To je jeden z dalších důvodů, proč používat kvalitní balíček pro internetovou bezpečnost.

Otrávení DNS

Druhému způsobu, jakým jsou uživatelé unášeni, je těžší se vyhnout. Říká se mu **otrava DNS.** K otravě DNS dochází, když hacker prolomí váš místní DNS server. DNS server (Domain Name System, systém názvů domén) je službou překládající název domény, který napíšete, na správnou numerickou číselnou adresu. Napíšete „www.google.com" a ona vás zavede na konkrétní internetovou adresu, kde žije Google. To vám obrovsky zjednodušuje používání Internetu, protože je mnohem snazší napsat adresu URL jako www.CNN.com, než si pamatovat internetovou IP adresu 192.123.0.0.

Otrávení DNS Zneužití serveru názvu domén tak, aby uživatele převáděl na jiné stránky, aniž by o tom jejich prohlížeč věděl.

Zneužitý DNS server může uživatelům Internetu pořádně zatopit. Když je váš DNS server otrávený, můžete klidně napsat správnou adresu přesně tak, jak má být napsaná, a stejně skončíte na webové stránce nějakého podvodníka. A co je horší, váš prohlížeč bude věřit, že se nacházíte na pravé stránce. Neexistuje snadný způsob, jak poznat, že jste byli uneseni.

I když je otrava DNS naštěstí mnohem méně častá než podvrhy nebo počítačové viry, dochází k ní. Jednomu dospívajícímu z Německa se podařilo přesměrovat spojení s německou verzí stránek eBay, eBay.de. Podle policejního mluvčího Franka Federaua nebyl ten chlapec ani

žádným odborníkem na počítače. Řekl policii, že narazil na webovou stránku, která tyto podvody vysvětlovala, a řekl si, že „by to mohla být zábava". Protože byl podle německého zákona obviněn z počítačové sabotáže, můžeme jen doufat, že svou představu o zábavě změnil.

I když je ochrana před otravou DNS těžší než neklikání na nastražené e-mailové odkazy, je stále možná. Pravděpodobnost, že se stanete obětí, můžete minimalizovat tak, že budete obchodovat jen na stránkách s platným digitálním certifikátem. O certifikátech si více řekneme v další části, ale prozatím si pamatujte, že by měl certifikát odpovídat místu, kam jste se chtěli dostat.

8.2.3 Online podvod (Fraud)

K online podvodu patří nedodání zakoupeného zboží, falešné šeky a elektronické šeky, které nejsou nikdy proplaceny, falešné nabídky práce z domu, které přináší zisk pouze podvodníkovi, a nabídky „bezplatných" dárků a výher, které si může uživatel vyzvednout pouze po zaplacení poštovného nebo daní. V takových případech se výhra nikdy neukáže, nebo je její cena podstatně nižší než manipulační poplatky, které jste před jejím vyzvednutím museli zaplatit.

Existuje také celá kategorie podvodů, kterým se říká nigerijské obchodní nabídky. Jedná se o jeden z nejstarších podvodů na Internetu, který začal už v 80. letech, a zdá se, že bude pokračovat donekonečna. Každý, kdo Internet používá déle než šest či osm měsíců, už těchto nabídek určitě dostal několik. Tento podvod je TAK běžný, že Oddělení finančních zločinů americké tajné služby jednu dobu registrovalo denně téměř 100 telefonních hovorů, které se ho týkaly.

```
LAGOS, NIGERIE. K RUKÁM: PREZIDENT/CEO

VÁŽENÝ PANE,

DŮVĚRNÝ OBCHODNÍ NÁVRH

PO KONZULTACI S MÝMI KOLEGY A NA ZÁKLADĚ INFORMACÍ ZÍSKANÝCH Z NIGERIJSKÉ
OBCHODNÍ A PRŮMYSLOVÉ KOMORY MÁM TU ČEST POŽÁDAT VÁS O VAŠI ASISTENCI PŘI
PŘEVODU ČÁSTKY 47 500 000,00 USD (ČTYŘICET SEDM MILIONŮ PĚT SET TISÍC AMERIC-
KÝCH DOLARŮ) NA VAŠE ÚČTY. VÝŠE UVEDENÁ SUMA POCHÁZÍ Z NADCENĚNÉHO KONTRAKTU
```

PROVEDENÉHO, PŘEDANÉHO A ZAPLACENÉHO PŘED PĚTI (5) LETY ZAHRANIČNÍM DODAVATELEM. TATO AKCE BYLA PROVEDENA ZÁMĚRNĚ A OD TÉ DOBY JE TATO ČÁSTKA ULOŽENA NA ÚČTU V CENTRÁLNÍ BANCE NIGÉRIE, APEX BANK.

NYNÍ JSME PŘIPRAVENI TUTO ČÁSTKU PŘEVÉST DO ZAHRANIČÍ, A PROTO VÁS ŽÁDÁME O POMOC. JE DŮLEŽITÉ VÁM SDĚLIT, ŽE JAKO STÁTNÍ ZAMĚSTNANCI NEMÁME POVOLENÍ POUŽÍVAT ZAHRANIČNÍ ÚČET, PROTO ŽÁDÁME O VAŠI ASISTENCI. CELKOVÁ SUMA BUDE ROZDĚLENA TAKTO: 70 % PRO NÁS, 25 % PRO VÁS A 5 % NA MÍSTNÍ A MEZINÁRODNÍ NÁKLADY SPOJENÉ S PŘEVODEM.

PŘEVOD JE PRO OBĚ STRANY ZCELA BEZ RIZIKA. JSEM ÚČETNÍM U NIGERIJSKÉ NÁRODNÍ ROPNÉ SPOLEČNOSTI (NNPC). POKUD JE PRO VÁS TENTO NÁVRH PŘIJATELNÝ, BUDEME POTŘEBOVAT NÁSLEDUJÍCÍ DOKUMENTY:

(A) NÁZEV, TELEFON, ČÍSLO ÚČTU A ČÍSLO FAXU VAŠEHO BANKÉŘE.
(B) VAŠE SOUKROMÉ TELEFONNÍ ČÍSLO A ČÍSLO FAXU – PRO DŮVĚRNOST A SNADNOU KOMUNIKACI.
(C) VÁŠ HLAVIČKOVÝ PAPÍR S RAZÍTKEM A PODPISEM.

TEXT, KTERÝ MÁ NA HLAVIČKOVÉM PAPÍŘE BÝT, VÁM TAKÉ MŮŽEME ZASLAT SPOLEČNĚ S PODROBNÝM VYSVĚTLENÍM VŠEHO, CO OD VÁS BUDEME POTŘEBOVAT. DOKONČENÍ TÉTO OPERACE NÁM BUDE TRVAL TŘICET (30) PRACOVNÍCH DNÍ.

ODPOVĚZTE PROSÍM BEZODKLADNĚ.
S POZDRAVEM

Tradiční nigerijská obchodní nabídka

Protože je tento podvod v oběhu již tak dlouho, existují pravděpodobně stovky jeho verzí. Někteří podvodníci napíší vše do předmětu zprávy, protože předpokládají, že její obsah číst nebudete.


Delete Reply Forward Not Spam Move...

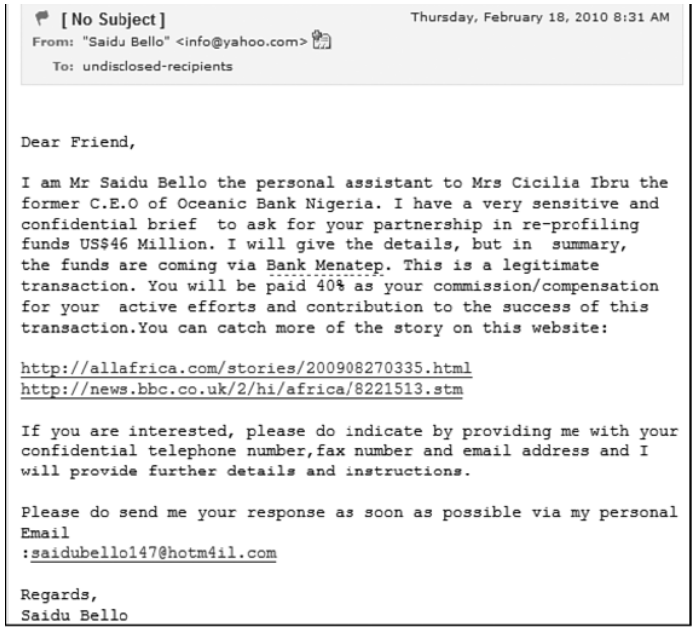
Attn: Beneficiary,This is to officially inform you that your (Atm Visa Card Number; 4539 7978 0214 3027) has been accredited in your favour. Your Personal Identification Number is 5050. The ATM Card Value is USD$8.3M and you will use the ATM card to make a withdrawal maximum of TWO THOUSAND FIVE HUNDRED DOLLARS (USD$2,500) per day with any ATM machine worldwide.You are advised to contact Rev paul the ATM CARD Director central Bank of Nigeria, Call +234-8062696500,with your following information:FULL NAME:DELIVERY ADDRESS (NOT P.O BOX)ANDCOUNTRY:PHONENUMBER:OCCUPATION/VALID I.D:SEX:AGE:Regards,Rev paul.DIRECTOR ATM CARD DEPARTMENT CENTRAL BANK OF NIGERIA.CBN.

Friday, February 19, 2010 4:21 PM

From: "REV FR PAUL JOHN" <jpmorgancustomercares@jpmorgan-chaseus.com>

To: undisclosed-recipients

Jiní začnou se stejným přístupem jako peněžní podvodníci, ale ve skutečnosti se snaží zavalit váš počítač malwarem, protože spoléhají na vaši zvědavost a na to, že zapomenete na zdravý rozum a kliknete na odkazy uvedené v e-mailu pro „další informace".


[No Subject]

Thursday, February 18, 2010 8:31 AM

From: "Saidu Bello" <info@yahoo.com>

To: undisclosed-recipients

Dear Friend,

I am Mr Saidu Bello the personal assistant to Mrs Cicilia Ibru the former C.E.O of Oceanic Bank Nigeria. I have a very sensitive and confidential brief to ask for your partnership in re-profiling funds US$46 Million. I will give the details, but in summary, the funds are coming via Bank Menatep. This is a legitimate transaction. You will be paid 40% as your commission/compensation for your active efforts and contribution to the success of this transaction.You can catch more of the story on this website:

http://allafrica.com/stories/200908270335.html
http://news.bbc.co.uk/2/hi/africa/8221513.stm

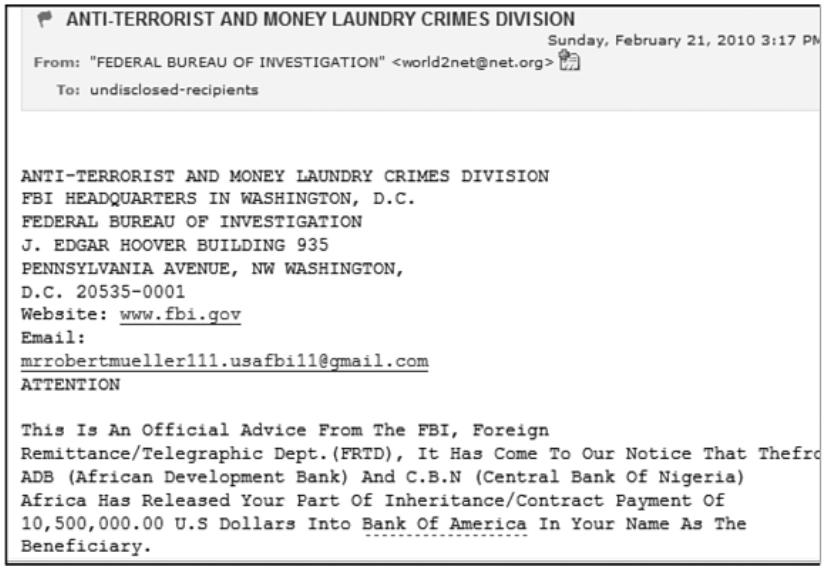
If you are interested, please do indicate by providing me with your confidential telephone number,fax number and email address and I will provide further details and instructions.

Please do send me your response as soon as possible via my personal Email
:saidubello147@hotm4il.com

Regards,
Saidu Bello

Někteří dokonce přiznají, o jak obvyklý podvod se jedná, a teprve poté v něm pokračují. To je skvělý přístup z oblasti sociálního inženýrství. Zloděj říká doslova: „Mám to ale těžké! Je hrozné být počestným obchodníkem v zemi, která je známá hlavně svými online zločinci."

Nejvíc jsme si ale oblíbili nigerijský podvod předstírající, že pochází od FBI.



ANTI-TERRORIST AND MONEY LAUNDRY CRIMES DIVISION

Sunday, February 21, 2010 3:17 PM

From: "FEDERAL BUREAU OF INVESTIGATION" <world2net@net.org>

To: undisclosed-recipients

ANTI-TERRORIST AND MONEY LAUNDRY CRIMES DIVISION
FBI HEADQUARTERS IN WASHINGTON, D.C.
FEDERAL BUREAU OF INVESTIGATION
J. EDGAR HOOVER BUILDING 935
PENNSYLVANIA AVENUE, NW WASHINGTON,
D.C. 20535-0001
Website: www.fbi.gov
Email:
mrrobertmueller111.usafbi11@gmail.com
ATTENTION

This Is An Official Advice From The FBI, Foreign
Remittance/Telegraphic Dept.(FRTD), It Has Come To Our Notice That Thefrc
ADB (African Development Bank) And C.B.N (Central Bank Of Nigeria)
Africa Has Released Your Part Of Inheritance/Contract Payment Of
10,500,000.00 U.S Dollars Into Bank Of America In Your Name As The
Beneficiary.

Jedním z nejlepších způsobů, jak si online nakupování užívat v klidu, je používat pouze služby důvěryhodných prodejců. Jako u mnoha bezpečnostních opatření se to samozřejmě snadněji řekne, než udělá. Jednoduchým prvním krokem je však nekupovat nic od spammerů. Téměř čtvrtina (24 %) internetových podvodů začíná nevyžádanou poštou.

Než kliknete na některou z těch nabídek, které znějí tak lákavě, že snad ani nemohou být pravdivé, měli byste si vzpomenout na radu Boba Krugera, viceprezidenta BSA. Poznamenává: „Na Internetu číhá hromada kyber darebáků, kteří by si rádi přivlastnili peníze nakupujících a zkazili jim tak předvánoční nákupy."

8.3 Jak nakupovat bezpečně

I když jsou internetové zpronevěry v posledních letech stále pokročilejší, vyvinula se i technologie, kterou můžete používat k ochraně integrity své online komunikace a finančních transakcí.
Obzvláště důležité jsou tři z těchto technologií: šifrování, autentizace (SSL, digitální podpisy,

digitální certifikáty) a bezpečnostní tokeny.

8.3.1 Šifrování

Šifrování je technika používaná k přeskládání obsahu souborů, u nichž nechcete, aby je četl někdo cizí. Tato ochrana je pro bezpečné online nakupování naprosto zásadní. Když nakupujete, odesíláte MNOHO informací, o kterých opravdu nechcete, aby se dostaly na veřejnost. Čísla vaší platební karty. Všechny vaše osobní informace – celé jméno, adresa, telefonní číslo (čísla) a e-mailová adresa (e-mailové adresy). Jeden nebo více způsobů šifrování jsou k ochraně všech těchto nákupních informací zásadní.

Když šifrujete soubor, aplikujete na něj „kód", takže si ho nikdo, kdo tento kód nezná, nemůže přečíst. Zpětnému uspořádání zašifrovaného souboru tak, aby byl opět čitelný, se říká dešifrování.

Šifrování si můžete představit jako použití tajného kódu. Pamatujete si na kódy, které jste používali v hodině matematiky při probírání logiky? „Rozšifrujte tajnou zprávu, jestliže A=1, B=2, C=3"? Tak přesně o to se jedná.

> **Šifrování** Aplikace tajného kódu (šifry) na zprávy nebo soubory, aby si je ostatní lidé bez vašeho svolení nemohli přečíst.

Použijme jako příklad jednoduchý kód. Řekněme, že budeme šifrovat zprávu tak, že každé písmeno nahradíme písmenem, které mu v abecedě předchází. Z každého B se stane A, z každého C se stane B a tak dál. Když se dostanete na začátek, uděláte kruh, aby se z A stalo Z. Pomocí tohoto kódu zašifrujeme následující větu:

```
Tato věta tě nemusí zajímat.
```

Když použijeme naši šifru (algoritmus předchozího písmene v abecedě), dostaneme tuto větu:

```
Szsn udsz sd mdltrh yzilzs.
```

V počítačové terminologii je první věta, ta, které snadno rozumíte, **plaintext** (obyčejný text).

To je váš text, jasný jako facka, tak, jak jste ho napsali na klávesnici. Přeházená věta pod ním je zašifrovaný text. To je váš text po použití šifry (někdy se jí říká kryptografický algoritmus). Pokud nevíte, jaká šifra byla použita, je velmi těžké zjistit, co druhá věta znamená. Takže dešifrovat zašifrovaný text je hodně obtížné.

Plaintext Obyčejná, snadno čitelná textová zpráva před zašifrováním.

Počítačové šifry jsou samozřejmě o dost složitější než jednoduchý kód, který jsme si ukázali. Většina používá alespoň 64bitové šifrování (často 128bitové). To znamená, že šifrovací klíč (druh hesla, který stanoví kryptografický algoritmus aplikovaný při šifrování textu) má alespoň 64 znaků – možná mnohem více – které musí osoba snažící se kód rozluštit sestavit do správného pořadí, aby měla jakoukoli šanci rozšifrovat vaši zprávu bez vašeho svolení.

Na poli internetové bezpečnosti se však i 64bitové šifry považují za poměrně jednoduché – vlastně skoro trapné. K vytvoření silnějších šifer se používají větší klíče. Obecně platí, že síla šifry se měří šifrovacím algoritmem a velikostí klíče. Větší klíč obvykle znamená silnější šifru.

Kryptoanalýza Snaha rozluštit zašifrovanou zprávu.

Kromě velikosti šifrovacího klíče se liší i metody šifrování. Dnes se k šifrování komunikace na Internetu používají dvě hlavní metody: symetrické šifry a šifry s veřejným klíčem. Symetrické šifry, také nazývané šifry s tajným klíčem, používají k zašifrování i dešifrování zprávy stejný klíč. U symetrického šifrování musí mít jak odesílatel, tak příjemce stejný klíč. Proto je nutné klíč udržet v tajnosti. Šifry s veřejným klíčem používají dva klíče: veřejný a soukromý. K zašifrování zprávy můžete použít kterýkoli z nich, ale k dešifrování lze použít jen jeden.

Zašifrovaný text Zpráva nebo soubor po zašifrování. Zašifrovaný text vypadá zkomoleně a bez dešifrování jej nelze přečíst.

Všechny tyto metody mají společné to, že k přeložení šifrovaného textu zpět na obyčejný text, který dává smysl, MUSÍTE mít šifru nebo klíč. Bez klíče se k obsahu nedostanete.

Jak si dokážete představit, kryptografie a umění počítačového šifrování jsou dost komplikova-

né a taky dost cool. Pokud se o nich chcete dozvědět více, doporučujeme vám ke čtení knížku Applied Cryptography (Aplikovaná kryptografie) od Bruce Schneiera.

8.3.2 Secure Socket Layer (SSL)

SSL (vrstva bezpečných socketů) je důležitou bezpečnostní vrstvou, pokud poskytujete osobní informace, jako při transakci s platební kartou. SSL je protokol, který šifruje přenášení dat přes HTTP. Že jste chráněni protokolem SSL poznáte tak, že prohlížeč v řádku adresy zobrazuje „https“ místo „http“ a v pravém dolním rohu stavového řádku prohlížeče uvidíte symbol zámku.

Běžné kódy a mrtvé krávy

Šifry – tajné kódy – jsou na síti docela obvyklé. Řeč v IM zprávách („MMT“ místo „moment“) je jedním z příkladů obvyklých online šifer.

Jiným populárním kódem je tak zvaný kód 1337 (v angličtině se na základě podobnosti písmen s čísly vyslovuje, jako by byl napsán písmeny „leet“ – čti „lít“). Je nazván podle nechvalně známého počítačového útoku skupiny hackerů, kteří si říkají „Cult of the Dead Cow“ – Kult mrtvé krávy.

Kód 1337 spočívá v tom, že jsou jednotlivá písmena ve slově psána pomocí čísel a symbolů, které fyzicky připomínají. Jednoduchým příkladem může být tato anglická věta:

```
31337 h4x0rz un j00! > Elite hackers own you! (Dostali tě elitní hackeři!)
```

Ti, kdo kódem 1337 mluví plynule (můžeme také napsat „sp33k3rz“ = „speakers“, mluvčí) používají ještě složitější záměny. Například písmena R mění na „/2“ a podobně a používají dost divoké záměny i u písmen, jako jsou M, N a W:

```
_|00 |2 4/\/ (_)83|2 |-|4><0|2! > You are an uber hacker! (Jsi super hacker!)
```

Všimněte si také, že i když mnoho komentářů psaných kódem 1337 obsahuje urážky (že by to souviselo s hráčským prostředím?), kód 1337 můžete použít i k poslání objetí a polibků, ><><><()()()><><><()()(), a dokonce i lásky, <3 !

8.3.3 Digitální podpisy, certifikáty a hašování

I když šifra chrání obsah vašich zpráv, nijak neprokazuje ani neověřuje, že osobou, která zprávu poslala, jste skutečně vy. Tomuto prokazování zdroje zprávy nebo webové stránky se říká **autentizace.**

Když nakupujete online, autentizace je dost důležitý koncept. Než předáte číslo platební karty svých rodičů serveru iTunes, abyste si mohli stáhnout nejnovější album své oblíbené skupiny, měli byste si být jisti, že skutečně mluvíte se serverem iTunes. V takovém případě, i když pořád trváte na tom, aby bylo číslo platební karty zašifrované, si chcete a musíte být také jisti, že je příjemce autentizovaný, to znamená ověřený.

Autentizace Ověření identity odesílatele zprávy nebo webové stránky.

K autentizaci se používají tři obvyklé metody: hašování, digitální podpisy a digitální certifikáty.

Hašování

Hašování (anglicky „hashing"), nejčastěji jednosměrné hašování, je metoda používaná k ověření dat, nikoli k jejich šifrování. Tato metoda na obyčejný text použije jednosměrný hašovací algoritmus. Výsledkem je „souhrn zprávy" připojený k původnímu obyčejnému textu zprávy. Tento souhrn funguje jako unikátní, identifikovatelný „otisk prstu" příslušné zprávy. Pokud bude zpráva jakkoli změněna, aplikací jednosměrného algoritmu vznikne „otisk prstu", který již nebude odpovídat připojenému souhrnu. Tento proces umožňuje příjemci zprávy porovnat přijatý text obyčejné zprávy se souhrnem zprávy a tak zjistit, zda se souborem nikdo nemanipuloval.

Kdo co poskytuje?

Důvěryhodní obchodníci vědí, že máte obavy z možné zpronevěry. Proto poskytují digitální podpisy a certifikáty, aby dokázali, že jsou skutečně tím, za koho se vydávají. Vy se jen podíváte, co dodavatel pro ochranu vašich dat dělá. UDĚLAT nemusíte nic.

Digitální podpisy

Digitální podpis je jiný způsob používaný k ověření odesílatele zprávy. Na rozdíl od hašování používají digitální podpisy šifrování – konkrétně typ šifry s veřejným klíčem, která používá dva algoritmy, jeden pro zašifrování a druhý pro dešifrování digitálního podpisu.

Jednoduše řečeno, digitální podpis je připojen k zašifrovaným datům ze dvou důvodů: (1) aby bylo zajištěno, že je zpráva autentická a nedotčená a (2) kvůli autentizaci odesílatele zprávy. Používání digitálního podpisu má stejný účinek, jako používání hašování společně s šifrováním. Jen se to prostě udělá trochu jinou metodou.

Digitální certifikáty

Digitální certifikát v porovnání s digitálním podpisem podstatným způsobem zvyšuje úroveň bezpečnosti, a to přidáním důvěryhodné třetí strany. Když něco kupujete přes Internet, například na stránkách Amazon.com, používáte infrastrukturu veřejného klíče. Problém používání pouze šifry s veřejným klíčem v tomto případě spočívá v tom, že pár soukromého a veřejného klíče může vytvořit kdokoli. Je to trochu složitější, ale v podstatě jde o to, že digitální podpis je možné zfalšovat. Podpis sám o sobě by stále odpovídal (kombinace veřejného/soukromého klíče by fungovala), ale autorem podpisu by mohl být někdo jiný, než si myslíte.

Aby nedocházelo k problémům s falšovanými digitálními podpisy, obchodníci na Internetu místo toho používají digitální certifikáty. Digitální certifikát obsahuje veřejný klíč dané osoby nebo příslušného podniku. Přesně jako u digitálního podpisu. Rozdíl je v tom, že digitální certifikát vydává důvěryhodná třetí strana, která nezávisle ověřuje, že certifikát náleží osobě, která se k jeho vlastnictví hlásí.

Digitální certifikát si můžete představit podobně jako občanský průkaz. Když žádáte o občanský průkaz, musíte ministerstvu vnitra nějakým způsobem dokázat, že jste to právě vy. Společnosti, které vydávají digitální certifikáty, jako například VeriSign, fungují jako ministerstvo a získávají přiměřenou identifikaci. Certifikační úřad VeriSign poté vydá pár veřejného/soukromého klíče (za nízký poplatek), uchovává odpovídající veřejný klíč v databázi, vydává digitální certifikát a přechovává kopii certifikátu ve své databázi.

8.3.4 Bezpečnostní tokeny

Šifrování chrání obsah vaší zprávy a souborů. Hašování, digitální podpisy a digitální certifikáty ověřují osoby a místa, se kterými obchodujete. **Bezpečnostní tokeny** ověřují VÁS.

Možná si říkáte: „Ale to dělám sám, když zadávám heslo." To je pravda. Problém je v tom, že hackeři mohou hesla snadno prolomit a ukrást. Bezpečnostní tokeny poskytují mnohem silnější dvoufaktorovou autentizaci, která zahrnuje jak data (často heslo), tak fyzické zařízení. Dvoufaktorová autentizace je něco, co už ve světě offline dávno používáte. Když v bankomatu vybíráte peníze ze svého účtu, používáte dvoufaktorovou autentizaci. Ověřuje vás fyzická platební karta (faktor jedna), stejně jako číslo PIN, které zadáváte (faktor dvě). I když je důležité neztratit ani jedno, jedno bez druhého jsou vám k ničemu. Zločinec si může s vaší platební kartou hrát celý den, ale pokud nezná PIN, k penězům ve vaší bance se z bankomatu nedostane.

Bezpečnostní token Metoda dvoufaktorové autentizace používající fyzické zařízení, stejně jako tajný kód.

Platební karta je pouze jedním příkladem bezpečnostního tokenu. Jinými formami bezpečnostních tokenů jsou fyzické tokeny (malá hardwarové zařízení), chytré karty a biometrické systémy. V biometrice představují fyzickou složku data, jako je otisk prstu nebo snímek rohovky.

9. Prohlížeč přeje připraveným

9. Prohlížeč přeje připraveným – 165

9.1 Aby soubory cookies pracovaly PRO vás – 165

9.1.1 Škodí mi soubory cookies? – 166

9.1.2 A co když nechci sdílet? – 168

9.1.3 Sbírání drobků – 169

9.2 Výběr prohlížeče – 169

9.3 Rozhodnutí pro Internet Explorer – 170

9.3.1 Mazání seznamu v panelu adresy – 171

9.3.2 Čištění dočasných souborů, historie Internetu a souborů cookie – 172

9.3.3 Nastavení způsobu zacházení se soubory cookies – 173

9.3.4 Uchovávání citlivých dat – 174

9.3.5 Používání procházení a filtrování InPrivate – 175

9.3.6 Provádění antiphishingových kontrol – 176

9.4 Rozhodnutí pro Firefox – 176

9.4.1 Detekce zastaralých funkcí plug-in – 178

9.4.2 Vypnutí pokročilých možností JavaScriptu – 178

9.4.3 Vypnutí Javy – 181

9.4.4 Používání hlavního hesla – 181

9.4.5 Funkce add-on pro Firefox, které usnadňují život – 183

9.5 Rozhodnutí pro Google Chrome – 185

9.6 Pochopení problému s funkcemi plug-in – 186

9. Prohlížeč přeje připraveným

Mike trávil na Internetu hodně času prohlížením stránek o počítačových hrách. Přesto ho zaskočilo, když navštívil jednu starou herní stránku, na které už pět nebo šest měsíců nebyl. Jen se ke stránce připojil, aniž by se přihlásil nebo zadal jakékoli informace, přivítali ho jako starého přítele:

Vítej zpět, Miku z Bendersville!

I když jejich cílem bylo vtáhnout Mika zpět do hry, ve skutečnosti ho vyděsili. Mike chtěl vědět, jak přesně herní stránka věděla, **kdo** vlastně je. Začalo ho zajímat, jestli se nestal obětí spywaru, o kterém už toho hodně slyšel...

I když je možné, že se Mike obětí spywaru stal, zdroj těch podrobností, které ho vyděsily, byl pravděpodobně uložen v jeho vlastním počítači, pěkně na dohled ve složce se soubory cookies. Když umožníte, aby soubory cookies sledovaly vaše aktivity, dáváte tím svému internetovému prohlížeči jen jednu z možností, jak vám může znepříjemnit život.

V této kapitole se dozvíte, co soubory cookies dělají, a jak je držet na uzdě, aby pracovaly pouze PRO vás, nikoli proti vám. Také se dozvíte o možnostech prohlížeče a o tom, jak je nastavit, abyste zvýšili své bezpečí a soukromí. Nakonec budeme mluvit o tom, proč někteří lidé volí alternativní prohlížeče, jako jsou Firefox nebo Google Chrome. A proč je zapotřebí záplatovat prohlížeč a být opatrný s funkcemi plug-in, ať už používáte jakýkoli prohlížeč!

9.1 Aby soubory cookies pracovaly PRO vás

Navzdory obecné představě nejsou soubory cookies programem. Samy o sobě nedělají NIC. Je to jen informace, kterou váš prohlížeč přijme, když navštívíte webovou stránku, jež vás a váš systém identifikuje. Cookies na vašem počítači přistávají téměř nepřetržitě, když surfujete Internetem. Tyto soubory cookies se poté předávají zpět webovým stránkám, které navštěvujete opakovaně. Webové stránky vaše soubory cookies používají k získání podrobností o vašich předchozích návštěvách, aby zjistily, zda jste momentálně ke stránce přihlášeni, ke změně některých vlastností stránky, k poskytnutí dalších funkcí stránky nebo k záznamu podrobných údajů o vaší návštěvě.

Příjem souborů cookies je nedílnou součástí používání většiny webových stránek. Některé webové stránky nebudou správně fungovat, když nepřijmete soubory cookies, které používají.

Cookie Informace, kterou navštívená webová stránka zapíše na váš pevný disk. Webová stránka může soubory cookies používat k tomu, aby vás poznala, když stránku v budoucnu znovu navštívíte.

Obecně řečeno, cookie je malá informace sestávající z jedné položky – páru název/hodnota. Ve většině případů je „název" shlukem názvu webové stránky a ID uživatele, které jste si vybrali (nebo vám bylo přiděleno) pro navštěvovanou stránku. „Hodnota" je jedinečná číselná hodnota, kterou stránka tomuto názvu přidělila. Společně vás tento pár název/hodnota jednoznačně identifikuje pokaždé, když webovou stránku ze stejného počítače navštívíte.

```
NSC_mc_xxx-nbjo_80441327223660us.myspace.com/153637783381763004734420362481763004734 4*
```

Obsah souborů cookies na stránkách MySpace

Jak vidíte, ze souborů cookies se toho zase tak moc nedozvíte. Je však velmi důležité o nich vědět.

Jedním z běžných omylů panujících o dnešním Internetu je, že když navštívíte webovou stránku, váš webový prohlížeč komunikuje pouze s jednou webovou stránku nebo jedním počítačem. Tak tomu vždy není. Ve většině případů se komunikace účastní více stránek a počítačů, z nichž každý poskytuje malou část webové stránky, kterou vidíte. To znamená, že soubory cookies lze nahrát nebo sdílet z mnoha jiných webových stránek jen tím, že otevřete jednu stránku.

9.1.1 Škodí mi soubory cookies?

Někdy soubory cookies stránce dovolují, aby si pamatovala vaše uživatelské nastavení. V opačném případě byste si každou stránku museli uživatelsky nastavovat pokaždé, když ji navštívíte. To by nebylo moc praktické. Soubory cookies také umožňují nastavení praktických

možností, jako je nákup a zaplacení jedním kliknutím na komerčních stránkách. A dovolují stránkám, aby si vás pamatovaly, takže nemusíte při každé návštěvě zadávat uživatelské jméno a heslo.

Ale tak jako čarodějové, ani soubory cookies nejsou vždy dobré. Stránky vás díky nim mohou sledovat. Mohou zaznamenávat, jak často je navštěvujete, a které části jejich stránek používáte. Riziko, že budete kvůli souborům cookies a jejich zlým bratrancům zvaným web bugy jako pod dohledem „Velkého bratra" je mnoha uživatelům webů nepříjemné.

Zda byste měli mít z konkrétního souboru cookie obavy obecně závisí na tom, jestli se jedná o primární soubor, nebo soubor cookie třetí strany.

Primární cookies

Primární soubor cookie, někdy také nazývaný cookie první strany, je ten, který do vašeho prohlížeče uloží navštívená webová stránka. Pokud jste navštívili stránku MySpace.com a na pevném disku vám přistál soubor cookie MySpace, je MySpace primární webovou stránkou. To asi nikoho nepřekvapí. Často je žádoucí, aby si primární webová stránka soubor cookie uložila a tak vám umožnila ji co nejlépe využít.

Cookies třetí strany

Soubory cookies třetí strany na váš počítač umisťují webové stránky, které jste ani nenavštívili, nebo si toho nejste vědomi. Už jsme se zmínili o souborech web bug, které jsou také někdy nazývány web beacon nebo transparentní GIF. Web bug je grafika, která tvoří součást webové stránky, a je příliš malá na to, abyste ji viděli. Když webovou stránku navštívíte, „neviditelná" grafika se stahuje z jiné webové stránky. Tato „jiná" webová stránka se nazývá stránka třetí strany, protože to není primární (první) stránka, kterou jste navštívili, ani to nejste vy (druhá strana). Proto se jedná o třetí stranu.

Soubor cookie třetí strany **Soubor cookie, který na váš počítač ukládá stránka, již jste ve skutečnosti NENAVŠTÍVILI.**

Technicky má zobrazování webové stránky, která obsahuje soubor web bug stažený ze stránky třetí strany, stejný účinek, jako kdybyste stránku třetí strany otevřeli ve svém prohlížeči. Veškeré soubory cookies, které by tato třetí stránka poslala, na vašem počítači i tak přistanou.

Pomocí této neviditelné grafiky mohou inzerenti a sběrači dat (lidé sbírající na Internetu informace o jeho uživatelích) umístit soubory cookies na váš počítač, aniž byste si uvědomili, že jste jejich webové stránky vůbec navštívili. Když jsou tyto soubory cookie třetí strany spojeny se soubory web bug posílanými e-mailem, mohou sběrači dat spojit vaši e-mailovou adresu se všemi podrobnostmi uloženými v souboru cookie. Když sběrači dat prohlédnou dostatek souborů cookies a k tomu e-mailovou adresu, budou zanedlouho schopni identifikovat nejen soubor cookie, ale přímo VÁS.

Sběrač dat Osoba, která si na Internetu vytváří narůstající sbírku (databázi) informací o uživatelích Internetu.

9.1.2 A co když nechci sdílet?

Pokud máte obavy ze souborů cookies, které se nahromadily na vašem pevném disku, můžete je kdykoli smazat. Tak vás inzerenti nebudou moci sledovat. Mnoho uživatelů webu tato myšlenka uklidňuje. Samozřejmě pokud smažete soubory cookies, možná si budete muset znovu nastavit mnoho webových stránek, které navštěvujete.

Soubory cookies obvykle neobsahují osobní informace, které by vás mohly identifikovat. To však neznamená, že si společnost, která tento soubor cookie uložila, o vás nezaložila databázový soubor, který vaše osobní informace obsahuje. Protože znají váš soubor cookie a používají ho k vaší identifikaci, když jejich stránku navštívíte, mohli by si tento soubor snadno uložit společně s údaji ve své databázi. Tak soubory cookies mohou být, a často také jsou, používány při sběru dat ke shromažďování dost podrobných informacích o tom, kdo jste a co online děláte.

Když navštívíte online jakoukoli stránku, její **Předpisy na ochranu soukromí** by vám měly říct, zda a jak tato stránka sbírá a sdílí informace o vás. Většina lidí bohužel tyto předpisy nečte.

Předpisy na ochranu soukromí Oficiální předpisy komerční webové stránky, které vám říkají, jaké (pokud vůbec nějaké) informace se o vás sbírají a co stránka s těmito informacemi dělá.

Existuje několik jednoduchých kroků, kterými můžete kontrolovat, jak se na vašem počítači

mohou soubory cookies nastavovat. Teoreticky můžete soubory cookies i úplně zablokovat. Pokud všechny zablokujete, mnoho internetových stránek asi nebudete moci vůbec používat. Pokud se například rozhodnete zablokovat všechny soubory cookies, nebude vůbec fungovat e-mailová schránka na serveru Yahoo!.

Také si pamatujte, že mnohé soubory cookies jsou vlastně užitečné. Poskytují webovým stránkám, které navštěvujete nejčastěji, větší bohatost a více funkcí. Takže všechny soubory cookies byste blokovat neměli, určitě ne všechny cookies první strany. Důležité je najít rozumný kompromis.

9.1.3 Sbírání drobků

Tak jako jsou skutečné cookies (anglicky „sušenky“) dobré pro chuťové buňky, ale ne pro postavu, elektronické cookies mohou být také dobré i špatné. Na první pohled je těžké vidět špatnou stránku elektronické zkratky, která vám umožňuje nastavit si velmi snadno způsob, jakým surfujete. To nejlepší, co se o souborech cookies dá říct, je, že šetří čas a díky nim je surfování pohodlnější, praktičtější a účinnější.

Zároveň jsou však soubory cookies hrozbou, protože sbírají informace o tom, co na síti děláte. Jako mnoho informací sbíraných bez vašeho přímého souhlasu, i tyto představují ohrožení vašeho soukromí.

Soubory cookies mohou také ohrožovat vaši identitu a osobní informace. I když soubory cookies jako takové neukládají hesla ani osobní informace, identifikují váš počítač webovým stránkám, na kterých jste možná tyto osobní údaje zadali. Pomocí souborů cookies spojených se soubory web bug mohou zkušení sběrači dat tyto kousky informací slepit dohromady – e-mailová adresa, osobní informace zadané online, zvyky při surfování Internetem. Soubor cookie sám o sobě nemůže obsahovat žádné citlivé údaje, ale je to mapa, která pro sběrače dat kousky informací spojuje dohromady.

9.2 Výběr prohlížeče

Jestli hledáte jasné doporučení o tom, který prohlížeč je pro vás nejbezpečnější, hledáte na špatném místě. Pravdou je, že většina hlavních prohlížečů má svoje výhody i nevýhody. Jeden

den mají všichni rádi Internet Explorer, protože u Firefoxu byla zjištěna bezpečnostní rizika. Další den všichni zase milují Firefox kvůli bezpečnostním rizikům nalezeným v prohlížeči Internet Explorer.

Pro většinu lidí není výběr prohlížeče velkým problémem. Používají ten, kterým byl jejich počítač z výroby vybaven, a moc o tom nepřemýšlejí. Samozřejmě že nejpoužívanějším prohlížečem je vždy ten, který se dodává nahraný na nových počítačích. V současnosti je to Internet Explorer dodávaný s počítači vybavenými systémem Windows. Někteří lidé si ani neuvědomují, že jsou i jiné možnosti.

I když většina lidí ví, že mají další možnosti, každý prohlížeč, který je nutné stáhnout a nainstalovat, je ve velké nevýhodě. To se týká všech důležitých alternativ, jako je Firefox, i méně známých prohlížečů, jako jsou Google Chrome, Opera, OmniWeb a Safari pro systém Windows.

Pokud jste spokojeni s prohlížečem, který máte, nebo jen nehodláte trávit čas učením se, jak nový prohlížeč používat, měli byste vědět, že většina lidí je na tom stejně. Prostě jen s čistým svědomím přeskočte na další část.

Pokud se svým současným prohlížečem spokojeni nejste, to je také v pořádku. I když většina uživatelů používá Internet Explorer, respektovaná menšina uvědomělých uživatelů dává rozhodně přednost prohlížeči Firefox. Firefox je bezplatný webový prohlížeč, který vyrábí společnost Mozilla. Je alternativou webových prohlížečů zahrnutých v operačních systémech, jako je Windows Internet Explorer nebo Safari 4 pro Mac OS X. Firefox je druhým nejoblíbenějším webovým prohlížečem (po prohlížeči Internet Explorer). Existují také další nezávislé webové prohlížeče, jako Opera nebo Google Chrome.

Bez ohledu na to, jaký prohlížeč si nakonec vyberete, mějte na paměti, že žádný z nich není úplně bezpečný. Vždy ho musíte pravidelně aktualizovat a ujistit se, že jsou rychle zazáplatovány všechny bezpečnostní díry, které se objeví.

9.3 Rozhodnutí pro Internet Explorer

Kdykoli dostanete nový počítač, kromě instalace antivirového programu a aplikace záplat

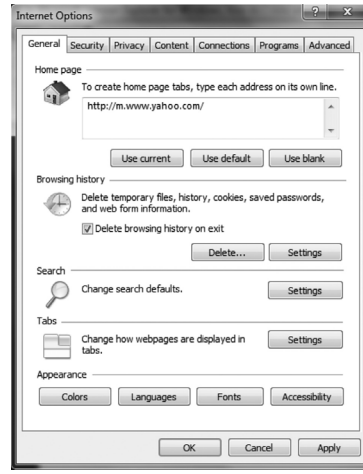
musíte vybrat nastavení soukromí. V ideálním případě byste tohle všechno měli udělat, než počítač vůbec začnete používat online. Pokud se rozhodnete používat jako webový prohlížeč Internet Explorer, měli byste si také rozmyslet, jaké možnosti chcete nastavit.

Systém Windows 7 a prohlížeč Internet Explorer se chovají trochu jako matka kvočna, co se týče sledování toho, co děláte online i offline. Sledují všechny webové stránky, které navštěvujete, které aplikace spouštíte, jaké soubory otevíráte a podobně. Proč? Protože mají tyto informace používat k tomu, aby upravili používání počítače na míru vašim zvyklostem. A také to dělají. Tyto informace však mohou být použity k tomu, aby komukoli, kdo se vám dostane do systému, ukázaly, co děláte. Kvůli tomu by mohlo být dobré využít výhod několika nových bezpečnostních prvků a nastavení.

9.3.1 Mazání seznamu v panelu adresy

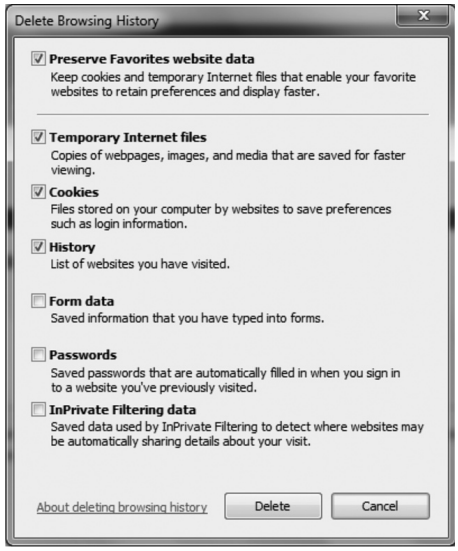
Mnoho adres webových stránek (URL) je dlouhých, komplikovaných a je těžké je napsat. Na vlastním počítači je hezké, když si Internet Explorer pamatuje, kde jste byli. Napíšete jen prvních pár písmen a Internet Explorer zbytek doplní za vás.

Na veřejném sdíleném počítači možná nechcete nechat záznam o každé stránce, kterou jste navštívili. Dokonce i na sdíleném rodinném počítači možná nechcete nechat úplný seznam. Pokud chcete Internet Explorer nastavit tak, aby si všechny stránky nepamatoval, zvolte možnosti **Nástroje > Možnosti Internetu > Obecné.** Můžete Internet Explorer požádat, aby smazal historii prohlížení pokaždé, když prohlížeč zavřete.



9.3.2 Čištění dočasných souborů, historie Internetu a souborů cookie

I když můžete historii prohlížení smazat vždy při zavírání prohlížeče, můžete také jedním šmahem smazat VŠECHNY dočasné soubory, které se o vás vytvořily. Jen klikněte na volby **Zabezpečení > Odstranit historii procházení.** Nabídnou se vám snadné možnosti, jak smazat mnohem více než jen adresový řádek:



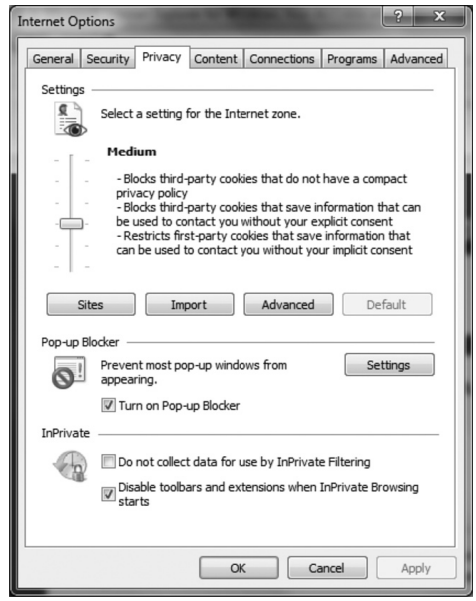
Tuhle možnost je výborné čas od času použít. Proč? Dočasné soubory se vytvářejí, když navštěvujete stránky a stahujete obrázky. Časem může adresář, který uchovává dočasné internetové soubory, zabírat zbytečně mnoho místa. Může také poskytovat jasný obrázek o tom, co jste online dělali – stejně jasný, jako prohlížení vaší historie. Výchozím nastavením prohlížeče Internet Explorer je ponechat si tyto dočasné informace 20 dní. Díky této možnosti můžete smazání urychlit.

Jednou z příjemných vlastností, které byly přidány do prohlížeče Internet Explorer 8, je možnost zahodit dočasné soubory, ale PONECHAT si oblíbené položky. To vám umožňuje zbavit se odpadu bez toho, abyste znovu říkali webové stránce s TV průvodcem, zda máte kabel nebo satelit, nebo zadáním PSČ znovu informovali oblíbenou stránku s předpovědí počasí o tom, kde žijete. Tato funkce může také zahodit formulářová data, která jste zadávali online, ale ponechat hesla k oblíbeným stránkám, u kterých jste prohlížeč Internet Explorer požáda-

li o zapamatování. To je celkově velmi příjemný kompromis mezi pohodlím a bezpečností. A to je přesně to, co z dlouhodobého hlediska hledáme.

9.3.3 Nastavení způsobu zacházení se soubory cookies

Když už zahazujete dočasné soubory a čistíte historii prohlížení, můžete zároveň na míru nastavit způsob, jakým váš prohlížeč zachází se soubory cookies. Momentálně používané nastavení najdete pod volbami **Nástroje > Možnosti Internetu > Osobní údaje.**



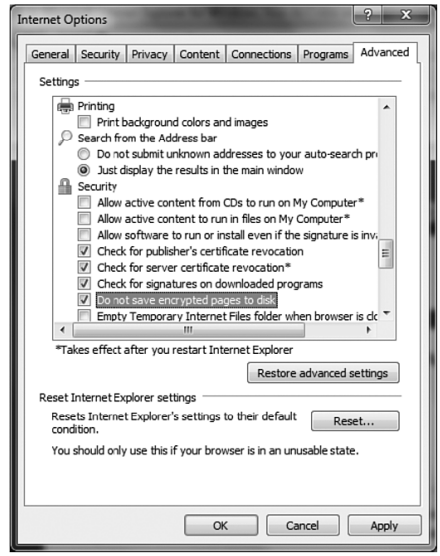
Výchozím nastavením vašeho soukromí je **Střední.** Pokud tuto možnost chcete nastavit přesně tak, aby blokovala soubory cookies třetích stran, a přitom umožňovala soubory cookie prvních stran, klikněte na tlačítko **Upřesnit.**

9.3.4 Uchovávání citlivých dat

Někdy, například když nakupujete online, musíte chránit data, která odesíláte přes Internet. Abyste mohli data bezpečně odeslat, musíte používat bezpečné připojení. V bezpečném připojení se vaše údaje při cestování Internetem šifrují. Čísla platebních karet, čísla účtů a další citlivé údaje jsou tak zakódovány, takže je nemůže přečíst nikdo kromě webové stránky, které je posíláte.

Pokud jste si přečetli ***kapitolu 8, Bezpečné nákupy v kyberprostoru,*** už víte o šifrování. Už jste možná dokonce uhodli, že zašifrovaná data jsou při příjmu prohlížečem dešifrována, aby je mohl prohlížeč zobrazit. Co jste asi neuhodli je, že některá rozšifrovaná data se ukládají ve vašich dočasných internetových souborech. To znamená, že pokud stáhnete bankovního trojského koně na počítač, který vaše máma používá k online bankovnictví, může tento trojský kůň získat přístup k podrobnostem bankovního účtu vaší mámy proskenováním dočasných souborů. To je také jeden z několika důvodů, proč byste měli být hodně opatrní při přístupu na bezpečné finanční stránky z veřejných počítačů v internetových kavárnách.

Abyste se vyhnuli riziku, že se budou vaše důvěrné údaje válet ve složce s dočasnými soubory, můžete dát prohlížeči Internet Explorer pokyn zašifrované stránky neukládat. Klikněte na možnosti **Nástroje > Možnosti Internetu > Upřesnit.** Seznam možností je dost dlouhý, takže srolujte dolů na část **Bezpečnost** a zaškrtněte políčko vedle volby **Neukládat šifrované stránky na disk.**



9.3.5 Používání procházení a filtrování InPrivate

Většina nastavení, na která jsme se zatím podívali, spočívá v požádání prohlížeče Internet Explorer, aby smazal informace, které si o vás ukládá. U funkcí InPrivate požádáte Internet Explorer, aby si tyto informace vůbec neukládal. Pokud chcete Internet Explorer požádat o to, aby nepřijímal soubory cookies, nezaznamenával historii procházení nebo nevytvářel dočasné internetové soubory, klikněte na volby **Zabezpečení > Procházení se službou InPrivate.**

9.3.6 Provádění antiphishingových kontrol

Phishingové filtry v prohlížeči Internet Explorer 8 vám umožňují vyhnout se online podvodům. Když zapnete filtr SmartScreen, Internet Explorer srovnává všechny odkazy s databází známých phishingových a malwarových stránek. A co je nejdůležitější, tuto kontrolu provede před tím, než stránku otevře.

Pokud chcete zapnout filtr SmartScreen v prohlížeči Internet Explorer, klikněte na volby **Zabezpečení > Filtr SmartScreen > Zapnout filtr SmartScreen.**

9.4 Rozhodnutí pro Firefox

Společnost Mozilla svůj prohlížeč poskytuje zdarma na své webové stránce (getfirefox.com). Nejen že je Firefox zdarma, ale volně je k dispozici také jeho zdrojový kód. To je pro programátory a aspirující programátory úžasná věc.

Kvůli volně dostupnému zdrojovému kódu programátoři Firefox opravdu milují. Nejen že se můžete na kód podívat, abyste viděli, co přesně dělá, ale můžete také přidávat své vlastní funkce. Pokud chcete, můžete tyto funkce sdílet s ostatními uživateli. Těmto funkcím přidaným na základní prohlížeč se říká „add-on“. Pro prohlížeč Firefox je k dispozici značné množství funkcí add-on.

Některé z nich mírně upravují způsob, jak prohlížeč Firefox funguje (například přidají do spouštění nabídky možnost „Restartovat Firefox"). Jiné funkce add-on poskytují kompletní aplikační funkci včetně celé sady nástrojů pro webové developery.

Jinou výhodou prohlížeče Firefox je to, že funguje na všech hlavních operačních systémech. K těm patří systémy Windows, Mac OS X a Linux. V současné době se dokonce vyvíjí verze pro mobilní zařízení, jako jsou chytré telefony. Prohlížeč Firefox je také rychlý a ještě se zrychluje. Dosud byla každá vydaná verze prohlížeče Firefox výkonnější než ta předchozí.

Stejně jako Internet Explorer, i prohlížeč Firefox má mnoho standardních bezpečnostních nastavení. V prohlížečích Internet Explorer i Firefox můžete:

• Blokovat vyskakovací okna (což jsou obvykle reklamy).

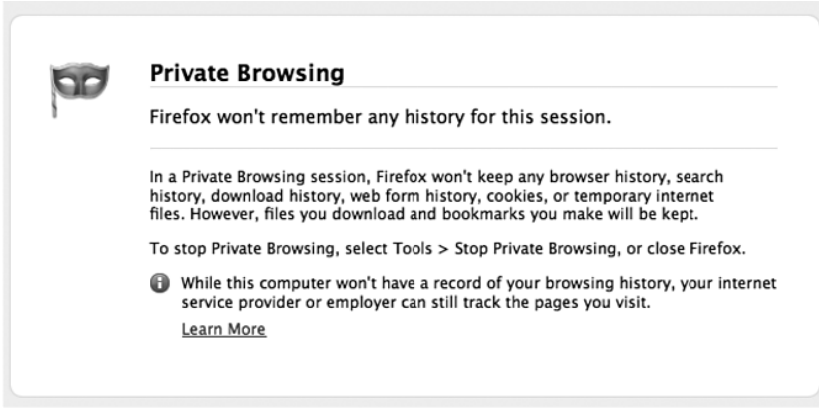
• Procházet weby anonymně (v prohlížeči Firefox se tomu říká „Anonymní prohlížení", v prohlížeči Internet Explorer „služba InPrivate". Chcete-li Anonymní prohlížení aktivovat, zvolte možnosti **Nástroje > Spustit anonymní prohlížení.**).

• Nastavit pravidla zacházení se soubory cookies (pokud chcete, můžete zakázat soubory cookies třetí strany).

• Smazat všechny dočasné soubory při zavírání prohlížeče.

• Provádět antiphishingové kontroly, nechat prohlížeč, aby webové stránky porovnával s databází známých phishingových stránek.

• Provádět každodenní kontroly aktualizací jádrového programu prohlížeče a funkcí add-on, které jste si instalovali. Firefox může také stahovat a instalovat aktualizace webového prohlížeče automaticky, podobně jako se instalují aktualizace systému Windows.



Prohlížeč Firefox také poskytuje další funkce usnadňující prohlížení webových stránek.

9.4.1 Detekce zastaralých funkcí plug-in

Starší funkce plug-in mohou mít softwarové zranitelnosti, které mohou váš počítač a data vystavovat rizikům. I když jsou aktualizace prohlížeče automatické, často je obtížné říct, kdy už je funkce plug-in zastaralá. Společnost Mozilla v současné době poskytuje webovou stránku sledující aktuální (nové) verze důležitých funkcí plug-in prohlížeče Firefox. V příštích verzích prohlížeče Firefox se plánuje tyto funkce automatizovat.

9.4.2 Vypnutí pokročilých možností JavaScriptu

JavaScript je jednoduchý, programovací jazyk orientovaný na objekty, který tvůrci webových stránek používají k vyladění svých stránek. Protože se JavaScript snadno používá, je hojně používaný k poskytování sofistikovaných zvukových, video a vizuálních efektů. Naneštěstí má JavaScript mnoho bezpečnostních problémů. I když je většina z nich pouze otravná, díky jiným mohou bezskrupulózní programátoři použít nedostatky JavaScriptu k ukradení vašich citlivých informací.

Add-on nebo plug-in?

Zajímá vás rozdíl mezi funkcemi add-on a plug-in?

Obě prohlížeči umožňují dělat to, co by sám nemohl. Rozdíl je v tom, že funkce plug-in je samostatným programem.

Add-on nikoli. Funkce add-on pouze přidává (anglicky „add") prohlížeči další funkce, ale v jiném prostředí by sama o sobě nefungovala.

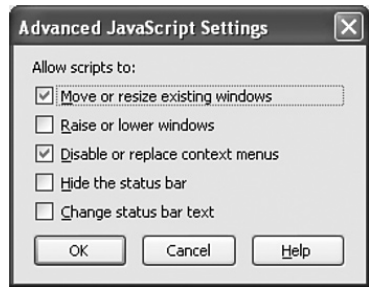
Funkce plug-in (jako např. Flash) pracuje sama NEBO s prohlížečem. Například Adobe Flash umožňuje sledovat animace ve videohrách offline stejně jako na webové stránce pomocí prohlížeče. Proto je to funkce plug-in, nikoliv add-on.

Ve výchozím nastavení má prohlížeč Firefox JavaScript povolený, dokonce podporuje i většinu jeho pokročilých vlastností. Teoreticky můžete Firefox nastavit tak, aby JavaScript úplně vypnul. Stejně jako u vypnutí souborů cookies to není řešení příliš praktické. Z JavaScriptu se stala klíčová technologie webových stránek. Jeho úplným vypnutím přestanou být webové stránky tak zábavné a zajímavé.

Naštěstí se můžete některým bezpečnostním potížím s JavaScriptem vyhnout tak, že vypnete pouze jeho pokročilé vlastnosti. Pokud chcete vypnout pokročilé vlastnosti JavaScriptu, postupujte takto:

1. V nabídce prohlížeče Firefox zvolte **Nástroje > Možnosti.**
2. V dialogovém okně, které se objeví, klikněte na záložku **Obsah.**

3. Ve výchozím nastavení bude možnost **Povolit JavaScript** zaškrtnutá. Nechte ji zaškrtnutou, ale klikněte na tlačítko **Rozšířené** vpravo. Zobrazí se dialogové okno s pokročilými možnostmi JavaScriptu.



4. Zrušte zaškrtnutí všech těchto položek.

Ačkoli vypnutí těchto vlastností vyřeší mnoho bezpečnostních problémů souvisejících s JavaScriptem, ještě lepším řešením je JavaScript bezpečně ovládat použitím funkce add-on NoScript, kterou popisujeme v ***Části 9.4.5, Funkce add-on pro Firefox, které usnadňují život.***

9.4.3 Vypnutí Javy

Asi si říkáte: Java a JavaScript jsou totéž, ne? Zní to tak, ale nejsou. Javu vynalezla společnost Sun Microsystems před tím, než společnost Netscape přišla s JavaScriptem.

Sun Microsystems? Netscape? Že jste o nich nikdy neslyšeli? To nás nepřekvapuje, protože ani jedna z těchto společností už neexistuje. Ve své době však byly obě velkými hráči na poli vývoje internetových aplikací. Java je velkým hráčem i nadále. Zatímco JavaScript byl původně určen k používání ve webovém prohlížeči, Java je obecný systém, který byl do prohlížečů integrován. Je to technologie určená k tomu, aby webovým designérům a podobným uživatelům umožňovala na své webové stránky snadno přidávat zajímavé funkce a vlastnosti.

Java je nesmírně všestranná technologie. Je možné ji použít ke spouštění velkých aplikací na ploše, jako je OpenOffice (bezplatný balíček kancelářských aplikací), nebo malých webových nástrojů (nazývaných „applety“).

Také Javu mohou autoři malwaru zneužívat. Aby bylo toto nebezpečí menší, applety Java mají určitá omezení. Applety nemají přístup k souborům ve vašem systému, ani nemohou provádět síťová připojení k žádnému systému. Přesto se vás operační systém čas od času zeptá na nějaký Java applet, který žádá o další přístup. Pokud si nejste naprosto jisti, co se tento applet pokouší udělat, obecně byste vždy měli odpovědět „Ne“. Také byste měli vždy používat nejnovější verzi Javy a aplikovat veškeré aktualizace, aby byly odstraněny potenciální bezpečnostní díry. Ačkoli společnost, která jako první Javu vyrobila, již neexistuje, nyní tento produkt vlastní společnost Oracle. Informace o aktualizacích najdete na jejích stránkách (www.oracle.com).

9.4.4 Používání hlavního hesla

Zásadní překážkou na cestě k bezpečnosti je pro mnoho uživatelů vytváření – a zapamatování – hesel. Protože je těžké silná hesla uhodnout, je také těžké si je pamatovat. Z toho důvodu mnoho lidí nastavuje dobré silné heslo a poté ho používají znovu a znovu na mnoha stránkách. Problém je, že když útočníci získají přístup k heslu narušením jedné ze stránek, které používáte, mohou tak získat heslo pro přístup k vašim dalším účtům.

Firefox tento problém s pamětí řeší tak, že pro vás uživatelská jména a hesla uchovává automaticky a nabídne vám je, když je potřebujete. Ještě lepší je, že si můžete nastavit hlavní heslo, které chrání všechna uložená hesla.

Při nastavení hlavního hesla postupujte takto:

1. V nabídce prohlížeče Firefox zvolte **Nástroje > Možnosti.**

2. V dialogovém okně, které se objeví, klikněte na záložku **Zabezpečení.**

3. Zaškrtněte políčko Používat hlavní heslo.

4. Zadejte silné heslo. Protože je to JEDINÉ heslo, které si budete muset pamatovat, neexistuje žádná výmluva, proč by nemělo být vynikající. Snažte se zobrazený ukazatel **Kvality hesla** posunout co nejvíce doprava.

Všimněte se, že na záložce **Zabezpečení** můžete kliknutím na možnost **Uložená hesla** zobrazit seznam uložených hesel a souvisejících uživatelských jmen. (Seznam uživatelských jmen je opravdu skvělá funkce. Lidé často zapomínají uživatelská jména i hesla pro stránky, které moc často nepoužívají.)

9.4.5 Funkce add-on pro Firefox, které usnadňují život

Kromě vestavěných vlastností můžete Firefox rozšířit stažením a instalací mnoha funkcí add-on, které poskytují další funkce.

NoScript

NoScript je funkce add-on, která vypíná JavaScript na webových stránkách, omezuje typy povoleného JavaScriptu a blokuje známé útoky. Jak jste se už dozvěděli, můžete JavaScript pomocí nástrojů prohlížeče Firefox jednoduše vypnout. Nevýhodou je, že v tomto nastavení si můžete vybrat pouze mezi možnostmi „všechno“ nebo „nic“. Pokročilé funkce jsou buď vždy povoleny, nebo vždy zakázány. Add-on NoScript povoluje JavaScript na stránkách, kterým věříte, a na všech ostatních webových stránkách jej blokuje. Tak máte moc ve svých rukou.

Musíte být jen opatrní a nevěřit příliš mnoha stránkám; v opačném případě vám tato funkce add-on moc ochrany nepřinese.

Better Privacy

Adobe Flash je multimediální funkce plug-in, kterou mnoho webových stránek používá k poskytování animací, videa a různých interaktivních funkcí. Mnoho uživatelů si neuvědomuje, že plug-in Flash Player si ukládá soubory cookies (tak jako soubory cookies prohlížeče), které mohou ostatním stránkám umožnit vás jeho pomocí sledovat. Na rozdíl od souborů cookies tradičních prohlížečů tyto soubory není možné spravovat ani mazat změnou nastavení prohlížeče. Better Privacy je funkce add-on, která tyto soubory cookies spravuje. Můžete ji použít tak, aby povolovala ukládání jen určitých souborů cookies a aby soubory Flash cookies mazala pravidelně, nebo jen když prohlížeč Firefox zavřete.

CookieSafe

CookieSafe je funkce add-on pro správu tradičních souborů cookies. Můžete řídit soubory cookies pro jednotlivé stránky tak, že je trvale zablokujete, povolíte je dočasně nebo na jedno spuštění prohlížeče, nebo je povolíte trvale, to vše pomocí ikony CookieSafe na stavovém řádku. Tato funkce add-on také spravuje seznam nedůvěryhodných stran a blokuje všechny jejich soubory cookies. Pomocí funkce CookieSafe můžete sdílet nastavení povolených souborů cookies a stránek s prohlížeči Firefox na jiných počítačích.

WOT – nástroj pro bezpečné prohlížení

Funkce add-on Web of Trust (WOT) je kolaborativní systém webové důvěry umožňující uživatelům hlásit, které stránky jsou opravdu důvěryhodné. S funkcí add-on WOT hodnotíte úroveň důvěry ve webovou stránku v mnoha kategoriích, jako je důvěryhodnost, spolehlivost dodavatele, soukromí a bezpečnost pro děti. Plug-in WOT kombinuje vaše hodnocení s hodnocením ostatních uživatelů. „Semafor“ poskytuje přehledný souhrn celkové úrovně důvěry.

Password Hasher

Kolik webových hesel máte? Doufáme, že máte jedinečné a obtížné heslo pro každou stránku, kterou navštěvujete. (Ta představa nás rozesmála.) Password hasher tento problém řeší tak, že vám umožní vytvořit jedno heslo, z něhož vytvoří silné a jedinečné heslo pro každou stránku, kterou navštěvujete. Tato individuální hesla jsou poté ukládána v zašifrované databázi hesel prohlížeče Firefox.

9.5 Rozhodnutí pro Google Chrome

Google Chrome byl na trh uveden v roce 2008 a je tak jedním z novějších prohlížečů. Zahrnuje podporu všech hlavních standardů pro webové prohlížeče, jakož i rozvržení a skripty webových stránek.

Jak si povede v souboji se zavedenými těžkými váhami na trhu (Internet Explorer a Firefox) se teprve uvidí. Na trh prohlížečů je nesmírně těžké proniknout. Společnost Google má ale výhodu velmi silného a známého jména. Také má k dispozici vynikající místo, kde prohlížeč Google Chrome propagovat – jeden z nejoblíbenějších vyhledávačů na světě.

Společnost Google také při vývoji prohlížeče Google Chrome zvolila velmi zajímavý přístup. Místo aby od základů vybudovala nový prohlížeč, vzala některé z nejlepších programů, které již byly k dispozici. Použila mnoho knihoven otevřených zdrojů použitých ke stavbě dalších prohlížečů, jako je Firefox nebo Safari. To jí umožnilo vybrat knihovny s vynikajícím výkonem (rychlostí). V některých případech společnost Google vyvinula i vlastní knihovny. Mnoho z těchto knihoven a část zdrojového kódu prohlížeče Google Chrome pak zveřejnila jako otevřený zdroj (open source). Pomocí tohoto kódu si mohou jiné společnosti nebo jedinci také postavit vlastní prohlížeče.

Společnost Google řeší bezpečnostní problematiku několika způsoby. Google Chrome pravidelně stahuje seznam známých webových stránek s malwarem a phishingem a varuje vás, pokud se některou z nich pokusíte otevřít. Kromě toho prohlížeč Google Chrome chrání vaše informace vzájemným izolováním mnoha funkcí. Tato izolační technika zabraňuje tomu, aby mohly k datům, které pomocí jedné funkce používáte, mít přístup i jiné funkce. Škodlivý kód má tak méně příležitostí získat přístup k vašim datům. Prohlížeč Google Chrome používá podobnou izolační techniku k řešení slabých míst ve funkcích plug-in prohlížeče, jako je Adobe Flash Player.

Stejně jako Internet Explorer i Firefox, také prohlížeč Google Chrome podporuje prohlížení v soukromí. To, čemu Internet Explorer říká služba InPrivate a Firefox zase Procházení v soukromí, se v prohlížeči Google Chrome jmenuje Anonymní prohlížení.

Teprve se uvidí, jestli se Google Chrome stane dominantním prohlížečem na trhu. Největší část války prohlížečů proběhla už před lety. Nováčci však málokdy mají tak silného podporovatele, jako je společnost Google. I kdyby Google Chrome následoval osud prohlížečů Netscape a Mosaic (které tu byly dříve a patrně jste o nich nikdy neslyšeli), můžeme si být jisti tím, že nové bezpečnostní techniky tohoto prohlížeče a zcela jistě jeho knihovny otevřených zdrojů budou použity v jiných webových prohlížečích. Takže odkaz prohlížeče Google Chrome bezpochyby uvidíte, i kdybyste se s prohlížečem samotným nikdy nesetkali.

9.6 Pochopení problému s funkcemi plug-in

V této kapitole jsme hovořili o řadě funkcí plug-in. Plug-in je program, který jinému softwarovému programu přidává funkce. Pro webové prohlížeče a internetové aplikace je k dispozici řada funkcí plug-in. Ty umožňují sledovat videa, poslouchat hudbu, hrát hry, číst dokumenty, účastnit se webových chatů a dokonce rychleji stahovat data – a to vše z vašeho prohlížeče.

Plug-in **Program, který jinému programu přidává funkce.**

Počítač, který nyní používáte, jste patrně dostali s mnoha předem instalovanými funkcemi plug-in, jako je Adobe Flash Player. Flash je možná nejpoužívanější funkcí plug-in pro prohlížeče na světě. Mnoho webových stránek, jako je YouTube nebo Hulu, bez něj nemůže fungovat. Ani mnoho aplikací na Facebooku a řada online her. Některé funkce plug-in, jako je Flash, QuickTime a Real Player, mají multimediální aplikace. Jiné poskytují funkce pro bezpečnost, šifrování a širokou škálu jiných oblastí.

Na funkcích plug-in pro prohlížeče je skvělé, že je může psát a rozšiřovat kdokoli. Funkce plug-in vyvíjejí velké společnosti, jako je Adobe, Google nebo Microsoft. Stejně tak je vyvíjejí malé společnosti a někteří jednotlivci. Obecně lze říci, že funkce plug-in pro prohlížeče zlepšují Internet.

V čem je háček? Tak jako váš samotný internetový prohlížeč i operační systém, také funkce plug-in, které používáte, se čas od času aktualizují. Tyto aktualizace někdy přináší nové funkce. Někdy zase aktualizace odstraňují bezpečnostní díry, které byly v předchozích verzích přehlédnuty.
Každopádně čas od času dostanete upozornění, že musíte konkrétní funkci plug-in aktualizo-

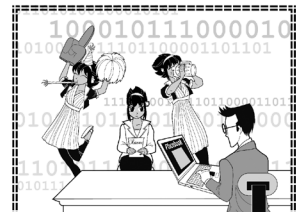
vat, abyste mohli používat svou oblíbenou stránku. Na to jste si asi zvykli.

Když webová stránka požaduje novou verzi funkce plug-in, aby mohla správně pracovat, také vám poskytuje praktický odkaz na to, kde si aktualizaci stáhnout. Většina z těchto odkazů je přesně tím, čím se zdají být. U malého počtu z nich tomu tak naneštěstí není. Některé stránky nyní používají falešná upozornění a aktualizaci funkcí plug-in jako způsob, jak uživatele lstí přimět ke stažení malwaru. Pokud dostanete odkaz ke stahování, nemusíte získat nejnovější verzi přehrávače Real Player. Místo toho můžete skončit se spywarem nebo trojským koněm, který umožní rekrutování vašeho počítače do botnetu.

Jak se tedy tomuto riziku vyhnout a přesto funkce plug-in využívat? Zaprvé zkontrolujte, zda je samotná funkce plug-in opravdová. Pokud webová stránka, kterou příliš neznáte, požaduje stažení funkce plug-in, o níž jste nikdy neslyšeli, mějte se na pozoru. Je-li funkce plug-in pravá, vždy stahujte aktualizace přímo ze zdroje. I když může být pohodlné kliknout rovnou na nabízený odkaz, vždy je bezpečnější otevřít přímo webovou stránku společnosti Adobe.

10. Soukromé blogy ve veřejném prostoru

10. Soukromé blogy ve veřejném prostoru – 191
10.1 Co je tedy blog? – 192
10.2 Blogy letí vzhůru – 193
10.3 To myslíš vážně?!!! – 194
10.4 Trvanlivost výrobku – 196
10.5 Bloggeři se požírají navzájem – 197
10.5.1 Útočné blogy – 197
10.5.2 Právní důsledky – 199
10.6 Myslet dopředu – 199
10.7 Jak správně blogovat – 200



10. Soukromé blogy ve veřejném prostoru

Dnešní ráno jsem strávila čtením online deníku své nejstarší dcery. A potom deníku její mladší sestry. Jejích sestřenic. Jejích nejlepších přátel. Jejího kluka...

Jak jsem se k tomu dostala? Strávila jsem 5 vteřin tím, že jsem si na Yahoo! našla jméno dceřina příteleho. První stránka, kterou jsem našla, byl jeho blog na serveru Xanga. Za malou chvíli jsem se proklikala jeho odběrateli a našla blog své dcery. Z jejího blogu jsem se prošla online úvahami jejích přátel. A jejich přátel. Každý nový blog mi dal odkazy na další. Začínám mít pocit, že jsem dnes ráno přečetla deníky poloviny dětí v tomhle okrese.

Samozřejmě jim to neřeknu. Nikdo z nich mi své odkazy nedal a jsem si NAPROSTO jistá, že nechtěli, abych si přečetla, co napsali. Obsah těch blogů mi otevřel oči. Ještě pořád jsem úplně paf z toho, jak osobní věci ty děti napsaly. Jako by byly na Internetu úplně samy! Zajímalo by mě, jaký budou mít z některých poznámek pocit, až dospějí, ale jejich puberťácké výlevy budou žít v kyberprostoru navždy...

–Anonymní máma

Pokud nejste naprosto netypický dospívající, asi o blozích alespoň v základních obrysech víte. Blog si vede čtrnáct procent dospívajících Američanů. A ještě více z nich „bloguje“ své zážitky na stránkách integrovaných sociálních sítí, které zahrnují blogovací funkce. Jaký je v tom rozdíl? Blog je mnohem podrobnější a určitě je v něm více textu. Stránky se sociálními sítěmi omezují zadávaný „stav“ (podobný příspěvkům na blogu) na krátký odstavec. Takže příspěvky jsou delší než tweet, ale určitě kratší než blog. Tradiční příspěvek na blogu vypadá spíš jako slohovka s pěti odstavci. To asi vysvětluje, proč si pravidelný blog vede jen 14 % dospívajících. Jak napsal Tom Ewing v knize Teens Don't Blog?: „Dobrovolné dlouhé psaní bude vždycky menšinovou záležitostí, ať už bude jak chce jednoduché, a není překvapivé, že více lidí přitahuje mnohem rychleji se pohybující a sociálnější svět aktualizací stavů.“ Přesto, 14 % představuje jednu šestinu a pro těch 60 milionů aktualizací stavu napsaných každý den na Facebook platí stejná omezení a nebezpečí, jako pro jejich delší příbuzné.

Pokud jste jedním z těch dospívajících, kteří si vedou blog (nebo pravidelně píšete aktualizace stavů), přemýšleli jste o tom, co je vhodné psát? A zajímali jste se o to, co se s vašimi příspěvky

stane v příštích letech? V této kapitole budeme hovořit o tom, co to znamená mít online blog, a jak ho vést, aniž byste ohrozili své bezpečí nebo budoucnost. Budeme také mluvit o historii blogovací komunity.

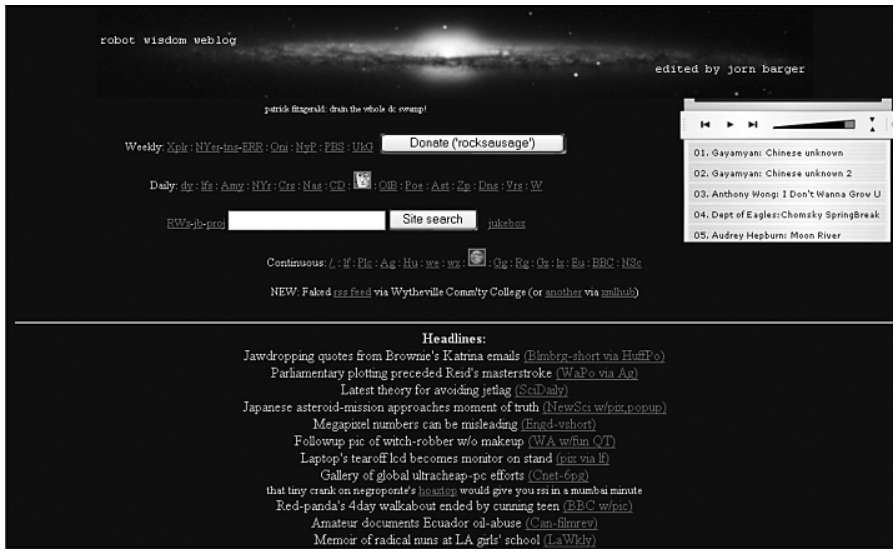
10.1 Co je tedy blog?

Blog je zkratka anglického slova „weblog" – webová stránka sestávající se ze série záznamů dat. Podobně jako online záznamníky nebo deníky, některé blogy jsou samostatné. To znamená, že neuvádějí odkazy na další stránky. Většina blogů však obsahuje odkazy na jiné blogy a stránky, které autora zajímají. I když může blog vypadat a někdy také fungovat jako deník, je to ve skutečnosti velmi veřejný záznam. Ve skutečnosti je jedním z problémů, které blogy představují pro ochranu soukromí jedince, že příliš mnoho uživatelů s nimi zachází, jako by to byly opravdu soukromé deníky, a ne veřejné záznamy.

Blog Záznam na webu obsahující textové příspěvky seřazené podle data (jako deník), stejně jako odkazy na další stránky.

Co se týče internetového průmyslu, jsou blogy poměrně novým fenoménem, který se objevil mezi polovinou a koncem 90. let. Podle některých odborníků byla prvním blogem stránka Mosaic's What's New Page, která vznikla v roce 1993, existují však pochybnosti, zda skutečně splňuje kritéria blogu, jak jej chápeme dnes. I když určitě obsahovala očekávané odkazy na jiné stránky, které autora zajímaly, chyběl jí „deníkový styl", který představuje základ dnešních blogů.

Někteří odborníci datují vznik prvního blogu do roku 1997. Tehdy John Barger ve skutečnosti vymyslel pojem weblog pro svou stránku *Robot Wisdom Weblog*. Jiný blogger, Peter Merholz, později termín „weblog" zkrátil na slovo „blog", které používáme dnes. Jak pochopíte z obrázku velmi těžce čitelné obrazovky, bylo to dlouho před tím, než bezplatné programy na tvorbu blogů zjednodušily vytváření webových stránek, které se snadnou čtou a procházejí.



Robot Wisdom Weblog Johna Bargera http://www.robotwisdom.com/

Dnes jsou blogy mnohem nablýskanější a je podstatně jednodušší je vytvořit. S příchodem bezplatných programů na tvorbu blogů už bloggeři nemusejí chápat **HTML** – programovací jazyk používaný k vytvoření webových stránek – ani mít jakoukoli znalost byť jen základů tvorby webových stránek.

HTML HyperText Markup Language. Programovací jazyk používaný k tvorbě webových stránek.

10.2 Blogy letí vzhůru

I když se počátky blogování datují do poloviny 90. let, moc se neujalo, dokud společnost Prya nepředstavila svůj nástroj Blogger. Ten méně technicky zdatným uživatelům umožňoval vytvářet a udržovat blogy bez toho, aby se z nich stali webmasteři. Nástroj blogger rozšířil blogovací komunitu z několika tuctů technologických elit a otevřel dveře zbytku internetové komunity.

Nastávající bloggeři těmito dveřmi proudili neuvěřitelnou rychlostí. V roce 1999 Jesse James Garrett, editor časopisu *Infosif,* zveřejnil webovou stránku se seznamem všech blogů, jejichž existence byla tehdy známa. Bylo jich 23. Dnes jsou jich miliony. Podle společnosti Technorati v San Franciscu, zabývající se sledováním Internetu, vznikají jeden nebo dva blogy každou vteřinu každého dne.

Nejlepší blogy dospívajících

Pokud si chcete vytvořit vlastní blog, nebo si jen chcete přečíst blogy pravděpodobně napsané dalšími dospívajícími, doporučujeme například některé z těchto stránek:

- Xanga
- LiveJournal
- Blogger.com

Dospívající, kteří se vzdělávají doma, mohou najít online blogovací komunitu na adrese Homeschool-Blogger.com.

Bloggeři probírají všechno od včerejších testů ze společenských věd, až po mezinárodní události a národní politiku. Politické blogy se tak rozšířily, že před posledními dvěma prezidentskými volbami v USA někteří bloggeři dostali oficiální novinářské průkazy, aby mohli napsat o hlavních sjezdech volebních stran.

Pro většinu dospívajících se však vedení blogu podobá více vedení veřejného deníku než psaní mediálních příspěvků. Proto většina dospívajících své blogy vede v prostředí přátelském k dospívajícím.

10.3 To myslíš vážně?!!!

Blogování se zjevně stalo trvalou součástí kultury dospívajících. To nemusí být nutně špatné. Na některých z těchto blogů vedou dospívající poměrně složité filozofické diskuze. Kevin Krim, vedoucí předplatného společnosti vlastnící blogovou stránku LiveJournal, zdůrazňuje: „Najdete stejně tolik mizerných fotografií jako dětí, které vedou opravdu zajímavé rozhovory o svých rozvíjejících se názorech na spiritualitu, nebo o tom, co si myslí o válce. Přemýšlet o takových věcech je dobré."

U blogů, stejně jako u všech oblastí internetové technologie, je nejdůležitější používat to, co je dobré, a vyhýbat se tomu, co je špatné nebo nebezpečné. Dobré je, že blogy poskytují jednoduché a motivující fórum, na kterém si dospívající bystří mysl, mimochodem praktikují schopnost psaní textu a v podstatě dokumentují své dospívání. Jak však podotýká Elizabeth Armstrong ze společnosti Christian Science Monitor, i když může být blog snadným online deníkem, je to „deník, do kterého nahlíží zbytek světa."

U blogování je nejnebezpečnější to, že dospívající poskytují PŘÍLIŠ mnoho informací. Velká část blogujících dospívajících na svých stránkách uvádí svá plná jména. Více než polovina zveřejní svou adresu nebo kontaktní údaje. Kdyby jedinými lidmi, kdo jejich blogy čtou, byli další dospívající, nemuselo by to vadit. Tak tomu ale není. Když na svůj blog vyvěsíte informace, díky kterým můžete být osobně identifikováni, vystavujete se velkému riziku ze strany některých nechutných online existencí.

Tam, kde se shromažďuje větší počet dospívajících, se samozřejmě vždycky mohou objevit slizouni. A blogy jedním z takových míst bezpochyby jsou. Mary Ellen Hendy, která pracuje jako technická koordinátorka na střední škole, udává, že si blogy vede celá třetina z jejích 250 studentů. To se dá čekat. Děsivé je, že pouze u 5 % z nich o tom ví rodiče. I když vás tak nízké číslo může překvapit, určitě by nepřekvapilo Edwarda Parmelee, zvláštního agenta z jednotky FBI pro kyberzločiny z Jacksonu ve státě Mississippi. Parmelee často pořádá přednášky na školách a uvádí, že když se rodičům zmíní o blozích, „koukají na nás jako spadlí z višně. Vůbec neví, o čem mluvíme."

Co se na blogu nedělá

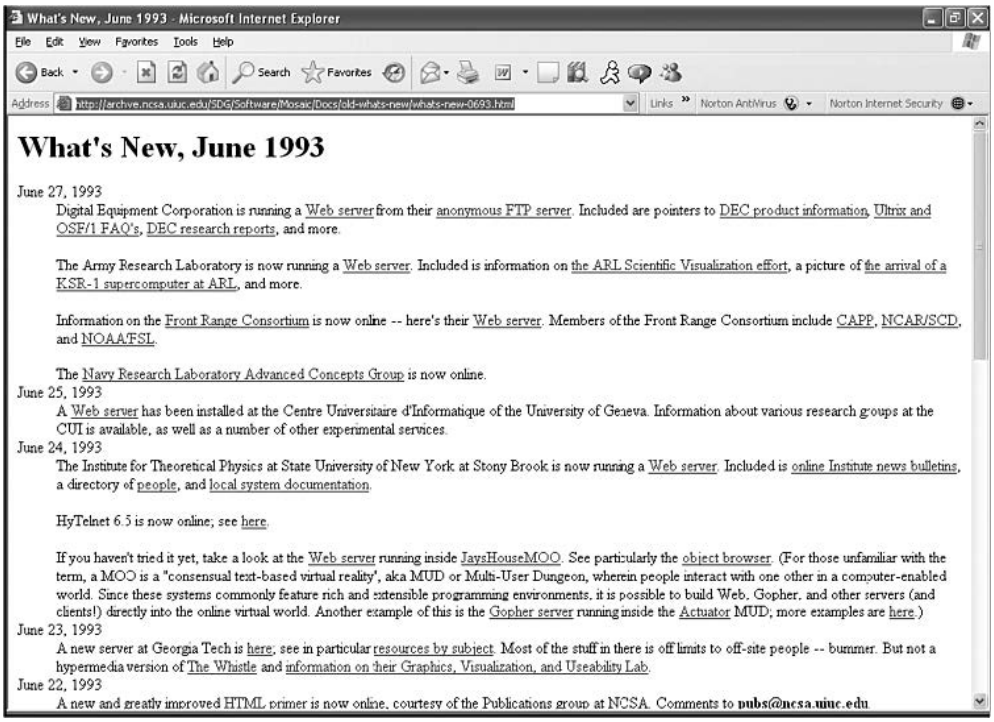
Buďte blogger, který chrání své bezpečí! Nikdy neuvádějte:

- Své celé jméno
- Svou adresu
- Své telefonní číslo
- Svůj věk
- Nic, o čem nechcete, aby to věděla vaše matka!
- Nic, o čem nechcete, aby to viděl váš budoucí zaměstnavatel
- Nic, co by mohlo ohrozit vaše přijetí na vysokou školu.

Pokud vaši rodiče patří k těm neinformovaným, teď máte šanci je zasvětit. I když možná nechcete, aby rodiče váš blog pravidelně četli, jsou to právě oni, kdo představuje vaši první a nejlepší obrannou linii. Měli byste jim dát dost informací k tomu, aby vám mohli pomoci přijmout správná rozhodnutí pro vaši ochranu.

10.4 Trvanlivost výrobku

Jiným problémem spojeným se šířením blogů dospívajících je to, že si většina jejich autorů vůbec neuvědomuje, jak dlouho budou blogy existovat. A to může být hodně, hodně dlouho. Jestli vás zajímá, jak dlouho mohou na síti zůstat staré blogové záznamy, které jste napsali, podívejte se na tento snímek obrazovky: Toto jsou příspěvky napsané na blogu Mosaic's What's New Page při jeho vzniku v roce 1993.



Mosaic's What's New Page, June 1993 http://archive.ncsa.uiuc.edu/SDG/Software/Mosaic/Docs/old-whats-new/whats-new-0693.html

Na rozdíl od fyzických deníků nebo záznamníků, blogové záznamy jsou veřejná stvoření, nikoli soukromá. Jakmile na svůj blog přidáte nový záznam, stanou se jeho slova snadno přístupná téměř všem lidem na světě, kteří mají přístup na Internet. Mnohé blogy jsou zcela otevřené, ani nevyžadují, aby se čtenáři přihlásili. Přesně tak je to u oblíbené stránky pro blogy dospívajících, Xanga.com. Anonymní máma v naší příkladové studii na začátku kapitoly se nepotřebovala na stránce Xanga zaregistrovat, aby si mohla přečíst příspěvky svých dospívajících dětí. Prostě jen použila vyhledávač Yahoo!.

Ani když se budete držet stránek, ke kterým mají přístup jen registrovaní členové, přístup k vašemu blogu tím moc omezený nebude. Jak těžké pro vás bylo vytvořit si bezplatný online blog? Tak proč si myslíte, že vaše máma, ředitel vaší školy, nebo dokonce potenciální zaměstnavatel za 10 let by to nemohli udělat také?

10.5 Bloggeři se požírají navzájem

I když jsou blogy dospívajících často příliš osobní, alespoň jsou většinou docela pozitivní. Někteří tak zvaní dospělí v **blogosféře** se tak dobře nechovají. Nežádoucím vedlejším účinkem nárůstu blogovací kultury byl vznik útočných blogů.

Blogosféra Celá blogující komunita. Patří k ní všechna blogovací fóra, blogovací stránky a jednotlivě spravované blogy.

Útočné blogy existují částečně, a občas výlučně, proto, aby jejich autoři mohli říkat nepříjemné věci o druhých. Někdy útočí na politické rivaly. Jindy se soustředí na konkurenci. Nebo prostě jen na lidi a produkty, které autor blogu nemá rád.

10.5.1 Útočné blogy

Negativní blogy, často zvané **útočné blogy,** se vynořily jako velký problém již v 90. letech. Útočné blogy měly často formu webových stránek útočících na různé společnosti a staly se způsobem, jakým nespokojení zákazníci, bezskrupulózní konkurence nebo zhrzení bývalí zaměstnanci na společnosti útočili s využitím široké platformy a relativní anonymity. Díky šňůře soudních žalob tato konkrétní vlna naříčení opadla. Místo ní nyní temná strana blogosféry hostí blogy s osobními útoky.

Útočný blog **Blog psaný specificky za účelem útoku na jedince, společnost nebo skupinu osob.**

Osobní útočné blogy jsou prostě dalším médiem pro kyberšikanu a obvykle mají jednu ze dvou forem. Nejzjevnější útočné blogy jsou otevřenými útoky na konkrétní osobu. Může se jednat o negativní prohlášení na blogu jiného dospívajícího, nebo celý blog věnovaný ponižování oběti. Jeden z takových blogů z názvem Kill Kylie, Incorporated (Zabijte Kylie, a.s.) byl naplněn vulgárními obviněními studentky 8. ročníku Kylie. (Kylie byla z útočného blogu, který zřejmě psali její spolužáci, tak rozrušená, že nakonec přešla na jinou školu.) Méně zjevné útočné blogy jsou sepsány tak, aby vypadaly, jako by je psala oběť. Jejich cílem je zničit pověst oběti předstíráním, že se tato osoba přiznává k něčemu hroznému, například že ve volném čase zabíjí kočky, nebo že podporuje dětskou pornografii.

Pokud jste obětí útočného blogu, možná víte, kdo je jeho autorem. Studie společnosti National Children's Home zjistila, že téměř tři čtvrtiny (73 %) obětí kyberšikany zná své útočníky. I když by vaší první reakcí na útok mohla být touha napsat vlastní příspěvky nebo dokonce vlastní reagující blog, často to není moc dobrý nápad. Pokud chcete umlčet ošklivou pomluvu, není ve vašem nejlepším zájmu křičet zpátky na někoho, kdo stojí na velkém a veřejném pódiu. A přesně tam také útočník stojí.

Na tohle byste si měli vzpomenout, když budete uvažovat o účasti v bitvě blogů, nebo se v jedné ocitnete. Dejte na radu Roberta Mahaffey, vyšetřovatele kyberzločinů z kanceláře státního návladního v Mississippi. „Internet je divoký západ 21. století a je třeba s ním tak zacházet." Útočné blogy naštěstí tvoří jen velmi malou část blogovací komunity. Daniel Lyons na stránkách Forbes.com poznamenává: „Útočné blogy tvoří pouze zlomek rychle expandující blogosféry." Pistolníci a kriminálníci samozřejmě také na Divokém západě tvořili menšinu. To neznamená, že nebyli skutečnou hrozbou. Útočné blogy jsou podobně nebezpečnou menšinou. Provokovat je posíláním reakcí určitě není moc chytré.

Zatímco online reakce účastníky často jen povzbudí, neznamená to, že byste útoky měli prostě ignorovat. Tím nejlepším, co můžete udělat, je šikanu nahlásit. Blogovací stránky nyní útočné blogy zakazují, takže můžete dosáhnout odstranění urážlivé stránky. Pokud jsou útočníci s vámi ve škole, hledejte také zastání oficiálními školními cestami. Mnoho škol útočné blogy

zakazuje – i kdyby se psaly mimo vyučování. Další informace o tom, jak se lépe chránit, najdete v ***kapitole 6, Kyberšikana.***

10.5.2 Právní důsledky

Jiným dobrým důvodem, proč na útočné blogy nereagovat, je, že nechcete být vtaženi do bitvy právních žalob. Když se dospělí navzájem bez důvodu obviňují, všechny strany mají sklon hledat zastání u právníka.

Pomlouvání (zveřejňování tvrzení, o kterém víte, že není pravdivé) není jen neslušné, je také nezákonné. Pokud vás usvědčí z pomluvy, možná budete muset zaplatit veškeré škody, které jste způsobili na pověsti nebo životě oběti. To může být velmi, velmi drahé. Představme si, že se skutečně rozhodnete strhat nový produkt na hubnutí od nějaké společnosti. Na blogu oznámíte, že jste nejen nezhubli, ale byli jste nafouknutí jako balón a na obličeji se vám objevila ošklivá vyrážka. Dokonce vystavíte svou fotku s tou ošklivou vyrážkou, kterou vám způsobili. A teď si představme, že by ten otok a vyrážku ve skutečnosti způsobilo vosí bodnutí. Ten obrázek jste jen použili, abyste jim uškodili, protože jste někde četli, že své výrobky testují na zvířatech. Váš motiv mohl být šlechetný, ale váš příspěvek je i tak pomluvou. Pokud by vás společnost zažalovala (což docela dobře může, kdybyste jí skutečně poškodili prodeje), můžete jim dlužit všechny peníze, které by jinak vydělali v příštích dvaceti letech, kdyby jejich pověst nebyla zničená.

Je pravděpodobné, že vás odsoudí za štiplavé poznámky, které si napíšete na blog? Asi ne. Na druhou stranu do vězení asi nepůjdete ani za to, že sousedovi každé ráno kradete noviny. Správné ale je psát na web jen pravdu (a na sousedovy noviny nesahat).

10.6 Myslet dopředu

Tak jako e-mail (který často zůstane na serveru ISP dlouho poté, co jste jeho kopii smazali a na jeho obsah zapomněli), záznamy na blogu ve skutečnosti nezmizí, když se váš život posune dál a vy na ně zapomenete. Žijí na záložních discích a v archivních souborech. Mohou dokonce žít dál na webové stránce někoho jiného. Kolikrát jste zkopírovali něco, co se vám zdálo ohromně chytré nebo vtipné, a vložili si to na svou stránku? Někdo jiný mohl totéž udělat s vašimi příspěvky.

Dospívající vždy v historii dělali a říkali hlouposti, kterých později, již jako dospělí, litovali. Změnilo se to, že blogy na stránce Xanga, videa na YouTube a fotky na serveru MySpace mohou nyní tyto chyby dokumentovat – možná navždy.

Nedávno muselo mnoho osob nominovaných do amerického Nejvyššího soudu stáhnout své kandidatury kvůli obviněním ze špatných rozhodnutí, která přijaly v 60. letech. Jen si představte, kdyby tato rozhodnutí kandidáti sami zdokumentovali online. Za 30 let možná členové komise Kongresu nebudou potřebovat, aby kandidáty na porotce prověřovala FBI. Bude jim stačit prohlédnout si archivní záznamy starých blogů. Když vezmeme v úvahu některé z blogů dospívajících, které jsme v poslední době četli, dokážeme si představit Nejvyšší soud s devíti prázdnými křesly. Když už nic jiného, určitě bychom viděli hodně starších osob ve velkých rozpacích. Nebuďte jedním z nich.

10.7 Jak správně blogovat

Doufáme, že tato část nezní příliš negativně. Vážně se snažíme nepopisovat vám Internet jako „velkou chlupatou bestii". Protože je však naším úkolem dát vám v této knize informace, které potřebujete, abyste se mohli chránit před temnou stranou kyberprostoru, nemůžeme se tomu úplně vyhnout.

Přesto nechceme, abyste si odnesli poznatek, že blogování je špatné. Není. Chápeme, že vaše blogy jsou důležitou součástí vašeho virtuálního života. Vaše příspěvky časem ukáží jasný obraz vašeho emocionálního dospívání, budou webovou dokumentací vašeho rozvoje v přemýšlejícího, úžasného jedince.

Abyste mohli využít výhod blogosféry, musíte jen dodržovat několik jednoduchých pravidel:

- **Buďte upřímní.** To znamená zachovávat si integritu na několika úrovních. Samozřejmě byste měli na blogu zveřejňovat jen to, o čem víte, že je to pravda. Měli byste být také upřímní s informacemi o sobě. Pokud musíte lhát o svém věku, abyste se mohli stát členy konkrétního blogovacího fóra, pak někde uvnitř dobře víte, že byste tam neměli být. Existují blogy otevřené dospívajícím v každém věku. Pro své vlastní dobro byste se neměli pohybovat na fórech pro dospělé a dospívající starší, než jste vy.

• **Nebuďte příliš upřímní.** Jsou věci, které čtenáři vašeho blogu opravdu nepotřebují vědět. Patří k nim veškeré osobní informace, které by mohly vést k vaší identifikaci. Vaše jméno. Vaše adresa nebo jen město, kde žijete. Název vaší školy. Celé jméno přátel nebo jen známých, které máte. Pro vaši vlastní ochranu nesmíte na Internetu sdílet žádné osobní informace.

• **Buďte obezřetní.** Vždy si pamatujte, že váš blog je VEŘEJNÝ záznam. Nepište tam nic, o čem byste si nepovídali s babičkou u večeře.

• **Myslete dopředu.** Nikdy nezapomínejte, že příspěvky na vašem blogu vás klidně mohou přežít. Než něco napíšete, zeptejte se sami sebe, co byste si o tom příspěvku mysleli za měsíc nebo za rok. Nebo za deset let. Opravdu to musíte psát na blog, nebo ho můžete vynechat a raději si promluvit naživo s nějakým kamarádem?

• **Když nemůžete říct nic hezkého, raději neříkejte nic.**

11. Socializace

– Obsah kapitoly

11. Socializace – 205
11.1 Kde jsou přátelé – 206
11.2 Přátelé: skuteční a virtuální – 207
11.3 Skupiny – 208
11.4 Aplikace třetích stran – 209
11.5 Rhybáři přátel – 209
11.6 Zveřejňování příliš mnoha informací. – 210
11.6.1 Pochybné fotografie – 211
11.6.2 Nebezpečné webkamery – 211
11.6.3 YouTube – 212
11.7 Online rozchod – 213
11.8 Zapípej, ptáčku – 213
11.9 Tipy k zachovávání bezpečí na sociálních sítích – 214

11. Socializace

Studentka vyššího ročníku střední školy Miranda se vždycky ráda fotila. Její máma si dělá legraci, že se Miranda snažila dostat se na rodinné snímky ještě před tím, než uměla chodit. Takže když na Facebooku našla vzkaz od své kamarádky Candy s textem: „Můj kamarád tě zachytil na skryté kameře...", prostě se musela podívat. Zvláštní bylo, že jí počítač v té chvíli fungoval nějak divně. Musela se znovu přihlásit na Facebook, i když se přihlásila pár minut před tím. Pak se na ty fotky nemohla podívat, dokud si nestáhla novou verzi Flashe...

Mirandě nedošlo, že Candy jí neposlala aktualizaci stavu. Do Candyina facebookového účtu se dostal nepříjemný červ. Facebook ani nechtěl, aby se Miranda znovu přihlásila. Byla to falešná obrazovka zobrazující přihlašovací stránku podobnou Facebooku, aby Mirandu přiměla zadat její uživatelské jméno a heslo. A ta aktualizace Flashe? Uhodli jste. Odkaz vůbec nevedl k funkci Adobe Flash. Miranda si stáhla falešný antivirový program. O několik minut později už viděla vyskakovací okna s informací, že byl její počítač infikován spywarem a že musí zaplatit 49,95 USD (v přepočtu přibližně 1 000 Kč) za aktualizaci bezpečnostního programu, aby se spywaru zbavila.

Jako mnoho uživatelů před ní, Miranda byla podvedena malwarem zaměřeným na sociální sítě. V tomto případě červ šířil odkaz na falešnou přihlašovací obrazovku, aby získal její heslo, poté ji přesvědčil ke stažení trojského koně, který přesměrovával její prohlížeč na podvodné webové stránky a nutil ji koupit si falešný antivirový program. Za méně než 15 minut se Miranda stala obětí téměř všech forem malwaru!

Sociální sítě jsou právě teď častým cílem podvodníků, protože tam lidé tráví větší a větší podíl času stráveného online. Proč jsou tak oblíbené? Být členem sociální sítě znamená být součástí online komunity, která umožňuje propojení mezi uživateli. Už od vzniku Internetu samozřejmě existovala místa, kam jste mohli jít a diskutovat o různých tématech s online „přáteli". První diskusní fóra a skupiny však měly svá omezení. Uživatelé psali své názory a často reagovali na příspěvky druhých, ale nebudovali si svá vlastní společenství, jak tomu je u dnešních sociálních sítí.

11.1 Kde jsou přátelé

V roce 2003 se první velkou **sociální sítí** staly stránky MySpace. Služba MySpace byla založena na předchozí jednodušší stránce zvané Friendster a rozbalila to ve velkém. Do roku 2010 měla americká stránka více než 70 milionů uživatelů. Když započítáte stránky MySpace z 30 zemí na celém světě, plus speciální stránky, jako např. MySpace Latino, dělá to asi 120 milionů uživatelů.

Stránka sociálních sítí Webová stránka umožňující uživatelům definovat vzájemné vztahy a spojovat se nejen se svými přáteli, ale také s přáteli přátel a přáteli přátel jejich přátel – neustále rostoucí online síť.

I když stránka MySpace nebyla první stránkou se sociální sítí, byla první, která se „virálně" rozšířila, co se týče pozornosti veřejnosti. I když technicky vzato uživatelům musí být alespoň 13 let, tento požadavek vychází z věku, který uživatelé sami uvedou.

Uživatelé stránek MySpace, i když mají MySpace rádi, mají často také účty na jiných sociálních sítích, jako je například Facebook. Facebook založil v roce 2003 druhák z Harvardu Mark Zuckenberg jako online verzi vysokoškolských ročenek. To byly knížky s fotografiemi každé třídy prváků (na menších školách) nebo každé koleje (na větších univerzitách) pomáhající studentům navzájem se seznámit. V té době neměl Harvard žádný adresář s fotografiemi studentů a webová mytologie tvrdí, že Zuckenbergova stránka dosáhla v prvních čtyřech hodinách svého života 22 000 zobrazení. Reakce byla tak silná, že se Zuckenberg rozhodl v roce 2004 spustit oficiální stránku jen pro studenty Harvardu. Do měsíce byla zaregistrována polovina studentů.

Teprve v září 2006 umožnil Facebook členství komukoli ve věku od 13 let, kdo měl platnou e-mailovou adresu. Do poloviny roku 2008 držely stránky Facebook a MySpace krok. Facebook se pak dostal do vedení v listopadu 2008, kdy přitáhl 200 milionů návštěvníků z celého světa. Ten měsíc síť Facebook navštívilo více než 20 % uživatelů Internetu. V březnu 2010 udávaly stránky Facebook 400 milionů aktivních uživatelů.

I když na trhu určitě dominují stránky MySpace a Facebook, rozhodně nejsou jedinými sociálními sítěmi, které dospívající navštěvují. K dalším populárním stránkám patří Friendster, Yoursphere a Bebo. Společně mají tyto stránky tolik uživatelů, kolik je obyvatel Latinské Ameriky. V roce 2009 už alespoň jednu sociální síť používalo 72 % dospívajících a mladých dospělých.

11.2 Přátelé: skuteční a virtuální

„Přítel" a „být v přátelích" jsou v chápání scény sociálních sítí nesmírně důležité koncepty. Když si zaregistrujete účet na stránkách MySpace nebo Facebook, služba vám nabídne vyhledání e-mailových adres ve vašem webovém prohlížeči a srovná je s adresami skutečných uživatelů stránek Facebook. V roce 2010 měl průměrný uživatel stránek Facebook 130 přátel.

Šťouchnutí Šťouchnutím na stránkách Facebook dáváte jiným uživatelům najevo, že stojíte o jejich pozornost. Mohou vás šťouchnout zpět, napsat vám na zeď nebo vás požádat o přátelství.

Sbírání „přátel" je zároveň největší výhodou i nejslabším článkem online sociálních sítí. Kvůli kontrole soukromí mohou většinu profilových informací o vás zobrazit pouze jiní uživatelé, které jste označili jako své přátele. Nebezpečí tkví v tom, že dospívající, kteří chtějí vypadat oblíbení, přijímají žádosti o přátelství od lidí, které vůbec neznají, a zveřejňují příliš mnoho informací, protože si myslí, že jejich stránku vidí jen jejich přátelé. Šestnáctiletý Eric z města Novato v Kalifornii si myslel, že mít 1 700 přátel je prostě super. Ve skutečnosti mohou být někteří z těchto přátel jen slizouni, kteří vám nahlížejí do života. Navíc vznikl i malware zneužívající této důvěry na sociálních sítích. Naivní uživatelé, kteří se domnívají, že k jejich příspěvkům mají přístup pouze jejich přátelé, jsou často znechuceni, když jsou tyto příspěvky zachyceny, poslány na jiných sítích a dostanou se do oběhu mezi lidmi, se kterými by je autoři nikdy nechtěli sdílet.

11.3 Skupiny

Sítě MySpace i Facebook mají oficiální předpisy proti „škodlivému obsahu“, stejně jako obsahu, který může být považován za urážlivý nebo hanlivý. I když jsou to teoreticky skvělé předpisy, praxe trochu pokulhává, zejména co se týče obsahu ve skupinách.

Jen na síti Facebook jsou založeny tisíce skupin, které umožňují setkávání a interakci uživatelů s podobnými zájmy – což je konec konců ten hlavní důvod, proč sociální síť vůbec mít. K těmto skupinám patří řada neškodných fanklubů, jako „Addicted to Project Runway“ (Závislí na reality show Heidi Klum: Svět modelingu, pozn. překl.) a poněkud fantaskní podivínské skupiny jako „Fyzika neexistuje, za všechno můžou trpaslíci.“ Některé znějí i trochu zoufale, jako „Musíme najít dárce ledviny pro našeho otce. Pomozte nám to rozšířit.“ Jiné podporují politické nebo emotivní náboženské proudy.

Jiné skupiny však bohužel patří k temné straně. Za prvních 10 minut, kdy jsme při přípravě této kapitoly procházeli skupiny, jsme měli možnost nahlásit celých 12 skupin správcům stránek Facebook za porušení pravidel, včetně nahoty na fotografiích, obscénního obsahu a vulgárního jazyka.

Kromě obecného vulgárního obsahu je větším problémem zamýšlený obsah mnoha skupin. I kdybyste nepočítali dost pochybný obsah některých skupin v kategorii Sexualita, stejně vám zůstane velký počet skupin podporující pití alkoholu u nezletilých. Na jejich obranu je třeba říct, že udržet sociální sítě čisté od nevhodného obsahu musí být dost těžký úkol, když vezmete v úvahu miliony uživatelů. I když jsou podobné příspěvky během několika hodin odstraněny, neustálé příspěvky nových uživatelů by stejně poskytly téměř nekonečný proud závadného materiálu.

Přítel všech

Zdá se vám, že nemáte moc přátel? Ať už uděláte cokoli, nepokoušejte se vyrovnat Tomu Andersonovi.

Spoluzakladatel stránek MySpace, 34letý Tom, je „výchozím“ přítelem přiděleným všem novým uživatelům sítě MySpace. V dubnu 2010 měl Tom 12 milionů přátel.

11.4 Aplikace třetích stran

Aplikace sociálních sítí jsou oddělené programy, které pracují v rámci sociální sítě a poskytují další funkce. Protože tyto funkce píší nezávislé společnosti, říkáme jim aplikace třetích stran. Pokud jste někdy hráli hry Farmville, Scrabble nebo jste na síti Facebook poslali narozeninové blahopřání, tak jste aplikace třetích stran použili. Pokud jste žádnou nepoužili, jste v menšině. Facebook udává, že 70 % aktivních uživatelů používá aplikace třetích stran každý měsíc. To nikoho nepřekvapí, když těchto aplikací existuje více než 500 000!

Protože aplikace třetích stran provozují jiné společnosti než sociální sítě, jejich používání má dopad na vaše soukromí. Když souhlasíte s používáním aplikace s narozeninovými přáními, dáváte této straně povolení přistupovat alespoň k některým z informací, které na síti Facebook nebo MySpace máte. Podle Pravidel užívání služby Facebook uvádí: „Když přidáte aplikaci nebo používáte platformu, váš obsah a informace jsou s touto aplikací sdíleny. Požadujeme, aby aplikace respektovaly vaše soukromí, ale způsob, jak aplikace smí používat obsah a informace, které sdílíte, se bude řídit vaší dohodou s danou aplikací." To znamená, že si před přidáním nové aplikace musíte podrobně přečíst uživatelskou dohodu. Nedělá vám to starosti? Možná si neuvědomujete, kolik informací vlastně sdělujete. Kromě seznamu vašich přátel mohou vaše uživatelské informace zahrnovat vaše jméno, profilovou fotografii, narozeniny, politické názory, koníčky, zájmy, vztah, vzdělání a práci stejně jako kopie všech fotografií ve vašich albech na síti Facebook. V rukou bezskrupulózního inzerenta je to zlatý důl.

Někdy aplikace poskytuje NĚCO NAVÍC, aniž jste o to žádali. Počátkem roku 2008 bylo zjištěno, že populární aplikace na síti Facebook Secret Crush rozšiřovala adware od společnosti Zango. I když to síť Facebook zastavila, v mnoha ohledech hrají s malwarem stejnou hru jako vy – jen v mnohem větším měřítku. Síť Facebook mění své předpisy a pokouší se blokovat zjevný malware, pokusy o phishing a adware. Lumpové hledají kličky v právnické řeči nebo v programu, aby mohli tato nová pravidla obejít. Protože jste obětí uprostřed tohoto boje, je vaším úkolem dávat pozor na podvody a sledovat, komu a s čím dáváte svolení.

11.5 Rhybáři přátel

Kolem roku 2009 se phishingové výpravy na Facebook staly téměř každodenní událostí. Některé z významnějších byly FBAction.net, Koobface a Areps.at. Většina těchto phishingových

podvodů měla formu napsaných stavů obsahujících vložené odkazy. Pokud jste na odkaz klikli, přesměrovaly vás na vnější webovou stránku, kde jste viděli přihlašovací obrazovku vyhlížející přesně stejně jako pravá obrazovka sítě Facebook. Pokud jste návnadu spolkli a bez přemýšlení jste se přihlásili, vaši přátelé začali brzy vídat aktualizace stavů s vloženými odkazy. Aby to bylo ještě horší, tato vnější stránka často infikovala váš počítač adwarem.

Tyto typy phishingových útoků jsou poslední dobou čím dál častější. Když toho o phishingových útocích již tolik víme, proč jim stále tolik lidí padá za oběť? Útočníci do velké míry spoléhají na sociální inženýrství. I když se uživatelé naučili být velmi opatrní s vloženými odkazy v e-mailech, odkazům v příspěvcích od přátel obvykle hodně věříme. Phisheři tak v podstatě zneužívají naší tendence důvěřovat přátelům. Aby útočníci získali ještě více kliknutí, používají text, který zaručeně upoutá vaši pozornost. Útok Koobface na sítě MySpace a Facebook v roce 2009 tvořil statusy jako *Paris Hilton hází na ulici trpaslíkem* a *Můj kamarád tě zachytil na skrytou kameru. Podívej se!*

11.6 Zveřejňování příliš mnoha informací.

Většina dospívajících na síti zveřejňuje příliš mnoho osobních informací. To může mít dlouhotrvající následky, o kterých jste možná nepřemýšleli. Podle serveru Carraře Boiler přibližně 30 % zaměstnavatelů při prověřování nových kandidátů kontroluje sociální sítě. A třetina manažerů zodpovědných za najímání nových pracovníků udává, že už nějakou žádost odmítli kvůli informacích, které našli online.

Odborníci se neshodnou na tom, zda je kontrola sociálních sítí ze strany zaměstnavatelů správná či nikoli. Pozitivní je, že ambiciózní dospívající mohou používat sociální sítě k tomu, aby představili své lepší stránky, sdíleli fotografie a příspěvky o zkušenostech ze své praxe a dobrovolnické práce. Negativní je, že studenti často píší hodně osobních informací, na které se zaměstnavatelé nesmějí ptát, protože tyto informace podle zákona nesmějí použít při rozhodování o přijetí. K těmto podrobnostem může patřit pohlaví, věk, rasa, náboženství, politické názory, tělesné nebo duševní nemoci a sexuální orientace uchazeče o zaměstnání. Strach byste neměli mít jen ze šťavnatých fotografií. Vaše fotografie z pochodu za práva gayů nebo demonstrace za právo na potrat se může zaměstnavatele nepříjemně dotknout. Měli by o vašem přijetí rozhodovat na základě těchto osobních informací? Opravdu ne. Problém je v tom, že jakmile je nějaká informace veřejná, je zkrátka veřejná.

Abyste své osobní informace chránili, dejte na radu sítě Facebook a „vždy kontrolujte, co sdílíte". Na všech sociálních sítích máte možnost zamknout svůj profil a omezit přístup ke svým osobním informacím a fotografiím pouze na své přátele. V mnoha případech můžete i vybrat konkrétní skupinu přátel.

11.6.1 Pochybné fotografie

Lidé, kteří milují sociální sítě, také MILUJÍ fotografie. Síť Facebook udává, že se na její stránky každý měsíc nahraje *miliarda* fotografií. To je hodně narozeninových oslav, výročí a promocí. Také jsou to miliardy příležitostí, při kterých uživatelé zveřejňují fotografie, které by si asi měli nechat pro sebe (nebo je vůbec nepořizovat!).

Fotografie na síti jsou výborným zdrojem zábavy – obzvlášť pro personální ředitele a osoby zodpovědné za přijímání nových zaměstnanců. Jak udává Allan Hoffman, odborník na technické práce v obrovské personální agentuře MONSTER: „Když hledáte práci, nemusí proti vám svědčit jen to, co říkáte. Je to také o tom, co posíláte na MySpace, píšete na blogu nebo vysíláte na YouTube." Fotky z loňského abiturientského večírku, nad kterými se dnes vaši přátelé baví, mohou způsobit, že v budoucnu nedostanete místo.

Díky fotografiím vás také mohou identifikovat stalkeři a pedofilové. Abyste se před těmito nebezpečími chránili, buďte velmi opatrní v tom, co sdílíte online. Také sledujte vaše fotografie, které sdílejí vaši přátelé, a na kterých vás označují. Označením na fotografii vás přátelé identifikují celému světu na fotografiích, které byste možná raději nesdíleli. ***Skuteční*** přátelé netrvají na tom, abyste na síti vypadali jako blázni.

11.6.2 Nebezpečné webkamery

Webové kamery v sobě skrývají všechna nebezpečí digitálních fotoaparátů a ještě některá navíc. Děsivým fenoménem poslední doby je nástup pedofilů na sociálních sítích, kde nezletilým nabízejí peníze za to, že si před kamerou sundají oblečení nebo se budou nevhodně chovat. Justinovi Berrymu bylo pouze 13, když mu udělal návrh pedofil. Následujících pět let používal svou webovou kameru k provádění toho, co se dá v podstatě označit jako dětská prostituce.

I když není pravděpodobné, že by z vás kamera udělala prostitutku/prostituta, pravděpodobně

z vás dříve či později udělá pitomce. Pokud jsou hloupé žertíky natočené na domácí video sdíleny s rodinou a blízkými přáteli, tedy lidmi, kteří vědí, že se takhle normálně *nechováte,* jsou velice zábavné. Cizí lidé se na takové video dívají jinak. Smějí se VÁM, ne s vámi. Znovu opakujeme, přemýšlejte o tom, co na síti sdílíte. Zvažte, co si o takovém videu budete myslet, až vám bude 30.

Mezitím pro vás vlastnictví webové kamery může přestavovat velké ohrožení soukromí. Představte si, jak byl Blake Robbins překvapený, když zjistil, že jeho střední škola aktivovala webovou kameru na notebooku, který mu poskytla, a špehovala, co dělal ve své vlastní ložnici. O špehování se dozvěděl, když ho škola potrestala za nevhodné chování a jako důkaz poskytla fotografii z webové kamery tohoto notebooku, pořízenou bez jeho vědomí. Jeho spolužáci byli šokováni. Savannah Williams, druhačka ze stejné školy na předměstí Philadelphie, byla znechucena. Uvedla, že si notebook s sebou často bere do koupelny a poslouchá hudbu, když se sprchuje.

11.6.3 YouTube

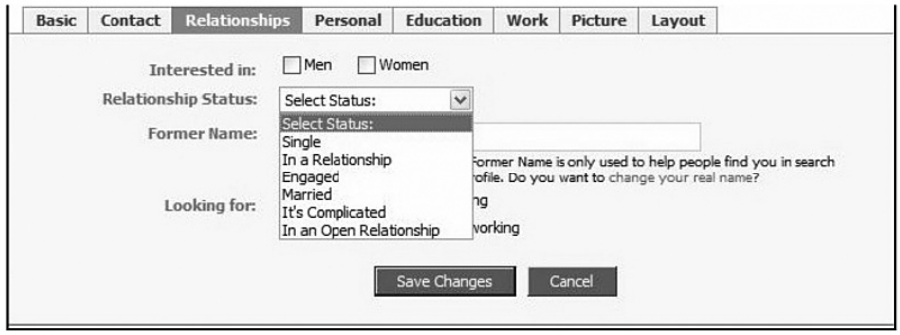
Webové kamery vám umožňují ztrapnit se před všemi přáteli ze sociálních sítí. YouTube vám dovolí toto ponížení sdílet s úplnými cizinci.

Na serveru YouTube jsme viděli videa, která byla neskutečně zábavná. Pro nás. Ale když tato zábavná videa dosáhnou milionů zhlédnutí, mohou vážně poškodit sebevědomí a duševní zdraví zobrazených osob. Představte si, jak by vám bylo, kdyby se vám smály miliony cizinců. Je to legrace, jen když se to stane někomu *jinému.*

A duševní zdraví není jediným problémem. Aspirující producenti to velmi snadno přeženou. V roce 2009 jedna matka zmínila, že její 15letý syn a jeho přátelé vytvořili pro server YouTube velmi znepokojující videa. „Měli tam všechno od hloupých žertíků až po sebepoškozování, jako když se bodali nebo si na ruce lili alkoholový čisticí prostředek a pak ho zapálili zapalovačem.“ Byl její syn problémovým dítětem? Ani ne. Snažil se být kreativní a měl pocit, že musí zajít do extrému, aby jeho video na síti upoutalo pozornost. Má štěstí, že mu nezůstaly trvalé následky.

11.7 Online rozchod

Další věc, na kterou je na sociálních sítích třeba pamatovat, je to, že více a více nahrazují skutečná setkání, rozhovory a sdílení emocionálních témat mezi lidmi. Při shromažďování materiálu pro tuto knihu jsme slyšeli o významném počtu dospívajících, se kterými se někdo alespoň jednou rozešel přes síť Facebook. Jak se to dělá? Na síti Facebook máte ukazatel vztahu. Když zadáváte do profilu své informace, můžete tam napsat také upravit **Rodinný stav.**



Citově nevyvinutí partneři, kteří by dříve prostě přestali komunikovat a vůbec by nezavolali, dnes jednoduše změní svůj **Rodinný stav.** Příliš mnoho věrných partnerů se dnes od svých přátel dozví, že stav jejich protějšku se změnil na **Nezadaný.** Tak se dostáváme k pravděpodobně nejlepšímu ukazateli toho, zda jste skutečně připravení pro sociální sítě – sebevědomí a zralost. Jste dost sebevědomí na to, abyste zvládli, když se s vámi někdo rozejde na síti? A ještě lépe, jste dost zralí na to, abyste to NEUDĚLALI někomu jinému? Viděli jsme jednoho dospívajícího úplně zničeného z toho, že mu jeho nejlepší kamarád řekl, že si Suzie (holka, se kterou čtyři roky chodil) změnila stav na **Nezadaná.** To není vůbec cool. Je to jen kruté.

11.8 Zapípej, ptáčku

Twitter vznikl v roce 2006. Je to sociální síť zaměřená na mikroblogy. Důležitá je předpona „mikro". Příspěvky na Twitteru, kterým se říká tweety, musejí být krátké a sladké.

```
Tweetování je jako posílání textových zpráv na sociální síti. Každý „tweet"
smí obsahovat jen 140 znaků... Tento „tweet" jich má přesně 140.
```

Twitter, kterému se často žertem říká blogování pro soundbitovou generaci, byl vyvinut pro uživatele na cestách, kteří píší z mobilních telefonů a zařízení. Proto je také délka příspěvků tak omezená. Textové zprávy jsou omezeny na 160 znaků, takže Twitter omezuje tweety na 140 znaků a 20 nechává pro označení autora.

Stejně jako jiné sociální sítě, i Twitter pracuje s aplikacemi třetích stran. V roce 2012 jich bylo 50 000. Je také zranitelný vůči mnoha malwarům a phishingovým útokům cíleným na sociální sítě.
Twitter se už také sám o sobě stal cílem. V roce 2009 se více než 184 milionů uživatelů nemohlo přihlásit kvůli útokům DoS zacíleným na tuto stránku. Někteří komentátoři spekulovali, že byl Twitter cílem, protože stránka agresivně filtruje adresy URL a blokuje ty, které obsahují škodlivé tweety, čímž tvůrcům malwaru snižuje příjem. Někdy prohrajete, i když vyhrajete.

11.9 Tipy k zachovávání bezpečí na sociálních sítích

Podvodníci míří na sociální sítě, protože tam lidé tráví velkou část času stráveného online. Zde je několik tipů, jak zůstat na síti v bezpečí:

- Dávejte si pozor na to, co sdílíte. Neodhalujte své celé jméno, adresu, telefonní číslo ani školu, kam chodíte.

- Pohybujte se ve skupině osob vašeho věku. Pokud je vám 13, nepředstírejte, že je vám 19. Mohli byste se dostat do konverzací a diskuzí, které vám budou nepříjemné, protože na ně ještě nejste úplně emocionálně zralí.

- Nesdílejte nic, o čem byste nechtěli, aby to viděli vaši rodiče. Pamatujte si, že informace, které sdílíte dnes, vás mohou dostihnout, až budete žádat o stipendium nebo o zaměstnání.

- Seznamte se s nastavením soukromí sociální sítě, kterou používáte. Pak tato nastavení použijte!

• Ani když svůj profil zamknete a definujete své příspěvky jako soukromé, nepředpokládejte, že je nemůže nikdo vidět. Některé druhy malwaru se soustředí konkrétně na „soukromé“ stránky.

• Pamatujte si, že nejste sami, kdo má fotoaparát nebo webovou kameru. Sledujte všechny fotografie nebo videa, která sdílejí vaši přátelé, a na kterých můžete být.

• Nepřijímejte přátele podle toho, jestli se vám líbí jejich obličej, když je ve skutečnosti neznáte. Ta 16letá dívka, se kterou jste se seznámili online, může ve skutečnosti být 65letý muž.
• Nenechte se od nikoho přesvědčit, abyste udělali cokoli, co se vám zdá divné, nebo je vám to nepříjemné. To obzvlášť znamená cokoli souvisejícího s webovou kamerou. Nevhodná videa NIKDY nezmizí. Zeptejte se Paris Hilton...

• Nikdy se s nikým v reálném životě poprvé nesetkávejte o samotě. Je to možná jasné, ale také je to opravdu nejlepší způsob, jak odradit online slizouny. Nevystavujte se nebezpečným situacím, pokud to není nutné.

12. Přátelé, slizouni a piráti

– Obsah kapitoly

12. Přátelé, slizouni a piráti – 219

12.1 Seznamování se na síti – 220

12.1.1 Kde se slizouni na síti zdržují – 221

12.1.2 Jak se chránit před slizouny – 221

12.2 Lháři, slizouni a kyberstalkeři – 223

12.2.1 Lháři – 224

12.2.2 Slizouni – 224

12.2.3 Kyberstalkeři – 225

12.3 Monitorování Internetu – 226

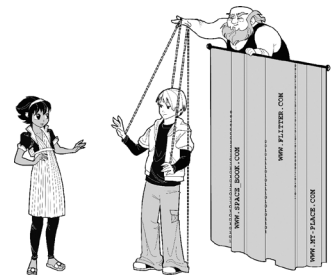
12.3.1 Monitorovací programy – 226

12.3.2 Bezplatné e-mailové účty – 227

12.4 Pirátství na informační dálnici – 228

12.4.1 Jste pirátem? – 229

12.4.2 Ohrožujete své rodiče? – 230



12. Přátelé, slizouni a piráti

Mindy, typická dospívající dívka z Michiganu, trávila hodně času na Internetu – hodně z toho se svými online přáteli. Během pěti měsíců strávila hodně času chatováním s „Georgem", online kamarádem z Londýna.

Jak se s ním postupně seznamovala (nebo si to aspoň myslela), zjistila, že George má problémy s penězi. Potíže s bankovnictvím, rodinné hádky – prostě komplikované věci související s britskými zákony o bankách. Měl samozřejmě spoustu peněz. Jen měl problém se k nim dostat. Mandy mu mohla pomoct. Musela jen vybrat hotovost na pár peněžních poukázek a poslat ji zpátky Georgovi. Samozřejmě si mohla pár stovek dolarů nechat za práci.

Peněžní poukázka je jako bankovní šek a používají ji lidé, kteří nemají šekový účet. Peněžní poukázku si můžete koupit za hotové na jakékoli poště a ve většině obchodů se smíšeným zbožím. Peněžní poukázky používá hodně lidí. Někteří internetoví prodejci k platbě vyžadují peněžní poukázky, protože je bezpečnější od cizího člověka přijmout peněžní poukázku než šek. To proto, že za peněžní poukázku se platí hotově. Nemůže se vrátit neproplacená jako šek, pokud na bankovním účtu majitele není dostatek peněz ke krytí šeku.

Protože Mindy věděla, že bankovní poukázky jsou bezpečné, a chtěla pomoct kamarádovi, souhlasila s tím, že na ně vyzvedne hotovost. Naštěstí pro ni si pošta hned všimla, že jsou peněžní poukázky falešné. A ještě větší štěstí měla, že se rozhodli stíhat George místo toho, aby obvinili ji.

„George" samozřejmě věděl, že všechny peněžní poukázky, které Mindy podstrčil, jsou padělky. Jeho pravé jméno pravděpodobně ani nebylo George. A asi nežil v Londýně. A žádná z těch stovek podrobností z jeho života, které Mindy za posledních pět měsíců řekl, asi také nebyla pravdivá. Ve skutečném životě mohl George klidně být 60letou ženou stojící v čele gangu padělatelů z východní Evropy. Jediné, co teď Mindy o Georgovi ví jistě, je, že je to slizoun.

Na Internetu se bohužel pohybuje hodně podvodníků. Podle poštovního inspektora Freda Van De Putte je podvod s peněžními poukázkami poměrně častý. Další online kriminálníci jsou zloději identity. Jejich cílem je poznat vás dost dobře na to, aby vám ukradli identitu, když se nedíváte. Další slizouni jsou ještě horší – pedofilové předstírající, že jsou teenageři, aby mohli ulovit další oběť.

Aby se z vás nestala oběť, musíte si být vědomi toho, co víte a co nevíte o svých známých na síti. A co byste jim sami měli nebo neměli říkat.

12.1 Seznamování se na síti

Internet je úžasný nástroj na to, abychom zůstávali v kontaktu se starými přáteli a poznávali nové lidi, kteří sdílejí naše zájmy a cíle. Kde jinde byste našli celou komunitu lidí, kteří milují stejnou hudbu, fanoušků soutěže *American Idol (Česko hledá Superstar)* nebo dokonce uklidňující podporu od dalších dospívajících s nadváhou či děvčat bojujících s vnímáním vlastní postavy? Dospívajícím v nesnázích Internet poskytuje mnoho příležitostí pro zdánlivě anonymní pomoc s vážnými problémy, o kterých se bojí nebo stydí mluvit doma.

Problém je v tom, že lidé, kteří nabízejí pomoc, nejsou vždy těmi, za koho se vydávají. „Dospívající" kamarád, se kterým si opravdu můžete promluvit o svém životě, možná ani není dospívající. Jen se zeptejte Amy, 14leté dívky ze Seattlu. Amy měla problémy s rodinou a byla nadšená, když na síti našla jiného dospívajícího, který chápal, čím prochází. Po mnoha měsících, kdy si navzájem online vylévali srdce, jí 14letý Carl nabídl, že jí pomůže utéct. Amy zahodila veškerou opatrnost (a zdravý rozum) a připojila se ke Carlovi v autobuse směrem do Missouri. Čím déle však cestovali, tím větší měla Amy o Carlovi pochyby. Během krátké zastávky na cestě se naskytla příležitost prohledat Carlovi peněženku. Zjistila, že 14letý Carl se ve skutečnosti jmenuje Robert a je mu 27. Zázrakem se jí podařilo utéct a vrátila se zpět k rodičům. „Carl" pravděpodobně dál loví své oběti. K velkému znechucení Amy i jejích rodičů nebyl nikdy z ničeho obviněn.

Amy dostala velmi tvrdou lekci, velmi nebezpečným způsobem. Dnes stále používá Internet, ale jen pod dohledem rodičů. Na dobu, kdy s Amy rodiče nejsou, nainstaloval její otec monitorovací program a pravidelně kontroluje, s kým a o čem Amy mluví.

Je příběh Amy neobvyklý? Ano a ne. Noví uživatelé Internetu často podstupují riziko a setkávají se s online přáteli osobně (**F2F,** Face to Face). Obrázek dospívajících vylévajících si srdce úplným cizincům je bohužel příliš obvyklý. Může se vám stát stejně hrozná věc jako Amy? Asi ne. Popravdě většina lidí, které na síti potkáte, jsou skutečně tím, za koho se vydávají. Ale pravdou je, že stejně tak jako existují slizouni ve skutečném životě, existují i na síti.

Skrývají se za každým druhým nickem? To těžko. Ale je jich dost na to, abyste potřebovali pochopit, jak snadno vám můžou lhát a skrývat se za digitální obličej, protože na ně nevidíte.

F2F Osobní setkání (z anglického „Face To Face", z očí do očí) s někým, s kým jste se seznámili online.

12.1.1 Kde se slizouni na síti zdržují

Panuje obecná představa, že slizouni tráví svůj online čas na pochybných chatech a v nechutných online komunitách. To může být pravda, ale to rozhodně nejsou jediná místa, kam chodí. Zkušení podvodníci a pedofilové hledají snadné cíle. Čím naivnější jejich kořist je, tím vyšší mají šance.

Mějte to na paměti, až zase budete chatovat online a nepředpokládejte, že všichni návštěvníci „neškodných" fór jsou sami také neškodní. To byla přesně chyba, kterou udělala 14letá Amy. Když vysvětlovala, proč Carlovi uvěřila jeho online identitu, řekla: „Protože to byl chat pro křesťany, předpokládala jsem, že tam budou hlavně křesťané. Takže to bude jako normální konverzace s lidmi." Pedofilové obvykle na svých online profilech nemají vytetované slovo SLIZOUN. Také dbají na to, aby chodili tam, kde najdou nejvíce zranitelné dospívající. Nebuďte překvapení, když je najdete v chatových místnostech souvisejících s církvemi, online náboženských komunitách, skupinách se skautskými tématy, sociálních sítích a na jiných „prospěšných" fórech pro dospívajících.

12.1.2 Jak se chránit před slizouny

Seznámit se na síti s novými lidmi je snadné. Vaši přátelé vás představí svým přátelům, ti zase svým a tak dál. Než se nadějete, bude vaše digitální síť OBROVSKÁ. Mluvit s lidmi na síti se vám může zdát snadné, protože se cítíte v bezpečí. Nesedí před vámi nikdo, kdo by soudil, jak vypadáte, mluvíte, chodíte nebo jak si češete vlasy. Setkávání s lidmi na Internetu však nikdy neberte na lehkou váhu. Pokud tu osobu neznáte ve skutečném životě, netušíte, kým skutečně je. Můžete si dokonce s novými přáteli připadat „napojení", ale nesmíte zapomenout, že někteří lidé na Internetu lžou.

Důležitou otázkou, kterou si musíte položit je, o čem se lže? A také jak velké lži to jsou? Přiznejme si, že na Internetu lidé lžou o mnoha různých věcech. Nejvíc o věku a pohlaví. Ta sexy holka, kterou váš kamarád balí, může být klidně 40letý muž.

Mít se na Internetu na pozoru před predátory vyžaduje selský rozum a několik opatření:

• Nesdílejte osobní informace.
To zahrnuje vaše celé jméno, domácí adresu a telefonní číslo domů. Ať už mluvíte na online fóru, na skupinovém chatu nebo v nové skupině na síti Facebook, pořád musíte udržovat své osobní údaje v tajnosti.

• Nepodílejte se na konverzacích, které jsou vám nepříjemné.
Pokud se diskuze zvrhne k tématu, ze kterého se vám dělá husí kůže, odhlaste se a již se tam nepřihlašujte. Pamatujte si, že Internet, stejně jako telefon, je tu pro vaše pohodlí. Jen proto, že s vámi lidé chtějí mluvit, nemáte povinnost jim odpovídat. Většina online komunit poskytuje způsob, jak konkrétní členy blokovat. Pokud si povídáte s novým přítelem na síti Facebook nebo MySpace a konverzace vám začne být nepříjemná, zrušte schválené přátelství. Pokud používáte IM zprávy, můžete uživatele, se kterými nechcete mluvit, zablokovat. Dokonce i v emailu můžete do filtrů SPAMU přidávat adresy a váš emailový program pak zprávy z těchto adres hodí automaticky do koše.

• NIKDY netolerujte obtěžování.
Pokud se z nepříjemných konverzací začne klubat obtěžování, řekněte to svým rodičům a společně danou osobu nahlaste úřadům. Kyberšikana a její ďábelský bratranec kyberstalking jsou trestné činy. Není to nic, s čím byste se museli smířit.

• Pokud se s vámi někdo, koho jste potkali online, chce setkat ve skutečném životě, řekněte to rodičům.
Setkávat se osobně s lidmi, které jste potkali na síti, není vždycky špatné a nepříjemné. Jak víme z online seznamek, někteří lidé tímto způsobem opravdu najdou lásku na celý život. Možná dokonce i váš učitel. V roce 2008 se na střední škole v New Oxford konalo několik svateb mezi učiteli, kteří našli svůj protějšek na stránce Match.com.

Někdy se lidé, kteří se potkají online, navzájem inspirují ke službědruhým. Před několika lety se zaměstnankyně mateřské školky v Gettysburgu, Paula, nechala inspirovat svou novou online kamarádkou a založila místní pobočku Projektu Linus. To je charita, která dětem v nouzi poskytuje zdarma doma vyrobené přikrývky. Její členové se scházejí, vyrábějí deky a poté je roznášejí na pohotovosti, do útulků pro bezdomovce apod. Je to jedna z několik skupin, které rozdělovaly přikrývky dětem evakuovaných kvůli hurikánu Katrina v roce 2005 a poté obětem zemětřesení na Haiti v roce 2010.

Stejně jako Paula, vaši rodiče budou mít daleko lepší představu o tom, zda je bezpečné osobně se setkat s někým, koho jste poznali online. Když nic jiného, budou lépe připravení ověřit identitu té osoby. Paula to udělala. Na rozdíl od mnoha dospívajících (kteří se v nových společenských situacích často cítí nepříjemně), Paule nebylo trapné zavolat úřadům spravujícím Projekt Linus a zeptat se na ženu, se kterou se chtěla setkat.

Pokud se opravdu chcete sejít s někým, koho „znáte“ online, vezměte ověřování této osoby stejně vážně. Pokud tvrdí, že jsou aktivními členy církevní skupiny v sousedství, zavolejte pastorovi a zeptejte se ho, zda je to pravda. Pokud se jedná o sestry a bratry skauty, zeptejte se vůdce jejich oddílu. Existuje spousta způsobů, jak si ověřit, že je někdo skutečně tím, za koho se vydává. Rodiče vám v tom mohou velmi pomoct.

• Vůbec NIKDY, NIKDY se s nikým poprvé nesetkávejte F2F o samotě.
Je to možná jasné, ale je to pravděpodobně nejlepší způsob, jak odradit online slizouny. Nevystavujte se nebezpečným situacím, pokud to není nutné.

12.2 Lháři, slizouni a kyberstalkeři

Většina dospívajících se Internetu nijak nebojí. To je dobře. Bát se Internetu by bylo jako bát se chodit do školy, do nákupního centra nebo na návštěvu ke kamarádovi. Nemůžete žít ve strachu. Zároveň si v životě musíte být vědomi svého okolí, chránit se a musíte přijímat správná rozhodnutí. Stejnou opatrnost a správná rozhodnutí musíte přijímat, i když jste online.

12.2.1 Lháři

Většinu z nás odmala učili, že lhát je prostě nepřijatelné. Stejně nás ohromuje počet dvanáctiletých, které známe, a kteří lhali, aby se mohli přihlásit k sociálním sítím. Všechny velké sociální sítě včetně služeb MySpace a Facebook vyžadují věk uživatelů alespoň 13 let. To je bezpečnostní opatření vycházející z toho, že dvanáctiletí často nemají sociální dovednosti a zkušenost, aby se mohli chránit před online lháři.

Když tito dvanáctiletí lžou o svém věku, aby se mohli připojit k sociálním sítím, sami se stávají podvodníky. Přemýšlejte o tom, až budete hodnotit potenciální online přátele. Je tomu potenciálnímu příteli opravdu 14, jak tvrdí ve svém profilu? Možná. Ale stejně tak mu může být 11 nebo 47. To se nedá poznat. Pokud vaše vlastní datum narození není přesně takové, jak udáváte, proč si myslíte, že je to u ostatních jinak?

12.2.2 Slizouni

Protože online fóra a sociální sítě umožňují lidem, kteří mohou být navzájem úplně neznámí, spolu opakovaně mluvit a opravdu se poznat, představují zvláštní riziko pro dospívající uživatele. Sexuální predátoři často tráví čas na webových stránkách, o kterých ví, že tam chodí dospívající, aby s teenagery navázali vztahy. Snaží se tato přátelství posilovat tím, že jsou příjemní a chápající a někdy nabízejí dárky. Za tyto dárky je nakonec potřeba zaplatit. Některé zprávy uvádějí, že téměř 20 % dětí ve věku 10 až 17 let na síti alespoň jednou dostalo neslušný návrh. Pedofilové spoléhají na anonymitu kyberprostoru, stejně jako na naivitu mladších surfujících. Jak vážný je problém sexuálního predátorství na síti? To záleží na tom, koho se zeptáte. Už v roce 2003 společnost Microsoft zavřela nehlídané chatové místnosti ve 28 zemích v Evropě, Africe, Asii, Latinské Americe a na Středním východě. Prohlásila, že se tyto chatovací místnosti „staly rejdištěm odesílatelů nevyžádané pošty a sexuálních predátorů." Chatovací místnosti v Americe zůstaly v provozu, ale přístup do nich byl umožněn jen registrovaným uživatelů služby MSN – lidem, jejichž identifikaci a platební informace společnost Microsoft znala.

Sexuální predátoři se bohužel neomezují na mezinárodní chatovací místnosti. Jen se zeptejte agentů ze skupiny Operation Blue-Ridge Thunder. Tato jednotka se zvláštním úkolem vznikla v roce 1997 na malém městě ve Virginii a věnuje se hledání sexuálních predátorů na síti. Agenti této služby navštěvují chatovací místnosti a online fóra a vydávají se za dospívající.

Důstojník Rodney Thompson tvrdí, že během dvou minut, kdy se jeden den vydával za 13letou dívku, ho oslovilo devět starších mužů. Od roku 1997 poskytla tato jednotka se zvláštním úkolem policejním složkám vodítka v případech více než 2 500 potenciálních pedofilů. Ještě děsivější je, že na jiných místech v zemi pracuje 46 podobných jednotek.

Většina predátorů naštěstí používá docela standardní přístup. Když víte, jak tito slizouni pracují, můžete se jim vyhnout. Pokud se dostanete do problémů, můžete je navíc nahlásit.

Chcete nahlásit slizouna?

FBI to zajímá. Vážně!

Přejdete na adresu www.fbi.gov a klikněte na odkaz **Nahlásit internetový zločin.**

Měli byste si také pamatovat, že ne všichni slizouni jsou staří úchylové. Když 16letá Celie dostala od online kamaráda zprávu, která obsahovala výhrůžky jeho spolužákům, neodbyla to tím, že by se prostě odhlásila. Zprávu si vytiskla a odnesla ji na policii. 17letý slizoun zjistil, že jsou jeho komentáře zveřejněny, a on sám je zatčený. Když policie prohledala jeho dům, našla zbraně a znepokojující nacistickou výzbroj. Častější je, že si dospívající jen stěžují a píší hloupé výhrůžky, které nikdy nemíní splnit. Vyhrožování online, i když to nemyslíte vážně, je však stejně nebezpečné, jako psaní výhružných dopisů. A taky stejně nelegální.

12.2.3 Kyberstalkeři

Kromě běžných slizounů a úchylů je Internet také domovem velmi malého, ale děsivého počtu lidí, kterým se říká **kyberstalkeři.**

> **Kyberstalker** Predátor, který používá Internet (chatovací místnosti, IM nebo e-mail) k obtěžování svých obětí.

Kyberstalking je technicky pokročilá forma klasického stalkingu. Při kyberstalkingu stalker používá online fóra, jako jsou herní fóra, sociální sítě a e-mail, k obtěžování své oběti. Stalking je častější, než si myslíte. Někteří odborníci tvrdí, že až 5 % dospělých bude někdy v životě obětí stalkingu. U kyberstalkingu nebezpečí nespočívá vždy v tom, co predátoři řeknou VÁM. Jde také o to, co řeknou O VÁS. V nedávných případech zveřejnili kyberstalkeři osobní informace (včetně adresy a telefonního čísla) na fórech spolu se zlovolnými lžemi, jejichž cílem

bylo poškodit pověst oběti. Falešná tvrzení o užívání drog a promiskuitě jsou poměrně běžná. I když pomluvu ignorujete, už to, že vás opakovaně kontaktuje a obtěžuje někdo, s kým nechcete mluvit, je samo o sobě dost nepříjemné.

Pokud máte pocit, že jste obětí stalkingu, je důležité to nahlásit policii. Mějte na paměti, že se to týká skutečného stalkingu. Je velký rozdíl mezi někým, kdo se vás snaží vtáhnout do neobvyklé konverzace, a někým, kdo vás pronásleduje a vyhrožuje vám. Od lidí, kteří vám lezou na nervy, se můžete snadno odpojit. Někdo, kdo provádí stalking nebo vám vyhrožuje, musí být nahlášen policii. Rozdíl poznáte.

Nebojte se špatné věci nahlásit. FBI bere online zneužívání vážně.

12.3 Monitorování Internetu

Vaši rodiče možná mohou mít obavy o to, s kým se na síti stýkáte. Pokud nemají, je to pravděpodobně proto, že si neuvědomují, kolik času na síti ve skutečnosti trávíte. Mnoho rodičů přehlíží skutečnost, že domácí počítače nejsou ani zdaleka jediným přístupem k Internetu, který jejich děti mají. Před několika lety byl přístup na Internet docela omezený. Dnes si mohou dospívající vybrat mezi domácím počítačem, počítačem jejich kamarádů, školními učebnami, knihovnami a internetovými kavárnami. Státní odpočívadla a dokonce i kempy dnes turistům nabízí přístup na Internet. Jak přesně říká Lawrence Magid z Národního centra pro pohřešované a zneužívané děti: „...děti nemusejí být při používání Internetu ve společnosti zodpovědného dospělého."

12.3.1 Monitorovací programy

Pokud mají vaši rodiče obavy, možná nainstalovali na váš domácí počítač program pro sledování pohybu na Internetu. Jestli to udělali, mohli si vybrat z mnoha možností – Parental Controls 2010, PC Tattletale, IAmBigBrother, Cyber Patrol, Safe Eyes, Net Nanny a podobně. Vaši rodiče mohou sledovat, jak Internet používáte, už za 29,99 USD (v přepočtu přibližně 600 Kč). Vaši rodiče ne? Tím si nebuďte tak jisti. Když je na trhu tolik produktů, něčí rodiče to určitě kupují!

Pokud se do své online identity ponoříte tak, že jste ochotni udělat nebo říct věci, které byste v reálném životě nikdy nedělali, měli byste se zamyslet nad tím, kým se stáváte. Možná je čas na chvíli odložit klávesnici a soustředit se na to, co je ve vašem životě důležité. Známky, vaše rodina, přátelé, kteří se počítají, a vaše budoucnost.

12.3.2 Bezplatné e-mailové účty

Jedním ze způsobů, které dospívající často používají, aby se zbavili dohledu rodičů, je sbírání **bezplatných e-mailových účtů.** Jedná se o webové e-mailové účty, které nejsou spojeny s poskytovatelem internetového připojení, a je k nim přístup z jakéhokoli počítače připojeného k Internetu. Hlavní služby poskytují společnosti Yahoo! (Yahoo! Mail), Microsoft (Windows Live Hotmail) a Google (Gmail).

Všichni vás sledují?

Pokud máte obavy, že vás rodiče sledují, a rozhodli jste se raději používat domácí počítač vašeho kamaráda, měli byste se zamyslet nad tím, že jeho rodiče ho možná sledují také.

Samozřejmě že dospívající nejsou jediní, kdo bezplatné účty používá. Již v roce 2008 překročil počet účtů na webové e-mailové službě Hotmail společnosti Microsoft 270 milionů. Některé z těchto účtů nepochybně mohly být spící účty (otevřené uživateli, kteří k nim zapomněli hesla, nebo účty prostě nikdy nepoužili). Stejně je ale počet skutečných uživatelů bezplatných účtů dost velký.

Bezplatný e-mailový účet Webový e-mailový účet, ze kterého je přístup odkudkoli, a který není svázán s poskytovatelem internetového připojení.

Jedním z dalších důvodů, proč používat bezplatné účty, je nepouštění SPAMu do „skutečného“ e-mailu. Mnoho online služeb vyžaduje, abyste zadali platnou e-mailovou adresu. Mít bezplatný účet je užitečné vždy, když máte poskytnout platnou e-mailovou adresu, a nechcete všechnu tu nevyžádanou poštu, která často následuje (dokonce i když zrušíte zaškrtnutí políčka „Ano, posílejte mi prosím další nabídky a informace!“). Používání bezplatného účtu vám umožňuje přesměrovat SPAM mimo důležitý e-mail vašeho poskytovatele připojení. Poskytovatelé bezplatných účtů také poměrně dobře filtrují SPAM, protože jsou zahlceni SPA-

MEM pro miliony svých uživatelů. To má několik výhod. Protože jsou bezplatné účty službami založenými na webu, neplýtváte připojením na stahování zpráv, které stejně jen smažete. Bezplatné služby také investují hodně času a snahy do udržování aktuálních filtrů SPAMu, aby se vyhnuly nejnovějším trikům, které spammeři používají. Identifikace všech klíčových slov apod. pro definici filtru ve vašem vlastním e-mailovém programu (jako je Outlook) by vám trvala mnohem déle. Mail služby Yahoo! tvrdí, že identifikuje 95 % SPAM zpráv, které okamžitě hodí do složky pro SPAM. Tu mohou uživatelé vyprázdnit, aniž by se na její obsah podívali.

Používat bezplatné účty kvůli boji se SPAMem nebo pro zkontrolování pošty z letního tábora může být užitečné. To se nedá říct o používání bezplatných účtů jako způsobu, jak se vyhnout monitorování Internetu. Samozřejmě je snadné vytvořit si účty na systému vašich kamarádů a používat bezplatné e-mailové účty na Internetu, aby vás rodiče nemohli sledovat. Ale jestli doma obcházíte kontroly používání Internetu, měli byste se sami naprosto vážně zeptat, proč to vůbec děláte.

Ať už používáte bezplatný e-mailový účet nebo domácí e-mail, musíte si pamatovat, že komunikace na Internetu není bezpečná. Neslušný e-mail, který jste smazali ze své složky s odchozí poštou, může na serveru poskytovatele vašeho připojení přežívat roky poté, co jste už zapomněli, co jste v něm napsali a proč. I webové stránky, které byly smazány už před stovkami let, pořád žijí na záložních páscích a v archivech vyhledávačů. Elektronická data nikdy nemizí. Jen je trochu složitější je najít. Proto byste NIKDY neměli psát e-mail, posílat IM zprávy nebo přenášet na Internetu obrázek, o kterých byste nechtěli, aby je viděla vaše matka. Pravdou je, že byste na Internetu nikdy neměli říkat ani sdílet nic, co byste nechtěli vidět na přední stránce časopisů *Wall Street Journal* nebo *National Enquirer!*

12.4 Pirátství na informační dálnici

Pokud si myslíte, že věk pirátů skončil krátce po éře rytířství, měli byste se zamyslet. Jen se zeptejte Asociace nahrávacího průmyslu v Americe. Na své webové stránce uvádí: „Dnešní piráti nepracují na divokém moři, ale na Internetu, v nelegálních továrnách vyrábějících CD, distribučních centrech a na ulicích." A největší krádeže se poslední dobou soustředí na Internet.

Babi?!!!

Dospívající jsou samozřejmě velkou součástí digitální generace, avšak nikoli součástí jedinou. V roce 2009 používalo Internet plných 38 % seniorů. Nový kamarád, kterého si nemůžete úplně zařadit, možná není váš spolužák – může to být vaše babička!

O tom byste měli přemýšlet, když se pokoušíte sdílet něco, co byste NIKDY neřekli u stolu při slavnostní rodinné večeři.

12.4.1 Jste pirátem?

Piráti nemusejí vždy vyrábět tisíce falešných disků CD v zemích třetího světa. Někdy si jen pro vlastní použití po jednom stahují písničky nebo filmy. Veřejnost se domnívá, že pokud si děláte kopie jen pro sebe a nemíníte je prodávat, nejste pirátem. Zábavní průmysl to tak nevidí. Pokud stahujete písničky nebo videa chráněná autorským právem, možná jste pirátem. Pokud používáte DVD vypalovačku ke zkopírování všech osobních videoknihoven vašeho kamaráda, tak jste pirátem určitě!

Nedávno se 14letý Mark ze San Francisca zeptal: „Proč bych měl platit za hudbu, když ji můžu mít zadarmo?“ Částečná odpověď zní: protože je to správné. A taky je to podle zákona.

Co je správné

Představme si, že s kamarády zakládáte novou kapelu. Můžete hrát heavy metal, pop rock, rap, country – cokoli, co vám jde. Váš kytarista Jamie má pro vás zvláštní výhodu. Jeho otec se živí jako producent hudby.

Nedlouho poté, co začnete, se vaše garážová kapela stane docela populární. Brzy vám Jamieho táta pomůže vydat vaše první komerční CD. Je to super! Dosáhli jste toho, o čem každá grunge kapela může jenom snít – máte hitovku a začínáte dostávat autorské poplatky. Měli jste velké štěstí, že? Pouze částečně. Museli jste HODNĚ dřít, abyste úspěchu dosáhli. S kapelou jste cvičili šest dní v týdnu, ne jen jeden. Málem jste se strhali, když jste pilovali texty.
Teď si představte, že se vaše CD objeví na všech stránkách, kde se stahuje hudba „zdarma“. Všichni vaši práci poslouchají, ale nikdo za ni neplatí. Jak by vám bylo? Nebylo by to správné, že?

Co je legální

Kdyby hudba, která se krade z Internetu, byla přímo vaše, asi byste byli dost naštvaní. Možná byste začali žalovat každého, koho byste při její krádeži přistihli. Tak asi takto se cítí celý hudební průmysl. Už jsou hodně unaveni z toho, jak se jejich příjmy kvůli stahování zmenšují, a začali požadovat, aby soudy potrestaly kohokoli, kdo se takto proviní.

Klíčovým slovem je zde KOHOKOLI. Hudební průmysl se samozřejmě soustředí především na zavírání hlavních pirátských továren v zahraničí. Ale jdou i po drobných pirátech doma. A k těm drobným pirátům patří i dospívající.

12.4.2 Ohrožujete své rodiče?

Když vyšla nová deska, mívali milovníci hudby jen dvě možnosti: všechno, nebo nic. Když jsme dospívali, často jsme si museli koupit celé nové album, i když jsme opravdu chtěli jen jednu písničku na něm. Je skvělé, že si můžeme koupit jednu písničku místo celého CD, nebo si můžeme stáhnout jen několik písniček a uložit si je na iPodu. Asi to zní ještě lépe, když je těch několik písniček „zadarmo".

Ve skutečném životě však moc věcí zdarma není. Ani stahování hudby, za kterou jste nezaplatili, k nim nepatří. Dopouštíte se tím krádeže na umělcích, kteří album nahráli. Tak zní zákon, a Asociace záznamového průmyslu v Americe (RIAA) a Filmová asociace v Americe (MPAA) už s praxí ztrácejí trpělivost. Není divu. V roce 2007 odhadovala MPAA, že její členové přicházejí kvůli internetovému pirátství o 3,8 miliardy USD (v přepočtu přibližně 76 miliard Kč) ročně.

Dříve si lidé mysleli, že trestným činem je jen udělat kopii, kterou chcete prodat. Díky snadnému stahování se však vyrábění vlastních kopií stalo tak běžným, že zábavní průmysl stojí celé jmění. Již mnoho let se prodej hudby a související zisky propadají nebo stagnují – jev, ze kterého mnozí viní všudypřítomné internetové pirátství. Když zisky trpí, lidé přichází o práci. Studie, kterou v roce 2007 provedl Institut pro inovaci předpisů, zjistila, že pirátství stojí americké pracovníky celkově 373 375 pracovních míst a 16,3 miliard USD (v přepočtu přibližně 326 miliard Kč) v ušlých ziscích ročně. Jestli si myslíte, že se vás to netýká, vezměte v úvahu, že daň z příjmů, daň z prodeje a podniková daň z těchto zisků by tvořily přibližně 2,6 miliard USD (v přepočtu přibližně 41,2 miliard Kč).

Když vláda přichází o zisky z daní kvůli pirátství, vynahradí si to na vyšších daních pro čestné lidi, jako jsou vaši rodiče.

Kvůli záchraně pracovních míst a zisků začali velcí hráči zábavního průmyslu tvrdě stíhat malé ryby. Jedním z jejich prvních cílů byla 12letá Brianna LaHara. Brianna žila ve státním bytě a těžko představovala typického člena velkého pirátského kruhu. Jako většina dospívajících si stahovala hudbu jen pro vlastní potřebu.

Tisk měl ze soudního procesu žně a věnoval se mu i Kongres. Při pozdějším soudním slyšení v senátu týkajícím se hudebního pirátství se jeden senátor předsedy asociace RIAA zeptal: „Míříte na základní školy, abyste pochytali typické podezřelé?" Pravdou ale je, že RIAA měla na své straně zákon, protože stahování nebo i jen kopírování materiálu dostupného ke stažení bez svolení jeho vlastníka není legální. I když Brianna nedostala obrovskou pokutu, která jí hrozila, stejně musela zaplatit 2 000 USD (v přepočtu přibližně 40 000 Kč). Jen si představte, kolik legálních CD si za to mohla koupit.

Nejčastěji kradené položky

Nejžhavější produkty, které se nelegálně stahují z Internetu:

- Hudba
- Filmy
- Programy
- Videohry

Brianna není ani zdaleka jediné dítě, které se stalo terčem kontrol. V roce 2005 byla Patti Santangelo z města Wappinger Falls ve státě New York šokovaná, když ji hudební průmysl zažaloval za pirátství. O svém případu informovala média a v národní televizi tvrdila, že ani neví, jak hudbu stahovat. Průmysl od žaloby upustil a poté zažaloval dvě z pěti Pattiných dětí. Když bylo v roce 2009 konečně dosaženo mimosoudní dohody, ani jedna ze stran nezveřejnila konkrétní sumu. Ale vsadíme se, že paní Santangelo nebyla z online pirátství svých dětí nadšená.

Může se zdát, že při pirátském stahování hudby o nic nejde, ale pokud vás chytí, může to vás i vaše rodiče stát hromadu peněz. I když se většina z prvních mimosoudních dohod pohybovala mezi 2 000 USD (v přepočtu přibližně 40 000 Kč) a 7 500 USD (150 000 Kč), americký

zákon na ochranu autorského práva umožňuje udělit pokutu až 150 000 USD (3 000 000 Kč) za jednu písničku. Než si stáhnete další mix hudby, možná zvažte, jestli tohle „bezplatné“ CD stojí za riziko, kterému své rodiče vystavujete. Agentury RIAA a MPAA provinilce aktivně hledají. Nebuďte pro ně snadným cílem.

I kdybyste svým stahováním rodiče neohrožovali legálními riziky, určitě ohrožujete jejich data. Jak jsme si řekli dříve, stahování bezplatných souborů v sítích rovnocenných uživatelů s sebou nese velké riziko stažení spywaru, adwaru a jiných škodlivých kódů. Proč riskovat poškození počítače nebo peníze, které vám rodiče šetří na vysokou? Nestojí to za to.

13. Sportování s porty

– Obsah kapitoly

13. Sportování s porty – 235

13.1 Co je to tedy síť? – 235

13.2 Jak sítě komunikují – TCP/IP – 238

13.2.1 Adresy IP – 238

13.2.2 Datové pakety – 241

13.2.3 Potvrzení – 242

13.3 Volaný port – 242

13.4 Trochu více o šířce pásma – 244

13.5 Požární stěna – 244

13.5.1 Co je to tedy firewall? – 246

13.5.2 Překlad síťové adresy – 247

13.5.3 Jak mě firewally chrání? – 248

13.5.4 Nastavení firewallu – 249

13.5.5 Firewally zdarma – 250

13. Sportování s porty

Byl pátek večer, obvyklý čas hraní online her s kamarády ze školy. Douglas, 15letý chlapec z města Novato v Kalifornii šel – jako obvykle – od večeře hned k počítači.

Douglas hraje počítačové hry velmi rád. Vlastní všechny herní systémy na trhu. Ve své ložnici má dokonce dvě sestavy Microsoft Xbox 360, Sony Playstation 3 a Nintendo Wii. Není třeba zdůrazňovat, že čas tráví také hraním své oblíbené hry, *World of Warcraft*, na Internetu. Uprostřed hry se mu přerušilo spojení a herní stránka ho odhlásila. Na počítačové obrazovce začal zářit nápis:

```
Spojení ztraceno, vyčerpána šířka pásma!
```

Douglas byl naštvaný, že nemohl dokončit svou hru, a netušil, co ta zpráva znamená. Začal si říkat, jestli ho to neodhlásilo kvůli firewallu v síti jeho rodičů. Douglas firewall vypnul, vstoupil na herní stránku a znovu začal hrát svou oblíbenou hru. Tentokrát ho to neodhlásilo. Douglas se rozhodl, že nechá firewall vypnutý, když bude hrát na Internetu svou hru.

I když vypnutí firewallu připadalo Douglasovi jako dobrý nápad, v něm problém nespočíval. Ve skutečnosti vytvořil nový problém, protože vypnutý firewall otevřel hackerům dveře do domácí sítě jeho rodičů. Problém s připojením souvisel se sítí v Douglasově domě. Do domu opravdu neproudila dostatečná šířka pásma. V této kapitole si řekneme, jak si můžete šířku pásma zdarma otestovat. Budeme také hovořit o základech síťových spojení a o tom, proč jsou firewally zásadním bezpečnostním komponentem.

13.1 Co je to tedy síť?

Počítačová síť je skupina navzájem propojených počítačů. Někdy jsou fyzicky spojeny pomocí drátů, kabelů, telefonních linek nebo nějakou jejich kombinací. Někdy neexistuje žádné fyzické spojení, tak jako je tomu u „hot spotů“ a bezdrátových sítí. Ve všech případech jsou však počítače v síti spojeny způsobem, který jejich uživatelům umožňuje sdílet zdroje (jako jsou soubory) nebo fyzická zařízení (jako tiskárny).

Ve škole můžete díky školní síti vytvářet své seminární práce na počítači v jedné učebně, ale

výtisk si vyzvednout v jiné. Tak také mohou učitelé zadávat známky do počítače na svém stole, ale výtisky vysvědčení studentů si vyzvednout ve sborovně.

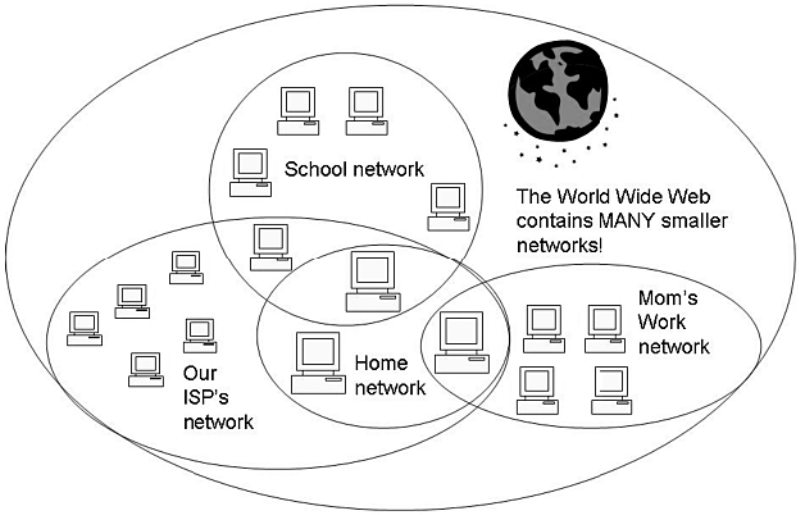
Počítačové sítě jsou známy už dlouho a pro komunikaci počítačů bylo vyvinuto několik technologií. Jednou z nejúspěšnějších je technologie zvaná **Ethernet,** kterou vynalezl Bob Metcalfe v roce 1973.

Ethernet Ethernet umožňuje počítačům na místní síti (LAN), jako je kancelářská budova, připojovat se k sobě navzájem a k dalším síťovým zdrojům, např. k serverům.

Dnes známe počítačové sítě mnoha typů a velikostí. Mohou být OBROVSKÉ. Velká univerzita může mít počítačovou síť spojující tisíce studentů, akademiků i personálu. Počítačová síť může také být docela malá. Vezměte si síť u Douglase doma. Ta spojuje jen tři počítače – Douglasův, mámin a tátův. Protože používají síťovou technologii, může celá rodina používat stejné připojení k Internetu a posílat soubory na stejnou tiskárnu.

Bez ohledu na svou velikost pracují všechny sítě v podstatě stejně a poskytují stejné funkce. To znamená, že všechny používají nějaký protokol, který počítačům a jiným zařízením umožňuje spolu komunikovat, a všechny poskytují sdílený přístup k síťovým zdrojům. Je také možné, aby některé zdroje v síti sdíleli jen někteří uživatelé. Proto vy posílat soubory na tiskárnu ve sborovně nemůžete.

Protokol Protokol je sada pravidel, které počítače používají ke vzájemné komunikaci.



Legenda: *Our ISP's network = Síť našeho ISP; School network = Školní síť; The World Wide Web contains MANY smaller networks! = Světová webová síť obsahuje MNOHO menších sítí; Mom's work network = Síť u mámy v práci.*

Svět je počítačových sítí doslova plný!

Jedna síť může zahrnovat celou jinou síť, nebo její část. Například počítač v domácí kanceláři vaší mámy je samozřejmě součástí vaší domácí sítě. Může být však také připojen k pracovní síti vaší mámy. A je také součástí sítě, která zahrnuje všechny přístroje používající stejného **poskytovatele internetového připojení (ISP).** A všechny tyto počítače jsou také součástí obrovské světové webové sítě (World Wide Web). Takže máme sítě uvnitř sítí v jiných sítích.

ISP Poskytoval internetového připojení (Internet Service Provider). To je společnost, která poskytuje síť umožňující vašemu počítači připojení k Internetu.

13.2 Jak sítě komunikují – TCP/IP

Být součástí sítě je jako být součástí komunity. V komunitě běží život hladce, pouze pokud spolu lidé tvořící komunitu komunikují. Aby spolu mohli členové dané komunity sdílet zdroje, musí spolu komunikovat způsobem, kterému všichni rozumí.

Počítačové sítě jsou skoro stejné. Aby mohly počítače sdílet zdroje, musí komunikovat společným jazykem. V počítačové terminologii se tomuto společnému jazyku říká protokol. Protokol je jen sada pravidel, které počítače používají ke vzájemné komunikaci.

TCP/IP je protokol nejčastěji používaný ke komunikaci na Internetu. TCP je zkratka slov „transmission control protocol", protokol kontroly přenosu. Když něco „přenášíte", někam to posíláte. „Přenos" je proto cokoli, co posíláte. TCP je tedy protokol řídící, jak se věci na Internetu přenášejí. Konkrétně protokol TCP pracuje tak, že data posílá v blocích zvaných pakety. (Když se data posílají přes Internet, jsou rozdělena do bloků dat nazývaných pakety). IP je zkratka pro „internetový protokol" a popisuje, jak si počítače tyto pakety dat navzájem posílají.

TCP/IP Protokol, který většina počítačů používá ke komunikaci na Internetu.

13.2.1 Adresy IP

Aby mohly pakety dat bezpečně cestovat z jednoho počítače na druhý, řídicí protokol musí vědět, kam pakety míří. Potřebuje adresu IP, kam má pakety posílat. Také potřebuje znát adresu, odkud pakety jdou, aby jí mohl poslat zpět odpověď dávající odesílateli vědět, že vše bezpečně dorazilo.

Tak jako má váš dům poštovní adresu, každý počítač má adresu IP. Každá adresa IP obsahuje čtyři skupiny čísel oddělené tečkami. Příkladem je adresa IP 192.168.1.1. Podle toho, jaký typ internetového připojení máte, a jak váš poskytovatel adresy přiděluje, můžete mít statickou nebo dynamickou adresu IP.

Statická adresa IP je vždy úplně stejná. Jako adresa vašeho domu. Tato adresa je přidělena, když se dům postaví, a zůstane stejná, dokud bude dům stát. Zatímco vaši poštovní adresu přiděluje pošta, adresu IP vašeho počítače přiděluje poskytovatel připojení, nebo ji mohou přidělovat nepřímo připojené počítače, pokud máte soukromou domácí síť.

Výhodou statické (neměnné) poštovní adresy je, že jakmile se jednou někdo vaši adresu naučí, bude ji vždy znát. U adresy IP je to nevýhoda. Jakmile se hacker naučí statickou adresu IP, vždycky bude vědět, jak se na daný počítač vrátit.

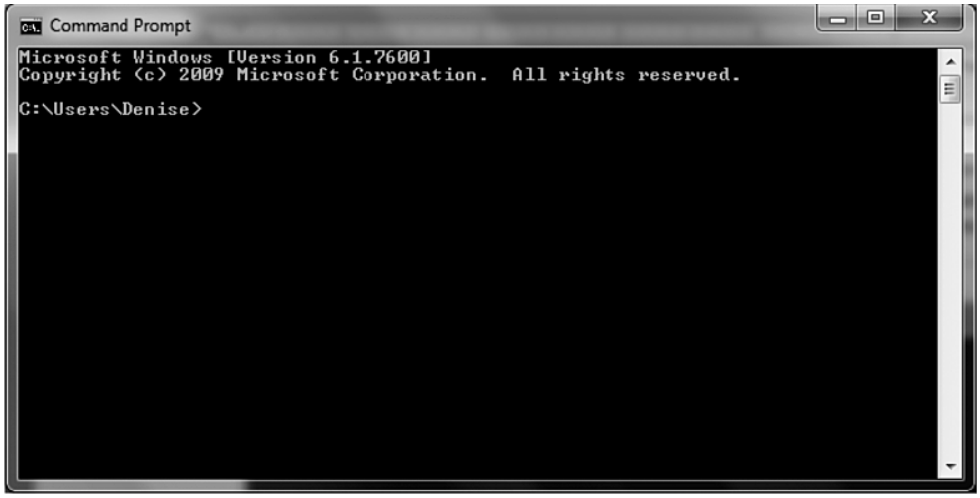
Dynamická adresa IP se vydává, když se kterýkoli den připojíte k Internetu, a tuto adresu si ponecháte, dokud nezavřete Internet nebo nevypnete počítač. Až se k Internetu připojíte příště, dostanete novou (a pravděpodobně jinou) adresu IP. Dynamické adresy IP vás pomáhají chránit před opakovanými útoky hackera, který se může do vašeho počítače snažit dostat. Váš ISP přiděluje dynamické adresy ze seznamu adres, které má k dispozici. Protokol, který řídí přidělování adres IP, se nazývá DHCP (dynamic host configuration protocol, protokol dynamické konfigurace hostitele).

DHCP Protokol dynamické konfigurace hostitele. DHCP je protokol, který poskytovatel připojení používá k přidělování dynamických adres IP.

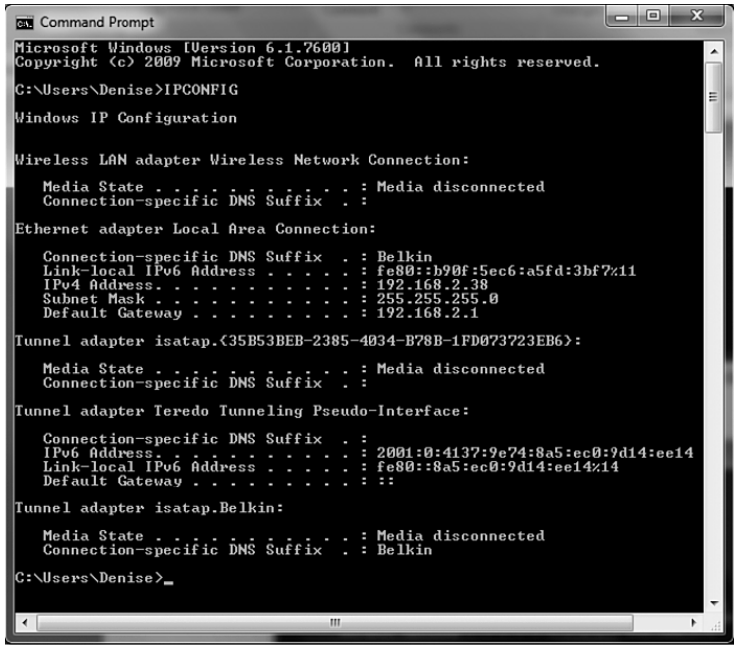
Zda máte adresu IP statickou nebo dynamickou, záleží na dvou věcech: (1) jaký typ internetového připojení máte a (2) jaké má váš poskytovatel předpisy.

Pokud máte připojení neustále aktivní a máte statickou adresu IP, útočníci mají větší šanci na vás úspěšně zaútočit. Je snadné pochopit, že když máte pořád stejnou adresu, je lehčí vás najít. To však neznamená, že by dynamické adresy IP byly bezpečné.

Pokud chcete zjistit adresu IP svého počítače, nejprve se ujistěte, že je počítač připojen k Internetu. Poté klikněte na volbu **Start > Všechny programy > Příslušenství > Příkazový řádek.** Otevře se okno s příkazovým řádkem.



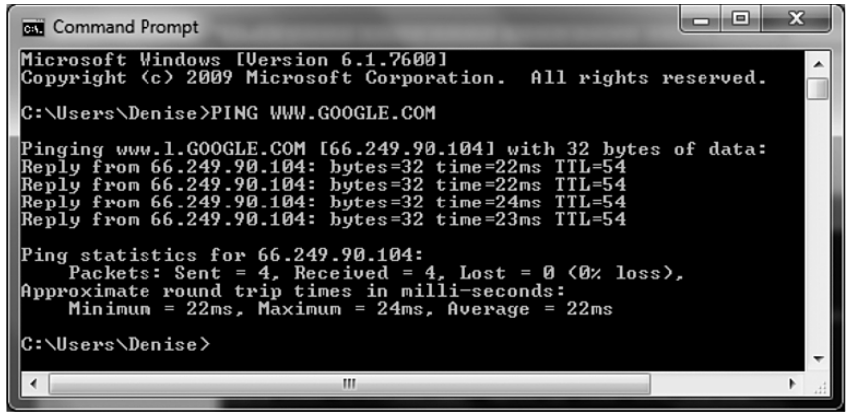
Na konec řádku **C:\...>** zadejte povel **ipconfig**. V okně, které se poté zobrazí, najdete vaši adresu IP.



Nyní vypněte počítač a router a opět je zapněte. Znovu se připojte k Internetu a podruhé zadejte příkaz **ipconfig**. Pokud je adresa, kterou dostanete, stejná jako poprvé, pak máte statickou adresu IP. Pokud se obě adresy liší, máte dynamickou adresu IP.

Pomocí příkazu **ping** můžete také zjistit adresy IP dalších počítačových systémů. Například ke zjištění adresy IP Googlu klikněte na položku **Start > Všechny programy > Příslušenství > Příkazový řádek** a znovu otevřete okno s příkazovým řádkem. Pak zadejte příkaz **ping www.Google.com.**

Dialogové okno, které se objeví, zobrazuje adresu IP stránky www.google.com pod textem **„Odpověď od“.**



Jak jsme právě řekli, adresa IP je podobná, jako adresa domu. Jakmile znáte domovní adresu, můžete zaklepat na dveře a možná se dostanete dovnitř. Když zjistíte adresu IP počítačového systému, v podstatě jste našli vstupní dveře. K ochraně vstupních dveří do vaší sítě potřebujete několik bezpečnostních vrstev včetně firewallu.

13.2.2 Datové pakety

Protokol TCP/IP pracuje tak, že rozdělí zprávy a soubory, které posílá po Internetu, do kousků zvaných pakety. Každý paket obsahuje část zprávy nebo souboru, plus adresu svého cíle.

Při tomto typu komunikace se počítačům posílajícím data tam a zpět říká hostitelé. Počítač posílající paket je zdrojový hostitel. Počítač přijímající paket je cílový hostitel.

Oba hostitelé používají stejný protokol, aby zajistili, že pakety dorazí bezpečně a ve správném pořadí.

Představte si, že posíláte knihu, kterou jste napsali, ze svého počítače na počítač vašeho učitele. Když posíláte soubor obsahující knihu, kontrolní protokol napřed knihu rozdělí na malé části (pakety). I když jsou skutečné datové pakety podstatně menší, pro jednoduchost si představme, že se z každé kapitoly stane jeden paket. Pokud má kniha šest kapitol, dostaneme šest datových paketů. Každý paket by obsahoval oddělenou kapitolu plus adresu IP počítače vašeho učitele.

Kontrolní protokol by také přidal informace o pořadí (řekněme číslo kapitoly), aby byly kapitoly při zpětném skládání paketů do jednoho souboru na počítači vašeho učitele pořád ve správném pořadí. Tím se dosáhne toho, že první je kapitola 1, následuje kapitola 2 atd. Aby vše bylo ještě spolehlivější, kontrolní protokol na počítači vašeho učitele by poslal vašemu počítači zpět potvrzení, že pakety dorazily v pořádku.

13.2.3 Potvrzení

Ve skutečnosti existuje mnoho protokolů, které by počítače ke vzájemné komunikaci mohly používat. TCP/IP je jen nejobvyklejší. Některé komunikace místo něj používají protokol zvaný UDP. Většina internetových připojení však používá protokol TCP/IP, protože je považován za nejspolehlivější.

Protokol TCP je považován za spolehlivější, neboť při jeho použití počítač odesílající data obdrží potvrzení, že data byla úspěšně přijata. Protokol UDP potvrzení neposílá. Proto je protokol UDP rychlejší než TCP, ale není tak spolehlivý. V některých případech to nevadí. Potvrzení, že zásilka opravdu dorazila do cíle, je pro některé programy důležité, a pro jiné ne.

13.3 Volaný port

Zatímco IP adresa identifikuje obecné umístění vašeho počítače, konkrétní místa, kterými se do vašeho počítače data dostávají, jsou nazývána porty. Port si můžete představit jako dveře do vašeho počítače. Na rozdíl od domu, který má jen dvoje nebo troje dveře ven, váš počítač jich má 65 535. Některé z těchto portů jsou přiděleny konkrétním aplikacím. Například program

pro zasílání zpráv AOL Instant Messenger používá port 5190. HTTP, protokol používaný ke komunikaci na webových stránkách, pracuje s porty 80 a 8080.
Když říkáme, že některá aplikace používá konkrétní porty, máme na mysli, že daná aplikace používá servisní program, který tento port monitoruje. Program Instant Messenger tak provozuje službu, která si hlídá port 5190. U tohoto portu naslouchá příchozí komunikaci a odpovídá, když takovou komunikaci zjistí. Tyto služby si můžete představit jako vrátné. Čekají u dveří, až někdo zaklepe. Když někdo opravdu zaklepe (to znamená když se k portu dostanou data), vrátný (služba) postupuje podle pravidel (protokolu), který dostal, a rozhoduje se, zda má či nemá klepajícího pustit dovnitř.

Útočníci na Internetu pravidelně pátrají po počítačích s otevřenými (nechráněnými) porty. Tomu se říká **klepání na porty.** Abyste svůj počítač a jeho data chránili, musíte zajistit, aby byly vaše porty chráněny.

Klepání na porty Procházení Internetu a hledání počítačů s otevřenými porty.

Jak jste se dozvěděli dříve, některé aplikace pracují s konkrétními porty. Samozřejmě je k dispozici 65 535 portů. Přístup na port pro konkrétní služby můžete nastavit pomocí firewallu. Váš firewall pracuje jako vyhazovač v exkluzivním baru – má „seznam hostů“ a vidí, komu je na jakém portu povolen vstup. Proto firewall blokuje přístup k portům, které se nepoužívají pro konkrétní aplikace. Správně nakonfigurovaný firewall nepřijme připojení k portům, pokud k tomu nedostane výslovný pokyn. Abyste svůj počítač a jeho data chránili, musíte zajistit ochranu svých portů. Seznam portů a služeb je příliš dlouhý na to, abychom ho zde uváděli. Pokud se chcete podívat, které porty a služby jsou doporučeny, a které jsou považovány za rizikové, měli byste navštívit webovou stránku dodavatele vašeho firewallu. Jiné dobré místo, kde se můžete dozvědět o portech a službách, je stránka www.grc.com.

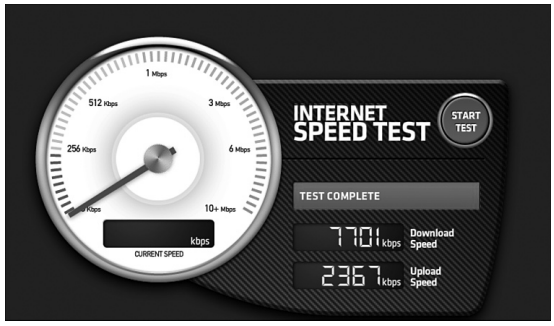
Zatímco si budete o firewallu zjišťovat více, jednoduchým krokem chránícím váš počítač je prostě počítač i router vypnout, když je nepoužíváte. Přemýšlejte o tom. Hackeři vědí, že mnoho domácích uživatelů nechává kvůli pohodlí své systémy zapnuté a připojené k Internetu. Proto má smysl počítač a router vypnout, když nejste k Internetu připojeni.

13.4 Trochu více o šířce pásma

Šířka pásma je rychlost, se kterou se data posílají komunikačním kanálem. Šířka pásma měří, jak rychle váš počítač komunikuje s Internetem. Náš hráč Douglas byl odhlášen ze hry, kterou hrál přes Internet, když se na obrazovce objevil nápis *Vyčerpána šířka pásma*. Jako většina uživatelů, ani Douglas se nikdy nestaral o to, jakou šířku pásma má, dokud mu nedošla. Víte, jakou šířku pásma máte?

Když Douglas narazil na chybu s šířkou pásma, jeho máma se podívala na účet od kabelové společnosti a na webovou stránku kabelové společnosti poskytující připojení k Internetu. Platila za šířku pásma 3 megabity za vteřinu. Když ale zkontrolovala skutečnou šířku pásma, kterou dostávala, ukázalo se, že je k dispozici jen 1,7 megabitů. Platila za více, než dostávala. Když to vysvětlila svému poskytovateli připojení, okamžitě šířku pásma zvedl.

Pokud máte obavy z podobného problému, na Internetu existuje mnoho míst, kde si můžete zdarma provést test šířky pásma. Jednou z bezpečných stránek je www.bandwidthplace.com.



Vaše potenciální šířka pásma bude záležet na internetovém připojení, které máte.

13.5 Požární stěna

Když jste tuto knížku začínali číst, asi jste netušili, že máte na počítači 65 535 portů. Hlídání a blokování všech těchto dveří na počítači je jedním z nejdůležitějších bezpečnostních úkolů, které je třeba plnit. Už jsme mluvili o mnoha produktech a technikách, kterými můžete svůj

počítač chránit. Firewall je *jednou z dalších* důležitých vrstev obrany.
I když firewall naprosto nezbytně POTŘEBUJETE, je to jen jeden díl skládačky tvořící bezpečnostní ochranu. Použití firewallu **NEZNAMENÁ,** že nebudete potřebovat další bezpečnostní produkty, jako je antivirový nebo antispywarový program, pokud není váš firewall součástí souhrnného bezpečnostního balíčku. (Některé bezpečnostní produkty se snaží poskytovat úplné nebo téměř úplné řešení bezpečnostní problematiky spojením celého balíčku různých typů ochranných programů do jednoho produktu.)

Firewally chrání proti hackerům

K „narušení" dochází, když útočník převezme váš počítačový systém. K takovému únosu počítačů se používá mnoho různých technik. Hackeři se mohou do vašeho systému vloupat, v klidu si projít vaše soubory a přečíst si osobní údaje; mohou využít vaše zdroje, spustit útok odmítnutí služby (DoS) nebo ukrást vaše osobní či finanční informace. Firewally vám mohou pomoci v ochraně proti mnoha těmto útokům tak, že vás upozorní, když se bude vnější program snažit o přístup do vašeho počítače přes porty, nebo když se program spuštěný na vašem počítači pokusí o přístup na Internet.

Co firewally mohou a nemohou dělat

Firewally mohou chránit proti hackerům a dohlížet na dodržování bezpečnostních pravidel. Nemohou vás však donutit k rozumnému chování a nechrání proti vloženým odkazům.

Firewally dohlíží na dodržování bezpečnostních pravidel

Firewally také dohlíží na dodržování bezpečnostních pravidel a poskytují tak ochranu zevnitř ven. Knihovna má firewall. Vaše škola má firewall. I společnosti mají firewally. V každém z těchto příkladů je firewall pravděpodobně nastaven tak, aby blokoval přístup k určitým stránkám. Škola nechce, abyste navštěvovali stránky s nevhodným nebo obscénním obsahem, které by se vašim rodičům nemusely líbit. Vaše knihovna pravděpodobně blokuje přístup na bezplatné e-mailové účty. Mnoho knihoven to tak dělá, aby počítače určené k provádění internetového výzkumu nebyly neustále obléhány lidmi, kteří si kontrolují mail.

Ve všech těchto případech představují činnosti firewallu pravidla, která jsou zavedena z určitého důvodu. Pokud jste schovaní za firewallem a pokusíte se ho obejít, víte, že byste to neměli dělat. Možná však nevíte, že firewall může zaznamenat, co se pokoušíte udělat.

Firewally vás nedonutí chovat se rozumně

Jak víte, když přijde chůva na hlídání, neznamená to, že se budou děti chovat slušně. Možná nebudou skákat z oken, ale klidně mohou hrát až do rána hru Guitar Hero. Stejně jako chůva, také firewall zmůže jen něco. Dobrý firewall bude dohlížet na dodržování bezpečnostních pravidel, která jsou v něm nastavena. To obvykle znamená, že může blokovat určité stránky, nebo některým programům bránit v přístupu na Internet. Co dělat nemůže a nebude je nutit VÁS, abyste se chovali rozumně. Firewall nemůže nijak ovlivnit, co si v IM zprávách píšete s přáteli, které stránky navštěvujete (pokud nejsou konkrétně zablokované), ani jaké e-maily posíláte. Tyto věci, společně s vaším dalším chováním na síti, jsou závislé na vaší volbě, ne na firewallu.

„Posláním firewallů není dohlížet na vaše chování."

–Marcus Ranum, vynálezce prvního firewallu a bezpečnostní expert, který připojil k Internetu Bílý dům.

Firewally vás nechrání proti vloženým útokům

Firewally také nechrání proti „útokům vedeným pomocí dat". Tyto typy útoků jsou zahájeny útočným nástrojem nebo malwarem, který jste si nechtěně stáhli, nebo ho přijali jako nežádoucí přílohu v poště. Když tyto útoky přijdou ve formě malwaru, který se stáhl bez vašeho vědomí nebo svolení, někdy se jim říká drive-by stahování. Další podrobnosti o tom, jak se vyhnout drive-by stahování, najdete v **kapitole 3, Špatný „ware."**

13.5.1 Co je to tedy firewall?

Firewall je program, který chrání váš počítač (nebo celou domácí síť) tím, že kontroluje typ přenosů, který je mezi sítěmi povolen. V mnoha ohledech funguje firewall jako zámek na dveřích vašeho domu. Zámek na vstupních dveřích zabraňuje ve vstupu zlodějům, potenciálním útočníkům a slídivým sousedům. Sledováním přenosů na váš počítač a z něj a sledováním programů, které s počítačem komunikují, plní firewall do značné míry stejnou funkci. Pracuje jako zámek, který zavírá vchodové dveře vašeho domu před Internetem, a buď schvaluje, nebo zamítá požadavky programů na odesílání dat do počítače či sítě nebo zpět.

Firewall **Program kontrolující typ přenosů, které jsou mezi sítěmi povoleny.**

Neuvěřitelné je, že mnozí lidé nevědí, zda firewall používají. Někteří uživatelé ve skutečnosti firewall mají a ani o tom nevědí. Pokud je váš domácí počítač připojen k síti, možná už máte firewall zahrnutý v routeru. Router je fyzické zařízení, které řídí tok informací mezi zařízeními v síti.

Hlavní funkcí firewallu je kontrolovat přenosy z Internetu a na Internet. Vraťme se zpět do Douglasova domu. V jeho síti je kabelový modem Comcast připojen k routeru Linksys. Rodinné počítače se pak připojují k Internetu pomocí routeru Linksys. Jediným zařízením, které je viditelné z Internetu, je router. Rodinné počítače se „skrývají za routerem". Router předává (směruje) všechny informace, které prochází na Internet a z Internetu. Žádná informace se do žádného z počítačů v Douglasově domě nemůže dostat, aniž by před tím přešla přes router.

Protože router chrání přístroje, ke kterým směruje data, funguje jako velká vstupní cesta. To z něj dělá logické místo pro firewall.

Router Fyzické zařízení, které řídí tok informací mezi zařízeními v síti.

Router samozřejmě není JEDINÉ místo, kde chcete mít firewall. Měli byste také mít „osobní" firewall na počítači samotném. Osobní firewall vám umožní sledovat aplikace spuštěné na vašem počítači a omezit, kdy a zda mohou tyto programy posílat data na počítač nebo z počítače. Používání osobního firewallu také poskytuje druhou vrstvu ochrany pro případ, že hacker poruší firewall na routeru. Pokud máte firewall na routeru, hackeři, kteří poškodí firewall na routeru, mohou získat snadný přístup ke všem počítačům připojeným k tomuto routeru. Když přidáte osobní firewall, dostal se tento hacker pouze přes první obrannou linii.

13.5.2 Překlad síťové adresy

Jako první obrannou vrstvu potřebujete mít firewall v místě, kde je k počítači připojený Internet – tento připojovací bod je v routeru. Další důležitou vlastností je překlad síťové adresy (Network Address Translation, NAT). NAT vám umožňuje používat externě jiné adresy IP,

než které používáte interně. To pomáhá skrýt vaši vnitřní síť a umožňuje vašim domácím počítačům „skrýt se“ za routerem. Dříve jsme v této kapitole mluvili o tom, jak poskytovatel připojení uděluje adresu IP. **NAT router** vezme tuto přidělenou adresu IP a poté distribuuje vlastní interní adresy IP počítačům uvnitř domácí počítačové sítě. Z Internetu je viditelná pouze adresa routeru. Protože NAT router přiděluje své vlastní interní adresy IP, adresa IP každého počítače zůstane soukromá.

Nákupní seznam pro router

- Network Address Translation
- Vestavěný firewall
- Možnost Wi-Fi

NAT router Router, který používá překlad síťové adresy, aby zůstala adresa IP vašeho počítače v tajnosti a nebyla viditelná z Internetu.

Stejně jako operační systémy a velké aplikační programy, také routery mají známé bezpečnostní díry. Proto je vhodné aplikovat všechny záplaty nebo aktualizace, jakmile jsou k dispozici. U většiny routerů bude také zapotřebí změnit výchozí přihlašovací jméno a heslo a zkontrolovat aktuálnost firmwaru.

13.5.3 Jak mě firewally chrání?

Firewally mají dvě hlavní obranné funkce:

- Povolují nebo odmítají požadavky k odesílání dat z vašeho počítače a na něj.
- Monitorují požadavky na přístup k portům.

Povolování nebo odmítání dat

Když nastavujete firewall, můžete si vybrat dvě strategie: strategii výchozího povolení nebo strategii výchozího zakázání.

- Strategie ***výchozího povolení*** znamená, že jste firewall nakonfigurovali tak, aby povolil všechny hostitele nebo protokoly, které nejsou výslovně zakázány.

• Strategie ***výchozího zakázání*** znamená, že uvedete konkrétní protokoly a hostitele, kteří mají povolení přes firewall procházet. Všechno ostatní se zakáže.

Asi jste si všimli, že se od sebe tyto dva přístupy liší jako den a noc. Zatímco výchozí zákaz je omezenější a potenciálně robustní přístup, je mnohem těžší jej nastavit. Pokud nebudete svým definicím věnovat hodně práce, mohla by být strategie výchozího zamítnutí tak omezující, že by internetové připojení už nebylo použitelné. Výchozí povolení je samozřejmě mnohem jednodušší nakonfigurovat – v podstatě jen zablokujete známá nebezpečí a přidáte nové blokování, když vyjdou najevo nebezpečí nová. U výchozího povolení umožňujete všechno, dokud se neukáže, že je to nebezpečné. U výchozího zakázání neumožňujete nic, dokud se neukáže, že je to bezpečné.

Monitorování požadavků na přístup k portu

Firewally monitorují a regulují připojení k vašemu počítači a z něj tak, že se dívají na všechno, co se snaží o přístup k portu. Firewall si můžete nakonfigurovat tak, aby vás upozornil pokaždé, když se nějaká aplikace nebo protokol pokusí o přístup k portu.

Samozřejmě že port, který data vypouští ven, je může také vpustit dovnitř. Útočníci se často pokoušejí získat přístup do počítačových systémů tím, že napřed hledají otevřené porty. Abyste svůj počítač chránili před klepáním na porty, musíte firewall nakonfigurovat tak, aby monitoroval a možná i blokoval příchozí připojení. Útočníci vědí, že domácí uživatelé často nemají nainstalované firewally a nezřídka nechávají otevřené porty – dokonce i porty, na kterých běží citlivé služby. Pokud se chcete dozvědět víc o portech, službách a o tom, jak firewally fungují, dobrým místem na Internetu je stránka Steva Gibsona www.grc.com.

13.5.4 Nastavení firewallu

Technicky zdatní uživatelé se mohou prohrabat až k srdci firewallu a blokovat konkrétní porty nebo aplikace. Většina ostatních uživatelů by to raději nedělala. Naštěstí většina firewallů poskytuje flexibilitu rychlé a snadné instalace jednoduchým nastavením firewallu na vysokou,

střední nebo nízkou úroveň. Které nastavení je pro vás nejlepší záleží na tom, co na Internetu děláte.

Důrazně doporučujeme začít tím, že firewall nastavíte na vysokou bezpečnosti. Pokud budete potřebovat, můžete úroveň snížit na střední. (Nízká bezpečnost obvykle není dobrý nápad.)

Když nastavujete firewall, nezapomeňte na záznamy (logy). Záznamy z firewallu udržují přehled o tom, kdo a co se pokouší se systémem komunikovat. Je dobré vědět, kdo brousí okolo vašeho počítače – nebo se do něj pokouší nahlédnout!

13.5.5 Firewally zdarma

V posledních letech se firewally staly mocnějšími, důležitějšími a – což je pro mnoho uživatelů stejně důležité – levnějšími. Ještě lepší než levné – některé firewally jsou ve skutečnosti zdarma. Bezplatný firewall Zone Alarm si můžete stáhnout ze stránky www.zonelabs.com. I když mu chybí některé pokročilejší funkce, kterými jsou vybaveni jeho komerční příbuzní, svou práci zvládne.

Bohužel ne všechny bezplatné firewally odvedou dobrou práci. Jedním z často používaných firewallů, na které si musíte dávat pozor, je firewall zabudovaný do systému Microsoft XP. Tento firewall blokuje pouze vnitřní připojení; připojení směřující ven neblokuje. Firewally systémů Microsoft Vista i Windows 7 tuto chybu řeší a blokují jak příchozí, tak odchozí připojení. Abyste pochopili svou firewallovou ochranu, musíte vědět, jaký OS je na našem počítači spuštěný.

Dovnitř nebo ven?

Firewally systémů Microsoft Vista a Windows 7 blokují jak příchozí, tak odchozí připojení. Firewall systému XP blokuje jen příchozí připojení.

14. Zkuste to bez drátů!

– Obsah kapitoly

14. Zkuste to bez drátů! – 253

14.1 Už žádné dráty – 253

14.2 Co je to bezdrátové připojení? – 254

14.3 Nejste sami – 256

14.4 Zamknutí sítě WLAN – 259

14.4.1 Stahování nejaktuálnějšího firmwaru – 260

14.4.2 Změna hesla a uživatelského jména k routeru – 261

14.4.3 Změna výchozího názvu sítě – 262

14.4.4 Aktivace šifrování – 262

14.4.5 Další kroky – 264

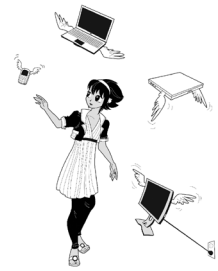
14.5 Veřejné hot spoty – 265

14.6 Mobilní zařízení – 266

14.6.1 Útoky na mobilní zařízení – 266

14.6.2 Sexting – 269

14.7 Stručně řečeno – 270



14. Zkuste to bez drátů!

Třináctiletý Michael byl štěstím bez sebe, když vyšel z prodejny Best Buy s novým notebookem v ruce. Notebook s nejvyšší rychlostí, nejlepšími funkcemi, za skvělou cenu a – což bylo nejlepší – připravený k bezdrátovému připojení. A tak se z Michaela brzy stal zloděj bezdrátového připojení.

Ještě než se s notebookem vrátil domů, zastavil se u svého kamaráda Juana. Několik vteřin poté, co vešel do dveří, už byl připojen na Internet přes router Juanových rodičů. A stejně to udělal v domě svého táty. Několik vteřin poté, co vešel, otevřel notebook a hned se nalogoval na svou oblíbenou herní stránku! Michael si bezdrátovou technologii okamžitě oblíbil. Zdálo se, že není nic snazšího.

Pak se Michael zkusil připojit k bezdrátové síti své nevlastní mámy. Smůla. Michaelova nevlastní máma si, na rozdíl od jeho táty a Juanových rodičů, dala tu práci a svou bezdrátovou síť zabezpečila. Nastavila heslo, definovala název sítě a aktivovala šifrování. Michael se nepřipojil. Myslíte? To se mýlíte. Hned se připojil k bezdrátové síti jednoho ze sousedů, který vysílal do širokého okolí.

Michaelovi sousedé si nestěžovali jen proto, že o tom nevěděli. Dál seděli doma, měli přístup na své oblíbené stránky, a vůbec netušili, že chlapec odvedle jim doslova krade šířku internetového pásma. Za méně než dvě hodiny se z Michaela, zpočátku trochu příliš nadšeného majitele nového notebooku, stal **zloděj bezdrátového připojení.**

Zloděj bezdrátového připojení Osoba připojující se k nezabezpečenému bezdrátovému připojení, které náleží někomu jinému.

14.1 Už žádné dráty

Možná jste jedním z milionů lidí, kteří se zbavují všech počítačových kabelů visících všude po domě. To je jeden z důvodů, proč se bezdrátové sítě vynořují na celém světě jako houby po dešti. Představují jednoduchý způsob, jak se připojit k Internetu bez klubek kabelů, z jakékoli místnosti v domě – dokonce i ze dvorku nebo zahrádky za domem. Bezdrátové připojení k Internetu se stává symbolem budoucnosti. Pokud jste ho ještě nezačali používat, brzy do uděláte.

Dnes už je těžké koupit nový notebook, který není vybaven bezdrátovým přijímačem (buď čipem nebo kartou).

Bezdrátový přijímač na počítači stále potřebuje k připojení na Internet přístupový bod, kterému se také říká „hot spot" – nemůžete se prostě připojovat do vzduchu. Jak bezpečná vaše síť asi je, a co uděláte pro to, abyste ji zabezpečili lépe, záleží do značné míry na tom, jaký hardware jste si koupili, a co může tento hardware a váš počítač nabídnout. Úroveň zabezpečení záleží také na tom, jak (a zda vůbec) tyto bezpečnostní vlastnosti nakonfigurujete. Mít bezpečnostní prvky je hezké, ale v mnoha případech je zapotřebí je ručně nastavit, aby bylo možné je vůbec používat.

14.2 Co je to bezdrátové připojení?

Tradiční počítačová síť používá k přenosu dat mezi fyzickými zařízeními (počítače, tiskárny atd.) v rámci sítě fyzické dráty, kabely a/nebo telefonní linky. **Bezdrátová síť** místo toho používá radiové vlny. Karta pro bezdrátové připojení ve vašem počítači je v podstatě dvousměrným rádiem, kterému se také říká přijímač-vysílač, a může přijímat a vysílat radiové signály.

Bezdrátová síť Počítačová síť, která používá radiové vlny k posílání a přijímání dat.

Existuje mnoho typů bezdrátových sítí. Máme obří bezdrátové sítě pokrývající stovky čtverečních kilometrů a poskytující bezdrátové připojení velkým městům (jsou to jiné sítě než ty, které používají mobilní telefony). Tak velké bezdrátové síti se říká MAN, což je zkratka anglického spojení Metropolitan Area Network – metropolitní síť. Když však mluvíme o bezdrátových sítích, ve většině případů máme na mysli sítě WLAN – **Wireless Local Area Networks** (bezdrátové místní sítě) nebo dokonce sítě WPAN – Wireless Personal Area Networks (bezdrátové osobní místní sítě). Protože mnoho lidí termín „PAN" nepoužívá, bezdrátovým osobním sítím v domech se často říká WLAN.

WLAN Bezdrátová místní síť.

Síť WLAN (jakékoli velikosti) pracuje tak, že používá radiový vysílací standard zvaný Wi-Fi

a standard IEEE 802.11. Wi-Fi (vyslov „vaj-faj“) je zkratkou anglických slov „wireless fidelity“ – doslova „bezdrátová přesnost“. Když to řekneme opravdu jednoduše, při používání bezdrátové sítě váš počítač odesílá a přijímá data pomocí radiových vln skoro stejně, jako při používání vysílačky. Hlavní rozdíl spočívá v tom, že vaše běžná vysílačka je neuvěřitelně pomalá. Protože většina lidí mluví dost pomalu, není to při přenosu hlasu problém. U mluvčích hovořících rychle, jako jsou například vyvolávači na dražbách, tomu tak vždy není. Zkuste do vysílačky něco říct opravdu rychle. Zjistíte, že čím rychleji mluvíte, tím hůře vám je na druhé straně rozumět. Počítače samozřejmě mluví DOST rychle. Posílají a přijímají data mnohem rychleji, než by to zvládl i ten nejlepší vyvolávač v aukční síni. Aby bezdrátové sítě s touto rychlostí udržely krok, používají zvláštní **standardní** způsoby, jak digitálně zakódovat odesílaná data, a tak umožnit rychlou a naprosto čistou komunikaci.

Standard Dokument zavádějící technické požadavky, které zajišťují, aby spolu mohla elektronická zařízení komunikovat.

IEEE, Institute for Electrical and Electronics Engineers (Institut pro elektrické a elektronické inženýrství), je mezinárodní skupina stanovující standardy používané ve většině oblastí komunikace. Jejich standardy zajišťují, že produkty vyrobené v různých společnostech spolu mohou komunikovat. Institut IEEE má ve skutečnosti několik standardů pro bezdrátové počítačové sítě založené na standardu Wi-Fi. K těmto standardům patří 802.11b, 802.11g, 802.11a apod. Všimněte si, že tyto standardy Wi-Fi mají společný začátek, čísla 802.11. To proto, že institut IEEE používá k „pojmenování“ standardů poměrně komplikovaný systém číslování. Díky tomuto systému číslování je těžké si názvy standardů pamatovat, ale snadno zjistíte, které standardy patří k sobě. Písmeno psané dolním indexem označuje verzi příslušného standardu. Například 802.11b je verze „b“ standardu 802.11.

IEEE Institute for Electrical and Electronics Engineers (Institut pro elektrické a elektronické inženýrství) Institut IEEE udává krok tím, že vytváří standardy pro počítačovou komunikaci.

Standardy Wi-Fi nastavují pravidla pro to, jak mnoho dat lze posílat v jeden okamžik, jakou rychlostí se data vysílají, jak daleko radiový signál dosáhne, jaké radiové spektrum se používá a jak komunikující zařízení řeší překážky, jako jsou zdi, kopce a zařízení jako mikrovlnné trouby.

Standard IEEE	Označení
802.11a	Tento standard poskytuje pouze polovinu přenosového rozsahu standardu 802.11b, ale pracuje s 5GHz radiovým spektrem, které není tak vytížené.
802.11b	Zařízení používající tento standard vysílají data rychlostí 11 megabitů za vteřinu a mohou posílat a přijímat data v dosahu přibližně 45 metrů.
802.11g	Zařízení používající tento standard také posílají a přijímají data v rozsahu 45 m, ale dělají to rychleji – při rychlosti zhruba 54 megabitů za vteřinu.
801.11n	Tento standard představuje vylepšení předchozích standardů o několik nových funkcí, včetně funkce multiple input multiple-output (MIMO, více vstupů a více výstupů).

V těchto (a dalších) oblastech spočívají konkrétní rozdíly mezi různými standardy 802.11. Celkově se však v domácnostech a hot spotech nejčastěji používají standardy 802.11b a 802.11g a většina Wi-Fi produktů nabízí standardy b, g, a n.

Když je bezdrátová síť v provozu, vytváří to, čemu se obvykle říká **hot spot**. Hot spot je oblast, ve které se můžete snadno připojit k bezdrátové síti. Pokud máte bezdrátovou síť spuštěnou doma, váš obývák je pravděpodobně hot spotem.

Veřejná místa nabízející bezdrátová připojení jsou také hot spoty. Hot spoty pravděpodobně najdete na většině letišť, v mnoha hotelích a téměř ve všech internetových kavárnách.

Hot spot Oblast, kde se můžete snadno připojit k bezdrátové síti.

14.3 Nejste sami

Pokud doma používáte bezdrátovou síť, nejste zdaleka sami. Bezdrátová připojení se rychle rozšiřují napříč většinou kontinentální části USA. Zatímco návštěvníci Seattlu s úžasem zírají

na věž zvanou Space Needle, pravděpodobně netuší, že se na jejím vrcholu brzy objeví anténa vysílající bezdrátové internetové připojení na část Seattlu o rozloze 13 čtverečních kilometrů. Jak velké mohou bezdrátové sítě být? Nová bezdrátová síť společnosti Microsoft, jejíž výstavba začala v roce 2005, má pokrývat až 1,5 milionu metrů čtverečních. Kromě mnoha jiných funkcí umožní tato bezdrátová síť až 25 000 připojení v jeden okamžik! To znamená, že síť bude moci používat 25 000 lidí zároveň.

Společnost Microsoft samozřejmě vždycky dělá věci ve velkém. Přesto mohou být bezdrátové sítě ještě větší. Australský poskytovatel internetového připojení Unwired, ve spolupráci se společností Navini z Texasu, staví kolem města Sydney bezdrátovou síť MAN pokrývající 3 100 kilometrů čtverečních a 3,5 milionu potenciálních uživatelů. Zatímco v největším městě Austrálie byste takové pokrytí čekali, asi byste je nehledali u farmářů na americkém venkově. Přesto jsou farmáři z okresu Walla Walla ve státě Washington součástí dokonce ještě větší

bezdrátové sítě – Wi-Fi hot spotu pokrývajícího 3 885 kilometrů čtverečních. To je větší rozloha, než jakou má celý stát Rhode Island!

Metropolitní síť (MAN) Bezdrátová síť pokrývající oblast velikosti středního nebo velkého města.

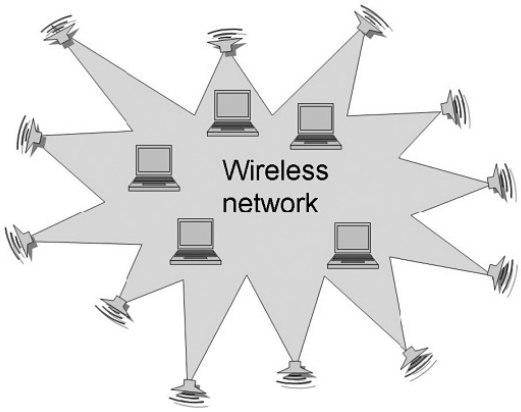
Protože jsou bezdrátové sítě určeny pro snadný přístup, jsou obzvláště zranitelné vůči útokům. V roce 2004 někteří analytici uvedli, že se již 30 % Wi-Fi sítí různých společností stalo cílem útoku hackerů. Jak uvedl Joe Kashi ve vydání časopisu *Law Practice Today* z listopadu roku 2005: „Hackování bezdrátových sítí je tak běžné, že se této praxi věnuje mnoho webových stránek a diskuzních skupin, z nichž si i člověk, který počítačům skoro nerozumí, může stáhnout dostatek volných programů k přemožení většiny malých bezdrátových sítí." Problém je dnes možná ještě horší a k dispozici je ještě více stránek a nástrojů.

Jak přesně se to dělá? Signály, které vaše bezdrátová síť vysílá, může přijmout jakékoli zařízení ve vašem dosahu. Hackeři to vědí a někteří dokonce brousí kolem – doslova projíždějí ulice komerčních oblastí – a hledají bezdrátové sítě. Počítačoví experti tomu říkají **war driving** (doslova válečná jízda). Tito váleční řidiči jen čekají na to, až jejich notebooky najdou nějakou bezdrátovou síť. V tom se moc neliší od našeho 13letého Michaela, který zdarma používá bezdrátovou síť svých sousedů.

(Michael samozřejmě nemusel ani vyjít z obýváku, natož jezdit po celém městě. Což je dobře, protože řidičák dostane nejdřív za pět let…)

War driving Populární způsob, jakým hackeři tráví volný čas. Jezdí po městě a snaží se najít bezdrátové sítě.

Bezdrátové sítě vysílají data všemi směry. Pomocí správných nástrojů může zdatný hacker tato data detekovat. Pokud používáte bezdrátovou síť doma, vaše data se také vypouštějí doslova do větru. Bez správného zabezpečení se může jakýkoli jiný počítač s bezdrátovým přijímačem ve vašem dosahu připojit k vašemu přístupovému bodu, někdy dokonce neúmyslně. Počítače mohou bezdrátové sítě v blízkosti detekovat automaticky. Tato funkce byla zavedena teprve nedávno a jejím cílem je usnadnit uživatelům připojování k místnímu hot spotu.



Bezdrátové sítě vysílají data VŠEMI směry!

Jak se bezdrátové sítě stávají běžnějšími, roste i počet jejich zlodějů. Zloděj bezdrátového připojení je osoba, která se připojuje k cizí bezdrátové síti bez svolení majitele – a obvykle aniž by o tom majitel vůbec věděl. Připojení může patřit důvěřivému sousedovi nebo nedaleké společnosti s nezabezpečeným přístupovým bodem.

Zloděj bezdrátového připojení si ani nemusí být vědom, že připojení krade. Bezdrátové karty mohou být nastaveny na volbu automatického připojení (neboli „spojení“) k jakékoli nechráněné síti. Pokud má někdo tuto funkci zapnutou a jeho vlastní síť přestane být k dispozici,

může se jeho počítač připojit k Internetu pomocí cizí sítě Wi-Fi, aniž by si toho byl jeho majitel vědom.
Michael, 13letý zloděj bezdrátového připojení, představuje příklad toho, jak snadné je připojit se k sousedově bezdrátové síti. Pokud jste si na své bezdrátové síti nenastavili zabezpečení, možná vám soused krade připojení právě teď. Nevíme jak vaši sousedé, ale naši se někdy pěkně vtírají. Raději bychom, aby se při připojování na Internet nelepili na naše sítě. Ani nechceme, aby šmejdili v naší internetové komunikaci. Naše komunikace je prostě – naše.

14.4 Zamknutí sítě WLAN

Abyste se chránili proti war drivingu a zabránili zlodějům bezdrátových sítí ve zneužívání vaší sítě, musíte provést několik kroků, kterými svou síť zamknete.

1. Stáhněte si nejnovější firmware pro svůj router.
2. Změňte uživatelské jméno a heslo routeru.
3. Změňte výchozí název sítě.
4. Aktivujte šifrování.

Všimněte si, že většina těchto kroků spočívá ve změně firmwaru nebo změně nastavení (konfigurace) bezdrátového **routeru.** Router je fyzické zařízení, které vytváří vaši domácí síť. V podstatě přesměrovává informace na správná místa v síti. Konkrétně to znamená, že vytváří připojení mezi vaším poskytovatelem internetového připojení (ISP) a počítači a zařízeními ve vaší domácí síti. (U některých bezdrátových karet je možné vytvořit „ad-hoc" bezdrátovou síť mezi dvěma počítači bez použití přístupového bodu, ale to nedoporučujeme a není tak možné zajistit bezpečnost nebo výkon, jaké zajišťuje přístupový bod.)

Router Fyzické zařízení, které řídí tok informací mezi zařízeními v síti.

Kromě připojení vašeho počítače (vašich počítačů) k Internetu router také počítače propojuje navzájem. Posílá informace z jednoho místa na druhé, nebo konkrétněji, z jednoho fyzického zařízení na druhé. Právě router posílá informace mezi vaším počítačem a Internetem nebo mezi počítačem vaší mámy v pracovně a tiskárnou fotek v obýváku. Stejně jako pošta používá adresy a směrovací čísla, aby doručila balíčky od jedné osoby osobě druhé, vaše data mají

adresu odesílatele i příjemce, které pomáhají dostat je z počítače tam, kam patří. V mnoha ohledech si router můžete představit jako pošťáka, který pomocí adresy na datech zajišťuje jejich doručení na správné zařízení a do správného programu.

Tradiční „drátový" router používá k přesunu vašich dat fyzické kabely a telefonní linky. Bezdrátový router místo toho informace ve vašem domě přesměrovává pomocí radiové frekvence definované standardem Wi-Fi, který používáte. I tak může používat telefonní linku nebo kabel ke komunikaci s vaším ISP. Nebo nemusí. Pokud máte satelitního ISP, může váš router ke komunikaci s ISP, stejně jako s počítači a jinými zařízeními u vás doma, používat radiové frekvence.

14.4.1 Stahování nejaktuálnějšího firmwaru

Bezpochyby už znáte pojmy hardware a software. Hardware je vše, čeho se můžete fyzicky dotknout. To znamená samotný počítač, tiskárna, digitální fotoaparát a disky CD. Software je instrukce, která hardwaru říká, co dělat. Na rozdíl od hardwaru, který se, jakmile je jednou složený, už fyzicky nemění, software je dynamický. Může se změnit, a to velmi snadno. Firmware je něco mezi hardwarem a softwarem. Tak jako software, i firmware sestává z počítačových programů, které počítači říkají, co dělat. Na rozdíl od tradičního softwaru však k firmwaru nemůžete snadno přidávat komponenty, ani je z něj odebírat. To znamená, že máte k dispozici pouze funkce poskytované verzí firmwaru, kterou právě používáte. Pokud chcete tyto funkce vylepšit, obvykle musíte provést upgrade na celý nový firmware, nestačí jen nainstalovat záplatu nebo přidat novou komponentu.

Firmware je pevnou součástí fyzických zařízení vašeho počítačového systému. Část firmwaru vašeho počítače, které se říká BIOS, vám umožňuje restartovat počítač a znovu nainstalovat software, i když si stáhnete virus, který vám úplně smaže pevný disk. Stejně jako počítač samotný, také váš router, který vytváří a spravuje bezdrátovou síť, má svůj firmware. Někdy se hackeři dostanou do systémů, jako jsou bezdrátové sítě, kvůli bezpečnostním dírám nebo nedostatkům bezpečnostních prvků ve firmwaru. Proto je velmi důležité, aby byl na vašem bezdrátovém routeru nainstalován nejnovější firmware. Musíte to ověřit i v případě úplně nového routeru, který jste právě rozbalili. Klidně se mohlo stát, že byl tento „nový" router odeslán do obchodu koncem minulého roku a několik měsíců seděl na polici vašeho oblíbeného obchodu s elektronikou.

Firmware může být zastaralý a od doby, kdyby byl router vyroben, mohli hackeři najít nové bezpečnostní díry.

Nikdy nezapomeňte zkontrolovat firmware svého routeru a webovou stránku dodavatele, abyste si byli jistí, že máte nejaktuálnější verzi. Prostě otevřete stránku dodavatele a najděte nejnovější firmware pro vaše zařízení. Nejjednodušší je vyhledat název vašeho routeru spolu se slovem „firmware." Při provádění upgradu postupujte podle pokynů společnosti, která router vyrobila. Důležité je stahovat firmware pouze z webové stránky původního dodavatele. Neinstalujte si firmware od třetí strany – např. ze stránky pro stahování bezplatných programů nebo z různých internetových fór.

14.4.2 Změna hesla a uživatelského jména k routeru

Tak jako mnoho důležitých fyzických zařízení, i váš router je vybaven ochranou heslem. Samozřejmě nechcete, aby kdokoli mohl měnit nastavení routeru a definovat, komu je povoleno používat vaši bezdrátovou síť.

Když si router přinesete v krabičce z obchodu domů, je na něm nastaveno výchozí uživatelské jméno a heslo. To je obvykle dost jednoduché, např. uživatelské jméno **Administrator** nebo **Admin** a heslo **System**. Kdokoli, kdo kdy viděl tento konkrétní router nebo pokyny k jeho instalaci, bude znát výchozí uživatelské jméno a heslo stejně, jako ho znáte vy. Protože nechcete, aby mohl kdokoli měnit nastavení vašeho routeru, musíte tyto výchozí údaje změnit, jakmile router vybalíte. Konkrétní pokyny najdete v uživatelské příručce, která by měla být k routeru přibalena. Nebo se můžete podívat na webovou stránku dodavatele.

V ideálním případě byste měli jako uživatelské jméno a heslo vybrat složitá slova nebo fráze. Nepoužívejte nic, co se jen vzdáleně podobá výchozím hodnotám. Jako uživatelské jméno nepoužívejte nic, co je naprosto zjevné. Obzvláště špatnou volbou je vaše jméno, váš oblíbený fotbalový tým, nejlepší online hra, kterou jste kdy hráli, a cokoli, co připomíná slovo **Administrátor** a **Admin.** U hesla postupujte podle pravidel pro výběr těžce prolomitelného hesla, které jsme probrali v ***kapitole 4, Hackeři a crackeři.***

Výchozí hesla a uživatelská jména…

…jsou pro hackery nejjednodušší cestou do vašeho routeru a pak k vaší domácí síti. Okamžitě je změňte!

14.4.3 Změna výchozího názvu sítě

Tak jako má každý počítač na webu jedinečnou adresu IP, každá bezdrátová síť má jedinečný název. Říká se mu SSID, což je zkratka anglických slov Service Set Identifier – Síťový identifikátor. SSID je jedinečný název sestávající z 32 znaků, který identifikuje vaši bezdrátovou síť a odlišuje ji od sítí v jejím okolí.

Protože váš bezdrátový router nemůže ve skutečnosti bez platného názvu SSID nic přesměrovávat, výrobce routeru nastavil jeho výchozí hodnotu. Výchozí názvy SSID pro všechny modely přístupových bodů – společně s výchozími uživatelskými jmény a hesly – jsou k dispozici online. Výchozí název může někdy hackerům pomoci identifikovat přístupový bod se známými bezpečnostními dírami. Abyste svou síť chránili před nečekanými návštěvníky, je dobré změnit výchozí hodnotu, jakmile router nastavujete. Měl by to být další krok poté, co jste změnili administrátorské uživatelské jméno a heslo routeru. Neměňte je však na nic, co je příliš zjevné, jako „Jirkova domácí síť" nebo dokonce vaše adresa, „Dlouhá ulice 143". Není žádný důvod takové informace zveřejňovat.

Ve většině operačních systémů změníte název SSID v rámci instalace bezdrátového routeru, pomocí administrátorského portálu routeru, nebo konfiguračního programu – ten je často přístupný přes webový prohlížeč. Konkrétní pokyny najdete v uživatelské příručce nebo v návodu od výrobce dodávaných společně s bezdrátovým routerem.

14.4.4 Aktivace šifrování

Když aktivujete šifrování, říkáte routeru, aby přeházel vaše data tak, že z nich neautorizovaní šmejdilové nebudou moct nic vyčíst.

V ***kapitole 8***, Bezpečné nákupy v kyberprostoru, jsme probrali typy šifrování používané k ochraně komerce na síti. Jiné, ale podobné typy šifrování se používají k ochraně dat vysílaných v bezdrátových sítích.

U bezdrátových sítí jsou možné tři typy šifrovacích metod, z nichž každá používá jiný bezpečnostní protokol.

WEP Wired Equivalent Privacy, soukromí odpovídající drátovým sítím

Tento standard je starý a v ochraně proti dnešním hackerům je k ničemu. Pokud je to nejlepší možnost, kterou máte k dispozici, musíte ji okamžitě změnit.

WPA Wi-Fi Protected Access, Wi-Fi s chráněným přístupem

Tato metoda šifrování používá protokol TKIP (Temporal Key Integrity Protokol, protokol integrity dočasného klíče). I když je mnohem lepší než WEP, má potíže s bezpečností adres, které mohou způsobit ohrožení vašich dat.

WPA2 Wi-Fi Protected Access 2, Wi-Fi s chráněným přístupem 2

Metoda WPA2 používá bezpečnostní protokol IEEE Advanced Encryption Standard (AES, Pokročilé bezpečnostní standardy). V současnosti je to nejlepší volba pro šifrování. Má však určitá hardwarová omezení, a se staršími zařízeními nemusí fungovat

Bez ohledu na to, zda si zvolíte metody WPA nebo WPA2, musíte definovat WPA-PSK. PSK je předem sdílený klíč, který se používá k šifrování (a následnému dešifrování) dat sdílených mezi vaším počítačem a bezdrátovým přístupovým bodem (vaším routerem). Když chcete používat šifrování, musíte definovat předem sdílený klíč. U většiny routerů se to dělá poskytnutím vstupní fráze, kterou router používá k vytvoření šifrovacího klíče.

Dobrou vstupní frázi, stejně jako dobré heslo, by mělo být těžké uhodnout a měla by obsahovat jak písmena a čísla, tak zvláštní znaky. Můžete začít s jednoduchou frází, třeba: „Skákal pes přes oves.“ Teď ji trochu vylepšíme tím, že všechny samohlásky nahradíme čísly. Změníme každé písmeno „a“ na číslo „4“, každé písmeno „e“ na číslo „3“ a písmeno „o“ na číslo „0“. Aby byla fráze ještě robustnější, přidáme na začátek a na konec věty nějaká interpunkční znaménka. Výsledek:

Místo: „Skákal pes přes oves."

máme:
„!*sk4k4l p3s pr3s 0v3s!!*".

14.4.5 Další kroky

Mnoho knih doporučuje další kroky k zabezpečení bezdrátové sítě. K těmto krokům často patří vypnutí vysílání SSID a omezení povolených síťových adres na specifické adresy MAC (filtrování MAC). Žádný z těchto kroků není nezbytný a ani je nedoporučujeme, protože k ochraně vaší sítě pomohou ve skutečnosti jen málo nebo vůbec.

I když máte identifikátor SSID vypnutý, síť lze ve skutečnosti snadno nalézt. Moderní operační systémy, jako Windows 7, umí detekovat přítomnost „skrytých" bezdrátových sítí. Kromě toho si i ten nejméně zkušený hacker může stáhnout jednoduché (a bezplatné) nástroje pro detekci nebo „vyčmuchání" síťové komunikace a detekci skrytých sítí.

Stejně tak používání filtrů MAC vaši síť nezabezpečí. Povolením přístupu k vaší síti pouze počítačům se specifickými adresami MAC (zřejmě tedy jen vašim počítačům) byste teoreticky mohli zabránit připojení neoprávněných osob. Ve skutečnosti může kdokoli vyčmuchat bezdrátovou komunikaci a zjistit, které adresy MAC jsou povoleny. Pomocí volně dostupného programu pak mohou povolené adresy MAC „zfalšovat". Zfalšováním se mohou vydávat za počítač, který je na vaší síti podle adresy MAC povolen.

Všechny tyto techniky se jen pokouší vaši síť skrýt. Zkušeného hackera žádná z nich neodradí, dokonce ani nezpomalí. Jen kvůli nim bude správa vaší sítě obtížnější a nebude pro oprávněné uživatele sítě příjemná. V závislosti na vašem routeru a objemu síťové komunikace může filtrování MAC také vaši síť zpomalit.

Někteří odborníci mohou namítat, že tyto techniky mohou příležitostným účastníkům war drivingu a zlodějům bezdrátových sítí zabránit v používání vaší sítě, ale přesně k tomu slouží šifrování. Až svou síť správně zabezpečíte pomocí jiných technik uvedených v této kapitole, nebudete si muset dělat starosti s jejím skrýváním.

14.5 Veřejné hot spoty

Čím je bezdrátová technologie levnější a oblíbenější, tím častěji se veřejné hot spoty objevují v kavárnách, hotelech, na letištích, v obchodech s knihami, řetězcích s rychlým občerstvením, a dokonce i ve vzduchu. Společnost Boeing staví letadla s bezdrátovými přístupovými body. V roce 2009 již některé společnosti začaly na vybraných trasách nabízet Wi-Fi připojení. Představte si letět ve výšce 10 000 metrů a mít notebook připojený k hot spotu.

Velkým problémem s veřejnými hot spoty však je, že pro snadné použití nepoužívají šifrování. To znamená, že pokud nepoužíváte šifrované webové stránky (https://), hackeři nebo odposlouchávači mohou číst vaši komunikaci.

S prováděním soukromých věcí na veřejném místě jsou vždy spojena rizika. Protože dospívající patří k těm, kdo technologie používají nejvíce, musejí si být těchto nebezpečí obzvláště vědomi a přijímat alespoň základní opatření pro vlastní ochranu.

Bezpečnostní tipy pro veřejné hot spoty

- **Buďte diskrétní.** Používat notebook na hot spotu je podobné, jako používat mobilní telefon uprostřed velké restaurace. Vaše konverzace nemusí být úplně soukromá. Neposílejte přes připojení nic, co byste nechtěli vidět na titulní stránce časopisu Wall Street Journal.

- **Své soubory si nechte pro sebe.** Vypněte sdílení souborů, aby neměli hackeři přístup k vašim souborům.

- **Držte krok.** Vždy mějte na počítači nainstalovány nejaktuálnější servisní balíčky a aktualizace pro svůj operační systém (který automaticky vypne sdílení souborů a nainstaluje kriticky důležité záplaty).

- **Pokud potřebujete, použijte VPN.** Pokud máte na notebooku citlivé údaje, měli byste při připojování k jakékoli síti používat soukromou síť (VPN), ať už používáte hot spot nebo ne.

- **Používejte stránky s protokolem SSL.** Posíláte jakékoli soukromé nebo citlivé informace? Zkontrolujte si, že příslušná stránka používá protokol SSL.

Pozor na zlé dvojče...

Zákeřní hackeři používají ke vloupání do bezdrátových systémů techniku zvanou Evil Twin (Zlé dvojče). Útočníci nastaví svůj identifikátor SSID tak, aby odpovídal SSID nějakého veřejného hot spotu nebo bezdrátové sítě nějaké společnosti. Potom proti „skutečné" síti zahájí DoS útok, který ji v podstatě vyřadí z provozu. Řádní uživatelé ztratí připojení k této „opravdové" síti a neúmyslně se místo ní připojí k jejímu „zlému dvojčeti". Někdy se tomuto útoku říká „man in the middle" (muž uprostřed)! Občas se hackeři ani neobtěžují kopírovat název sítě a prostě poblíž ní nastaví přístupový bod s název jako „free Wi-Fi", aby lidi nalákali k připojení.

14.6 Mobilní zařízení

Notebooky už nejsou jediná zařízení, která lidé používají na bezdrátových sítích. Vlastně se na Internet můžete dostat s čímkoli jiným, než je notebook – zařízení PDA (Personal Digital Assistant, Osobní digitální asistent), BlackBerry, iPhone, iPad, Droid, organizátor, digitální fotoaparát a dokonce i starší mobilní telefony.

Některé z novějších mobilních zařízení v sobě dokonce kombinují funkce všech výše uvedených. Lidé, kteří hodně cestují, často spoléhají na své chytré telefony, které jim poskytují mobilní telefon, digitální fotoaparát, webový prohlížeč, přístup k e-mailu, MP3 přehrávač, sociální sítě a organizátor – to vše v jednom zařízení. I když tato zařízení poskytují funkce několika různých kusů vybavení v jednom, nesou s sebou také všechna jejich zranitelná místa.

Abyste zatrhli tipec nebezpečím ohrožujícím váš telefon, potřebujete ostražitost, selský rozum a ochranný program!

14.6.1 Útoky na mobilní zařízení

Hackeři začínají útočit na mobilní zařízení, konkrétně chytré telefony a PDA. Chytré telefony jsou obzvláště častým cílem, protože jen málo uživatelů myslí v souvislosti se svými mobilními telefony na internetovou bezpečnost.

Ale měli by. Na trh mobilních telefonů už vtrhlo několik dost odporných útoků. Jeden z těchto útoků přišel ve formě trojského koně skrytého v instalačním souboru oblíbené hry lákající uživatele, aby si ji stáhli do telefonu. Po instalaci hra do telefonu vypustila červa s názvem Cabir. Cabir nebyl naštěstí zhoubný – rozšířil se do dalších telefonů, ale po cestě nepůsobil téměř žádnou škodu.
Měl však nepříjemný vedlejší účinek spočívající ve spotřebovávání baterie, takže uživatelé skončili s vybitými telefony, které měly být ještě nabité.

Na konferenci Black Hat v červenci 2009 ukázali bezpečnostní odborníci publiku, jak se vloupat do iPhonu odesláním škodlivého kódu ve zprávě SMS, aniž by uživatel vůbec věděl, že se právě stal terčem útoku. Ačkoli společnost Apple rychle zveřejnila záplatu, takové útoky ukazují, jak rychle lumpové hledají chyby a vytvářejí škodlivé kódy, které nalezených chyb zneužívají.

Stejně jako počítače, které používají operační systémy Windows nebo Mac OS, i mobilní zařízení jsou řízena operačním systémem. Abyste své mobilní zařízení chránili před útokem, musíte vědět, jaký operační systém používá, a jak jej chránit. Kromě toho, že mobilní zařízení spoléhají na jiné operační systémy, než jejich větší protějšky notebooky, obvykle také používají jiné komunikační standardy. Většina dnešních mobilních zařízení používá pro přístup k jiným bezdrátovým zařízením, jako jsou tiskárny a jiné telefony, technologii Bluetooth. Většina chytrých telefonů (iPhone, Android, BlackBerry apod.) se může k Internetu snadno připojit prostřednictvím Wi-Fi přístupového bodu.

Bluetooth Otevřený bezdrátový protokol, který umožňuje výměnu dat mezi mobilními zařízeními na krátké vzdálenosti.

Zatímco mobilním zařízením zcela jistě hrozí útoky škodlivých kódů, hrozí jim také fyzické riziko, které jiným typům bezdrátové technologie nehrozí. Vzhledem k velikosti (a ceně) notebooků si na ně většina uživatelů dává velmi dobrý pozor. Stejní uživatelé však nemusí být stejně pečliví při hlídání svých mobilů. Už jsme viděli mobilní telefony zapomenuté ve školách, kavárnách a restauracích. Mnoha uživatelům také vyklouznou telefony ze zadních kapes a najdou si cestu pod gauč u přátel nebo pod sedadlo automobilu. Nezapomeňte si zálohovat data pro případ, že telefon ztratíte. Seznamte se s možnostmi zálohování vašeho zařízení, které jeho dodavatel poskytuje.

Populární mobilní operační systémy

- Apple iPhone
- BlackBerry
- Google Android
- Microsoft Windows Mobile

Abyste se chránili pro případ, že se váš telefon ocitne v nepovolaných rukách, potřebujete také dost obtížné heslo k ochraně jeho obsahu. Nedělejte stejnou chybu jako Paris Hilton. Paris Hilton, která se nikdy nesnažila opravdu chránit své osobní informace, v roce 2004 zjistila, že její PDA adresář i s fotografiemi zveřejnili na Internetu narušitelé, kteří se prolomili do jejího T-Mobile účtu a zjevně jí četli i e-maily. Jak získali její heslo? Stejně jako mnoho uživatelů, i Paris si vybrala slabé heslo. Zvolila si jméno svého psa. A samozřejmě každý, kdo byl někdy svědkem (ať už dobrovolným či nedobrovolným) jejích životních eskapád, ví, že Tinkerbell je její miláček. Vy si určitě najdete bezpečnější heslo!

Zálohujete si mobilní zařízení?

Zálohování počítače je asi jako používání dentální nitě. Všichni víme, že bychom to měli dělat, ale většina z nás tuto znalost neuvádí do praxe (nebo jen zřídka).

Až si příště „najednou vzpomenete", že musíte zazálohovat své počítačové soubory, nezapomeňte zazálohovat i mobilní zařízení. Stejně jako počítač, i váš mobil asi obsahuje důležitá data (adresář, schůzky apod.), které opravdu nechcete navždy ztratit.

Chloe dnes musela odejít z hodiny angličtiny, protože policie chtěla zkontrolovat její telefon. Chloe totiž před třemi měsíci poslala svou nevhodnou fotografii Kylovi. Včera, když se s ním rozešla, Kyle tuto fotografii přeposlal všem lidem v adresáři svého telefonu. Policie si prohlédla také Kylův telefon a telefon jeho přátel. Na chodbách se šeptá, že Kylea možná obviní z distribuce dětské pornografie. Byl středoškolským hráčem basketbalu a chtěl získat stipendium na vysoké škole. Teď se místo toho možná dostane do registru pachatelů sexuálních přestupků. Alespoň nikdo neviděl jeho choulostivá místa. Chloe vůbec neví, kdo všechno její fotku viděl. Říká se, že Kylův přítel Jon pomocí svého iPhonu nahrál fotku Chloe na stránku s amatérským pornem. Možná to Chloe nikdy nezjistí. I kdyby to chtěla zjistit, nemůže svou fotku dohledat.

14.6.2 Sexting

Nejhorší škodu někdy nenapáchají hackeři ani lumpové. Děláme si ji sami. Tak tomu určitě je v případě sextingu. Sexting je posílání obscénních nebo velmi odvážných fotografií elektronickým způsobem. To teoreticky zahrnuje nevhodné fotografie posílané e-mailem a programem pro IM zprávy. V praxi většina lidí slovem sexting myslí fotografie posílané mobilním telefonem.

Sexting Posílání nahých, polonahých nebo sexuálně vyzývavých fotografií MMS zprávami nebo přes Internet.

Se sextingem je spojeno několik zásadních problémů. Nejzjevnějším je, že děti, které tyto fotografie dnes posílají, budou nakonec ztrapněny a nebudou chápat, jako mohly kdy udělat něco tak hloupého.

Další problém se sextingem je, že úřady nevědí, jak k němu přistupovat. Vezměte si smutný případ, který jsme uvedli. Chloe a Kyle (což samozřejmě nejsou jejich pravá jména) jsou skutečné děti, které chodí na střední školu v malém městě ve státě Pensylvánie. Zákony Pensylvánie – tak jako ve většině států v USA – neposkytují prokurátorům jasné vodítko. Podle osobního přístupu místního prokurátora se v tomto případě může stát jedna ze tří věcí:

- Chloe a Kyle mohou dostat oficiální „napomenutí“ a jak se vypořádají se svým ponížením bude na nich.
- Kyle může být obviněn ze sexuálního obtěžování.
- Kyle i Chloe by OBA mohli být obviněni z šíření dětské pornografie.

Pokud dojde k poslední možnosti, oba dospívající mnohou skončit v pěstounské péči nebo zařízení pro nápravu mladistvých. Pokud budou usvědčeni, ani jeden z nich už nikdy nedostane vysokoškolskou půjčku, vysokoškolské stipendium, službu v armádě ani mnoho typů zaměstnání.

V tomto případě k sexuálnímu obtěžování jasně došlo, když Kyle fotografii přeposlal. Představme si ale, že by fotka zůstala jen mezi nimi dvěma. Podle zákona mnoha států by mohli být jako Kyle, tak Chloe obviněni z distribuce a přijímání dětské pornografie, I KDYŽ nikdo jiný fotku neuvidí. A Kyle s Chloe by zdaleka nebyli sami.

Nedávný výzkum ukazuje, že až 20 % dospívajících poslalo nebo přijalo nějakou formu sexuální zprávy. Je toto chování hloupé? Samozřejmě. Zaslouží si za to obvinění z trestného činu? To záleží na tom, koho se zeptáte. Andy Hoover, právní ředitel Pensylvánské kapituly Americké unie občanských svobod (ACLU) říká: „Děti se budou vždycky chovat nezodpovědně. Nejlepší způsob, jak to řešit, je vzdělávat je, ne jim dávat záznam do trestního rejstříku." Hoover samozřejmě není prokurátor a ne všichni prokurátoři s výkladem unie ACLU souhlasí. Jeden obzvláště horlivý oblastní prokurátor v Pensylvánii obvinil z trestného činu dětské pornografie dvě dospívající děvčata, která se vyfotila ve sportovních podprsenkách na pyžamové party. Je třeba dodat, že nabídl stažení žaloby, pokud budou děvčata souhlasit s účastí na sérii školení, která se mu zdála vhodná, napíší esej vysvětlující, proč bylo fotografování v podprsenkách nevhodné, a budou souhlasit s tím, že jsou v podmínce a v náhodných intervalech jim budou prováděny drogové testy. To jejich rodiče odmítli a místo toho šli k soudu.

I když dáme stranou kriminální stránku věcí (která je ale velmi důležitá), sexting představuje velké ohrožení soukromí z dlouhodobého hlediska. Fotografie mohou během vteřin migrovat z telefonu na web a zanechat tam digitální stopu na desítky let. Chcete riskovat, že se vaše pochybné fotografie z dospívání vynoří, až budete hledat práci? A co až budou za 10 nebo 15 let vaše děti na Internetu vyhledávat rodinnou historii kvůli školnímu projektu?

Krátkodobé soukromí je také ohroženo. Důrazně vám doporučujeme zařídit se podle rady 19leté Breeny Aguila. „Neudělala bych to. Nevěřila bych tomu klukovi, že je nikomu neukáže." Vy ano?

14.7 Stručně řečeno

Vzdát se drátů je pouze prvním krokem na cestě k bezdrátové bezpečnosti a svobodě. Svou novou bezdrátovou síť musíte také zamknout, aby zůstala bezpečná.

Změna hesla, stažení nejaktuálnějšího firmwaru, změna výchozího názvu sítě a aktivace šifrování jsou nezbytnými kroky na cestě k bezdrátovému životu. Ani poté neprovádějte finanční transakce na nezabezpečených sítích.

Pamatujte si, že většina veřejných hot spotů není bezpečná. Veřejné hot spoty jsou dobré na prohlížení Internetu a ke kontrole e-mailu, ale nikoli pro finanční transakce.

A nakonec musíte mít na paměti, že ne všechna bezdrátová zařízení jsou si rovna. Stejně jako vaší bezdrátové síti musíte věnovat pozornost i bezpečnostnímu programu pro svůj mobilní telefon a PDA. Hlavně si musíte uvědomovat nebezpečí a pamatovat na ně při rozhodování o tom, kdy a jak bezdrátovou technologii bezpečně používat.

- Přemýšlejte, než pošlete jakékoli zprávy telefonem. Textové zprávy nejsou vždycky soukromé.

- Nepoužívejte svůj telefon k útokům na druhé. To je druh kyberšikany.

- Netolerujte šikanující textové zprávy od druhých. Pokud vás někdo přes mobilní telefon obtěžuje, ponechte si záznam zpráv a promluvte si s rodiči. Možná bude zapotřebí obrátit se na úřady.

- Nepoužívejte telefon pro přístup k pornu, ani k posílání nahých fotografií nikoho jiného (přítele, nepřítele ani neznámého člověka). Mohli byste být obviněni z distribuce dětské pornografie a skončit v registru pachatelů sexuálních deliktů.

- Nezapomeňte, že vaši kamarádi také mají na telefonech fotoaparáty. Mohou pořídit videa a obrázky a poslat je na web bez vašeho vědomí. Pokud vaši přátelé pořizují nevhodné fotografie nebo videa, odejděte

15. Jak získat pomoc

15. Jak získat pomoc – 275

15.1 Nezbytné bezpečnostní prvky – 276

15.2 Další vychytávky – 277

15.3 Souhrnná bezpečnostní řešení – 279

15.4 Zálohovací produkty a postupy – 280

15.5 Nástroje pro odstraňování škodlivého kódu – 281

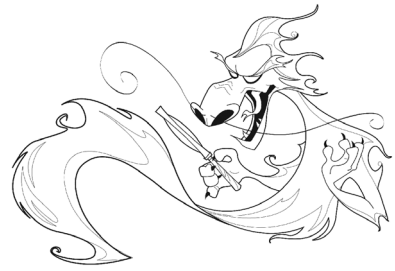
15.6 Dodavatelé bezpečnostních programů – 282

15.7 Aktualizování programu – 283

15.7.1 Nastavení automatických aktualizací – 283

15.7.2 Kupte si novou verzi – 284

15.8 Buďte v obraze, co se týče bezpečnost – 284



15. Jak získat pomoc

Tim, 16letý chlapec z města Los Gatos v Kalifornii, si na Internetu stáhl sadu nástrojů pro vytvoření vlastního viru. Tim se začínal věnovat programování a stejně jako většina dospívajících hledal, jak své znalosti vyzkoušet.

Díky soupravě pro vytvoření viru se Timovi v rekordně krátkém čase podařilo vytvořit vlastní virus. Samozřejmě ho nevypustil do oběhu. Nikdy se nechtěl stát záškodníkem. Jenom chtěl vědět, co by mohl udělat, kdyby chtěl. Opravdu nepřemýšlel jako zločinec.

A na to právě doplatil. Kdyby přemýšlel jako škodolibý hacker, napadlo by ho, že viry jsou opravdu hnusné kódy. I když se mu díky hackerským nástrojům podařilo vytvořit vir až směšně snadno, nezjistil nic o tom, jak se nového viru zbavit.

A výsledek? Aspirující hacker si úplně zničil počítačový systém. Mějte to na paměti, pokud budete v pokušení zkusit si vytvořit škodlivý kód nebo jen zveřejnit nepříliš zdvořilý záznam na blogu. Na Internetu, stejně jako v reálném životě, se vám téměř vždy vrátí zpět to, co uděláte.

Dosud každá kapitola této knihy začínala příběhem o bezpečnostních potížích nějakého dospívajícího. Kromě toho, že jsou tyto příběhy pravdivé, také ukazují, jak snadno se můžete stát obětí hackerů nebo škodlivého kódu, když není váš počítač chráněn správným bezpečnostním programem.

Od té doby, co se díky viru Michelangelo a jiným známým virům dostal koncept ochranného programu do povědomí veřejnosti, se nástroje dostupné k ochraně domácích počítačů hodně rozrůznily a zkomplikovaly. V minulosti stačilo mít jen firewall. Pak jste potřebovali ochranu proti virům, poté proti SPAMu, potom antispyware, následně program pro detekci narušení, možná program na filtrování, ochranu soukromí a ochranu proti podvodníkům na webu. Seznam se každý den prodlužuje. To je dobré pro dodavatele bezpečnostních programů, ale ne tak dobré, když si musíte na všechny tyto programy kupovat licence a každý rok je obnovovat.

Než si koupíte jakékoli bezpečnostní produkty, musíte pochopit, které komponenty jsou nezbytně nutné. Někteří bezpečnostní dodavatelé nabízejí souhrnná řešení – kombinaci několika produktů pod jednou licencí. To je obzvlášť důležité, pokud potřebujete chránit více než jeden

počítač. Až bude vaše domácí počítačová flotila růst (a ona bude), budete chtít počítačovou bezpečnost zjednodušit. Dobrým způsobem, jak toho dosáhnout, je zkombinovat co nejvíce funkcí pod jednu licenci. Pokud to váš dodavatel nenabízí, najděte si jiného.

15.1 Nezbytné bezpečnostní prvky

Existují základní bezpečnostní produkty (a soubory ke stažení, jako jsou záplaty), které MUSÍTE mít, abyste se chránili před škodlivým kódem a nechtěnými návštěvami ve svém počítačovém systému. K těmto základním prvkům patří:

- **Záplaty** – jako prevence problémů před tím, než k nim dojde.
- **Antivirový program** – aby váš počítač nenakazily nové viry.
- **Program proti adwaru a spywaru** – jako ochrana před adwarem i spywarem.
- **Firewall** – aby nezvaní návštěvníci zůstali za dveřmi.
- **Zálohovací program** – pro jistotu, abyste nepřišli o soubory.

Všimněte si, že první položkou je postup, nikoli produkt. Tím myslíme, že záplaty si nemusíte kupovat, ale musíte si zvyknout je aplikovat, nebo – což je ještě lepší – nastavit počítač tak, aby se záplaty aplikovaly automaticky. Mnohému škodlivému kódu, který ochranný program odráží nebo odstraňuje, by bylo možné se vyhnout zazáplatováním všech bezpečnostních děr v operačním systému, aplikačních programech a ochranných nástrojích, jakmile dojde k identifikaci bezpečnostních děr. Prozatím si jen pamatujte, že aplikace záplat je naprosto zásadní. Pokud to nebudete dělat, nemusí ostatní nástroje, které budeme probírat, správně fungovat, a v některých případech nebudou fungovat vůbec.

Ostatní výše uvedené položky tvoří kategorii zvanou „ochranné programy“. Ideální by bylo, kdybyste se mohli zastavit na prodejně Best Buy, zajít do uličky označené jako „ochranné programy“ a vybrat si jakýkoli ze stovek dokonalých programů, z nichž každý by splňoval veškeré potřeby na ochranu vašeho počítače.

Ve skutečném životě to není tak jednoduché. Většina ochranných programů na trhu obsahuje dvě nebo více z uvedených funkcí. Vaším úkolem je najít správnou kombinaci produktů a postupů, aby prováděly všech pět funkcí. Protože někteří z dodavatelů shrnují více bezpečnostních řešení pod jednu licenci, možná se vám podaří získat všechny tyto vlastnosti

v jednom produktu způsobem splňujícím vaše potřeby. Díky práci s jedním produktem je správa domácího vybavení snazší. Musíte se však rozhodnout, zda vám všechny shromážděné vlastnosti poskytují bezpečnost, kterou potřebujete. A často samozřejmě dostanete jen to, za co jste zaplatili. Čím je balíček robustnější a napěchovanější funkcemi, tím je obvykle dražší. Jen vy můžete stanovit, zda ochrana vašeho počítače, dat, soukromí a identity stojí za to.

15.2 Další vychytávky

V poslední části jsme zmínili jen naprosté bezpečnostní nezbytnosti. Existují také další vlastnosti, které nejsou úplně nutné, ale mohou vám velmi zjednodušit život. Patří k nim:

• Blokování / filtrace SPAMu
Neuvěřitelné množství škodlivého kódu cestuje s nechtěnými, nevyžádanými emaily. Blokováním SPAMu snižujete své vystavení takovému kódu. Taky si ušetříte hodně času a nervů. Blokování SPAMu je součástí nabídky mnoha balíčků určených k eliminaci spywaru, stejně jako některých antivirových balíčků.

• Blokování / filtrace SPIMu
SPIM je verze SPAMu zasílána IM zprávami. První obrannou linií při blokování SPIMu je zapnutí „seznamu přátel". Možná by se vám také hodil produkt pro ověřování a šifrování IM zpráv, zaznamenávání IM komunikace a podobně. Šifrování je nesmírně důležité, protože vše, co pošlete pomocí IM, se vypouští doslova do větru. Takže pokud si ceníte svého dědictví, nepoužívejte IM na stejném počítači, na jakém vaši rodiče používají online bankovnictví! Také se podívejte, jestli váš antivirový program vyhledává škodlivé kódy v přílohách IM zpráv.

• Ochrana proti podvodům, ochrana soukromí a identity
Mnoho balíčků pro počítačovou bezpečnost dnes obsahuje ochranu proti podvodům, ochranu soukromí a ochranu před krádeží identity. Krádeže identity a porušování soukromí se rychle stávají největším problémem, kterému uživatelé počítačů čelí. Pokud vás produkt, který používáte, před těmito hrozbami nechrání, možná byste měli změnit dodavatele.

• Prevence narušení
Detekce útoků a potenciálních narušení soukromí bývaly starostí velkých společností. To bylo před tím, než domácí uživatelé počítačů zjistili, že byly jejich počítače rekrutovány do botnetů pro koordinovaný útok odmítnutí služby (DoS). Většina firewallů prevenci narušení poskytuje, všechny však nikoli.

• Šifrování emailů a souborů
Šifrování je dvojsečnou zbraní. Používá se sice k ochraně dat, ale pokud je nebudete používat opatrně, může vaše data ochránit tak dokonale, že si je nebudete moct přečíst ani vy. Dobré je, že pokud se pro šifrování rozhodnete, některé z nejlepších nástrojů jsou zadarmo nebo jsou součástí operačního systému. Co se týče emailu, je zlatým standardem „Pretty Good Privacy" (Dost dobré soukromí, PGP) ze stránek pgp.com. Nevýhodou PGP je, že funguje jen pokud ho osoba, které email posíláte, také používá. Operační systém Windows 7 poskytuje šifrování disku. Šifrujte ale opatrně. Lepší může být chránit soubory heslem a vždy mít na paměti, že cokoli posíláte emailem, může uniknout na veřejnost. Takže posílejte jen emaily, o kterých by vám nevadilo, kdyby se staly titulkem na stránkách novin New York Times.

• Blokování vyskakovacích oken
Několik dost nepříjemných verzí adwaru, které byly v oběhu v roce 2010, se rozšířilo díky maskování za kontroly spywaru. Tyto verze měly jen málo společného (vytvořily je různé společnosti v různých zemích světa), ale všechny obtěžovaly uživatele zobrazováním vyskakovacích oken (často maskovaných tak, že vypadaly jako zprávy od samotného systému Windows). Když už jste se v této knížce dostali až sem, víte o bezpečnosti TOLIK, že na tento trik určitě neskočíte. Pokud ale používáte stejný počítač jako váš mladší sourozenec nebo spolužák, který se o bezpečnost tolik nestará, můžete se stát obětí této lsti i vy. Výborným způsobem, jak se tomuto riziku vyhnout, je blokovat vyskakovací okna. Blokování vyskakovacích oken je součástí nabídky mnoha antispywarových balíčků, stejně jako samotného systému Windows.

15.3 Souhrnná bezpečnostní řešení

Ačkoli není pravděpodobné, že byste našli jeden produkt splňující všechny bezpečnostní potřeby vašeho počítače, stejně by pro vás mohlo být výhodné koupit si některé ze souhrnných řešení. Když už nic jiného, alespoň se ujistěte, že vámi kupované řešení nabízí víc než jen ochranu proti virům.

Koupě souhrnného produktu má mnoho výhod. Zaprvé, každý bezpečnostní produkt, který si koupíte, má licenci. Když dojde k aktualizaci produktu, musíte si ji koupit. To má mnoho finančních důsledků. Když si k ochraně svého počítače koupíte čtyři různé produkty, musíte samozřejmě zaplatit za čtyři licence. I když si vyberete „freeware" verzi ochranného programu, stejně investujete čas a energii do hodnocení, výběru, stahování a instalace čtyř balíčků. A opravdové potíže, potenciálně také větší finanční zátěž, přijdou na řadu, když začnete hledat aktualizace těchto čtyř produktů. Kromě nákladů spojených s platbou za čtyři oddělené aktualizace pro vás nekonečné instalování aktualizací znamená i časovou zátěž. Není pravděpodobné, že by čtyři dodavatelé nabízeli aktualizace zároveň. Ochranu proti virům můžete aktualizovat v lednu, firewall v únoru, ochranu proti spywaru v březnu apod. Z časového hlediska je to prostě moc práce, obzvlášť, když máte doma víc počítačů. Aby počítačové zabezpečení správně fungovalo, musí se stát přirozenou součástí práce s počítačem. Neměla by to být těžká práce!

Souhrnné balíčky mohou být obzvlášť výhodné pro domácnosti s několika počítači. Většina nejlépe hodnocených souhrnných balíčků je k dispozici ve verzi pro domácnosti podporující tři až šest počítačů.

Pokud máte obavy o cenu zabezpečení byť jen jednoho domácího počítače, nemusíte se bát. Na Internetu najdete mnoho vynikajících bezpečnostních balíčků, které jsou bezplatné. Je jen důležité stáhnout si tento bezplatný program z důvěryhodných stránek. Určitě si nechcete omylem stáhnout trojského koně. Proto je důležité vědět, které dodavatelské stránky jsou důvěryhodné.

Dalším faktorem, který je při používání několika produktů pro ochranu počítače třeba zvážit, je, že ne všechny produkty umí dobře spolupracovat. Konkrétně byste neměli používat několik verzí firewallu a *nemůžete* mít spuštěné dvě verze antivirového programu.

15.4 Zálohovací produkty a postupy

Jedním často přehlíženým typem ochrany je zálohování počítače. Možná je tomu proto, že k zálohování nepotřebujete nový program, jen musíte změnit svůj přístup.

K dispozici je několik typů zálohovacích programů. Pravděpodobně jste nějaký typ zálohovacího programu dostali spolu s CD mechanikou. Pokud ano, používejte ho! Pokud ne, může stačit zkopírovat si důležité soubory na paměťovou kartu nebo na USB disk. Uživatelé, kteří vytvářejí velké množství souborů nebo fotografií zabírajících hodně místa, si mohou koupit externí disk. Dnešní externí disky jsou malé, levné a mají velkou kapacitu. Někteří lidé také k bezpečnému ukládání souborů používají online úložiště. My máme z domova zkušenost se všemi výše uvedenými možnosti.

Nedávno jsme se na konferenci setkali se ženou, která si na hotelovém pokoji polila notebook celou lahví vody. Byla tisíce mil od domova s nefunkčním notebookem a nemohla se nijak dostat k souborům, které potřebovala pro práci. Byla však zaregistrovaná u služby automatického zálohování společnosti Carbonite (www.carbonite.com). Koupila si nový notebook a ten samý den si mohla stáhnout všechny své soubory z online zálohy.

Pokud máte na domácím počítači důležité záznamy, například bankovní výpisy nebo doprovodné dopisy k přihláškám na vysokou, na kterých jste pracovali několik měsíců, bylo by dobré mít jednu kopii záložních souborů na jiném místě než doma. Pokud doma vyhoříte nebo vás vyplaví voda, alespoň tak nepřijdete i o své soubory. Zajímavé je, že někteří lidé mají doma sejf, kde skladují důležité cennosti, a předpokládají, že je to vhodné místo i pro záložní soubory. Pravděpodobně to tak NENÍ. Znáte klasickou knihu Raye Bradburyho *451 stupňů Fahrenheita?* Při 451 stupních Fahrenheita (233 stupňů Celsia) *hoří papír.* CD a DVD disky, stejně jako USB disky, se taví při mnohem nižších teplotách. Vaše milovaná sbírka zakázaných knih může být v tradičním domácím sejfu v bezpečí, ale jedné kopii záložních počítačových souborů bude lépe mimo dům!

Nezapomeňte na to! Aby byly záložní soubory použitelné, musí být dost aktuální. Jak aktuální, to záleží na tom, jak často počítač používáte, a co na něm děláte. Pro většinu uživatelů je naprostým minimem zálohování jednou týdně. Tak si vyberte čas a způsob a začněte zálohovat hned teď!

15.5 Nástroje pro odstraňování škodlivého kódu

Obrana váš systém vždy neochrání. Někdy také potřebujete vyčistit nepořádek poté, co počítačová obrana selže. I když je nejlepší – a nejsnadnější – myslet dopředu a škodlivé kódy si na počítač vůbec nepouštět, musíte také vědět, co dělat, když se to nepodaří.

Pokud používáte Internet dostatečně často a dlouho, časem se budete potýkat s něčím, na co nejste připravení.

Stane se to každému. Eric z Fairfaxu v Kalifornii si ve svém systému jednou ze školy domů přinesl virus Vundo.B. Děsivé, že? Jak se to stalo?

Erica dostali během „prodlevy". Vždy, když se do oběhu dostane nový virus, dojde k malé prodlevě mezi okamžikem, kdy se virus dostane na Internet, a okamžikem, kdy antivirové společnosti přidají ochranu proti tomuto konkrétnímu viru. Pamatujete si, jak jsme mluvili o signaturách virů? Eric byl jedním z mnoha hráčů, které napadl vir Vundo.B poté, co se dostal do oběhu, ale před tím, než se signatura této varianty viru dostala do antivirového programu.

Pokud k tomu dojde a na váš počítač se dostane virová infekce, často je jediným způsobem, jak se jí zbavit, použití odstraňovacího nástroje. Pokud vám to připadá zvláštní, uvědomte si, že úkolem antivirového programu je ZABRÁNIT nakažení viry a identifikovat veškeré viry, kterými jste byli nakaženi. Samotný antivirový program není určený k tomu, aby vás každé infekce zbavil. To by nebylo praktické. Nezapomeňte, že existuje více než 100 000 různých malwarů a každý den přibývají nové kódy a nové varianty.

Jakmile byl Ericův počítač virem Vundo napaden, zpomalil tak, že se sotva plazil. Byl tak pomalý, že dokonce i Eric, který je velký hráč a vytrvale bloguje, to vzdal a přestal svůj počítač používat.

Abychom se o viru něco dozvěděli a dostali ho z Erikova počítače, postupovali jsme takto. Napřed jsme si otevřeli webovou stránku našeho antivirového programu. Eric používal program Norton Internet Security, takže jsme otevřeli webovou stránku Symantec.com a podívali se na informace o viru Vundo.B. Hned se nám otevřel popis. Ukázalo se, že Vundo ve skutečnosti není virus. Je to trojský kůň, jehož cílem je dostat do počítače adware. Bylo jasné,

proč tak vysává všechny zdroje Ericova systému. Poté jsme klikli na uvedený odkaz a stáhli si nástroj pro odstraňování škodlivého kódu. Ericův počítač už byl tak pomalý, že jej nešlo používat, tak jsme si odstraňovací nástroj stáhli na jiný počítač a zkopírovali ho na disk CD. Potom jsme tento disk CD zasunuli do Ericova počítače, zkopírovali nástroj na pevný disk a spustili ho. Pokud jsme mohli soudit, začal počítač zase pracovat normálně. Abychom si byli jistí, Eric spustil vyhledávání virů a zkontrolovali jsme, že je antivirový program aktuální.

Pokud používáte antivirový balíček se všemi službami, měl by tento postup fungovat bez ohledu na to, která společnost váš antivirový programe dodává.

15.6 Dodavatelé bezpečnostních programů

Abyste si vybrali nejlepší bezpečnostní řešení pro své potřeby, musíte se seznámit s produkty alespoň několika společností a srovnat je. Když to uděláte, zjistíte, že každá společnost nabízí alespoň čtyři nebo pět (a někdy více) balíčků s různými typy a úrovněmi ochrany. Protože jsou na trh neustále uváděny nové produkty, neuvádíme seznam jednotlivých produktů. Sestavili jsme však seznam nejlepších společností zabývajících se počítačovou bezpečností s obecnými informacemi o typech ochranných programů, které každý dodavatel poskytuje. Další informace o konkrétních produktech najdete na webových stránkách příslušného dodavatele. Nezapomeňte také, že bezplatný bezpečnostní program může nabízet i váš poskytovatel internetového připojení. Zákazníci společnosti Comcats si mohou stáhnout bezplatnou verzi balíčku Symantec. Společnost Verizon poskytuje bezplatnou verzi bezpečnostního balíčku McAfee. Rovněž Microsoft's Security Essentials poskytuje svým zákazníkům bezplatný antivirový program.

Dodavatelé bezpečnostních programů

Název a webová stránka společnosti	Antispam	Antivirus	Bezplatný antivirus	Firewall	Bezplatný firewall	Ochrana soukromí a identity	Rodičovská kontrola / filtr webových stránek	Zálohovací program	Ochrana Wi-Fi, telefonu nebo PDA
AVG Security www.avg.com Bezplatná verze produktů: www.freeavg.com	A	A	A	A	A	A	A		
Avira www.avira.com	A	A		A			A		A
CA www.ca.com		A		A		A	A	A	
Carbonite www.carbonite.com								A	

Dodavatelé bezpečnostních programů (pokračování)

Comodo www.comodo.com	A	A	A	A	A			A	A
Emsisoft www.emsisoft.com		A		A			A		
ESET www.eset.com		A		A					A
F-Secure www.f-secure.com	A	A		A			A	A	A
Immunet www.immunet.com			A						
Kaspersky Lab www.kaspersky.com	A	A		A		A	A		A
McAfee www.mcafee.com	A	A	A	A	A		A	A	
Microsoft www.microsoft.com	A	A	A	A	A		A		
Norman www.norman.com	A	A		A	A	A			
Panda Security www.pandasecurity.com	A	A	A	A			A		A
Prevx www.prevx.com		A							
Sophos www.sophos.com	A	A		A					
Sunbelt Software www.sunbeltsoftware.com	A	A		A			A		
Symantec www.symantec.com	A	A	A	A	A	A	A	A	
Trend Micro www.trendmicro.com	A	A		A			A		A
Webroot www.webroot.com		A		A				A	
Zone Labs www.zonelabs.com	A	A		A	A	A	A	A	A

15.7 Aktualizování programu

Bez ohledu na to, jaký program si pro ochranu svého počítače před škodlivým kódem vyberete, je naprosto zásadní, aby byl neustále aktuální. To znamená dvě věci: nastavení automatických aktualizací ochranného programu a kupování nebo stahování nových verzí.

15.7.1 Nastavení automatických aktualizací

Když nastavujete ochranný systém, máte možnost vybrat automatické aktualizace. Udělejte

to! Pokaždé, když se připojíte na Internet (nebo ve stanoveném intervalu, obvykle častěji než jednou týdně), se ochranný balíček připojí na svou webovou stránku a zkontroluje důležité změny. Řekněme, že se do oběhu dostal škodící vir, který řádí na Internetu. Automatická aktualizace by měla automaticky stáhnout a nainstalovat novou signaturu, která vás před tímto virem ochrání, i když jste se právě nedívali na CNN a netušíte, jak velké nebezpečí vašim datům hrozí.

Poznej svého dodavatele

Volba správné ochrany před adwarem je zásadní. Volba špatného programu může váš systém nechat otevřený vůči útokům. V některých případech může volba špatného programu útok dokonce zahájit. Některé bezplatné ochrany proti adwaru jsou ve skutečnosti trojské koně, které na váš systém adware *nainstalují*.

15.7.2 Kupte si novou verzi

U většiny ostatních programů jsou každoroční aktualizace ve skutečnosti drobnými změnami, které pro běžné uživatele moc neznamenají. U bezpečnostního programu tomu tak není. Aktualizace bezpečnostního programu počítače při každé nové verzi je naprosto nezbytná! Metody používané k útoku na počítačové systémy se bez upozornění mění. Zdá se, že s každou zazáplatovanou bezpečnostní dírou už mafiáni vymýšlejí nové způsoby, jak na váš počítač dostat škodlivý kód. Nezničte si notebook za 16 000 Kč tím, že si nekoupíte aktualizace za 1 000 Kč.

15.8 Buďte v obraze, co se týče bezpečnosti

Malware, způsoby útoku a počítačová bezpečnost se často popisují jako pohybující se cíle. To se asi nezmění. Proto mnoho velkých bezpečnostních dodavatelů poskytuje na svých stránkách bezplatné bezpečnostní informace. Abyste byli v obraze, nebo se o konkrétních oblastech počítačové bezpečnosti dozvěděli více, můžete také využít tyto zdroje:

Webové stránky zaměřené na dospívající, školy a rodiče

- Cyber Smart (www.cybersmart.org)
- Family Online Safety Institute (www.fosi.org)
- FTC (www.ftc.org)
- Get Net Wise (www.getnetwise.org)
- iKeepSafe (www.ikeepsafe.org)
- i-SAFE (www.isafe.org)
- Look Both Ways (www.lookbothways.org)
- Microsoft Online Safety (www.Microsoft.com/protect)
- NetFamilyNews (www.netfamily news.org)
- Netsmartz (www.netsmartz.org)

Další obecné stránky (pro odborníky a nastávající odborníky)

- CERIAS (www.cerias.purdue.edu)
- On Guard Online (www.onguardonline.gov)
- SANS Institute (www.sans.org)
- School Climate at the Center for Social and Emotional Education (www.schoolclimate.org)
- Searchsecurity.com (www.searchsecurity.com)
- Security Focus (www.securityfocus.com)
- Stay Safe Online (www.staysafeonline.org)
- Stop Badware (www.stopbadware.org)
- Wired Safety (www.wiredsafety.org)

16. Vyladění

16. Vyladění – 289

16.1 Přednostní nastavení firewallu – 289

16.2 Záplatování bezpečnostních děr – 291

16.2.1 Kdo hledá díry? – 292

16.2.2 Proč je dobré aktualizovat v úterý? – 293

16.3 Používání automatických aktualizací – 294

16.4 Vytváření uživatelských účtů – 295

16.4.1 Co je administrátorský účet? – 296

16.4.2 Proč jsou standardní uživatelské účty dobré? – 297

16.4.3 Jak se vytváří nový uživatelský účet? – 298

16.5 Ochrana účtů heslem – 299

16.6 Vytvoření možnosti pro resetování hesla – 300

16.7 Testování bezpečnosti, kterou jste nastavili – 302

16. Vyladění

Alison si poslední dobou dost stěžuje, že si připadá jako chudá příbuzná. Na rozdíl od svého majetného bratrance Wesleyho nemá špičkový bezpečnostní balíček, který by její počítač chránil. Místo toho používá vestavěný firewall systému Windows a bezplatný antivirový program, který si stáhla z Internetu.
Za posledních šest měsíců byl její počítač nakažen třemi viry, trojským koněm a alespoň pěti různými typy adwaru. Wesleyho počítač takové problémy neměl. Takže zatímco Wes surfuje na Internetu a hraje hry, Alison tráví čas prohledáváním fór o odstraňování spywaru a telefonováním svému poskytovateli internetového připojení. Alison si často stěžuje, že Wes si žije, protože na to má.
Možná. Ale když jde o bezpečnost, nejsou peníze vším. Alison se mohla vyhnout všemu malwaru, který její počítač napadl, aniž by utratila jediný halíř. Adware? Žádný by nebyl, kdyby Alison před klikáním na odkazy chvíli přemýšlela. Viry a trojský kůň? Těm se mohla vyhnout, kdyby aplikovala záplaty a používala automatické aktualizace.

V předchozí kapitole jste se dozvěděli o některých bezpečnostních produktech, které potřebujete k ochraně dat. V této poslední kapitole se dozvíte, jak program, který už máte, „vyladit", aby byl váš počítač bezpečnější. K tomuto vyladění patří:

- Přednostní nastavení firewallu
- Záplatování bezpečnostních děr
- Používání automatických aktualizací
- Vytvoření uživatelských účtů
- Ochrana všech účtů heslem
- Vytvoření možnosti pro reset hesla
- Testování bezpečnosti, kterou jste nastavili

16.1 Přednostní nastavení firewallu

Už se zdá, že se pořád opakujeme....Otevřete krabici. Vytáhnete nový počítač. Připojíte se na Internet? NE! Když to uděláte, je jen otázkou času, než dojde ke krádeži či zničení vašich dat, nebo než bude váš systém použit k útoku na jiné systémy.

Než začnete uhánět po informační superdálnici, MUSÍTE si stáhnout všechny záplaty, které potřebujete k uzavření děr na novém počítači. A před tím, než to uděláte, musíte mít na počítači nainstalovaný firewall.

To může znít nepochopitelně. V předchozí kapitole jsme mluvili o firewallu jako o produktu, který si můžete koupit v rámci souhrnného bezpečnostního balíčku. To je pravda. Také existuje několik bezpečnostních programů zahrnujících firewall, které si můžete stáhnout zdarma. Abychom řekli pravdu, existuje mnoho dobrých firewallových programů, bezplatných i komerčních, a tyto firewally zahrnují různé prvky a funkce, které mohou z některých dělat lepší volbu než z jiných.

K tomu je ještě i operační systém dodáván s firewallem. Jak dobrý ten firewall je, a zda ho budete chtít používat, nebo si vyberete jiný, závisí na tom, jakou verzi operačního systému používáte. Systém Windows 7 je například vybaven poměrně dobrým firewallem.

Pokud se rozhodnete stáhnout si JINÝ firewall a dlouhodobě ho používat, stejně musíte zapnout firewall operačního systému, než se připojíte na Internet a stáhnete si nový firewall. Představte si svůj nový počítač jako auto. I když chcete příští týden přejít k jiné pojišťovně, při jízdě novým autem z prodejny domů potřebujete být chráněni svým starým pojištěním. Jinak byste si nové nepojištěné auto mohli úplně zničit cestou do pojišťovny. Stejně tak nechcete, aby se váš nový počítač zničil malwarem, když budete surfovat a hledat stránku ke stažené firewallu. Firewall operačního systému vám dává alespoň dočasné krytí, zatímco vybíráte a instalujete dlouhodobé řešení.

V některých případech můžete použít firewall operačního systému jako dlouhodobé řešení. To často záleží na tom, jaký bezpečnostní program si vyberete. Tuto volbu za vás může provést poskytovatel internetového připojení (ISP). Například společnost Verizon svým zákazníkům používajícím vysokorychlostní Internet (DSL) poskytuje zdarma program McAfee. Společnost Comcast svým zákazníkům používajícím kabelové internetové připojení nabízí zdarma program Symantec. Pokud používáte bezpečnostní programy McAfee nebo Symantec, firewall operačního systému bude během instalace bezpečnostního programu vypnut automaticky. Pokud váš ISP neposkytuje bezpečnostní program zdarma, můžete se rozhodnout stáhnout si bezplatný antivirový program, který nezahrnuje firewall. Například bezplatná verze programu AVG nezahrnuje firewall, takže uživatelé operačního systému Windows 7 budou chtít nadále

používat firewall Windows 7.

Bez ohledu na to, jaký operační systém, ISP nebo bezpečností program si vyberete, je zásadní nejprve instalovat firewall a poté si stáhnout záplaty. Jinak se do vašeho počítače může útočník dostat ještě před tím, než jste měli šanci stáhnout si aktualizace a zavřít díry.

16.2 Záplatování bezpečnostních děr

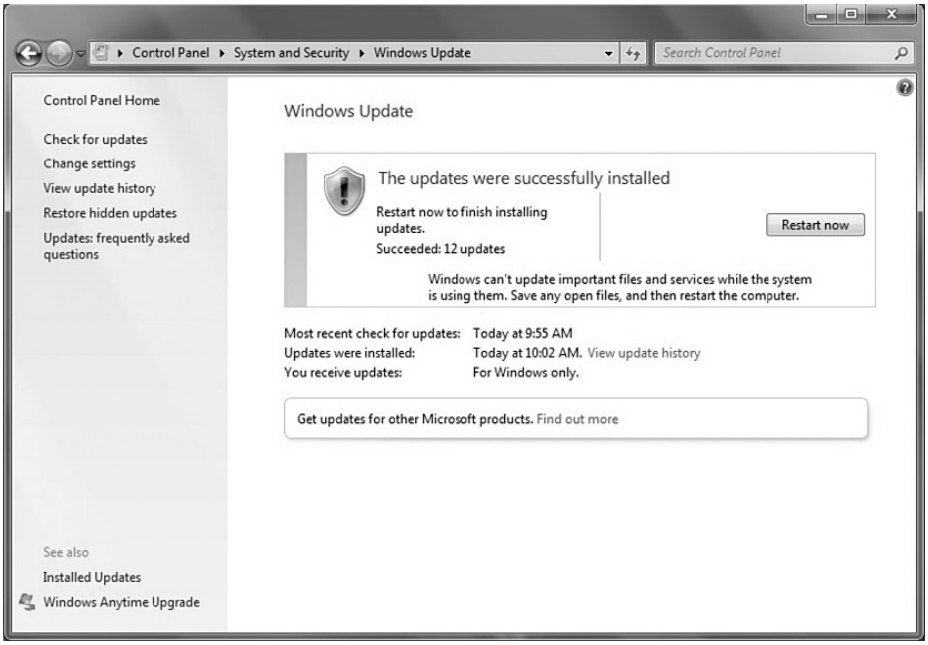
Mnohému škodlivému kódu, který ochranný program odráží, by bylo možné se vyhnout zazáplatováním všech bezpečnostních děr v operačním systému, aplikačních programech a ochranných nástrojích, jakmile jsou díry zjištěny. Pokud to nebudete dělat, nemusí žádný z produktů, které jsme probírali v kapitole 15, správně fungovat, a v některých případech nebudou fungovat vůbec.

Jakmile máte zapnutý firewall, můžete si vybrat, který antivirový program chcete používat, a poté si hned stáhnout jeho záplaty. To je krok, na který příliš mnoho uživatelů zapomíná. Předpokládají, že protože si nastavují nový počítač, nemusejí ještě nic aktualizovat. Tak to téměř nikdy není. Každý den, kdy váš nový počítač ležel na policích v obchodech Best Buy (Datart) nebo Staples (AutoCont), přicházely do oběhu nové malwary a nové varianty starých malwarů. Hackeři a podvodníci usilovně hledali nové chyby, které by mohli zneužít, a nové způsoby, jak zneužít chyby staré.

Pokud používáte systém Windows, je instalování všech aktualizací nebo záplat dost jednoduché:

1. Klikněte na tlačítko **Start.**
2. Zvolte položky **Ovládací panely > Systém a zabezpečení > Windows Update.**

   Po stažení aktualizací budete muset restartovat počítač, aby byla dokončena jejich instalace.



Každý den jsou zjištěny nové chyby, takže udržovat krok s novými záplatami je nezbytně nutné. I když to můžete dělat ručně (opakováním výše uvedených kroků), nejpraktičtější je používat automatické aktualizace.

16.2.1 Kdo hledá díry?

Zřejmě víc lidí, než byste si mysleli.

Společnosti, které program vytvářejí, samozřejmě hledají díry ve vlastním kódu, aby neměli jejich zákazníci problémy, které by pak společnost musela řešit. Alespoň doufejme, že to dělají. Hackeři hledají díry, protože se do nich chtějí dostat. Někteří hackeři hledají díry, protože chtějí zničit, prodat nebo ukrást podniková data. Další vedou tažení proti konkrétní společnosti a chtějí ji pomocí bezpečnostních děr ztrapnit nebo poškodit. A jiným jde zase o zisk, který jim přinese krádež osobních informací, jako jsou bankovní účty a hesla.

K hledání bezpečnostních děr existuje téměř tolik důvodů, kolik je způsobů jejich zneužívá-

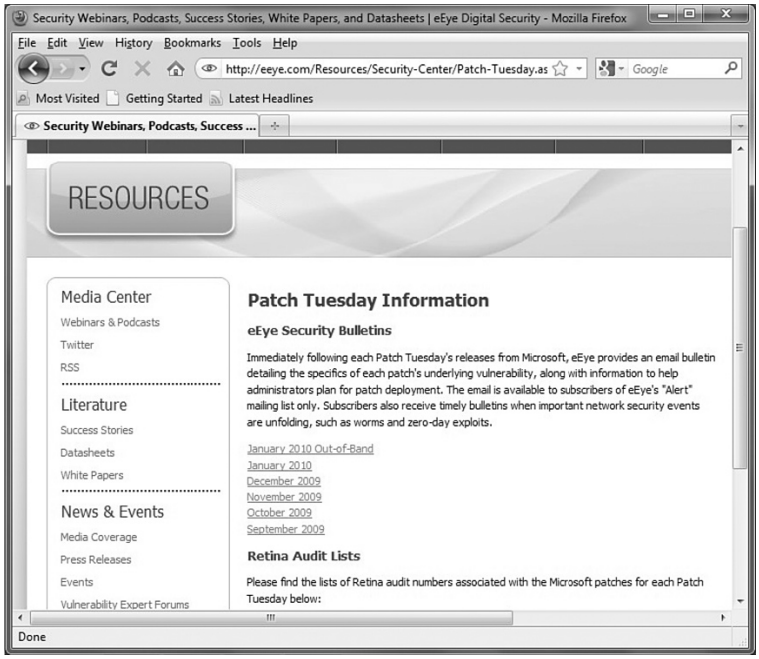
ní. Existují také bezpečnostní odborníci, jejichž prací je díry hledat. To znamená, že hledají zranitelná místa. Tři z těchto společností jsou eEye.com, Secunia.com a ISS.com X-Force (převzata společností IBM). Tyto společnosti prodávají proaktivní programy a poskytují informace a webináře o nejnověji nalezených zranitelných místech. Webinář je informativní seminář pořádaný přes Internet. Účastnicí webináře (studenti) se ve stanovený čas sejdou na stejné webové stránce, kde probíhá výuka nebo ukázka. Během webináře mohou účastníci klást otázky a interagovat s „učitelem". Je to jako malá třída, která se učí online. Podniky mají webináře rády, protože je to jako poslat zaměstnance na konferenci se speciálním školením, aniž by je ve skutečnosti museli někam posílat a platit za letenky, ubytování v hotelu apod.

Webinář Informativní seminář pořádaný přes Internet.

Teoreticky by se mohlo zdát, že když odborníci hledají díry, je to dobrá věc. V praxi to tak vždy není. Výzkumníci, kteří díry objeví, je někdy ohlásí veřejnosti PŘED TÍM, než má dodavatel čas vytvořit záplatu, nebo ji zpřístupnit uživatelům. Dodavatelem samozřejmě myslíme společnost, která vyrábí produkt obsahující zranitelná místa. Jindy dodavatel a veřejnost – což zahrnuje hackerskou komunitu – najdou chybu ve stejný okamžik. Hackeři poté okamžitě začnou dávat do oběhu útočné nástroje, které nové zranitelné místo zneužívají.

16.2.2 Proč je dobré aktualizovat v úterý?

Pokud chcete ručně kontrolovat aktualizace, nejlepší den je druhé úterý každého měsíce. Proč? Společnost Microsoft oznamuje nové aktualizace druhé úterý každého měsíce. Pokud vás zajímá, co řeší každoměsíční záplata vydaná toto úterý, můžete si přečíst přehled na webové stránce společnosti eEye. Hledejte pod hesly **Resources (Zdroje), Security Center (Středisko zabezpečení), Patch Tuesdays (Úterní záplaty).**



Copak se na problémy vždycky přijde jen v úterý? Samozřejmě ne. Kriticky důležité záplaty společnost Microsoft oznamuje i jindy během měsíce. Protože se aktualizace řešící závažné zranitelné místo může objevit kdykoli, opravdu byste měli svůj počítač aktualizovat každý den.

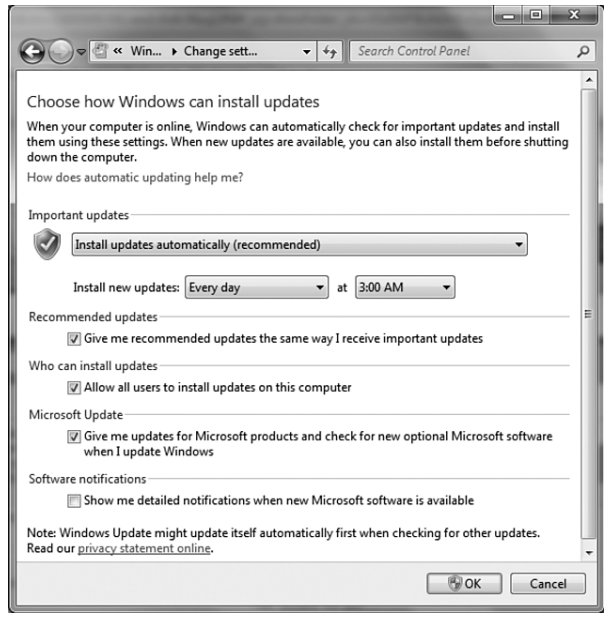
16.3 Používání automatických aktualizací

Nejlepší způsob, jak zajistit, aby se bezpečnostní záplaty dostaly na váš počítač rovnou, je používat automatické aktualizace. Protože vás to může rušit při práci na počítači, nejlepší je vybrat čas, kdy systém nepoužíváte.

V operačním systému Windows 7 můžete automatické aktualizace naplánovat takto:

1. Klikněte na tlačítko **Start.**
2. Zvolte položky **Ovládací panely > Systém a zabezpečení > Windows Update.**
3. Klikněte na položku **Změnit nastavení.**
4. Zvolte možnost **Každý den** a vyberte čas, který se vám hodí. Mnoho uživatelů vybírá

3 hodiny ráno, protože v tu dobu počítač pravděpodobně nebudou používat.



Co se stane, když počítač není ve 3 ráno zapnutý? Nebo když je zapnutý, ale nejste připojení k Internetu? To není problém. Systém Windows prostě automatickou aktualizaci spustí, až se příště dostane na Internet.

Nováček?

Když nastavujete automatické aktualizace úplně nového počítače, může to chvíli trvat.

Proč? Když poprvé spustíte automatické aktualizace, počítač stáhne všechny bezpečnostní záplaty, které byly zveřejněny od doby instalace operačního systému. Poté už potřebuje aplikovat pouze „nové" aktualizace.

16.4 Vytváření uživatelských účtů

Jiný způsob, jak bezplatně chránit počítač, je používat administrátorský účet jen tehdy, když potřebujete používat administrátorská oprávnění. Pokud nevíte jistě, kdo je administrátor – a při restartu počítače jste nikdy neviděli možnost Administrátor – je pravděpodobné, že jste

administrátorem vy. Pokud nevíte, co to znamená, měli byste to zjistit.

16.4.1 Co je administrátorský účet?

Operační systém Windows 7 má čtyři typy uživatelských účtů:

- Vestavěný administrátorský účet
- Uživatelský účet s právy administrátora
- Standardní uživatelský účet
- Účet pro hosta

Některé úkoly mohou provádět jen **administrátoři.** Pokud například váš účet nemá administrátorská oprávnění, nemůžete instalovat nové programy.

Administrátor **Osoba, která provádí údržbu počítačového systému. Administrátoři mají zvláštní oprávnění, která běžní uživatelé nemají.**

S každým typem uživatelského účtu jsou spojena jiná oprávnění. Oprávnění je určitým typem povolení. Oprávnění vašeho účtu stanoví, co můžete dělat. Existují například tři základní povolení pro práci se soubory: číst, psát a spustit. „Číst" znamená, že se na soubor můžete podívat. „Psát" znamená, že soubor můžete uložit. Také ho můžete měnit. Pokud máte povolení „Psát", můžete měnit soubor, který jste si přečetli, a uložit změněnou kopii. A konečně „Spustit" znamená, že soubor můžete spustit. (Předpokládá se, že souborem je program. Proto se také souborům programů často říká *executables* – spustitelné).

Protože oprávnění účtu řídí to, jaká povolení máte, je velmi důležité, zda používáte standardní uživatelský účet nebo uživatelský účet s oprávněními administrátora. Mnoho lidí se dopouští té chyby, že používají jeden účet s oprávněními administrátora. Takže všichni členové domácnosti sdílejí jeden účet. To může být nebezpečné.

Čtyři typy uživatelských účtů se v mnohém ohledu liší.

Vestavěný administrátorský účet
Tento účet při přihlašování neuvidíte, protože je před běžnými uživateli skryt. Jediný způsob, jak se k tomuto účtu dostat, je restartovat počítat v chráněném režimu. Proč je tak tajný? Pozor! Vestavěný administrátorský účet nemá žádná omezení.

Pomocí tohoto účtu můžete udělat změny, které počítač zničí, když nevíte, co děláte. Pokud nejste opravdový počítačový odborník, doporučujeme vám držet se od tohoto účtu dále.

Administrátorský uživatelský účet
Tento typ účtu je určen pro běžné uživatele s administrátorskými oprávněními. Většina domácích počítačových uživatelů má jeden účet s administrátorskými oprávněními. Osoba s tímto účtem může instalovat a odstraňovat programy a provádět jiné administrátorské funkce.

Standardní uživatelský účet
Všichni lidé, kteří domácí počítač používají, mohou mít standardní účet. Běžní uživatelé mohou systém POUŽÍVAT, ale nemohou provádět jeho správu. Takže standardní uživatel může vytvořit prezentaci v programu PowerPoint, ale nemůže smazat šablony tohoto programu ani odinstalovat sadu Microsoft Office. Tyto věci může dělat administrátor, nebo osoba s oprávněním administrátora. Proto byste si měli dát dobrý pozor na to, kdo oprávnění administrátora má. Čím víc pravomocí uživatel má, tím víc má možností váš systém zničit, byť nechtěně.

Účet pro hosta
Účet pro hosta je přesně tím, čím se zdá. Je to účet pro někoho, kdo systém obvykle nepoužívá. Host se může připojit na Internet a zkontrolovat si e-maily, nebo prohlížet webové stránky. Nemůže však instalovat software ani hardware, nastavovat hesla ani měnit žádná nastavení systému.

16.4.2 Proč jsou standardní uživatelské účty dobré?

Čím větší oprávnění účet má, tím více věcí s ním můžete dělat. To také znamená, že všechny programy, které na svém účtu spustíte, mají stejná oprávnění. Když administrátorská oprávnění nepotřebujete, měli byste používat standardní uživatelský účet. S tím je spojeno několik

nepříjemností. Kdykoli budete chtít instalovat nějaký program, budete se asi muset odhlásit a přihlásit se znovu na administrátorském účtu. To je však jen velmi malá nepříjemnost ve srovnání s možností zničení celého systému.

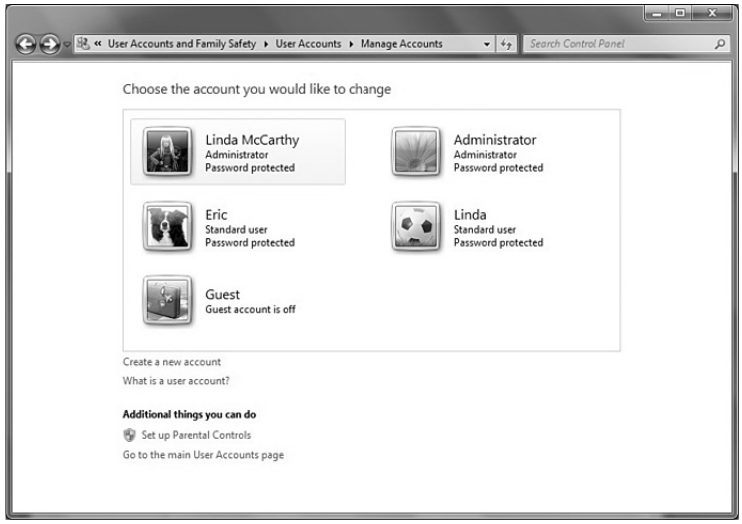
Chcete velet?

Dospívající jsou často lepšími administrátory, než jejich rodiče, protože na počítači tráví mnohem více času. Nevýhoda? Dospívající také mnohem častěji než jejich rodiče používají IM zprávy. Chatování pomocí IM zpráv na administrátorském účtu je riskantní. To platí i pro čtení mailů, prohlížení webových stránek a stahování. Pokud chcete být sami administrátory, nezapomeňte si také vytvořit standardní uživatelský účet. Opravdu je bezpečnější, když nebudete adminem POŘÁD! Jestli se chcete o administrátorských účtech dozvědět více, doporučujeme přečtení knihy Windows 7 Tweaks od Steva Sinchaka a jeho webovou stránku, tweaks.com.

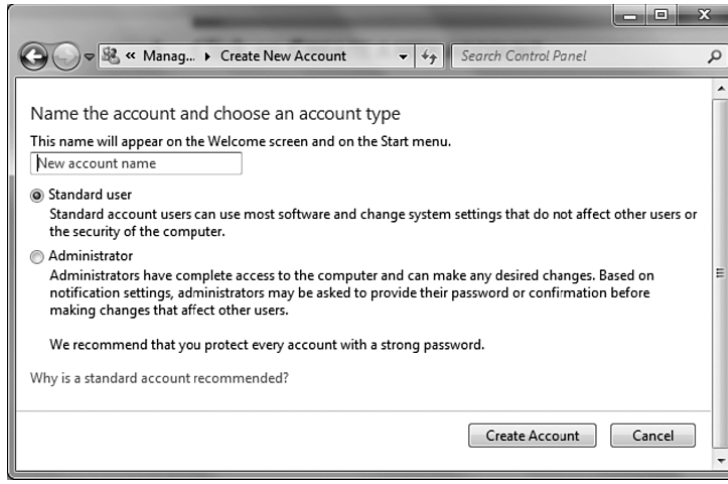
16.4.3 Jak se vytváří nový uživatelský účet?

Pokud chcete v systému Windows 7 vytvořit nový uživatelský účet, postupujte takto:

1. Klikněte na tlačítko **Start.**
2. Zvolte možnost **Ovládací panely > Uživatelské účty a zabezpečení rodiny > Uživatelské účty.**
3. Klikněte na volnu **Přidat** nebo **odebrat uživatelské účty.**



4. Klikněte na volbu **Vytvořit nový účet.**



16.5 Ochrana účtů heslem

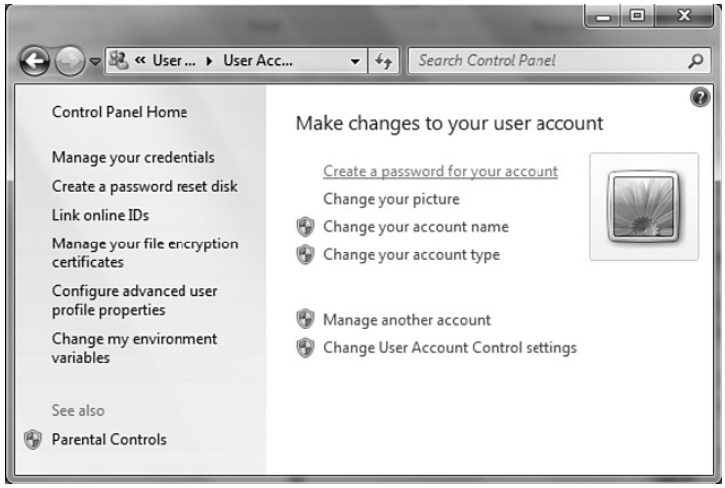
Zatím jste si pro sebe nastavili dva účty, standardní uživatelský účet a administrátorský účet. Možná byste také chtěli nastavit další uživatelské účty pro ostatní členy domácnosti, kteří mohou počítač používat. Jak na to?

Posledním krokem při vytváření nového uživatelského účtu je jeho ochrana heslem:

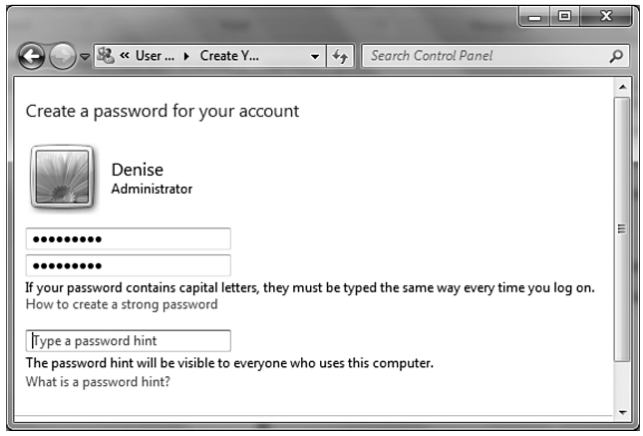
1. Klikněte na tlačítko **Start.**

2. Zvolte možnost **Ovládací panely >**
Uživatelské účty a zabezpečení rodiny> Uživatelské účty.

3. Klikněte na možnost **Změnit heslo systému Windows.**



4. Klikněte na volbu V**ytvořit heslo pro svůj účet.**



16.6 Vytvoření možnosti pro resetování hesla

Nevýhodou ochrany účtů heslem je nebezpečí, že heslo (hesla) zapomenete. Před touto možností se můžete chránit vytvořením diskety, CD, flash paměti pro resetování hesel nebo využi-

tím paměťového disku k uschování souboru pro obnovu hesel.
Při vytváření diskety pro resetování hesla postupujte takto:

1. Klikněte na tlačítko **Start.**

2. Zvolte možnost **Ovládací panely > Uživatelské účty a zabezpečení rodiny > Uživatelské účty.**

3. Klikněte na volbu **Vytvořit disketu pro resetování hesla.**

4. Postupujte podle pokynů v **Průvodci při zapomenutí hesla.**

I když to může znít, jako by vám tento průvodce pomohl v případě, že heslo zapomenete, je to vlastně zavádějící název. Disketu pro resetování hesla musíte vytvořit PŘED TÍM, než heslo zapomenete!

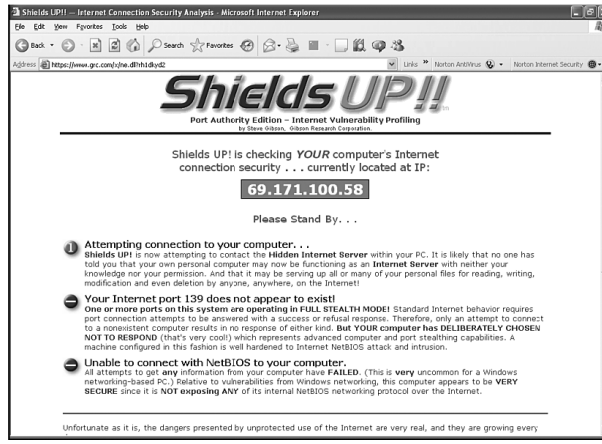
16.7 Testování bezpečnosti, kterou jste nastavili

Jakmile nainstalujete všechny bezpečnostní programy včetně firewallu, je zapotřebí zabezpečení pro jistotu otestovat.

Diamanty možná trvají věčně, ale bezpečnost má jepičí život. Dnes si můžete nainstalovat nejšpičkovější bezpečnostní program a nová bezpečnostní chyba může váš počítač otevřít hned zítra. Proto nemůžete zabezpečení prostě nastavit a dál se o ně nestarat. Co pořád opakují odborníci? „Nastavte bezpečnost, otestujte bezpečnost, aktualizujte bezpečnost, poslouchejte, jestli někdo nejde...Nastavte bezpečnost, otestuje bezpečnost...“

Možná to není chytlavá fráze, jedná se ale o účinný postup. A i když vás nemůže před kulkou uchránit na 100 %, alespoň uděláte pro zajištění bezpečnosti svých dat vše, co je v lidských silách – pro teď. Systém stejně není neprůstřelný. Ani nezničitelný.

Několik dodavatelů nabízí bezplatné testování zabezpečení na Internetu. Mezi ně patří velcí hráči na poli bezpečnostní ochrany: Symantec, Computer Associates a MacAfee. Naše oblíbená stránka ale nepatří žádné z hlavních bezpečnostních společností. Doporučujeme Shields UP, bezpečnostní stránku Steva Gibsona na adrese grc.com.



Otestování je samozřejmě jen prvním krokem. Pokud test najde problém, musíte vědět, co dělat dál. Představte si, že výsledky vašeho bezpečnostního scanu indikují otevřený port. Co teď? Musíte zjistit, proč je port otevřený, jaké hrozí nebezpečí a jak jej zavřít, pokud je to zapotřebí. Nemáme zde dost prostoru na to, abychom vypsali každou službu a každý port, ale otevřené porty a rizikové služby mohou otevírat dveře zločincům.

Tato bezplatná stránka naštěstí poskytuje podrobný bezpečnostní seznam, popisy rizik a doporučení dalšího postupu, pokud test selže. Nepovedou vás za ruku, ale poskytnou vám dostatek podrobností o každém neúspěšném testu, abyste mohli při řešení problému vykročit správným směrem.

A. Poznámka pro rodiče

Poznámka pro rodiče

Gratulujeme! Umožněním přístupu na Internet z domova, ze školy nebo z místní knihovny jste svému dospívajícímu poskytli odrazový můstek pro cestu na informační superdálnici! Několik úhozů do klávesnice vašemu dospívajícímu zpřístupní encyklopedické znalosti, snadné seznámení s vysokými školami a rychlou, spolehlivou globální komunikaci. Pokud jste, tak jako my, nevyrostli v digitální generaci, asi vás také ještě pořád udivuje, kolik toho Internet ve skutečnosti umožňuje. Doufáme, že jste neskočili na lep skandálním mediálním příspěvkům, které úplně ignorují nespočetné kybernetické úspěchy a soustředí se téměř výhradně na temnou stánku kyberprostoru.

Pokud by se vaše znalost Internetu zakládala jen na televizních zprávách, mohli byste si myslet, že je zaplněn výhradně phishery, podvodníky a potenciálními pedofily. Miliardy poctivých a čestných netizenů se z nějakého důvodu do zpráv nikdy nedostanou. Nebezpečí samozřejmě přesto existuje. A vyhnout se mu vyžaduje znalost, ochranu a přiměřená preventivní opatření. Vždyť jste svého dospívajícího nechali očkovat proti nebezpečným onemocněním, ačkoli pravděpodobnost nákazy dětskou obrnou je v západním světě jednadvacátého století mnohem nižší, než pravděpodobnost phisherského útoku online. Byl to rozumný preventivní krok.
Je důležité myslet na technologii, kterou mají vaše děti v rukou. Dali jste svým desetiletým a šestnáctiletým dětem iPhone? Uvědomili jste si, že mají 100% přístup na Internet 24 hodin denně, 7 dní v týdnu? Máte obavy o to, co mohou na síti vidět nebo dělat? Koupili jste svému 16letému potomkovi notebook za 20 000 Kč a přitom jste nevěděli, že musíte přidat firewall, aplikovat záplaty nebo nastavit automatickou aktualizaci antivirového programu?

Svému 5letému dítěti byste nedali do ruky knihu a neřekli mu, že se má sám zorientovat první den ve školce. I dospívající potřebují vaše vedení na cestě celosvětovou webovou sítí. Aby byli vaši dospívající na síti chráněni, zvažte tato rozumná bezpečnostní opatření:

- **Udělejte pro ochranu svého vybavení, cokoli je potřeba.** To zahrnuje antivirový program, ochranu proti spywaru a dobrý firewall. Patří sem také aplikování záplat a aktualizací.

- **Uvědomte si, že sítě se sociálními stránkami tu budou vždy.** Pokud máte obavy, sedněte si společně se svým dospívajícím dítětem a podívejte se na jeho stránky na

sítích MySpace, Facebook nebo Bebo. Vtloukejte svých dětem a jejich přátelům do hlavy, aby nezveřejňovali svá celá jména, adresy, názvy škol ani jiné informace, které by je mohly osobně identifikovat.

• **Počítače svých dětí ponechávejte na veřejném místě.** To znamená otevřený prostor, kde vidíte, co se děje – ne za zavřenými dveřmi ložnice. Snad se naučí důležité bezpečnostní zásady, než se z nich stanou dospívající s notebooky a budou mít přístup všude, kam půjdou.

• **Rodinné záležitosti ponechávejte jen v rodině.** Pokud máte doma bezdrátovou síť, zajistěte, abyste ji nevysílali všem sousedům.

• **Nedovolte webové kamery.** Dospívající jsou příliš často lákáni, aby webové kamery používali k posílání fotografií, kterých mohou v budoucnu velmi litovat. Odstraňte toto pokušení z dosahu! Dávejte pozor na notebooky, které jsou vybaveny vestavěnou kamerou.

• **Nebojte se být dospělí.** Pokud máte obavy, že by vaše dospívající dítě mohlo navštěvovat nebezpečné stránky, instalujte program rodičovské kontroly, který tyto stránky blokuje. Pamatujete si, jak jste zabezpečovali kuchyň bezpečnostními zarážkami a kryty do zásuvek, aby si vaše dítě neublížilo? Když vaše dítě dospívá, je naprosto v pořádku podobným způsobem zabezpečit Internet.

• **Nebojte se být ani policistou, pokud je to zapotřebí.** Pokud máte podezření, že se vaše dítě na síti dopouští něčeho nevhodného, dobře zvažte koupi monitorovacího programu. Pokud vaše dospívající dítě dělá něco nevhodného, je lepší, když je u toho chytne starostlivý rodič, než skutečný zástupce výkonné moci.

• **Pokud to jde, ponechávejte si důležitá data na vlastním počítači,** ne tam, kde pracují děti. Berte to jako ochranu kapesného vašeho dítěte nebo úspor na vysokou. Obzvlášť pokud vaše dospívající dítě stahuje programy, hudbu nebo jiné položky, měli byste přechovávat finanční podrobnosti a bankovní informace na vlastním počítači – ne na tom, kde váš teenager hraje hry a stahuje si programy z Internetu.

• **Pokud si nemůžete dovolit druhý počítač,** zvažte koupi programu určeného k ochraně finančních transakcí a osobních informací. Určitě takový program instalujte, pokud používáte online bankovnictví nebo používáte rodinný počítač k jiným finančním transakcím, jako je online placení účtů nebo nakupování.

• **Nezapomeňte, že aplikace záplat uzavírajících bezpečnostní díry** není jednorázovou záležitostí, kterou provedete a máte od ní pokoj. Nové bezpečnostní díry se objevují pořád. Nastavte své systémy na automatické aktualizace a tak udržujte všechny díry záplatované.

• **Připomínejte svých dospívajícím dětem, že musí myslet na budoucnost.** Co dospívající dnes sdílí, to na Internetu zůstane roky a bude tam i v době, kdy budou budovat svou kariéru. Dnešní hloupé fotografie a komentáře mohou vést k nezaměstnanosti v příštích letech.

• **Dávejte pozor na sociální inženýrství.** Když vám někdo zavolá a řekne, že je z FBI, nemusí to ještě být pravda! Ověřte si to. Naučte své dospívající děti, že po telefonu, e-mailem, IM zprávami a podobně nesmějí předávat žádné osobní informace, podle kterých by mohla být identifikována jejich poloha, ani žádné klíčové osobní informace.

• **Pamatuje na kyberšikanu.** V poslední době jsme svědky PŘÍLIŠ mnoha novinových zpráv o dospívajících, které šikana vedla k sebevraždě. Naučte své děti, aby kyberšikanu nahlásily, pokud ji vidí, a nikdy se jí samy neúčastnily.

• **Čas od času se podívejte na fotografie v telefonu svých dětí.** Sexting (posílání nahých nebo polonahých fotografií textovou zprávou) je mezi dospívajícími narůstajícím problémem. Mnoho dospívajících chycených při této činnosti bylo obviněno ze sexuálního trestného činu a získali celoživotní nálepku pachatele sexuálního deliktu. Nedovolte, aby vaše děti takovou noční můru zažily a zničily si život. Naučte je, že nesmějí posílat ani přeposílat žádné fotografie intimních tělesných partií, ať už vlastních nebo patřících jejich kamarádům.

• **Vzdělávejte se.** Jste první obrannou linií, co se týče bezpečnosti Vašich dětí na Inter-

netu. K výborným stránkám, kde se o online bezpečnosti můžete dozvědět více, patří Ikeepsafe (www.ikeepsafe.org), Getnetwise (www.getnetwise.org), Enough is Enough (www.enoughisenough.org), Family Online Safety Institute (www.fosi.org), Look Both Ways (www.lookbothways.org), MySpace Safety Tips (www.myspace.com), Wired Safety (www.wiredsafety.org) a STOP Cyberbullying (www.stopcyberbullying.org).

• **Buďte pozitivní!** Se správným bezpečnostním programem a rozumnými preventivními opatřeními se nemusíte Internetu vůbec bát. Vy i vaše dospívající dítě byste měli využívat úžasných možností, které poskytuje!

Poděkování

Editoři vyjadřují upřímný dík všem, kdo svými odbornými znalostmi a vizemi přispěli k tomuto aktualizovanému vydání knihy Buď pánem svého prostoru. Rádi bychom obzvláště poděkovali dospívajícím a mladým dospělým, kteří jsou součástí našich životů – Ericovi, Douglasovi, Tabithě, Nině, Kayle a Nathanovi. Tím, že si tak laskavě stahovali červy, přijímali viry a nevědomky instalovali zhoubný adware, nás neúmyslně seznámili s nebezpečími, které Internet představuje pro nic netušící rodiny.

Děkujeme všem bezpečnostním odborníkům, kteří se k našemu týmu připojili pro práci na příští verzi, stejně tak jako expertům, kteří zapůjčili své schopnosti a snahu pro tuto aktuální verzi:

- Jacku McCulloughovi za aktualizaci části o bezdrátovém připojení
- Richardu Fordovi za odborné informace o malwaru
- Keithu Watsonovi za aktualizace obsahu i za nápad

připravit bezplatnou online verzi této knihy.

A zvláštní dík Erikovi (17) za vedení diskuzí dospívajících a práci s webovými designéry a návrháři obálky. Chceme poděkovat zejména všem dospívajícím, kteří nám poskytli své nápady, sdíleli s námi své zkušenosti a dali nám zpětnou vazbu. Bez nich by tato kniha nevznikla. I když jsme neuvedli jejich příjmení, protože chceme chránit jejich soukromí, opravdu nemůžeme slovy vyjádřit, jak nesmírně důležitá je pro tento projekt jejich zpětná vazba.

A. Poznámka pro rodiče

Přispěvatelé

Jack McCullough
Bezdrátová bezpečnost
Odborný bezpečnostní konzultant a autor

Keith Watson
Výzkumník v oblasti bezpečnosti

Linda McCarthy
Výzkumnice v oblasti bezpečnosti

Richard Ford
Harris Proffesor of Assured Information
Florida Technology Institute

Denise Weldon-Siviy
Spisovatelka, editorka a máma

Názory dospívajících
Eric (17), Novato, Kalifornie
Brian (17), Novato, Kalifornie
Hala (17), Pleasanton, Kalifornie

Dospívající přispěvatel
Tabitha (17), Littlestown, Pensylvánie
Kayla (15), Gettysburg, Pensylvánie
Gino (13), Lodi, Kalifornie
Dominic (11), Lodi, Kalifornie
Waqas (14), Tacoma, Washington

Buď pánem svého prostoru
Jak sebe a své věci chránit, když jste online
Editovaly Linda McCarthy a Denise Weldon-Siviy

KNIHA PRO DOSPÍVAJÍCÍ, KTEROU BY SI MĚLI PŘEČÍST VŠICHNI RODIČE

Společný projekt pro poskytnutí bezplatného bezpečnostního školení dospívajícím a rodinám na síti. Projekt je sdílený podle licence Creative Commons a jeho vznik umožnila podpora jednotlivců i podnikových sponzorů.

Každý den si miliony amerických školáků otevřou webové stránky nebo se někam přihlásí a učiní rozhodnutí, které může ohrozit jejich bezpečí, ochranu a soukromí. Všichni jsme slyšeli hororové příběhy o ukradených identitách, kyberstalkingu a zvrhlících na Internetu. Děti musejí vědět, jak na Internetu zůstat v bezpečí, a jak Internet používat tak, aby neohrozily své soukromí ani nepoškodily svou pověst v příštích letech.

Naučte se, jak

- zabíjet viry, červy, trojské koně a spyware
- řešit kyberšikanu
- zkrotit SPAM a rozdrtit webové bugy
- pochopit míru veřejnosti „soukromých" blogů
- udržet zloděje bezdrátového připojení za branami
- si nezničit život sextingem.

O týmu
Linda McCarthy, dřívější výkonný ředitel pro internetovou bezpečnost společnosti Symantec, napsala první vydání knihy Buď pánem svého prostoru. Linda má v tomto odvětví více než 20letou praxi a najímají si ji společnosti, aby testovala zabezpečení jejich sítí na celém světě. Ve vydání z roku 2010 jsou Lindiny odborné znalosti doplněny celým týmem poskytujícím ty nejlepší bezpečnostní zkušenosti pro dospívající a jejich rodiče na Internetu. Do tohoto týmu patří odborníci na zabezpečení, animátoři a recenzenti z řad rodičů, stejně jako nadšené skupiny dospívajících recenzentů, webový designéři a zkušební čtenáři.

knihy.nic.cz
ISBN 978-80-904248-6-9
9 788090 424869

O knize Zajímá vás, jak se bránit proti kyberšikaně, jak předejít zavirování vašeho počítače, jak si zachovat soukromí na sociálních sítích či například jak se nestát obětí darebáků, číhajících na Internetu? Zajímalo vás někdy, kdo jsou to ti rhybáři, hackeři, crackeři, piráti, kyberstalkeři a další obyvatelé virtuálního světa, zvaného Internet? Všechny tyto otázky a mnohé další zodpovídá poutavým způsobem kniha Buď pánem svého prostoru, která je určena především dospívajícím čtenářům a jejich rodičům. Kniha se nevyhýbá ani tématům techničtějším a tak se v ní mladí uživatelé internetu mohou dozvědět také informace o technickém pozadí fungování internetového připojení, či informace o bezpečném nastavení domácích wi-fi sítí. Tato kniha by určitě neměla chybět v knihovničce žádného teenagera aktivně používajícího Internet.

O autorovi Linda McCarthy je uznávaná autorka a bezpečnostní expertka s více než dvacetiletou zkušeností v oblasti bezpečnostních auditů, poradenství a školení. Působila na pozici ředitele v oddělení internetové bezpečnosti ve společnosti Symantec, jako víceprezident oddělení profesionálních služeb ve společnosti Recourse Technologies a jako manažer v oddělení bezpečnostního výzkumu a vývoje ve společnosti Sun Microsystems. Je také zakladatelkou společnosti Network Defense. Linda McCarthy získala v roce 2004 prestižní ocenění Women of Influence pro oblast počítačové bezpečnosti, udělované časopisem CSO a společností Alta Associates. Věnuje se také psaní knih a článků na téma bezpečnosti. Mezi její publikované práce patří Digital Drama: Staying Safe While Being Social Online, Own Your Space: Keep Yourself and Your Stuff Safe Online, Facebook Security Guide, An Online Reputation that Counts, IT Security: Risking the Corporation, Intranet Security: Stories from the Trenches.

Když kolem roku 2004 zaznamenala změnu cílů útoků z firemních sítí na sítě domácích uživatelů, vytvořila ve společnosti Symantec internetový vzdělávací program pro mládež. V roce 2006 pak publikovala knihu Own Your Space (Buď pánem svého prostoru: Jak sebe a své věci chránit, když jste online), kterou napsala především pro náctileté čtenáře a jejich rodiny. Právě tuto knihu vám nyní v rámci Edice CZ.NIC přináší správce české národní domény.

O edici Edice CZ.NIC je jedním z osvětových projektů správce české domény nejvyšší úrovně. Cílem tohoto projektu je vydávat odborné, ale i populární publikace spojené s Internetem a jeho technologiemi. Kromě tištěných verzí vychází v této edici současně i elektronická podoba knih. Ty je možné najít na stránkách knihy.nic.cz.