

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 Síť 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 Sbíráání 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 požívají 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

- **Obsah**

11.6.3 YouTube – 212

11.7 Online rozchod – 213

11.8 Zapípej, ptáčku – 213

11.9 Tipy k zachovávaní 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**

- **Obsah**

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

Příspěvatelé – 312