Buď pánem svého prostoru

Jak chránit sebe a své věci, když jste online

Editovaly Linda McCarthy
a Denise Weldon-Siviy

Edice CZ.NIC

Editovaly Linda McCarthy a Denise Weldon-Siviy

BUĎ PÁNEM SVÉHO PROSTORU
Jak sebe a své věci chránit, když jste online

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

1. vydání, Praha 2013
Kniha vyšla jako 7. publikace v Edici CZ.NIC.
ISBN 978-80-904248-6-9

© 2010 100 Page Press
Obsah této publikace licencován podle licence Creative Commons Attribution-Noncommercial-No Derivative Works 3.0 United States, která je k dispozici na adrese http://creativecommons.org/licenses/.

cz.nic | SPRÁVCE DOMÉNY CZ

ISBN 978-80-904248-6-9

Autor i vydavatel postupovali při přípravě této knihy velmi pečlivě, avšak neposkytují na její obsah žádnou výslovnou ani předpokládanou záruku a nepřijímají žádnou zodpovědnost za chyby ani nedostatky, které se v ní nachází. Nepřijímáme žádnou zodpovědnost za náhodné ani následné škody vzniklé v souvislosti s použitím informací nebo programů zde uvedených, nebo z takového použití plynoucí.

Hlavní editor: Denise Weldon-Siviy
Řídící editor: Linda McCarthy
Ilustrace: Heather Dixon*

* Poznámka vydavatele: tyto informace se vztahují k originálu *Own your space*.

– 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.

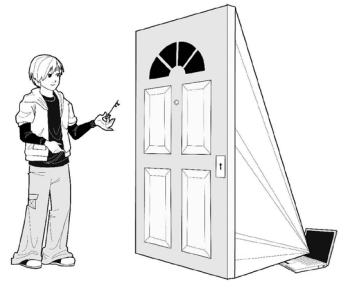
Napadlo vás něco? Moc rádi se dozvíme, co si o této knížce myslíte. Pošlete nám svůj názor na adresu lindamccarth@gmail.com.

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