edice PRŮVODCE

GRADA

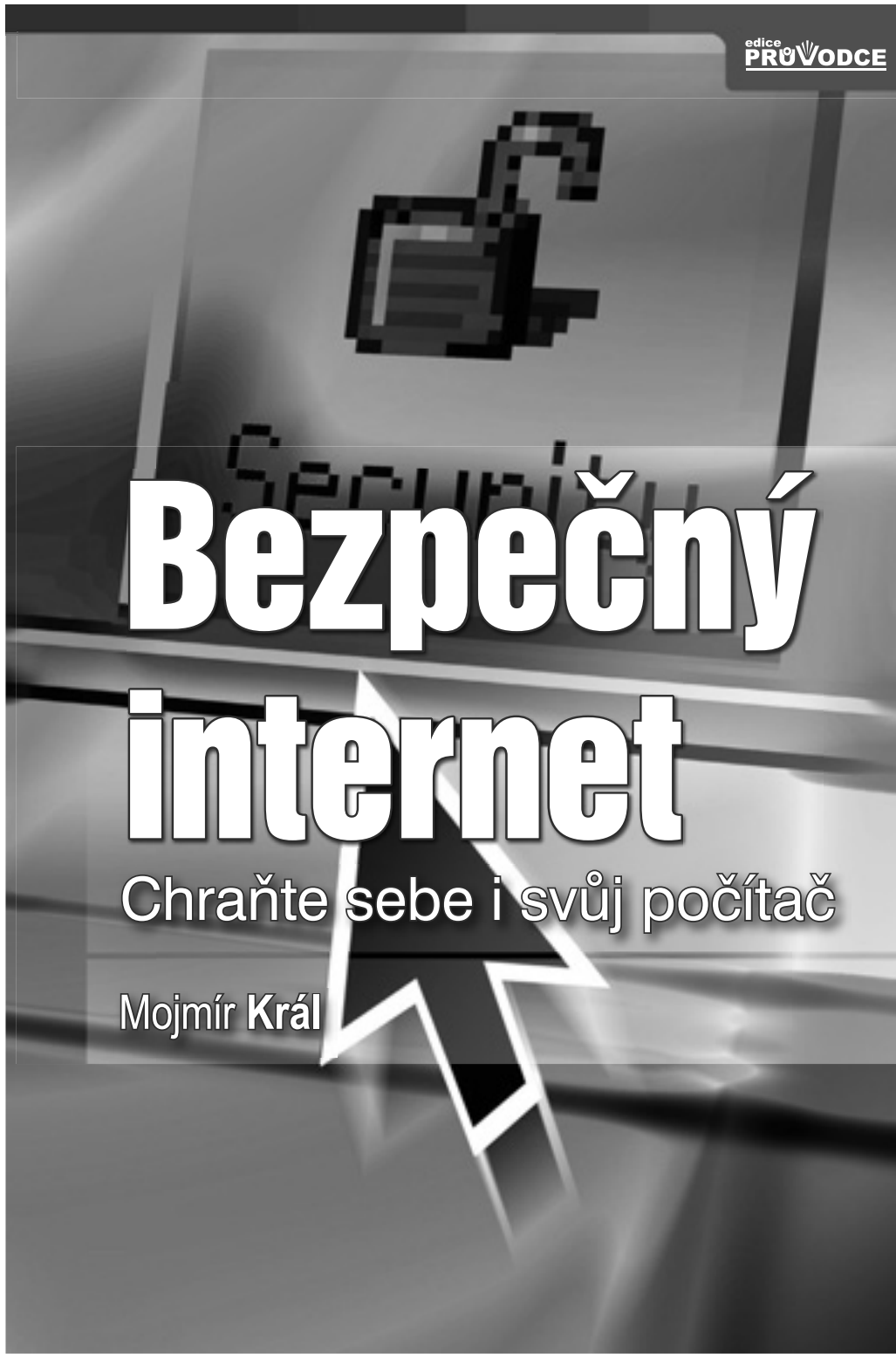
# Bezpečný internet

## Chraňte sebe i svůj počítač

Mojmír **Král**

- ochrana počítače (hesla, aktualizace, antiviry, firewall)
- vyhledávače
- rodičovská ochrana
- bezpečné používání sociálních sítí
- internetové bankovnictví a nakupování
- ochrana mobilních zařízení (telefony, tablety, notebooky)

GRADA®


edice
PRŮVODCE
Bezpečný internet
Chraňte sebe i svůj počítač
Mojmír Král

**Ing. Mojmír Král**

# Bezpečný internet

## Chraňte sebe i svůj počítač

**TIRÁŽ TIŠTĚNÉ PUBLIKACE:**

Kapitolou 12 do knihy přispěli Ing. Ladislav Pilař, MBA, Ph.D.; Ing. Jitka Pokorná, Ph.D., Česká zemědělská univerzita v Praze. Provozně ekonomická fakulta

Vydala Grada Publishing, a. s.
U Průhonu 22, Praha 7
obchod@grada.cz, www.grada.cz
tel.: +420 234 264 401, fax: +420 234 264 400
jako svou 5907. publikaci
Odpovědný redaktor Petr Somogyi
Sazba Jakub Náprstek
Počet stran 184
První vydání, Praha 2015
Vytiskly Tiskárny Havlíčkův Brod, a. s.



ISBN 978-80-247-5453-6

**ELEKTRONICKÉ PUBLIKACE:**

978-80-247-9821-9 (elektronická verze ve formátu PDF)
978-80-247-9832-5 (elektronická verze ve formátu EPUB)

## Poděkování

Chtěl bych na tomto místě poděkovat především své mamince, která mne nesmírně podporuje, bez její pomoci bych tuto knihu nikdy nenapsal. Poděkování zaslouží i pánové Lukáš Nimrichter, Štefan Šafár, Petr Šnajdr, Josef Džubák, kteří přispěli k práci nad rukopisem této knihy cennými radami a postřehy. Díky patří rovněž všem pracovníkům nakladatelství Grada Publishing, kteří se na vzniku knihy nějakým způsobem podíleli.

# OBSAH


1 Nebezpečí na internetu ... 13
1.1 Malware ... 14
1.1.1 Základní druhy malwaru ... 14
1.1.2 Jak mohou napadené počítače škodit? ... 15
1.1.3 Kdo a co nás může ještě sledovat? ... 18
1.2 Další častá nebezpečí ... 18
1.2.1 Nevyžádané předplatné ... 18
1.2.2 Stahování dat ... 19

2 Kontrola zabezpečení ... 21
2.1 Programy ... 21
2.2 Webové stránky ... 22

3 Účty a hesla ... 25
3.1 Uživatelský účet ... 25
3.2 Účet Host ... 27
3.3 Hesla ... 28
3.3.1 Nevhodná hesla ... 28
3.3.2 Bezpečné heslo ... 29
3.3.3 Heslo a Windows 8 ... 36

4 Aktualizace ... 37
4.1 Aktualizace systému Windows ... 37
4.2 Aktualizace prohlížečů webových stránek ... 40
4.2.1 Aktualizace prohlížeče Mozilla Firefox ... 40
4.2.2 Aktualizace prohlížeče Google Chrome ... 42
4.3 Aktualizace antivirového programu ... 43
4.3.1 Microsoft Defender ... 43
4.3.2 Antivirový program AVG ... 43
4.3.3 Antivirový program Avast! ... 44

5 Firewall ... 45
5.1 Firewall ve Windows ... 45
5.1.1 Aktivace či deaktivace Windows Firewallu ... 46
5.1.2 Povolení přístupu ... 46
5.2 Externí firewally ... 48
5.2.1 ZoneAlarm Free AntiVirus + Firewall ... 48
5.2.2 AVG Internet Security a Firewall ... 53
5.2.3 Avast! Internet Security a firewall ... 55
5.2.4 ESET Smart Security ... 56

6 Antivirová kontrola ..... 63
6.1 VirusTotal ..... 63
6.2 Jak vybrat správný antivirus? ..... 64
6.2.1 Virus Bulletin ..... 64
6.2.2 Požadavky na antivirový program ..... 65
6.3 Windows Defender ..... 65
6.4 Ostatní antivirové programy ..... 69
6.4.1 Avast! ..... 69
6.4.2 AVG Antivirus Free ..... 70
6.4.3 ESET NOD32 Antivirus a ESET Smart Security ..... 72
6.4.4 ZoneAlarm ..... 75

7 Sítě a WiFi sítě ..... 79
7.1 WiFi sítě ..... 79
7.1.1 Přihlášení ke správě routeru ..... 79
7.1.2 Přihlašovací jméno a heslo ..... 80
7.2 Zabezpečení WiFi sítě ..... 80
7.2.1 Název WiFi sítě ..... 81
7.2.2 Skrytí názvu sítě ..... 81
7.2.3 Šifrování ..... 81
7.3 Parental Control ..... 82
7.4 Externí programy ..... 84

8 Online bankovnictví a nakupování ..... 85
8.1 Online bankovnictví ..... 85
8.1.1 Typy útoků ..... 86
8.1.2 Způsoby ochrany ..... 86
8.1.3 Chytré telefony ..... 87
8.2 Online nakupování ..... 87
8.2.1 Možné problémy ..... 87
8.2.2 Obrana před nepoctivými prodejci ..... 87

9 Mobilní nebezpečí ..... 89
9.1 Tetheringový hotspot ..... 89
9.2 Veřejné hotspoty ..... 90
9.3 Smartphony a kontrola zabezpečení ..... 91
9.4 Správce zařízení Android ..... 92
9.4.1 Správce zařízení Android ve smartphonu ..... 92
9.4.2 Hledání smartphonu ..... 94
9.5 Smartphony a (nejenom) viry ..... 95
9.5.1 AVG Antivirus ..... 96
9.5.2 Cerberus ..... 100
9.5.3 AndroidLost ..... 101
9.6 Aplikace ..... 105
9.7 Bluetooth ..... 106

10 Bezpečně na internetu ... 107
10.1 Pravidla chování ... 107
10.2 Registrace na internetu ... 107
10.3 Pomoc od společnosti Google ... 108
10.3.1 Domovská stránka ... 108
10.3.2 Pro všechny ... 109
10.4 Internet Explorer ... 110
10.4.1 Zóny zabezpečení ... 110
10.4.2 Automaticky otevíraná okna ... 112
10.4.3 InPrivate ... 113
10.4.4 Cookie ... 113
10.4.5 Vyplňování osobních údajů ... 114
10.4.6 Dočasné soubory sítě internet ... 115
10.5 Opera ... 116
10.5.1 Soukromí a bezpečnost ... 116
10.5.2 Weby ... 118
10.6 Mozilla Firefox ... 119
10.7 Google Chrome ... 121
10.8 AVG Internet Security ... 123
10.8.1 Web ... 124
10.8.2 Identita ... 125
10.8.3 E-mail ... 125
10.9 Kontrola prohlížečů webů ... 127
10.10 ZoneAlarm ... 127
10.11 Ochrana proti spamu ... 129
10.11.1 Základní způsoby ochrany proti spamu ... 129
10.11.2 Antispamová ochrana v Outlooku ... 129
10.12 CERT/CSIRT ... 134

11 Co ještě můžete potřebovat? ... 135
11.1 Získání a instalace programů ... 135
11.1.1 Nastavení složky pro ukládání souboru ... 135
11.1.2 Získání programu ... 138
11.1.3 Instalace programu ... 139
11.2 Ovládací panely ... 142
11.3 Zjišťování MAC adresy ... 142
11.3.1 Nástroje operačního systému Windows ... 142
11.3.2 Externí nástroje ... 143
11.4 Zjišťování IP adresy ... 145
11.5 Sdílené složky a zařízení ... 146
11.5.1 Nástroje operačního systému Windows ... 146
11.5.2 Externí nástroje ... 147
11.6 Ochrana souborů ... 148
11.6.1 Free Hide Folder ... 148
11.6.2 Crypt4Free ... 149
11.6.3 AVG Internet Security a Datový sejf ... 150

11.7 Sledování aktivit počítače ... 152
11.7.1 Manic Time ... 153
11.7.2 Spyrix Free Keylogger ... 153
11.7.3 Activity Monitor ... 154
11.8 Provoz na síti ... 155
11.8.1 Nástroje operačního systému Windows ... 155
11.8.2 Externí nástroje ... 157
11.9 Gmail ... 160
11.9.1 Oprávnění k účtu ... 160
11.9.2 Služby a aktivity ... 160
11.9.3 Historie účtu Gmail ... 161
11.9.4 Účet Google+ ... 162
11.10 Anonymní surfování ... 163
11.10.1 Prohlížeče webových stránek ... 163
11.10.2 Anonymní režimy v prohlížeči ... 163
11.10.3 Proxy servery a VPN ... 163
11.10.4 TOR služby ... 165
11.10.5 Anonymní e-mail ... 166
11.10.6 CyberGhost VPN ... 167
11.11 Sandboxie ... 167
11.12 Safetized ... 169

12 Bezpečné používání sociálních sítí ... 171
12.1 Bezpečnost sociálních sítí obecně ... 172
12.2 Facebook ... 172
12.2.1 Vytvoření účtu na Facebooku ... 172
12.2.2 Ochrana soukromí na Facebooku ... 174
12.3 LinkedIn ... 175
12.3.1 Jak založit profil na LinkedIn ... 175
12.3.2 Ochrana soukromí na síti LinkedIn ... 177

# Úvod

Internet a sítě (i ty v malých firmách či v domácnostech) se staly běžnou součástí našeho života. Bohužel mnoho uživatelů stále podceňuje zabezpečení počítačů i mobilních zařízení a vystavuje tak svá zařízení (a potažmo i sebe a své blízké) různým nebezpečím – například ztrátě dat, možné ztrátě peněz apod.
Jelikož se však (naštěstí) o těchto možných rizikách debatuje jak mezi odbornou, tak i laickou veřejností, píše se o nich ve sdělovacích prostředcích i v diskuzích na různých webových stránkách a fórech, mnoho uživatelů začíná tuto problematiku vnímat a věnovat se jí. Každý uživatel počítače a internetu tedy řeší (ve větší či menší míře) problém, jak ochránit sebe, své blízké i svoje účty před možným napadením.
Cílem knihy je poskytnout čtenářům vyvážený, přehledný a dostatečný návod, jak svá zařízení správně ochránit. Zjistíte, co běžný uživatel potřebuje, čím se má zabývat a čemu má věnovat zvýšenou pozornost. Budete upozorněni na nejrůznější nebezpečí a taktéž se dozvíte, jak optimálně chránit počítač v případě různých způsobů jeho využití. Po přečtení knihy by měl čtenář porozumět zejména tomu, jak jednotlivé útoky fungují a jak se před nimi bránit.
Na následujících stránkách rovněž najdete doporučení na jednotlivé programy pro zabezpečení počítače (zejména takové, které jsou k dispozici zdarma, tedy freeware a opensource , ale i programy placené). Hlavní části knihy se věnují standardní ochraně počítače (hesla, aktualizace, firewall, antiviry), rodičovské ochraně, internetovému bankovnictví a nákupům na internetu. Samozřejmě nebudou chybět ani možnosti ochrany mobilních zařízení. U laptopů (tedy notebooků a netbooků) lze používat stejná opatření jako u stolních počítačů, u dalších zařízení (jako jsou například tzv. chytré telefony neboli smartphony) může být situace mírně odlišná, v závislosti na použitém operačním systému – ale i zde existují možnosti ochrany.

## Struktura knihy

Hlavním cílem knihy je upozornit uživatele na nebezpečí, jež mu mohou používáním moderních technologií připojených k internetu[1] hrozit, a také mu doporučit, jak takovýmto možným nebezpečím předcházet či je napravovat.
Snažil jsem se psát všechny kapitoly tak, aby jim porozuměl i běžný uživatel počítače. Pokročilí uživatelé budou (jak předpokládám) většinu uvedených informací znát. Vzhledem k výše uvedenému může dojít k situaci, že některé pasáže knihy popisují činnosti, které vás nezajímají – můžete je tedy klidně vynechat.
A nyní stručný přehled hlavních témat jednotlivých kapitol:
První kapitola knihy nese název **Nebezpečí na Internetu**. Uživatel se v ní dozví, jaká nebezpečí na něho vlastně mohou čekat a jakým způsobem může být jeho zařízení napadeno.
Druhou, sice krátkou, ale také důležitou kapitolou je **Kontrola zabezpečení**. Je velice důležité ihned po instalaci operačního systému vaše zařízení otestovat na výskyt možných nebezpečí, stejně tak je vhodné tuto kontrolu provádět i později, v různých časových intervalech.
Zejména pro správce počítačů bude mít význam kapitola **Účty a hesla**. Přístup do systému (jako základní bezpečnostní opatření) je totiž zabezpečen uživatelským jménem a heslem. Právě možnostmi nastavení těchto dvou základních bezpečnostních nástrojů se zabývá podstatná část této kapitoly.
Velice důležitou je kapitola **Aktualizace**. Jak možná už z jejího názvu vyplývá, věnuje se aktualizacím programů v počítači, a to jak aktualizaci operačního systému (zde Windows 8.1), tak i aktualizacím prohlížečů webových stránek a antivirových programů (přesněji aktualizacím jejich virových databází).
Kapitola **Firewall** je zaměřena na velice důležitou oblast – ochranu počítače přímo pomocí operačního systému Windows. Zabezpečení před všemožnými průniky zvenčí pomocí brány firewall je dokonce nezbytnou a základní součástí ochrany počítače, neměli byste ji tedy v žádném případě opomenout. Můžete kromě toho ale využít i externí nástroje a i o těch bude v této kapitole pojednáno.
Ani kapitola **Antivirová ochrana** nemůže být považována za oddechovou – naopak patří k těm nejdůležitějším. Antivirový program je totiž jednou z hlavních součástí zabezpečení vašeho zařízení, jeho instala-

1 U stolního počítače, laptopu se předpokládá operační systém Windows 8, resp. 8.1.

ce a nastavení by mělo následovat ihned po instalaci operačního systému. Antivirový program je součástí operačního systému (Windows), ale můžete používat i externí řešení od renomovaných firem – potřebné informace na dané téma naleznete právě v této kapitole.
Problematice zabezpečení sítí (včetně bezdrátových) se věnuje kapitola **Sítě a WiFi sítě**. Naleznete v ní nastavení routeru právě z hlediska zabezpečení sítě, nezapomeneme ani na rodičovskou kontrolu. I když se rozhraní pro nastavení jednotlivých routerů může lišit, v současné době jsou všechna konstruována na bázi webového prohlížeče (a jsou si tudíž dost podobná), uvedený návod může být tedy prospěšný pro všechny uživatele.
**Online bankovnictví a nakupování** je rovněž běžně využívanou aplikací moderních technologií. I když v oblasti online bankovnictví je zabezpečení na poměrně vysoké úrovni, přesto není opatrnosti nikdy nazbyt a dodržovat alespoň ta základní pravidla je více než patřičné a doporučeníhodné. A velice důležitým způsobem (v poslední době navíc stále oblíbenějším) využití internetu je i online nakupování. Řeč bude o tom, jak nakupovat prostřednictvím internetu, na co si dát pozor, jak se vyhnout možným rizikům… Nakupování online zažívá veliký rozmach, je tedy velice důležité zachovávat pravidla bezpečnosti i v této oblasti využití moderních technologií.
**Mobilní nebezpečí** jsou kapitolou určenou pro uživatele mobilních zařízení, zejména tzv. chytrých telefonů (smartphonů). I pro tato zařízení existují možnosti ochrany před zneužitím, určitě neuškodí o nich vědět a některá z nich i používat.
Kapitola **Bezpečně na internetu** nese název, jaký by klidně mohla mít i celá tato kniha, nicméně si v ní popíšeme základní pravidla, jak se chovat v prostředí internetu a jak nastavit nejčastěji používané prohlížeče. Probereme i téma ochrany proti spamu.
Poslední kapitolu jsem pojmenoval **Co ještě můžete potřebovat?** Je věnovaná mixu různých, podle mého soudu potřebných informací a nástrojů, které vám mají pomoci s hlavním tématem celé knihy – tedy se zabezpečením vašeho zařízení. Předpokládám, že zde uvedené informace se vám budou hodit.

## Čeština a angličtina

V knize naleznete (kromě jiného) i popisy dialogových oken, jednotlivých nabídek, příkazů apod. Jelikož programy můžete používat nejenom v českém, ale i v originálním anglickém jazykovém prostředí, vždy najdete u jednotlivých popisů jak české, tak i anglické znění. Přestože by se některým čtenářům mohlo zdát, že se tím kniha stává poněkud méně přehlednou, věřím, že si na tuto formu zvyknete a naopak oceníte, že nyní práci s programem zvládnete bez problémů i v jiném jazyce.

## Ovládání počítače

Ještě krátký dovětek k pojmům, na něž v knize narazíte a které souvisí s ovládáním počítače:

- Pokud je třeba použít tlačítko myši bez bližšího určení, myslí se tím vždy levé tlačítko myši, v případě, že máte nějakou akci vykonat **pravým** tlačítkem myši, vždy to bude v textu výslovně zmíněno.
- Pojem **klepnout** znamená jedno krátké, jemné zmáčknutí tlačítka myši, pojem **poklepat** potom dvakrát rychle stisknout tlačítko myši. Pojmem **táhnout** rozumíme stav, kdy myší najedete na určité místo, stisknete a držíte příslušné tlačítko a za jeho stálého držení se posunete na jiné, konečné místo. Tam tlačítko myši uvolníte.
- Při používání tzv. klávesových zkratek postupujete tak, že podržíte první uvedenou klávesu či klávesy a tu poslední stisknete – tedy například klávesová zkratka Shift+Ctrl+N znamená, že stisknete a držíte klávesy Shift a Ctrl a poté klávesu N.

# 1 Nebezpečí na internetu

Používání internetu přináší mnohé výhody, ale také mnohá rizika. Kromě toho, že je každý počítač připojený k internetu vystaven pokusům o útok ze strany různého malwaru, určitá „anonymita" dává uživatelům navíc pocit, že mohou o sobě prozradit takřka cokoli, anebo naopak od mnohých cokoli chtít. Považuji proto za užitečné vědět o různých nebezpečích, jež prostředí internetu přináší, a znát také různé možnosti obrany proti nim.

> Pro označení osoby, která se neoprávněně pokouší dostat k vám do počítače (ať již s jakýmkoli záměrem) budu používat pojem **útočník**. Velice často se sice používá termín hacker, ale protože toto označení není úplně výstižné – existuje více druhů útoků[2] s různou motivací, zvolil jsem raději český výraz útočník.

Obecně platí, že hrozící nebezpečí jsou buď **vnější**, nebo **vnitřní**. Mezi ta vnitřní patří:

- **Poškození technických zařízení** (například havárie pevného disku) – zde jsou potřebná zejména preventivní opatření jako zálohování dat (na externí disky nebo kvalitní DVD média[3]).
- **Výpadek elektrického proudu** (nebo výkmity napětí) – opět zálohujte data a pořiďte si přepěťovou ochranu zařízení, případně včetně záložního zdroje.
- **Programové** (programátorské) **chyby** – zálohujte potřebná data, aktualizujte programy (viz dále).
- **Kolize technického** či **programového vybavení** – používejte vzájemně spolupracující programy, aktuální ovladače pro daný operační systém.
- **Chyba uživatele** – mnoho problémů způsobují/umožňují samotní uživatelé.[4] Řešením je jejich důkladné proškolení a vzdělávání, k čemuž má napomoci i tato publikace.

Vnějšími riziky potom mohou být:

- **Krádež zařízení** – zabraňte nepovolaným osobám ve fyzickém přístupu k daným zařízením, zabezpečte i vlastní zařízení (například zámky Kensington).
- **Neoprávněný přístup k zařízení** – pro přihlášení k počítači používejte heslo (viz dále), při každém odchodu od počítače používejte systémový zámek (pro Windows platí klávesová zkratka Win+L). Osoba, která se bez vašeho vědomí dostane k počítači, může nejen odcizit nebo pozměnit data, ale také instalovat do počítače škodlivý program.
- **Počítačová infiltrace** – zde se používá pojem malware (z angl. **mal**icious soft**ware**). Protože tato publikace je zaměřena na nebezpečí, která zařízením mohou hrozit připojením k internetu, zaměříme se v knize právě na tuto oblast možné infiltrace.

Z hlediska ochrany všech zařízení je nejdůležitějším (a také nejproblematičtějším) prvkem **uživatel** – proto jakékoli doporučení musí začínat tím, aby uživatelé počítačů a dalších zařízení nad svými kroky přemýšleli (většinu problémů si uživatelé způsobují sami tím, že nechají zařízení bez dozoru, nechráněné heslem, bez bezpečnostních programů v aktuálním stavu, případně tím, že spouští neznámé stránky či programy, které na internetu objeví). Buďte proto prosím opatrní.

---

2 Více o dané problematice naleznete v publikaci Bezpečnost domácího počítače prakticky a názorně (10).

3 Například jako kvalitní DVD médium se jeví DVD+R Verbatim, k zálohování dat lze používat i NAS zařízení.

4 Je tomu tak často.

## 1.1 Malware

**Malware** je vlastně jakýkoli škodlivý/nežádoucí program, který se dostal do počítače (většinou bez vašeho vědomí).[5]

### 1.1.1 Základní druhy malwaru

Podívejte se nyní na přehled základních druhů malwaru podle **škodlivé činnosti**:

- **Adware** (*advertising-supported software*) je nevyžádaná reklama všeho druhu.[6] Bývá občas součástí freewarových (zdarma distribuovaných) nebo sharewarových programů, protože někteří vývojáři se snaží zobrazováním reklamy financovat své vlastní programy. Projevy adwaru mohou být nenápadné (například zobrazování banneru ve spuštěném programu), nebo naopak velmi nepříjemné (nastavení jiné úvodní stránky v internetovém prohlížeči, tzv. vyskakovací (pop-up) okna…). Jako základní obranu můžete nastavit prohlížeč webových stránek tak, aby reklamní okna neotvíral (viz dále), či použít některý z doplňků na blokování reklamy.
- **Backdoor** jsou programy, které vytvářejí tzv. zadní vrátka a umožňují tudy cizím osobám nepozorovaný přístup do vašeho počítače a jeho případné další zneužití (odcizení dat, instalace dalších programů, vykonávání příkazů útočníka).[7] Backdoory jsou zvláštní skupinou tzv. trojských koní (*trojan horses*). Hlavní obranou je nespouštět programy, u nichž nevíte, co obsahují – a (pochopitelně) kvalitní a aktualizovaný antivirový program.
- **Dialer** měnil v dobách modemového připojení k internetu vytáčené číslo. Napadený počítač využíval pro připojení drahé linky, většinou zahraniční. Uživatel tuto skutečnost zjistil až tehdy, když mu přišel velmi vysoký účet za telefon. V dnešní době existuje podobný typ útoku na mobilní zařízení, kdy může dojít k nepozorovanému posílání prémiových SMS.
- **Keylogger** (klávesová špionáž) je speciální typ spywaru, který sleduje stisky kláves a tyto informace posílá útočníkovi. Ten takto získává zejména přihlašovací jména, hesla apod. Ochrana je možná především prostřednictvím speciálních programů, na otestování bezpečnosti lze použít například 1-Click PC Care, Remote Spy Software a další antivirové programy, třeba AVG (viz dále).
- **Ransomware** (vyžadování výkupného) je typ malwaru, jehož prostřednictvím útočník vyžaduje pod různými výhružkami peníze, v lepším případě se na počítači může zobrazovat výzva k zaplacení „pokuty" za údajné porušení autorských práv nebo používání nelegálního softwaru, v horším případě dojde k zašifrování dat na disku (přičemž není jisté, že po zaplacení útočník data opravdu odblokuje) – viz obrázek 1.1.
- **Scareware** (panika) – nejčastěji se jedná o falešné antivirové nebo bezpečnostní programy, kdy po instalaci zkušební verze proběhne fiktivní kontrola počítače, která najde desítky až stovky údajně infikovaných souborů, jež je nutné vyčistit nebo odstranit. Pokud se uživatel nachytá, zaplatí zbytečně za bezcenný program.
- **Spyware** (špionáž) jsou programy, které sledují vaši činnost a získávají různé údaje: v lepším případě jen pozorují vaše zvyklosti, například nejčastěji navštěvované stránky, aby na vás mohly namířit cílenou reklamu, v horším případě získávají přístupová jména a hesla, osobní údaje, registrační údaje atd.

Přehled základních druhů malwaru podle **způsobu infiltrace**:

- **Trojan horse** (trojský kůň) je program, který se vydává za nějaký jiný užitečný program, hru či jiný zábavný software (který si chcete nainstalovat), ale ve skutečnosti skrytě – bez uživatelova vědomí – provádí jinou činnost. Často bývá součástí crackovacích programů.
- **Virus** je nežádoucí program, který se sám šíří a infikuje další počítače bez vědomí uživatele. Využívá k tomu zejména spustitelné soubory nebo makra dokumentů. Oblíbeným médiem pro přenos virů na další počítače jsou i USB flash disky. Mohou škodit různými způsoby – v minulosti se viry na napade-

5 Definici jednotlivých nežádoucích programů a také jednotlivých typů útočníků můžete nalézt například v knize Bezpečí na internetu pro všechny (18). Podrobněji se problematikou zabezpečení počítače zabývá publikace Bezpečnost domácího počítače prakticky a názorně (10) a taktéž i kniha První kroky s internetem (7).

6 Bohužel, současný internet je jí přímo přehlcen.

7 Backdoor většinou sám o sobě neprovádí nic – čeká, až dostane pokyny k vykonání nějaké akce.


**Obrázek 1.1: Ukázka ransomwaru**

ném počítači často projevovaly různými zvukovými nebo obrazovými efekty, případně škodily ničením souborů a dat. V současnosti se naopak snaží chovat co nejméně nápadně a případně stahovat další nežádoucí a škodlivé programy do napadeného počítače. Viry představují velkou skupinu malwaru.

- **Worm** (červ) je program šířící se pomocí počítačové sítě, může k tomu používat sdílené disky nebo jiné komunikační kanály, nejčastěji je to prostředí elektronické pošty, kdy se šíří pomocí e-mailů.[8] Za zmínku stojí, že adresa odesílatele je většinou podvržena.

**Základní obranou** proti všem těmto útokům je:

- Udržovat aktualizovaný operační systém.
- Používat kvalitní antivirový program s pravidelnou aktualizací virové databáze.
- Neinstalovat programy z nedůvěryhodných zdrojů.
- Mít nastaveno zobrazování přípon všech souborů (přičemž rozhodující je ta poslední).
- Nespouštět soubory v e-mailu od neznámých odesílatelů (pokud vám i od známého odesílatele přijde podezřelý e-mail, je lepší se ujistit, zda vám ho dotyčný opravdu poslal).
- Sledujte, zda se v počítači neděje něco podezřelého, jako je například neobvyklý nárůst přenosu dat, výrazné zpomalení počítače, zvýšená činnost pevného disku apod.
- Používejte rozum! Chovejte se obezřetně (útočníci jsou většinou „o krok" napřed a v některých případech ani nejlepší antivirový program nemusí reagovat na nejnovější hrozby).

### 1.1.2 Jak mohou napadené počítače škodit?

V předchozích odstavcích bylo popsáno, jakým způsobem je možné nejčastěji počítač infikovat a co napadené počítače mohou uživateli přímo způsobit. Existuje ale i další problém – napadený počítač může nevědomky sloužit k útokům a škodit ostatním.

8 Pokud máte v systému nastaveno zobrazování přípon, potom některé takovéto soubory zobrazují i dvě přípony.

**Bot a botnet**: Škodlivý program může nenápadně čekat na vzdálené příkazy útočníka. Takový počítač se nazývá **zombie**. Útočník si postupně vytváří celou „armádu" zombie počítačů (někdy také označovaných jako „bot" (od slova ro**bot**) a buduje tzv. **botnet**, tedy obrovskou síť, čítající i několik (set) tisíc počítačů, rozmístěných po celém světě, které čekají na povel.

**Klasické viry (zejména ty destruktivní) již tolik „netáhnou". Relativně novým typem jsou proto botnety, tedy programy, reagující na příkazy útočníka zadávané na jiném počítači. Bot je program, který je tajně nainstalován na uživatelském počítači, obsahuje komunikační a řídící modul a umožňuje útočníku vzdáleně tento počítač ovládat a využít pro plnění různých příkazů.[9] Bot je velmi flexibilní, neboť je ovládán na dálku: dokáže měnit svoji funkčnost přidáním nového kódu či změnou stávajícího. Pro počítač infikovaný botem se používá termín zombie (živá mrtvola), čili stroj ovládaný útočníkem bez vědomí uživatele.**

Tyto počítače (infikované botem), které jsou sdružovány do sítí s označením **botnet** (*bot network*), lze potom použít k provedení koordinovaného útoku. Vlastníci botnetů mohou tuto síť za peníze pronajímat jiným kyberzločincům nebo ji sami zneužívat k další nekalé činnosti.
I když hranice rozdílů mezi jednotlivými druhy malwaru je neustále tenčí, bot na rozdíl od virů může být modifikován a na rozdíl od rootkitů může být šířen v masovém měřítku.
Bot musí komunikovat se svým řídicím orgánem, boty mohou být ovládány několika různými způsoby, například přes P2P (*peer to peer*) sítě či diskusní skupiny, avšak nejběžněji přes chatovací kanály IRC (*Internet Relay Chat*) – tento protokol IRC útočníci velmi dobře znají, IRC serverů existuje velké množství a připojit se k nim lze víceméně anonymně.

**Útočník může do vašeho počítače proniknout pomocí malwaru, například pomocí backdooru (zadní vrátka), a škodlivý kód potom šířit pomocí tzv. exploitu (programy využívající bezpečnostní chyby). Jednu z dalších cest představuje použití webových stránek nebo protokolu elektronické pošty SMTP, a to často za aktivní účasti uživatele. Hacker naláká uživatele k návštěvě webové stránky (viz phishing a pharming), která se tváří jako legitimní, nicméně skrývá zákeřný kód. Riziko představuje i stahování a spouštění programů z neověřených zdrojů či otevírání podezřelých příloh v e-mailu.**

Bot potom provádí škodlivou činnost, nejčastěji se jeho prostřednictvím rozesílá **spam**, běžné je i zneužití k **phishingu**, velmi nebezpečné jsou i botnety páchající typicky spywarové funkce jako **sniffing**. Botnety se používají i pro rafinované podvody typu zneužití reklamních systémů pay-per-click, kde počítače napadené botem jsou zneužívány pro automatické klikání na reklamní bannery (tvůrcům botu pak nesou nemalé zisky). Infikované počítače mohou být navíc kontrolovány na dálku, lze tak tedy upravovat seznam reklamních serverů, na něž se mají soustředit, a také maximální počet kliknutí z jedné IP adresy. Počítače spojené jako botnet se také používají i k útokům typu **DoS/DDoS** (viz dále).

**Ochrana proti botnetům** pochopitelně možná je:
- Udržujte operační systém a webové prohlížeče v aktuálním stavu – záplatujte, aktualizujte.
- Používejte správně nastavený firewall.
- Udržujte aktuální i antivirový program (i další antimalwarové programy).
- Sledujte, zda se v počítači neděje něco neobvyklého, zda v něm neběží nějaké služby, které běžet nemají, zda nejsou přenášena data (neobvyklý nárůst přenosu dat, zejména v době, kdy nepracujete).
- Správcové sítí pozorně sledují (a případně dále uvedené porty blokují) provoz zejména na portech:
  a) 6666 a 6667 (použití pro IRC),
  b) 136, 137, 138, 139 (pro komunikaci programů na různých počítačích),
  c) 593 (komunikace počítačů na internetu),
  d) 445 (pro sdílení souborů),
  e) 1024 a vyšší (porty pro volné použití).

9 Další informace naleznete na URL: http://www.lupa.cz/clanky/botnety-internetova-hrozba/ (17).

**DoS**/**DDoS** (*Denial of Service/Distributed DoS*) – útoky odepření služby. Jednotlivé zombie počítače se pokoušejí přistupovat na přístupový zdroj či na cílové stránky a posílat takové množství požadavků, aby zahltily server oběti tak, že potom neplní svoji funkci (v praxi je takto možné na určitou dobu odstavit například stránky konkurenčního e-shopu). Když se potom zákazník nemůže připojit či je spojení velmi pomalé, odchází jinam – ke konkurenci. Ochranou je kvalitní a dobře nastavený firewall a antivirový program.

**Hoax** (poplašné zprávy, fámy) je kategorie kolujících řetězových (varovných nepravdivých) zpráv,[10] které si přeposílají sami uživatelé. Zpráva většinou popisuje nějaké nebezpečí a pro důvěryhodnost se v ní uvádí, že pochází od nějaké velké, známé firmy a je ji potřeba sdělit co největšímu okruhu uživatelů (přičemž někteří vyděšení uživatelé jsou opravdu schopni takovou zprávu odeslat na všechny adresy ve svých kontaktech). Typickými hoaxy jsou nesmyslná varování před neexistujícími viry, různé nabídky a nesmyslné rady… Přeposílání hoaxů může vypadat jako neškodná zábava, ale pokud se taková zpráva s velkou sbírkou e-mailových adres dostane na infikovaný počítač, může škodlivý program e-mailové adresy posbírat a odeslat útočníkovi (k dalšímu zneužití). Základní obranou je neotvírat takovéto zprávy, rovnou je mazat a hlavně na ně nereagovat.

**Phishing** (rhybaření) a **pharming** (pharmaření), ale také **phreaking** (pomocí klasického telefonu) jsou mimořádně škodlivé aktivity, neboť vyžadují zaslání informací například o internetovém bankovnictví (přístupová jména a hesla), velice těžko se odhaluje zejména pharming (falšované webové stránky, viz dále).

**Phishing** neboli podvodné e-maily je forma útoku, kdy se útočník snaží uživatele zmást a vylákat z něho údaje obvykle osobního charakteru (přístup k e-mailu či k jiným službám). Často se zneužívá v online bankovnictví[11] a vyžaduje přístupové údaje (jméno uživatele, heslo…). Podvodné e-maily na první pohled vypadají, že jsou odesílány přímo z banky, a snaží se přesvědčit uživatele, aby klepnul na uvedený odkaz. Jestliže tak učiní, dostane se na podvodné stránky, kde jsou po něm požadovány přístupové údaje k účtům, platebním kartám, nebo jiné důvěrné informace (viz dále).

**E-mailový spoofing** jako jedna z podkategorií znamená pozměnění odesilatele e-mailové zprávy (e-mail vám oznamuje, že váš bankovní účet byl deaktivován, pro jeho aktivaci musíte na e-mail odpovědět a zaslat potřebné přihlašovací údaje).

**Nigerijské podvodné e-maily** (SCAM419, často falešná dědictví) – v tomto případě vás e-mailem osloví neznámý útočník s informací ve smyslu, že zdědil něčí majetek ve výši několika (desítek) milionů dolarů a potřebuje pomoci při převodu do zahraničí. Za to vám slibuje velkou odměnu ve výši až několika desítek procent z celkové částky. Princip podvodu spočívá v tom, že oběť je neustále nucena platit nečekané „administrativní" poplatky a převod majetku se (samozřejmě) stále oddaluje.

**Falešné loterie**: princip tohoto podvodu je podobný jako u nigerijských falešných e-mailů: uživatel dostane oznámení o veliké výhře v cizí měně (nejčastěji dolary, eura apod.). V případě, že oslovený kontaktuje „provozovatele" loterie, mu je sděleno, že výhra bude vyplacena, jakmile zaplatí manipulační poplatek v řádu několika desítek tisíc korun, který (jak jinak) není možné odečíst ze slíbené výhry. V případě, že uživatel poplatek zaplatí, jsou po něm požadovány stále další a další poplatky, dokud je ochoten platit. Zaplacené peníze a slíbenou výhru ovšem nikdy neuvidí.

**Pharming** je pokročilejší variantou phishingu, jde o útok, kdy je správná IP adresa změněna na IP adresu webu škůdce, napadený potom komunikuje s útočníkem v domnění, že se jedná o správnou instituci (například banku) – viz dále.

**Spam** čili nevyžádané pošta jsou zprávy (e-maily), které jste nechtěli, většinou reklamního charakteru. Pokud je váš počítač infikován patřičným programem, může se stát, že tento program v počítači prohledá místa, kde se obvykle nacházejí kontakty a e-mailové adresy. Na ty pak podle vzdálených příkazů rozesílá reklamní nabídky, podvodné e-maily nebo jiný malware). Uvedená nevyžádaná reklamní sdělení mohou mít charakter nabídek různého zboží či služeb, často pochybného charakteru (například různé léky, u nichž nelze zaručit jejich původ, funkčnost či dokonce nezávadnost).[12] Ochrana proti spamu je možná na několika úrovních:

---

10 Podrobnosti viz http://www.hoax.cz/hoax/co-je-to-hoax (5), http://bezpecnasit.webnode.cz/hoax/ (4), další informace lze najít na http://e-bezpeci.cz (2).

11 Podrobněji v knize Bezpečnost domácího počítače prakticky a názorně (10).

12 O hoaxech, phishingu a dalších podvodných e-mailech můžete získat další informace na specializovaném serveru http://www.hoax.cz, který se již cca 15 roků věnuje této problematice.

a) nezadávejte e-mailovou adresu v klasické podobě, ale ve tvaru: *jmeno.prijmeni(at)firma.cz*,
b) v programech pro elektronickou poštu (například Outlook, Lotus Notes, Mozilla Thunderbird, eM Client, The Bat!, IncrediMail) nastavte a používejte antispamové filtry,
c) dávejte pozor na to, co (zejména v případě e-mailové adresy) a do jakých formulářů na webu vyplňujete,
d) hromadnou poštu raději posílejte na adresy v políčku **Skrytá kopie** (**Bcc**), ať nedochází ke zbytečnému zveřejňování cizích e-mailových adres ostatním uživatelům),
e) používejte externí antispamové programy (typu Spamihilator).

### 1.1.3 Kdo a co nás může ještě sledovat?

Při používání prohlížečů internetových stránek není zaručena úplná anonymita uživatele. Většina webových stránek používá tzv. **cookies** (sušenky) – jde o malé množství dat, která server předá prohlížeči a při opětovné návštěvě je prohlížeč naopak pošle serveru zpět. Ten je potom schopen identifikovat uživatele a získat o něm určité informace. Cookies se tedy vyskytují na webových stránkách a jsou nutné pro některé činnosti, ale zároveň odesílají informace o tom, jaké stránky navštěvujete, jaké informace vyhledáváte – útočník je potom využívá například pro posílání nevyžádané cílené reklamy.
Podobně se na webových stránkách vyskytují hojně používané **skripty**,[13] přičemž většina z nich je užitečná, pomáhá stránky oživit a uživatelům zpříjemnit. Některé z nich však mohou být vytvořeny se zlým úmyslem, mohou zneužívat bezpečnostní díry v programech a snažit se infikovat počítač nějakým malwarem. Pro tyto účely mohou být vytvořeny i specifické stránky a pokud administrátor svůj web řádně nezabezpečí, může na něj útočník škodlivý skript propašovat. V jednotlivých prohlížečích webových stránek může být spouštění cookies a skriptů (prvků ActiveX) potlačeno, ale potom se stránky nezobrazují úplně – viz dále.
Kromě toho lze dále rozlišovat (v abecedním pořadí):

- **Exploit** (česky: vytěžení) – tento typ využívá bezpečnostní mezery v systému a propašovává do něj malware. Řešením jsou zejména včasné aktualizace programů (viz dále).
- **Grooming** aneb lákání na schůzky představuje jednu z dalších sociotechnik (viz dále).
- **Hijacker** (únosce) alias **URL injection** – mění adresy zadaných webových stránek a přesměruje vás na stránky nežádoucí.
- **Sniffing** (čmuchání) je technika, při níž dochází k ukládání a následnému čtení TCP paketů. Používá se zejména při diagnostice sítě, zjišťování používaných služeb a protokolů a odposlechu datové komunikace. Útočník tak může získat potřebná data. **Sniffing – bot modul** (viz dále) změní napadený počítač v odposlouchávací stanici, jejímž prostřednictvím monitoruje síťový provoz a získaná data posílá útočníkovi. Velmi oblíbené je také rozšíření botu o keylogger (viz výše), který registruje všechny vstupy z klávesnice. Takto může hacker získat uživatelská jména, hesla, čísla platebních karet, licenční klíče apod. Jako ochrana poslouží program Wireshark nebo SpyBot Search & Destroy.

## 1.2 Další častá nebezpečí

Určité webové stránky mohou být nepříjemné i kvůli nevyžádanému předplatnému, problémy mohou nastat také při stahování dat z internetu. U obou z těchto způsobů internetových podvodů mohou problémy nastat především tehdy, jestliže je po vás vyžadována registrace.

### 1.2.1 Nevyžádané předplatné

**Nevyžádané předplatné** představuje jednu z dalších možností podvodů pomocí internetu (přičemž nemusí být právně postižitelné). Většinou tento trik funguje tak, že zmínka o nutnosti za nějakou službu

13 Někdy nazývané i prvky ActiveX.