# Zabezpečte si své PC za 10 minut

Nechráněný počítač je pro internetovou mafii lákavé sousto, takže šance, že unikne její pozornosti, je minimální. My vám poradíme, jak se lze proti podobným útokům chránit. Navíc vám ukážeme, jak počítač **ZABEZPEČIT BĚHEM NĚKOLIKA MINUT**...

FABIAN VON KEUDELL

Vaše peníze chrání bankovní sejf, vaše auto imobilizér a alarm – svá data však máte na počítači „volně dostupná". Tento model chování, který je bohužel příznačný pro velké procento uživatelů, znamená pro internetovou mafii jediné – ráj. Profesionální hackeři totiž s minimální námahou rabují konta neopatrných uživatelů a se získanými penězi svůj „business" dále zdokonalují. Asi nikoho už nepřekvapí odhady odborníků, že zisky internetové mafie dávno překonaly její (mnohem rizikovější) aktivity na poli drog a zbraní...

## Vaše volba

Je pouze na vás, zda se zařadíte mezi okrádané, nebo zda se postavíte hrozbě čelem. My se vás pokusíme přesvědčit o tom, že druhá možnost nemusí být nijak náročná. Je sice jasné, že během několika minut ze svého počítače neuděláte nedobytnou pevnost, rozhodně se však nestanete obětí prvního hackerského útoku. Věnujte zabezpečení svého počítače alespoň deset minut a pomocí našich tipů a nástrojů odolá váš počítač i zákeřnějším útokům. Poradíme vám také, jak zabezpečit notebook, aby byl k nepotřebě i případnému zloději. Počítejte tedy s námi...

### Jedna minuta: Instalace záplat

První krok je už poněkud ohraná písnička – záplaty do Windows. Celá řada uživatelů nad nimi mávne rukou a prohlásí, že jim Windows fungují bez problémů (nebo mají pirátskou verzi a funkce Windows Update se bojí). Celá „legrace" se záplatováním se však ukáže v jiném světle, uvědomí-li si uživatel, že doposud bylo ve Windows XP a Windows Vista nalezeno více než sto bezpečnostních děr, tedy více než sto všeobecně známých potenciálních bran pro hackery.

V celé řadě případů stačí jednoduchý řádek kódu, aby byl systém oběti paralyzován – bez ohledu na to, jestli je disk zašifrován, jestli je nainstalován antivirový program, nebo zda uživatel pracuje bez oprávnění administrátora. Jediným řešením tedy stále zůstává „záplatování".

Pozor! Poměrně často lze narazit na uživatele, kteří si u automatických aktualizací nastavili jen jejich „oznamování", protože si chtěli jejich stahování a instalaci řídit sami. Po několika dnech ale na nastavení zapomenou a malá ikonka v systémové liště už jejich pozornost neupoutá. Pokud tedy chcete mít svá Windows vždy v nejlepší možné kondici, nechte vše pod kontrolou Windows.

Postup: Klikněte na nabídku »Start«, zvolte »Ovládací panely | Automatické aktualizace« a zde vyberte možnost »Automaticky (doporučeno)«. Aktualizace váš počítač zpomalí vždy jen na pár desítek sekund a instalace poté běží automaticky na pozadí.

### Jedna minuta: Instalace virového skeneru

Výrobci antivirových nástrojů denně detekují přes 6 000 nových typů hrozeb. Pokud není váš systém chráněn, mohou si viry a malware snadno najít cestu do počítače. Tam pak mažou soubory nebo čmuchají ve vašich datech. V našem velkém srovnávacím testu bezpečnostních balíků (v Chipu 01/2009) se jako nejlepší antivirová řešení ukázaly výrobky firmy Symantec **(www.symantec.cz)**, Kaspersky **(www.kaspersky.cz)** a F-Secure **(www.f-secure.cz)**.

Instalace antivirového programu zabere přibližně jednu minutu a rozhodně to bude jedna z nejlépe využitých minut vašeho počítače.

Výhodou antivirových nástrojů je skutečnost, že mají integrovánu zvláštní „heuristiku", aby byly schopny ochránit počítač i před novými hrozbami. Funguje to takto:

## NA DVD

### Nástroje proti hackerům

**EasyCrypto Deluxe** ► nástroj pro šifrování souborů a složek

**Mozilla Firefox 3** ► alternativa Internet Exploreru

**IE7 pro** ► vylepšená verze Internet Exploreru

**KeePass** ► nástroj na ukládání hesel a informací

**Logon Key** ► pomůcka pro bezpečnější přihlašování

**NoScript** ► rozšíření chránící Firefox před nebezpečnými skripty

**Spamihilator** ► nejrozšířenější nástroj proti spamu

**Thunderbird** ► alternativní poštovní klient

**TrueCrypt** ► nástroj na šifrování disků

**Wireshark** ► pomocník pro analýzu síťové komunikace

► **NA DVD:** Všechny nástroje najdete na DVD pod indexem **ZABEZPEČENÍ**.

# Antiviry dokáží zablokovat i útoky hackerů


**Vše v jednom:** Alternativou je použití kvalitního bezpečnostního balíku, který vás ochrání nejen před viry, ale i před malwarem a spamem...

Nástroj „na pozadí“ ověřuje, zda je forma spuštění charakteristické „virové povahy“, a jakmile virový skener detekuje potenciální malware, upozorní uživatele a přesunuje malware do karantény. Virový skener zároveň zasílá podezřelý kousek výrobci antiviru (tedy pokud je tato možnost povolena), který posléze aktualizuje signatury. I z tohoto důvodu je vždy důležité pravidelně aktualizovat virový skener.

## Tři a půl minuty: Antispamové nástroje

Podle společnosti Sophos, výrobce bezpečnostního softwaru, tvoří přibližně 92 procent všech e-mailových zpráv spam. Ucpaná e-mailová schránka je pak jen jedním z mnoha rizik, která spam přináší.

Z hlediska bezpečnosti počítače je mnohem důležitější skutečnost, že velké procento spamu v sobě skrývá další hrozby. Použití antispamového filtru tak nejen odlehčí vašemu mailboxu, ale také odfiltruje velké procento potenciálních hrozeb. Antispamových programů existuje celá řada, my doporučujeme nástroj Spamihilator, který vám pomůže vytřídit reklamy a hrozby z vaší pošty a který najdete i na našem DVD. Na rozdíl od antivirového nástroje ale samotnou instalací „práce nekončí“.

Zasilatelé spamu neustále mění své adresy a speciální opatření providerů obcházejí pomocí vkládání zvláštních znaků nebo pomocí méně používaných formátů pošty. A jak Spamihilator funguje? Nejprve je nutné si uvědomit, že tento nástroj je efektivní pouze s e-mailovými klienty typu Outlook či Thunderbird, a to především proto, že Spamihilator pracuje jako „proxy server“ mezi providerem a poštovním klientem. Během stahování pošty kontroluje všechny maily na podezřelý obsah, a pokud je to nutné, vymaže ho.

Tímto způsobem eliminujete i spam, který pronikl bezpečnostním sítem providera (při nasazení Spamihilatoru u českých freemailů lze dosáhnout téměř stoprocentní účinnosti).

**V PRAXI:** Nejprve si z DVD nainstalujte Spamihilator. Nástroj automaticky identifikuje přednastaveného mailového klienta a použitý protokol. Nejsou nutná žádná jiná nastavení, protože nástroj ihned nastaví nejdůležitější filtry, především efektivní DCC

filtr (Distributed Checksum Clearinghouse). Ten funguje takto: Jakmile obdržíte mail, Spamihilator okamžitě zašle jeho kontrolní součet na DCC server. Zde se zjišťuje, kolikrát mail s tímto kontrolním součtem byl již dříve poslán. Pokud se tak stalo vícekrát, DCC server zprávu klasifikuje jako spam a informuje Spamihilator. Spamihilator pak příslušný mail vytřídí. Kromě DCC filtru je Spamihilator vybaven také klasickými antispamovými opatřeními – od filtrování zadaných pojmů až po blacklist a whitelist. K nakonfigurování těchto funkcí spusťte svůj poštovní program a klikněte pravým tlačítkem na symbol Spamihilatoru. Poté zvolte možnost „Tutorial“ a klikněte na »Další...«

Vidíte-li nějaký e-mail od známé osoby, otevřete ho pomocí „Read Message“. Pokud se i pak ukáže, že jde o nevyžádanou poštu, označte ji jako „spam“. Po několika podobných „operacích“ si Spamihilator zapamatuje obsah mailu a další podobné maily automaticky vymaže.

Důležitou doplňkovou funkcí jsou „whitelisty“. Ve Spamihilatoru v nabídce »Settings | Sender« přidejte všechny své přátele do tohoto seznamu („my friends“) – lze to udělat i pomocí metody drag and drop. Pokud vám spam chodí i nadále, je čas vylepšit váš poštovní program. Chip vám ukáže, jak efektivně nastavit Outlook a Thunderbird.

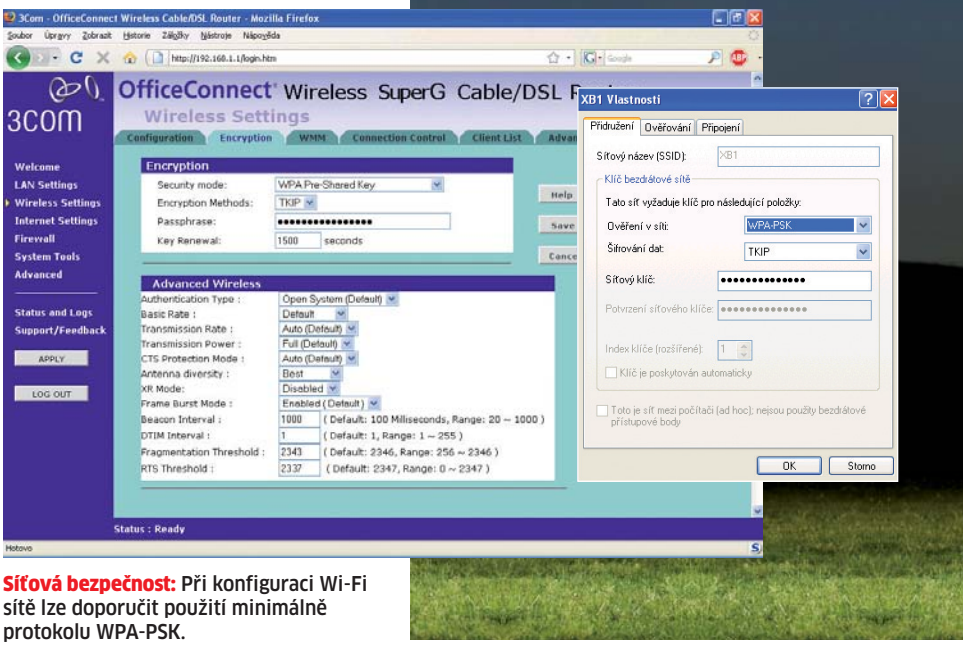
**OUTLOOK:** Abyste tohoto poštovního klienta od Microsoftu udrželi „čistého“, zvolte »Nástroje | Možnosti«. Zde v kartě předvolby (v sekci E-mail) klikněte na tlačítko »Nevyžádaná pošta...«. V okně, které se objeví, nastavte vysokou úroveň ochrany.

Dále nastavte, aby Outlook ihned vymazal spamové maily, jinak jimi bude složka „Nevyžádaná pošta“ zaplavena. Ve finále nezapomeňte určit whitelist (zde se jmenuje „Bezpečí odesilatelé“), který bude zahrnovat všechny kontakty z vašeho adresáře Outlooku.

**THUNDERBIRD:** Také nástroj Mozilly si dokáže zapamatovat maily, které klasifikujete jako spam. Vše, co musíte udělat, je informovat klienta o postupu, jak nakládat se zjištěnou nevyžádanou poštou. Pro tento účel zvolte nabídku »Tools | Options | Data protection «. Zde aktivujte položku „If messages...“ a opusťte nastavení. Nyní jakmile obdržíte spamový mail, označte ho a klikněte na »Junk« v seznamu symbolů. Čím častěji to provedete, tím efektivněji Thunderbird spam vytřídí.

## Jedna minuta: Nastavení WPA2 u Wi-Fi

Windows důvěřují počítačům v uzavřené síti více než datům z webu. To je sice dobré, ale ne pokud víte, že hacker potřebuje pouhých 50 sekund, aby se pomocí Wi-Fi naboural do interní sítě (tento údaj platí, pokud není Wi-Fi síť zabezpečená nejnovějšími šifrovacími postupy). Ukážeme vám, jak během chvíle vytvořit z potenciálního rizika bezpečnou síť.




**Síťová bezpečnost:** Při konfiguraci Wi-Fi sítě lze doporučit použití minimálně protokolu WPA-PSK.

Nejdůležitější „položkou“ sítě je router – hlavní komunikační centrum. A právě na jeho zabezpečení se nyní podíváme. Příklady nastavení vám ukážeme pomocí routeru FritzBox WLAN 7270, u jiných výrobců ale budou stejná nebo podobná. Naprostá většina routerů (snad kromě Air-Port Extreme od Applu) může být nakonfigurována přes webové rozhraní. Pro přístup k jejich konfiguraci tedy stačí do adresní lišty prohlížeče zadat například **http://fritz.box**.

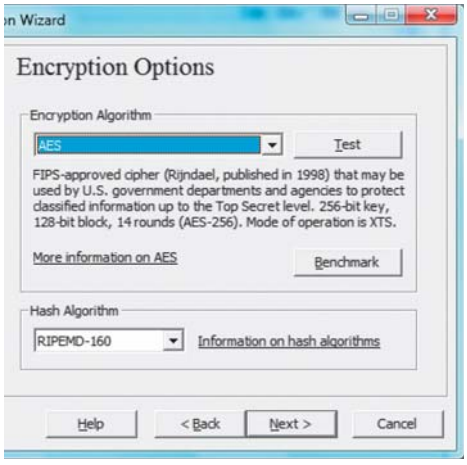
U jiných modelů může být požadováno zadání IP adresy (obvykle bývá 192.168.1.1). Tu můžete zjistit následujícím způsobem: V nabídce Start klikněte na »Run« a zadejte „cmd“. Poté do příkazového řádku zadejte příkaz ipconfig a potvrďte stisknutím klávesy [Enter]. Požadovanou IP adresu najdete pod označením „Výchozí brána“. Jakmile do prohlížeče zadáte adresu routeru, zařízení vás vyzve k zadání hesla administrátora. Většina zařízení má určitá implicitní nastavení (pro FritzBox je například „User name“ „admin“ a heslo prázdné.), ta je však nutné ihned po přihlášení změnit – tedy pokud nechcete, aby vám po zadání implicitního hesla později síť konfiguroval cizí hacker...

Heslo lze změnit (u modelů FritzBox) například tímto způsobem: Klikněte na »Settings | Advanced settings | System« a zde na «Fritz-Box password». U položky „Activate password protection for this Fritzbox“ aktivujte zatržítko a zadejte nové heslo.

Abyste změnili zabezpečení původní sítě, postupujte následovně: V nastavení routeru si můžete vybrat mezi šifrovacími metodami WEP (Wired Equivalent Privacy), WPA – PSK (WiFi Protected Access – Pre Shared Key) a WPA2 – AES (WiFi Protected Access2 – Advanced Encryption Standard).

Metoda WEP je z hlediska bezpečnosti poměrně nespolehlivá, protože může být cracknuta pomocí speciálního softwaru během několika minut. Stará zařízení s WEP šifrováním ohrožují celou síť. Spoléhejte se tedy pouze na WPA. Vědečtí pracovníci již přišli s teoretickou metodou, jak hacknout „Pre-Shared Key“, v reálném světě však stále platí ochrana pomocí šifrování WPA – PSK za bezpečnou. Jak tedy v praxi změníte šifrování sítě?

Nejdříve v nabídce »Advanced settings | WLAN« klikněte na »Network settings« a zaškrtněte zatržítko vedle „Activate




**Přísně tajné:** Program TrueCrypt dokáže zašifrovat celý disk, takže zloději nepomůže ani krádež celého počítače...


**Přihlaste se prostřednictvím USB disku:** Program Logon Key dokáže zabezpečit a zrychlit přihlašování a odhlašování...

## INFO

### Šifrování USB disku

Mnoho uživatelů ukládá na svůj USB flash disk i důležitá data a neuvědomuje si, že jsou tam zcela nechráněná. Existují sice dražší, otiskem prstu chráněné USB disky, my vám však poradíme mnohem jednodušší řešení, nabízející kompletní ochranu vašich dat.

**OCHRANA PROTI HACKERŮM ZDARMA**

Program TrueCrypt (najdete ho jak na našem DVD, tak i na adrese **www.trucrypt.org**) dokáže zašifrovat disk pomocí 256bitového klíče a AES kódování.

**PROTI HACKERŮM V PRAXI**

Sandisk (**www.sandisk.com**) vyvinul platformu U3, nabízející na USB disku další partition. Kromě jiného na tomto disku najdete i software umožňující obsah zašifrovat. Tyto USB disky stojí jen o něco málo více než klasická média.

network (WLAN)“. Nyní si v sekci „Name of the network SSID“ zvolte jméno sítě. To se později objeví na seznamu dostupných sítí pod Windows.

Poté otevřete konfigurační dialog FritzBoxu a postupně se proklikejte k nabídce »Settings | Advanced settings | WLAN«. Zde v sekci „Security“ aktivujte položku „Activate WPA-encryption“ a poté v sekci „WPA mode“ zvolte mod „WPA+WPA2“.

Opět si zvolte heslo, pomocí něhož budete později moci přidat k bezdrátové síti individuální klienty. Heslo, alespoň deset znaků dlouhé (obsahující písmena i číslice), vložte do položky „WPA-Network key“. Bezpečnostní nastavení aktivujte kliknutím na tlačítko »OK«.

## Jedna minuta: Přihlášení pomocí USB

Většina z vás určitě zná upozornění „Nikdy nenechávejte svá zavazadla bez dozoru“. To, co platí pro vaše cestovní zavazadla, by mělo platit i v případě vašeho PC. Především u mobilních zařízení by měla být ochrana prioritou. Zabezpečení účtu uživatele heslem je víc než běžné, kdo si ale zamyká počítač pokaždé, když chce jít jen na kávu? Zkušenější uživatelé používají klávesovou zkratku [Win]+[L], neustálé manuální přihlašování ale není zrovna pohodlné. Zajímavější alternativou je nástroj Logon Key. Program, který najdete na našem DVD, používá standardní USB jako autentifikační zařízení.

Funguje následujícím způsobem: jakmile je USB odpojeno, počítač se automaticky uzamkne.

S prací můžete pokračovat, až když USB opět připojíte. Nástroj je možné zdarma 30 dnů zkoušet, poté se můžete sami rozhodnout, jestli je tato ochrana pro vás to pravé. Cena kompletní verze je 21 eur.

Mechanismus nástroje je jednoduchý. Jako první si nainstalujte program Logon Key, poté nastavte USB disk jako hlavní „password medium“.

To provedete takto: Připojte USB disk do portu a v okně programu Logon Key, které se objeví, klikněte na »Configure USB stick«. V dalším okně vložte své heslo do Windows a klikněte na »OK«. Abyste zaručili, že se PC automaticky zamkne, jakmile bude USB disk odpojen, klikněte na »Options« a zvolte příkaz »Execute | Lock«. Nastavení potvrďte pomocí »OK«. Od dalšího restartu už můžete používat svůj USB flash disk jako své „zabezpečovací zařízení“. Další výhodou, kterou tento způsob zabezpečení přináší, je rychlé přihlášení – stačí jen zasunout USB disk a jste přihlášeni...

## Jedna a půl minuty: Používejte Password Safe

Bezpečné heslo obsahuje alespoň dvacet znaků a jde o kombinaci velkých a malých písmen, číslic a zvláštních znaků. Každé konto pak samozřejmě musí mít jiné heslo. Jak jste na tom s pamětí? Program Password Safe vám pomůže zapamatovat si hesla, abyste nemuseli při každém přihlašovacím dialogu panikařit. Vše, co budete potřebovat, je hlavní heslo – o ostatní se postará program. Podobně funguje i program KeePass 2.06, který jako freeware najdete i na našem DVD.

Použití v praxi: Dříve než je možné v programu ukládat hesla, je nutné nejprve nastavit zabezpečení. Klikněte na »File | New« a určete umístění v paměti. V nabídce „Master Password“ si určete tzv. „master key“ – pomocí tohoto klíče budete později moci přistupovat k uloženým datům. Nastavení potvrďte dvojitým kliknutím na »OK«. Pomocí příkazu »Edit | Add entry« pak můžete vložit nové heslo k zapamatování.

Ukážeme vám, jak to funguje například pro freemail Email.cz. V programu KeePass po vytvoření nového hesla zadejte v sekci „Title“ název pro heslo (například Email.cz), pak do „User name“ vložte své přihlašovací jméno a do políček „Password“ a „Repeat“ své heslo. Nakonec vše potvrďte kliknutím na »OK«. Pokud se poté chcete automaticky přihlásit ke svému mailu, označte zvolenou položku v programu KeePass, přejděte na adresu freemailu a stiskněte klávesovou zkratku [CTRL]+[ALT]+[V].

## Jedna minuta: Šifrování disku

Po provedení všech výše zmíněných opatření je váš počítač z 95 procent zabezpečen proti útokům. O zbývajících pět procent se postará kódování kompletního disku pomocí nástroje TrueCrypt (který také najdete na našem DVD). Nainstalujte si program a v menu klikněte na »Encrypt | System«. Spuštění šifrování pomocí tohoto průvodce vám nezabere ani minutu, samotný proces šifrování trvá 20 až 30 minut v závislosti na velikosti disku.

AUTOR@CHIP.CZ