Knihovnicko-informační zpravodaj U Nás
Vyšlo: 16. 3. 2017
Číslo: Ročník 27 (2017), Číslo 1
Sekce: Jak na to?
Název článku: Jak na bezpečné internetování
Autor: Zuzana Němcová
Zdroj: http://www.svkhk.cz/Pro-knihovny/Zpravodaj-U-nas/Clanek.aspx?id=20170115

Jak na bezpečné internetování

Zuzana Němcová

Komunikační technologie v posledních letech zažívají obrovský vzestup a rychlý vývoj, což můžeme pozorovat i u internetu. Ten se stal běžnou součástí života lidí, dokonce u mnohých součástí nepostradatelnou. Masové využívání nástrojů, které internet nabízí, s sebou přináší mnoho výhod a přínosů, má ale také negativní stránky. Poskytuje totiž anonymizované prostředí, ve kterém se neopatrný či nedostatečně informovaný uživatel může snadno stát obětí nekalého jednání, nebo dokonce nechtěně přivést do nepříjemností někoho z blízkých. Proto jsem pro vás sumarizovala několik důležitých zásad bezpečného chování na internetu.

V rámci obrany proti virům používejte kvalitní a aktuální antivir, antispyware, firewall a pravidelně aktualizujte používaný operační systém a užívané programy. Vždy se ujistěte, že software, který instalujete, pochází z důvěryhodného zdroje. Důležitá, citlivá a osobní data pravidelně zálohujte. Pamatujte, že smazaná data nejsou na disku ve skutečnosti smazána, ale pouze označena k přepsání. Pro skutečné vymazání je nutné je mnohonásobně přepsat nebo použít specializovaný software.

Používejte vždy silné heslo – minimálně o délce osmi znaků, obsahující malá a velká písmena, číslice, diakritiku a jiné znaky; nemělo by jít o obvyklé slovo nebo frázi a nemělo by být odvoditelné od osoby vlastníka. Heslo dostatečně často obměňujte a nepoznamenávejte ho nikde v okolí místa zadávání. Doporučuje se také neukládat hesla do prohlížeče a nepoužívat stejné heslo pro více služeb.

Pro větší zabezpečení dat na disku je vhodné použít program pro jejich šifrování, například TrueCrypt. K zabezpečení e-mailové komunikace používejte vhodné programy, jako PGP, GnuGP aj. Informujte se také o možnosti dvoufázového ověřování pro přihlášení do svého e-mailu.

Podvodníkům se můžete vyhnout i tak, že budete pozorní při vyřizování své pošty - neodpovídejte na podezřelé e-maily nebo zprávy a neotvírejte neznámé či podezřelé soubory, programy nebo přílohy zpráv. Pokud zpráva žádá o přeposlání vašim dalším kontaktům, může se jednat o tzv. hoax neboli poplašné, zbytečné, nebezpečné a podvodné řetězové zprávy. V tomto případě doporučuji podívat se na http://www.hoax.cz/cze/, kde se nachází pravidelně aktualizovaná databáze takovýchto zpráv, ve většině případů spolu s odborným komentářem.

Nepište na neznámé stránky, které po vás žádají osobní informace, nebo dokonce informace o vašem majetku. U podezřelých stránek vždy zkontrolujte jejich skutečnou adresu v řádku prohlížeče.

Připojujte se k internetovému bankovnictví, e-mailové schránce či jiným citlivým službám zásadně přes šifrovaný protokol – poznáte jej tak, že adresa začíná písmeny HTTPS a je doplněna ikonkou malého zeleného zámečku (někdy také názvem stránky).

Pomocí automatického dokončování úloh například v prohlížeči (ale i v systému) je možné zabránit dalšímu objevování hlášek. Zde je na místě zvážení, zda je dobré automatickou akci potvrdit, protože kvůli automatickému dokončování již o podobné situaci nebudete příště informováni. Platí tedy obecná zásada - nejprve čtěte, pak klikejte.

Nikdy neposílejte přes internet důvěrná data (číslo kreditní karty nebo hesla). Když už o sobě nějaké údaje poskytujete, zvažte, jaká data a komu vkládáte do rukou. Například při zakládání účtu v e-shopu není většinou nutné vyplňovat všechny údaje, ale pouze ty, které jsou označeny (např. hvězdičkou) jako povinné.

K citlivým službám se připojujte pouze z vlastního počítače - nikdy přes neznámou wifi nebo z internetové kavárny. Vhodným zabezpečením komunikace přes neznámou wifi může být VPN – tzv. virtuální privátní síť. U internetového bankovnictví a vlastně jakýchkoli účtů se vždy řádně odhlašujte ze služby (pomocí tlačítka k tomu určeného – nestačí zavřít prohlížeč). Pokud používáte počítač sdílený více lidmi, je možné využít anonymní mód prohlížeče.

K eliminaci rušivých reklam používejte Adblock – rozšíření internetového prohlížeče, které umožňuje blokovat tyto reklamy na stránkách a učinit tak stránky přehlednějšími a mnohdy rychlejšími. Pokud vám není vaše soukromí lhostejné, je dobré v prohlížeči také blokovat tzv. cookies třetích stran.
V sociálních sítích kontrolujte nastavení bezpečnosti a soukromí a určete si, jak a s kým chcete sdílet svůj obsah na síti. Ověřujte si informace a nevěřte hned prvnímu zdroji. Odlišujte spolehlivé a nespolehlivé zdroje. Vždy je lepší vnímat obsah spíše kriticky. Mějte na paměti, že máte i svou digitální reputaci, nereagujte na nevhodné a hanlivé zprávy. Je velice snadné na internet něco umístit, ale prakticky nemožné to vzít zpět.
Závěrečnou myšlenku věnuji tvrzení, že internet sám o sobě není ani bezpečný, ani nebezpečný. Je to velmi užitečné a rychle se vyvíjející prostředí, ve kterém se jako jeho uživatelé sami rozhodujeme, zda se svými kroky vydáme po prověřeném mostě, nebo budeme balancovat na laně.

Kontakt na autorku: zuzana.nemcova@uhk.cz