JAK NA INTERNET

Bezpečnost počítače

Internet je již nedílnou součástí našeho života. Jen málokterá firma nebo osoba s ním nepřišla do styku. Internet využíváme v průběhu celého dne pro pracovní, vzdělávací nebo pro soukromé účely a zábavu. Hlavně však podporuje komunikaci mezi lidmi. Pokud se ale touto džunglí pohybujeme, je opravdu zapotřebí myslet i na to, že ne všichni uživatelé se zde chovají podle pravidel. Ve chvíli, kdy se připojíte do této sítě, jste rázem otevřeni k jakékoliv komunikaci s více než miliardou lidí a strojů, které se zde pohybují. Věřte, že ne všichni uživatelé mají dobré úmysly. Je celkem pravděpodobné, že jste se již setkali, nebo že se v nejbližší době setkáte, s nějakým typem nebezpečí.

Může to být například:

- **Phishing** – vydávání se za různé společnosti za účelem získání osobních informací či šíření virů
- **Vir** – program, který je schopen sám vytvářet své kopie ve vašem počítači, které ho mohou poškodit; k tomu, aby virus nakazil počítač nebo se začal šířit, je obvykle třeba něco udělat, například otevřít nakaženou e-mailovou přílohu
- **Červ** – autonomní program schopný vytvářet své vlastní kopie, které rozesílá do dalších počítačových systémů nebo sítí, kde vyvíjí další činnost, pro kterou byl naprogramován
- **Scam** – e-mail, v němž nás někdo žádá o finanční podporu, nebo který obsahuje lživé informace o výhře v loterii
- **Spam** – nevyžádaná reklamní pošta či jiné nevyžádané sdělení, které je šířeno Internetem
- **Odposlech** – při připojení k Internetu může být vaše komunikace odposlouchávána
- **Podvodné přesměrování domén** – touto technikou se realizuje phishing a jiné typy útoků; uživatel je většinou bez jakéhokoli varování nasměrován na falešný web

Jakým způsobem se na Internetu bránit všemožným útokům a zranitelnostem?

- Legální a pravidelně aktualizovaný operační systém
- Antivirový program a firewall
- Pravidelně aktualizovaný webový prohlížeč
- Používat DNSSEC
- Používat bezpečné heslo

Jak se mohu stát obětí útoku?

Vyhněte se použití pirátských verzí programů. Je to neetické a nelegální. Pirátské verze mohou také obsahovat viry i jiný škodlivý software.

JAK NA INTERNET

Nikdy neotvírejte přílohu e-mailu, která vám přišla od neznámé osoby. Tato příloha může obsahovat nebezpečný vir nebo jiný škodlivý obsah. Pokud máte jakékoliv podezření na nebezpečný obsah, ale přílohu máte potřebu nebo musíte otevřít, zkontrolujte tuto přílohu svým antivirovým programem. Téměř všechny antivirové programy umožňují ještě před spuštěním daného souboru tento soubor zkontrolovat.

Skoro stejné je to i s jinými e-maily. Pamatujte, že například vaše banka vám určitě nepošle zprávu, v níž vás bude žádat o vaše osobní údaje. Nebude vám ani posílat aktivní odkaz na nové stránky internetového bankovnictví. Vždy proto u podezřelých stránek zkontrolujte jejich skutečnou adresu v řádku prohlížeče.

Při surfování na Internetu můžete narazit také na útočnou stránku obsahující vir nebo jiný nebezpečný software. Z 90 % je označena červenou obrazovkou, která vás o tomto stavu informuje. V tuto chvíli máte dvě možnosti – buďto prohlížeč okamžitě zavřít a na danou stránku již nechodit, nebo kliknout na tlačítko „Rychle odsud pryč“.

Rada na závěr

Nevěřte každé informaci, kterou na Internetu najdete, raději používejte zdravý rozum.

CZ.NIC | SPRÁVCE DOMÉNY CZ