Bezpečný Internet – druhy nebezpečí

- Při práci a pohybu na Internetu hrozí nám i našemu počítačovému vybavení řada nebezpečí.
- Řekneme si, jak postupovat, aby práce s Internetem neohrozila naše soukromí, nebo techniku, kterou využíváme.

- Ohrožení software, počítačových dat a hardware – viry a trojské koně, spam, spyware.
- Ohrožení soukromí – zneužití a krádež různých dat, osobních dat – Phishing, Spoofing.
- Ohrožení osobní bezpečnosti – případný kontakt s nebezpečnou osobou, vydávající se za někoho jiného – email, komunikační programy, Facebook, sociální sítě.
- Ohrožení důstojnosti – kyberšikana.

- Při užívání Internetu stále více používáme aplikace sloužící ke komunikaci mezi účastníky – ICQ, Skype, Chat, Facebook, stahujeme do počítače soubory a programy.
- Množství jiných uživatelů Internetu se tak o nás může dozvědět řadu informací a s přenosem dat z Internetu můžeme do počítače přenést i řadu nebezpečí..

Bezpečný Internet – zásady

- Vždy mít na počítači nainstalován antivirový program. Existuje řada antivirů, placených i volných – **AVG, Norton Antivirus, Nod 32**…… Pro uživatele legální licence Windows je zadarmo a volně ke stažení **program Microsoft Security Essentials.**

- Existuje řada programů dalších k odstranění škodlivých programů – **Spyware Doctor, Advanced Systemém Care, Ad Aware SE Personal, AVG Antispyware…,** které jsou volně stažitelné z Internetu.

- Aktualizovat operační systém a programy. Tyto aktualizace obsahují prvky zabezpečení systému i různých programů.

- Mít zapnutu nějakou **bránu Firewall.**

- Věnovat zvýšenou pozornost **odkazům na web**! Mnoho podvodů na internetu spoléhá na kliknutí uživatele na vložený link.

- Pokud **e-mail,** který jste neočekávali **obsahuje nějaký odkaz**, je lepší napsat odkaz raději přímo do webového prohlížeče. Pokud webový odkaz pochází ze stránky, kterou často navštěvujete, použijte raději vaše internetové záložky pro přístup na tuto stránku.

Bezpečný Internet – zásady

- **Neotevírat nevyžádanou poštu**, mazat ji a neodpovídat na ni.
- Je vhodné **být opatrní při předávání svých osobních nebo finančních údajů** na Internetu. Nevyplňovat formuláře v e-mailech, které vás žádají o osobní nebo finanční informace.
- **Používat silná hesla** a neopakovat je.
- **Pohybovat se obezřetně v prostředí sociálních sítí**. Místo pravého jména používat spíše **nickname – přezdívku**.
- **Zvážit, které údaje uvedu do svého profilu v sociální síti.**
- Být opatrní také při **umisťování soukromých fotografií na Internet**.
- **Důležité:** To co jsme umístili na Internet, se odtud velmi těžko definitivně odstraňuje a může se to kdykoli objevit, i za delší dobu.
- I vyhledávač může najít a zveřejnit některé informace z profilů, které by měly být soukromé, a zobrazí je komukoliv.

Bezpečný Internet

- **Nebezpečí škodlivých programů – viry, spyware, spam.**
  - Počítačové viry jsou programy, které se dokáží samy šířit bez vědomí uživatele. Některé viry mohou škodit počítači i programům (např. mazat soubory na disku), některé jsou poměrně neškodné popřípadě pouze obtěžující.
  - Spyware je program v počítači, jenž bez vědomí uživatele odesílá data přes internet. Ta mohou být vyhodnocena a zneužita k různým účelům, jako je přístup k citlivým datům, heslům nebo v některých případech pouze k lepšímu cílení reklamy.
  - Spam je nevyžádané, většinou reklamní sdělení hromadně rozšiřované prostřednictvím internetu. Mohou to být nevyžádané reklamní e-maily, spamem jsou již postiženy i ostatní druhy internetové komunikace.

- **Mezi nebezpečí hrozící z internetu patří také různé triky a podvodná jednání.**
- Phishing je podvodné jednání s cílem vylákat vaše osobní data jako např. čísla kreditních karet, hesla a další důležité údaje. Dá se také popsat jako krádež identity nebo jako typ sociálního inženýrství. Někdy se pro něj v češtině razí název „rhybaření“.

- Falešné webové stránky – Spoofing – používání podvodných informací, za účelem přesvědčit člověka, že je na pravé webové stránce. Cílem je a přimět ho prozradit své osobní údaje, jako je např. číslo kreditní karty, heslo k účtu apod.

Kyberšikana: co všechno se pod tím skrývá?

- **Kybernetická šikana (kyberšikana)** – druh šikany, kdy se při trýznění oběti zneužívají nové technologie: internet a mobil.
- **Mezi projevy kyberšikany patří:**
- Nadávky a výhrůžky přes SMS, mail nebo chat. Mnohdy nevíme, kdo je autorem útoku.
- Někteří spolužáci nebo, známí tě záměrně přehlížejí při různých činnostech na internetu – v různých skupinách na internetových fórech nebo v online hrách.
- Urážky, které náhodou najdeme někde zveřejněné na internetu (Facebook). Někdo se někomu posmívá, třeba spolužákovi a ten nemá možnost se proti tomu bránit.
- Zveřejnění e-mailu nebo SMS se soukromými informacemi. Vadí nám, že se k soukromým informacím dostávají lidé, kterým nejsou určeny.
- Ponižující filmy a fotky. Předávání dalším osobám, případné zveřejnění na internetu může být velmi ponižující.
- Někdo vytváří nepřátelské stránky nebo skupiny, které mají jediný cíl: zesměšnit jedince a ponížit jej.
- Telefonický teror: neustále nám někdo telefonuje, prozvání nás nebo různě vyhrožuje.

Desatero bezpečného Internetu

- Chraňte svůj počítač před viry a jinými hrozbami . Není rozumné otevírat přílohu zprávy, která přišla z neznámé adresy (pozor na soubory s příponou .exe).
- Ne všechny informace, které najdeme na internetu jsou pravdivé.
- Neposílejte nikomu, koho neznáte, svou fotografii a už vůbec ne intimní. Svou intimní fotku neposílejte ani kamarádům – nikdy nevíte, co s ní mohou někdy udělat.
- Hesla (k e-mailu i jiné) nesdělujte ani blízkým kamarádům.
- Neodpovídejte na neslušné, hrubé nebo vulgární maily a vzkazy. Nevšímejte si jich.
- Nedávejte nikomu neznámému adresu ani telefon.
- Nedomlouvejte si schůzky přes Internet, aniž byste o tom řekli někomu jinému (rodičům).
- Pokud narazíte na obrázek, video nebo e-mail, který vás svým obsahem šokuje, opusťte webovou stránku.
- Svěřte se dospělému, pokud vás stránky nebo něčí vzkazy uvedou do rozpaků, nebo vás dokonce vyděsí.
- Nenechte se přinutit ke komunikaci s protějškem, se kterým se nechcete bavit.

Zdroj: www.bezpecnyinternet