

Jaké hrozí nebezpečí v oblasti informačních technologií

Počítačové podvody, úniky dat, pomluvy, škodlivé kódy a viry, spamy – tyto všechny představují nebezpečí, které si mnohdy neuvědomujeme. Hasičský záchranný sbor JMK ve spolupráci s Policií ČR – Krajské ředitelství Brno a Diecézní charitou Brno Vám poradí, jak se vyhnout nepříjemnostem spojených s tímto nebezpečím.

Možná nebezpečí a obrana proti nim

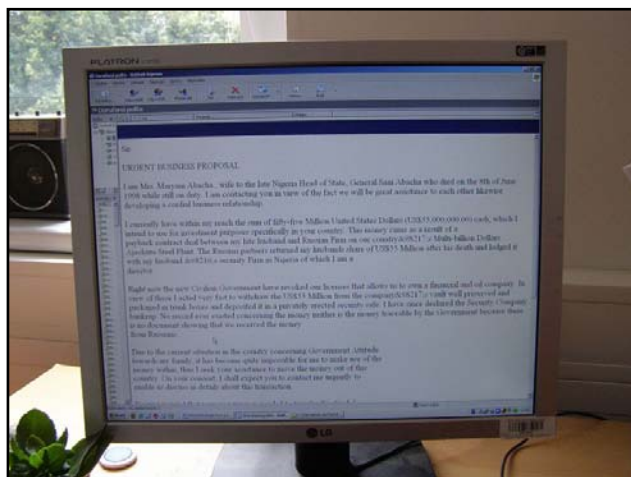
Podvody

Počítačové podvody mohou mít různé podoby (podvodné aukce, snaha vylákat z lidí různé platby, atd.).

Proslulé jsou především tzv. **nigerijské podvody**, kdy je důvěřivcům nabízen podíl z částky ve výši desítek milionů za pomoc s převodem peněz do zahraničí. Když vyhlédnutá oběť na něco podobného kývne, dostává se do nekonečného kolotoče nutnosti platit různé manipulační poplatky, úplatky, nečekané výdaje apod. Člověk tak neustále vkládá čím dál víc peněz, protože si nepřipouští, že by mohl předchozí investici prohrát (syndrom gamblera).



Obr. 1: Využívání informačních technologií.



Obr. 2: Detail tzv. nigerijského dopisu.

důvěryhodných příběhů (bezpečnostní ověření, selhání hardware apod.) se tak hackeři dostanou k Vaším důvěrným informacím.

Obrana:

- maximální obezřetnost, zejména v oblasti internetového bankovníctví,
- ověřovat informace,
- využívat pouze oficiální informační kanály bank (např. neklikat na odkazy, které přijdou v emailu),

Obrana:

- obezřetnost,
- ověřovat předkládaná tvrzení,
- nenechat se zlákat nesmyslnými nabídkami.

Phishing (nebo-li „lov informací“)

Jedná se o snahu vylákat z důvěřivého uživatele soukromé informace (např. přihlašovací jméno a heslo k bankovnímu účtu). Za využití falešných webových stránek nebo

- nesdělovat citlivé informace (číslo účtu, PIN, heslo) na telefonický dotaz (může se jednat o „voice phishing“),



Obr. 3: Kontrola stavu bankovního účtu po platbě kartou.

- hlídat si pravidelně stav svého bankovního účtu (a to i v souvislosti s možnými neoprávněnými „opravnými“ platbami kartou, kdy si obchodník může bez Vašeho vědomí strhnout z účtu doplatek za již dříve dodané a zaplacené zboží či služby).

Pomluva / hoax

Prostřednictvím elektronické pošty se mohou šířit různé **pomluvy**. Takovým příkladem jsou např. řetězové dopisy o závadných potravinách v některých hypermarketech, zaručené zprávy o blížícím se krachu nějaké banky a nutnosti vybrat z bankomatu co největší hotovost a další podobné zprávy. Na závěru každé z nich se zpravidla objeví: „Pošlete co nejvíce lidem.“

Podobným způsobem funguje tzv. **hoax**, vymyšlené zprávy senzačního charakteru, a na ně často navázané různé petice proti popisovanému jevu (např. případ „koťátka ve zkumavkách“).

Obrana:

- nepomáhat šíření nesmyslných nebo lživých zpráv,
- ověřovat informace,
- jestliže se stanete obětí pomluvy, zatněte zuby a případ nerozmazávejte,
- nepřipojovat se k pochybně vypadajícím peticím, slouží jen k získání údajů o Vás.



Obr. 4: Ověřování informací.

Škodlivé kódy a viry

Patří k nejstarším nebezpečím. První viry se objevily již před čtvrt stoletím. Z pouhých vandalských nástrojů, jejichž cílem bylo napadnout co nejvíce počítačů a smazat z něj nějaká data, se vyvinuly nesmírně silné aplikace, které jsou schopné zjistit hesla k internetovému bankovníctví, provádět průmyslovou špionáž, instalovat na počítač další nástroje apod.

Příkladem mohou být tzv. **dialery** – programy, které modifikují volané číslo v případě internetového spojení realizovaného přes telefonní linku. Namísto několika korun za hodinu je pak spojení s internetem realizováno pomocí linky třeba na Kajmanských ostrovech a sazba je v řádu desítek korun za minutu.

Obrana:

- obezřetnost,
- vyhýbat se nebezpečným webovým stránkám a zdrojům,
- používat legální software,
- používat kvalitní antivirový program.

Spam (nevyžádaná elektronická pošta)

V dnešní době představuje 70 – 90 % celkového objemu veškeré elektronické pošty. Jedná se o zprávy, o které nikdo nestojí, nicméně boj s tímto fenoménem je velice obtížný. Jaké představují spamy nebezpečí? Kromě toho, že zbytečně vytěžují kapacitu elektronické pošty, mohou být spamy nositeli virů, podvodů anebo slouží k průzkumu bojem pro hackery apod.

Obrana:

- snažit se o to, aby se Vaše e-mailová adresa nedostala do rukou útočníků (nezveřejňovat ji na webu, nevyplňovat internetové formuláře, nepřeposílat hromadnou poštu s kontakty na předchozí odesílatele atd.),
- neotvírat zejména odkazy a přílohy podezřelých zpráv od Vám neznámých odesílatelů a ihned takovou zprávu odstranit,
- instalovat specializovaný program k filtraci e-mailů.

Chcete se dovědět více o tom, jak se správně chovat při mimořádných událostech? V rámci projektu „Vaše cesty k bezpečí“ Vám Hasičský záchranný sbor JMK ve spolupráci s Policií ČR a Diecézní charitou Brno nabízí další tipy našich chytrých blondýnek, které Vám na webové adrese www.firebrno.cz/vase-cesty-k-bezpeci poradí, jak nejlépe vyřešit i jiné situace, ohrožující Vaši bezpečnost, zdraví, životy a majetek.