//(ne)bezpečný internet

Dnes je internet dostupný prakticky všade.

Len na Slovensku vo februári 2013 prekročil počet užívateľov hranicu 3 miliónov, celosvetovo ich počet za rok 2012 dosiahol 2,3 miliardy. Internet prináša nespočetné množstvo možností a výhod, ako napr. dostupnosť a rôznorodosť informácií, relatívne lacnú komunikáciu nielen prostredníctvom textu, ale aj hlasu a obrazu, multimédiá, nové možnosti zárobku a pod. Je tu však aj nový fenomén, a to bezpečnosť pri používaní internetu a úskalia, akými sú internetová a kyberkriminalita. Informácie o problémoch bezpečnosti na internete nám poskytli Ing. Viliam Koza a Ing. Peter Pálházy zo spoločnosti NWS.

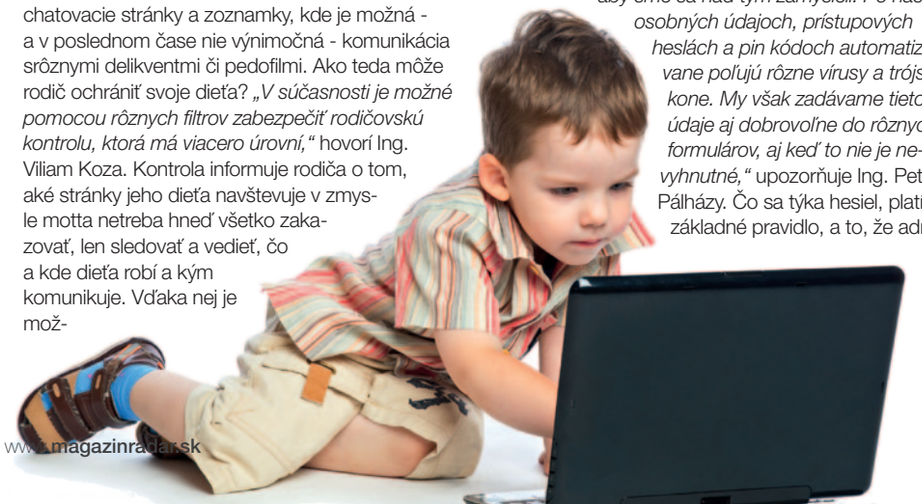
> V SÚČASNOSTI JE MOŽNÉ POMOCOU RÔZNYCH FILTROV ZABEZPEČIŤ RODIČOVSKÚ KONTROLU, KTORÁ MÁ VIACERO ÚROVNÍ

Chráňte svoje deti

Hlavne na tých najmenších, ktorí ešte mnohokrát nevedia vyhodnotiť vážnosť situácie, striehnu rôzne formy nebezpečenstva. Sú to stránky s nevhodným obsahom pre deti, napríklad erotickým či násilným, alebo tiež stránky s návodmi na použitie či výrobu zbraní a výbušnín, sekty a samozrejme rôzne chatovacie stránky a zoznamky, kde je možná - a v poslednom čase nie výnimočná - komunikácia srôznymi delikventmi či pedofilmi. Ako teda môže rodič ochrániť svoje dieťa? *„V súčasnosti je možné pomocou rôznych filtrov zabezpečiť rodičovskú kontrolu, ktorá má viacero úrovní,“* hovorí Ing. Viliam Koza. Kontrola informuje rodiča o tom, aké stránky jeho dieťa navštevuje v zmysle motta netreba hneď všetko zakazovať, len sledovať a vedieť, čo a kde dieťa robí a kým komunikuje. Vďaka nej je možné zablokovať niektoré služby a stránky tak, že sa k nim dieťa vôbec nedostane. Možné je aj získavanie samotného obsahu komunikácie (zaznamenávanie textu, obrázkov, súborov, komunikácie, prípadne aj prístupových hesiel atď.). Existujú tiež systémy, ktoré posudzujú, nakoľko je obsah stránky bezpečný. Napríklad Webutation, ktorý vyhodnocuje reputáciu stránky. Do prehliadačov sa dajú nainštalovať možnosti blokovania stránok pod určitú úroveň dobrej reputácie. Systémy na kontrolu, sledovanie a riadenie práce s internetom sú dostupné nielen domácnostiam, ale aj firmám, ako napríklad systém IMS (Internet Management Systeme) od spoločnosti NWS, prípadne produkt Bezpečný internet od internetového providera.

Chráňte svoje údaje

Spoločnosť si v tomto uponáhľanom a pretechnizovanom svete vôbec neuvedomuje, ale ani sa často nezamýšľa nad tým, aké údaje skladuje vo svojich elektronických zariadeniach a ako s nimi nakladá. Osobné údaje sú stále veľmi jednoducho zneužiteľné a získateľné. Napriek stúpajúcim hrozbám je bezpečnostné povedomie ľudí veľmi nízke. *„Nevedomosť spôsobuje nezáujem, mnohokrát aj ignoráciu a ľahostajnosť. Bežne zadávame svoje osobné údaje, ID čísla rôznych preukazov, dátumy narodenia, adresy, a dokonca aj rodné číslo a čísla kreditných kariet, rôzne prístupové heslá do on-line systémov bez toho, aby sme sa nad tým zamysleli. Po našich osobných údajoch, prístupových heslách a pin kódoch automatizovane poľujú rôzne vírusy a trójske kone. My však zadávame tieto údaje aj dobrovoľne do rôznych formulárov, aj keď to nie je nevyhnutné,“* upozorňuje Ing. Peter Pálházy. Čo sa týka hesiel, platí základné pravidlo, a to, že administrátor alebo správca systému od používateľa nikdy nepotrebuje, aby mu svoje heslo prezradil. Preto pri rôznych registráciách by ste nikdy nemali udávať osobné informácie, napríklad číslo kreditnej karty alebo bankové údaje, poskytnite ich iba v prípade, že je to opodstatnené. Nikdy nezadávajte väčšie množstvo bezpečnostných kódov, ako je nevyhnutné alebo obvyklé, ani ďalšie prístupové parametre, ktoré ste inde nezadávali. Ak je na webovej stránke telefonický kontakt, najprv si overte, prečo od vás tieto údaje žiadajú, a či je spoločnosť vôbec reálna.



> OSOBNÉ ÚDAJE SÚ STÁLE VEĽMI JEDNODUCHO ZNEUŽITEĽNÉ A ZÍSKATEĽNÉ

K dôležitým údajom môžeme zaradiť aj osobné bezpečnostné heslá. Heslá by nemali byť príliš jednoduché, ale ani príliš komplikované, a nemali by ste ani opakovať alebo používať to isté heslo vo viacerých systémoch. Heslá by mali byť ľahko zapamätateľné, aby nebolo potrebné si ich zapisovať, ale zároveň ťažko uhádnuteľné. *„Nemali by byť založené na báze základných osobných údajoch osoby, ako napr. rodné číslo, priezvisko, meno, dátum narodenia a podobne. Ideálna minimálna dĺžka hesla je 8 – 12 znakov, pri dodržaní požiadaviek na zložitosť hesla. Je vhodné, aby heslo obsahovalo malé aj veľké písmená, číslice, ale aj aspoň jeden špeciálny znak,“* hovorí Ing. Viliam Koza. Je potrebné zdôrazniť, že zložitosť hesla výrazne ovplyvňuje bezpečnosť. Existuje však aj praktická pomôcka, ako je možné si heslo napísať napr. na papierik a aj pri jeho strate alebo ukradnutí zaistiť, aby ostalo bezpečné. Ak vás zaujíma, ako je to možné, navštívte užitočnú stránku venovanú tejto problematike www.nebezpecny-internet.sk, ktorú pre vás už za krátky čas spustíme online. Heslo by ste si z času na čas, minimálne raz za rok, mali zmeniť.

Chráňte svoje peniaze

Spoznať neseriózny e-shop alebo predajcu so 100 % istotou sa v podstate nedá. Čo sa opäť dá, je minimalizovať riziko. Na stránke by mali byť uvedené kontaktné údaje a seriózna spoločnosť by mala byť vyhľadateľná v obchodných/živnostenských registroch. Prvýkrát nekupujte väčšie množstvo tovaru alebo drahší tovar. Najprv si overte e-shop menším nákupom. Skúste vyhľadať na internete a na fórach, či na daný e-shop existuje referencia alebo sťažnosti. Problémy môžu nastať aj pri používaní Internet bankingu na verejných počítačoch. *„Na verejných PC by som úplne zakázal zadávanie akýchkoľvek prístupových alebo osobných údajov,“* hovorí Ing. Peter Pálházy z NWS. *„Nikdy totiž neviete, kto tam sedel pred vami, ako je daný prehliadač alebo PC modifikovaný a kto sa k údajom, ktoré ste zadali, dostane. Mohol tam nainštalovať napr. softvérový alebo hardvérový keylogger a pod.“*

Vo všeobecnosti netreba zabúdať ani na bezpečnostné aktualizácie a efektívny antivírový program (AV). Odkedy je internet ľahko dostupný, enormne sa zjednodušila aj možnosť infiltrácie do počítačov prostredníctvom vírusov a rôznych červov. Dokonca v poslednej dobe sú ohrozené nielen počítače, ale aj smartphony a tablety. Denne vznikajú mutácie vírusov a trójskych koňov, ktoré môžu vaše dáta poškodiť alebo spôsobiť ich únik. Preto neaktualizované AV programy sú už po relatívne krátkom čase neúčinné.

Ako hovorí Ing. Viliam Koza zo spoločnosti NWS: *„V súvislosti s používaním internetu sa určite nedá nikdy nebude dať hovoriť o stopercentnej bezpečnosti a taktiež nikdy nebude možné úplne sa ubrániť kyberútokom a nástrahám, ktoré nám tento novodobý fenomén, akým internet bezpochyby je, prináša. Je však možné minimalizovať riziko a okruh ľudí, ktorí by nám prostredníctvom neho chceli alebo mohli ublížiť.“* //