Bezpečne na internete aj v roku 2014

Príchod nového roka je časom predsavzatí. Hodnotíme uplynulý rok, premýšľame o zmenách vo svojom živote, bilancujeme. Ruku na srdce, kto si predsavzal, že bude pravidelne športovať alebo začneme zdravo jesť? Zvyky možno zmeniť. Ba dokonca netreba ani vstať zo stoličky alebo z gauča. Od počítača alebo mobilu. Áno, ide o on-line bezpečnosť, ktorá je stále podceňovaná.

Prinášame vám niekoľko zaručených a overených pravidiel, ako sa správať v on-line prostredí bezpečnejšie voči sebe, svojmu majetku i svojim blízkym.

Kúpte si a udržujte na svojom počítači a mobilných zariadeniach originálny a bezpečnostný softvér, ktorý pravidelne aktualizujte.

Vybavte sa kvalitným antivírusovým programom. Tvrdenia, že antivírus nepotrebujete sú klamlivé. Platí, že čím je platforma, ktorú používate otvorenejšia a čím viac má používateľov, tým je pre útočníkov atraktívnejšia. Spomeňme napríklad Android.

Sociálne siete využívajte rozumne. Hackeri sa dnes už ľahko môžu dopracovať k súkromným dátam a istotu nemajú ani veľké spoločnosti ako Facebook, Twitter, Pokec či LinkedIn. Zvážte, komu a aké dáta o sebe sprístupníte.

Neustále kontrolujte a v prípade potreby upravujte nastavenia súkromia na Facebooku. Facebook ich totiž dosť často mení a nie vždy o tom dostatočne dôrazne informuje. Obmedzujte počet priateľov, ktorí môžu prezerať vaše príspevky. Pamätajte, že čokoľvek je na internete, už viac nie je súkromné.

Ak ste za posledné obdobie používali v niektorom z amerických obchodov Target debetnú kartu, okamžite si zmeňte PIN. Ak ste používali kreditnú kartu, skontrolujte mesačné výpisy a reklamujte akékoľvek podozrivé čiastky, ktoré objavíte .

Pri on-line platbách používajte prednostne kreditnú kartu. V prípade hackerského útoku a straty peňazí, má banka spoluúčasť na vzniknutých škodách. Pri debetných kartách idú straty „na vaše tričko“. Rovnako tak pri krachu aeroliniek či cestovných kancelárií máte väčšiu šancu, že vám budú prostriedky vrátené ak ste platili kreditnou kartou.

Nakupujte on-line iba u serióznych obchodníkov, ktorí majú certifikáty (u nás napríklad SAEC). Bankové prevody a prevodné príkazy z bežného účtu sa pre on-line nákupy neodporúčajú, pretože po odoslaní už je minimálna šanca získať peniaze späť. Využívajte kreditnú kartu a overené platobné systémy, napr. PayPal, PaySec, GP webpay. Patria medzi najbezpečnejšie platobné systémy.

Kontrolujte komu a kde platíte. Ak ste omylom zaslali transakciu na existujúce číslo účtu príjemcu, ktorý nemal byť príjemcom, požiadajte banku o sprostredkovanie navrátenia platby. Používajte len overené a chránené počítače, nie tie v internetových kaviarňach.

Zmeňte si heslá na všetkých webových účtoch a uistite sa , že má každé aspoň desať znakov a obsahuje kombináciu veľkých a malých písmen , číslic a špeciálnych znakov, napríklad

podčiarkovník, €, & alebo % . Heslá meňte v nepravidelných intervaloch a po veľkých hackerských útokoch okamžite.

Nereagujte na tzv. hoax, teda podvodné fámy a „zaručené“ správy o rôznych udalostiach. Časté sú napríklad rôzne podozrivé zbierky pod hlavičkou neznámych organizácií. Najčastejšie hoaxy sú uvedené na stránka http://www.hoax.cz/cze/

Nenechajte sa napáliť e - maily s tzv. phishingom. Buďte opatrní a v rozumnej miere podozrievaví. Doslova každá správa, ktorá sa objaví vo vašej schránke, môže byť pokusom o ukradnutie vašej identity, vašich osobných údajov. Veľmi časté sú e-maily, ktoré vyzerajú ako z vašej banky, ale v skutočnosti iba lákajú, „lovia“ údaje a prístupové heslá. Preberajte súbory iba z dôveryhodných webov.

Kontrolujte, aká skupina ľudí a kto konkrétne vidí vaše príspevky ešte predtým, ako stlačíte „Odoslať“ alebo „Zdieľať“. Niektoré fotografie alebo texty sú na webe celé roky a nemožno ich vymazať, ba ani súdnou cestou. Stačí ak si ich niekto uloží na svoj disk mimo siete a potom ich opakovane nahrá na web. Vaše osobné údaje môžu hackeri zneužiť napríklad pri nákupe na splátky.

Uistite sa, že dokážete pri svojom pôsobení na internete „pozametať digitálne stopy“. Prihlásiť sa a registrovať sa kdekoľvek je veľmi jednoduché. O to komplikovanejšie býva registráciu zrušiť.

Zamykajte svoj mobilný telefón a tablet pomocou PIN-u alebo bezpečnostného kódu. Nastavte si zámok obrazovky s časovým limitom tak , aby sa vaše zariadenie po určitej dobe nečinnosti automaticky uzamklo.

Krádež telefónu okamžite ohláste svojmu operátorovi, aby zablokoval SIM kartu. Každé zaváhanie môže znamenať stratu.

Ak používate zariadenie (tablet, notebook, smartfón) aj na pracovné účely uvažujte o kryptovacích, šifrovacích a heslovacích programoch, ktoré blokujú počítač po stanovenom limite a znemožňujú jeho používanie.

Ak máte deti, bez škrupúľ im obmedzte prístup na internet a sledujte ich on-line aktivity . Deti a seniori sú totiž najohrozenejšou skupinou, kvôli svojej neznalosti a dôverčivosti. Tzv. rodičovská zámka býva bežne súčasťou bezpečnostného softvéru.

Zdroj: Trend Micro Incorporated,

www.specialistinabezpecnost.sk