1. Nespúšťajte pripojené programy v e-mailoch od ľudí, ktorých nepoznáte a nesťahujte programy z neznámych a neoverených serverov

Jedným z nebezpečenstiev, ktoré striehnu na používateľa internetu, sú e-mailové vírusy a trójske kone. Útoku sa však dá pomerne ľahko vyhnúť. Väčšina vírusov k vám prichádza ako malý program, pripojený k správe elektronickej pošty. Tento vírus zväčša prečíta obsah adresára a rozošle sa na všetky adresy, ktoré sa v ňom nachádzajú, a tak si zabezpečí svoje šírenie. Na to však potrebuje, aby ste ho spustili. Ak sa chcete útokov vyvarovať, jednoducho nespúšťajte programy priložené k e-mailom, ak na 100 % neviete, kto vám ich posiela a čo je ich obsahom. Nastavte tiež svoj e-mailový klient tak, aby automaticky neotváral každú správu a nedovoľte mu automaticky sa pripájať na odkazy obsiahnuté v správach elektronickej pošty, pretože aj takýmto spôsobom – vinou bezpečnostnej chyby softvéru – môže dôjsť k napadnutiu vášho počítača.

Na internete je množstvo nových a zaujímavých programov, ktoré uľahčujú prácu s počítačom. Možno ich nájsť na veľkých oficiálnych serveroch, ktoré sa zaoberajú distribúciou softvéru, ale aj na rôznych súkromných a undergroundových stránkach. V druhom prípade však často môže ísť o podvod alebo vtip zo strany majiteľa stránky a program, ktorý si stiahnete, môže byť napadnutý vírusom alebo môže oslabiť bezpečnosť nášho počítača a otvoriť ho útokom z internetu.

2. Nepoužívajte jednoduché a ľahko uhádnuteľné heslá. Pri tvorbe hesla používajte čísla a špeciálne znaky

Veľa ľudí má problém vymyslieť si ľahko zapamätateľné heslo. Väčšina používa ako heslá mená rodinných príslušníkov, dátumy narodenia, čísla 12345 atď. Tento prístup je však veľmi nezodpovedný, pretože potenciálny útočník ľahšie uhádne ich heslo a získa tak neoprávnený prístup k ich osobným dátam. V dnešnej dobe existuje veľké množstvo programom na lámanie, „crackovanie" hesiel. Tie dokážu jednoduché heslá ako mená, či postupné číselné sekvencie uhádnuť v priebehu minút. Heslo by malo byť kombinované z čísel a znakov (prípadne dokonca špeciálnych znakov ako „# & % ^" a pod.), avšak nemalo by byť príliš zložité, aby ste si ho ľahko zapamätali a vyhli sa tak nutnosti zapisovať si ho.

3. Chráňte svoje heslá – nezapisujte ich, neposielajte ich nekryptovanou poštou, neposkytujte ich iným ľuďom, neukladajte si ich počítači ani v jeho okolí. Vypnite ukladanie hesla PRED prihlasovaním sa do verejne prístupného počítača!

Prax dokazuje, že najbezpečnejším miestom pre uloženie hesla je vaša hlava. Nie je pripojená na internet, nie je bežne prístupná iným užívateľom a údaje z nej máte poruke v (takmer ;) každom momente. Ak chcete svoje heslo či iné prístupové údaje ochrániť pred napadnutím, naučte sa ich naspamäť. Používajte napríklad tri ľahko zapamätateľné, ale komplexné (viď. bod 2) heslá. Je tu isté riziko následkov vyzradenia jedného z hesiel a získanie prístupu do viacerých vaši systémov naraz, avšak je stále menšie, ako keby ste mali ťažko zapamätateľné heslo nalepené na spodnej strane klávesnice...

Bežná elektronická pošta prechádza na svojej ceste k prijímateľovi rádovo desiatkami cudzích počítačov. Každý, kto má administrátorské privilégiá na jednom z týchto počítačov, si teda môže bez väčších problémov prečítať všetky nešifrované správy, ktoré cez tento počítač prechádzajú. Ak teda odosielate bežnou poštou heslá či kódy, môže sa k nim dostať tretia osoba a zneužiť ich. Preto je veľmi vhodné používať rôzne druhy programov na kryptovanie odosielanej elektronickej pošty.

Dôvera ľudí niekedy nepozná hranice, a preto je aj tu opatrnosť na mieste. Už veľakrát sa stalo, že útočník, ktorý sa vydával za pracovníka internetovej alebo telekomunikačnej spoločnosti, si vypýtal heslá a prihlasovacie mená s cieľom získať neoprávnený prístup do

systému. Váš internetový aj telekomunikačný operátor by mal vaše prístupové údaje poznať a nemalo by sa stávať, že ich žiada od svojich zákazníkov. Ak sa tak stane, je potrebné si dôkladne overiť, či je tento človek oprávnený ich používať.

Ak chcete predísť zneužitiu vášho počítača či už doma alebo na pracovisku, je potrebné všetky prístupové heslá (a to nielen do počítača samotného, ale aj do e-mailovej schránky či do internet bankingu) uchovávať mimo bezprostredného okolia počítača. Najideálnejšie je, ak viete prístupové mená a heslá naspamäť.

Niektoré internetové prehliadače vám umožňujú zjednodušenie práce s internetom tým, že si pamätajú prístupové mená a heslá k rôznym službám, ktoré internet ponúka (web pošta, rôzne chatovacie či diskusné servery a pod.). V prípade, že je táto funkcia zapnutá na verejne prístupnom počítači, môže sa stať, že program pri prihlasovaní iného užívateľa na službu, ktorú používate aj vy, automaticky vyplní vaše meno a heslo. Cudziemu človeku tak bude umožnený prístup do vašej poštovej schránky alebo do diskusného fóra pod vaším menom. Preto je nutné vždy si overiť ešte pred začiatkom práce, či sú všetky podobné funkcie vypnuté.

4. Používajte antivírový softvér a pravidelne ho aktualizujte!

Antivírový softvér by mal patriť k základnému softvérovému vybaveniu každého počítača. Vzhľadom na komplexnosť služieb, ktoré najnovšie antivírové programy ponúkajú, je tento druh zabezpečenia najvýhodnejší. Antivírový softvér vás ochráni ako pred e-mailovými vírusmi, tak aj pred rôznymi programami stiahnutými z internetu, ktoré by mohli zavíriť váš počítač. Zároveň sleduje operačnú pamäť počítača a v prednastavených časových intervaloch kontroluje celý obsah disku. Na správne fungovanie a zachovanie čo najväčšej bezpečnosti je potrebné antivírový softvér pravidelne aktualizovať.

5. Používajte Anti-spyware softvér!

V posledných rokoch sa na internete objavilo nové riziko – spyware a adware. Sú to programy, ktoré buď sledujú vašu aktivitu na počítači, internetovú komunikáciu a údaje o nej (v horšom prípade aj s vašimi prístupovými heslami) odosielajú výrobcovi softvéru alebo vám priamo na obrazovke zobrazujú nevyžiadanú reklamu. Príkazy pre svoje spustenie ukladajú do Windows Registry – centrálnej databázy nastavení operačného systému Windows a snažia sa svoju prítomnosť na počítači zakryť. Na ich vyhľadávanie a zabránenie ich rozšíreniu na počítači použite softvér proti spywaru. Microsoft poskytuje takýto nástroj pre Windows XP, alternatívou sú programy Spybot Search&Destroy a SpywareBlaster.

6.Používajte Firewall!

Ak je váš počítač zvyčajne pripojený na internet počas dlhšej doby (DSL, káblové pripojenie a pod.) je vystavený stále vyššiemu riziku napadnutia z internetu. Ľudia každý deň objavujú nové bezpečnostné diery v programoch a operačných systémoch a snažia sa ich využiť. Ako najpraktickejším riešením pre ochranu počítača sa teda ukázalo blokovanie všetkých nechcených dát prichádzajúcich z internetu špeciálnou „ohňovou stenou" – firewallom. Firewall je špeciálne zariadenie, alebo softvér, ktoré sa umiestňujú medzi váš počítač a sieť internet a blokujú prístup k Vášmu počítaču zvonka. Umožňujú používanie základných internetových služieb – e-mailu, webu, ftp a podobne, ale je možné ich samozrejme nastaviť aj pre používanie iných služieb (on-line hry, internetové telefonovanie, messengery a pod.). Pre koncových používateľov býva jednoduchšie a efektívnejšie nainštalovať si firewall priamo do svojho počítača (odpadá nutnosť nákupu špeciálnych zariadení či počítača). Jedným z najrozšírenejších firewallov je Kerio Personal Firewall, ktorý môžete zdarma stiahnuť na www.kerio.com.

7. Aktualizujte svoj softvér!

Tak ako treba autá opravovať a doplňovať im tekutiny – aktualizovať ich - je nutné aktualizovať aj váš softvér. Či už je to samotný operačný systém (Windows má pomerne dobre funkčný systém Windows Update), váš antivírový softvér (sťahovanie aktuálnych vírusových databáz), alebo váš antispyware softvér či antivírus. Jednotlivé programy vedia aktualizácie často vyhľadávať a v niektorých prípadoch aj aplikovať samé. Majte na pamäti, že len aktuálna verzia softvéru dokáže účinne čeliť internetovým rizikám.

8. Používajte vždy najvyššie dostupné zabezpečenie pri všetkých príležitostiach!

Internetové prehliadače a e-mailové programy poskytujú niekoľko možností zabezpečenia. Je dobré sa s týmito možnosťami oboznámiť a používať najvyššie možné zabezpečenie. To síce môže v niektorých prípadoch obmedzovať prehliadanie stránok alebo komplikovať prijímanie špeciálnych e-mailov (s priloženými obrázkami, zvukmi a videami), avšak výrazne znižuje pravdepodobnosť napadnutia počítača vírusom alebo neznámym útočníkom.

9. Premýšľajte čo robíte, majte oči otvorené – phishing, social engineering

Mnoho útočníkov a internetových podvodníkov zneužíva vo svoj prospech nepozornosť užívateľa. Už mnohokrát sa stalo, že ľudia zadali svoje číslo kreditnej karty a iné informácie nutné pre realizáciu platby na falošných webstránkach imitujúcich veľké internetové spoločnosti či firemné stránky. Riziká sa líšia od prípadu k prípadu, ale či už je to finančná ujma, alebo zverejnenie vašej e-mailovej adresy v erotickej e-mailovej konferencii či v spamerských databázach – následky nebývajú príjemné. Dávajte si preto pozor na akých webstránkach sa nachádzate, aké zabezpečenie používate pri prenose citlivých informácií a najmä na čo všetko dávate súhlas stlačením tlačítka „OK" či zaškrtnutím políčka na webstránke.

10. Dávajte pozor, kde uvádzate svoj e-mail!

Ľudia vám bežne na počkanie neprezradia adresu svojho bydliska – je to osobná informácia a nemusí ju vedieť každý. Podobne by ste mali pristupovať aj k vašej e-mailovej adrese. Je jedno či ju používate na súkromné, alebo pracovné účely, dostávať denne desiatky reklamných e-mailov je otravné a zdržujúce. Dávajte si preto pozor kde uvádzate svoj email – pýtajú si ho od nás často krát rôzne stránky pri sťahovaní programov, či registrácii pre používanie služieb, avšak neskôr môže byť zneužitý na zasielanie nevyžiadaných