

## Bezpečné používanie internetu

Informačné a komunikačné technológie sú nenahraditeľnými pomocníkmi. Čím je však ich význam väčší a čím viac sme od nich závislí, tým väčšie problémy vznikajú pri ich neopatrnom používaní alebo zneužívaní.

Jedným z najväčších nebezpečenstiev pre používateľa sú počítačové vírusy, ktoré môžu v okamihu zlikvidovať výsledok práce vytvorenej za dlhú dobu. Je preto potrebné dodržiavať niektoré bezpečnostné zásady. Niektoré najdôležitejšie pravidlá sme pre vás vybrali na túto stránku.

- 1. Kúpte si a nainštalujte kvalitný antivírusový softvér a vykonávajte jeho pravidelný update, alebo si tieto služby kúpte od spoľahlivého dodávateľa.**

Existuje množstvo kvalitných antivírusových programov, avšak samotné zakúpenie a inštalácia na chránený počítač nikdy nestačí. Takmer každý deň sa objavujú nové škodlivé kódy alebo ich mutácie. Len pravidelná aktualizácia antivírusového programu umožňuje spoľahlivú detekciu a odstránenie aj najnovších vírusov. Väčšina výrobcov poskytuje tieto aktualizácie denne. Najjednoduchším riešením je prenechať antivírusovú kontrolu elektronickej pošty na vášho dodávateľa, ktorý kompletne zabezpečí všetky potrebné činnosti.

- 2. Aj napriek použitiu antivírusového programu nikdy neotvárajte e-mailovú prílohu, ktorú ste nepožadoval(a)!**

Prudký nárast škodlivých kódov šíriacich sa pomocou elektronickej pošty už spôsobil obrovské ekonomické škody. Preto sa odporúča nevyžiadané prílohy neotvárať, prípadne overiť si u odosielateľa, či ich poslal vedome. Určite si vo svojom v e-mail kliente vypnite nastavenie automatického otvárania príloh! Najvhodnejšie je riešenie antivírusovej ochrany e-mailov priamo na poštovom serveri, ktoré odmietne akúkoľvek poštu s vírusom. Jeho výhodou je podpora - každý deň dostávate databázu nových vírusov. Ďalšou možnosťou je nainštalovať si vlastný antivírusový softvér.

- 3. Majte kontrolu nad svojim počítačom a nad tým, kto ho používa!**

Riziko vírusovej nákazy a straty dát vzrastá úmerne s počtom ľudí, ktorí majú ku konkrétnemu počítaču prístup. Stačí jediný nezodpovedný človek, ktorý prinesie z domu zavírenú disketu alebo otvorí e-mailovú prílohu s vírusom a negatívne dôsledky ponesú aj všetci ostatní. V súčasnej dobe sa stáva dôležitým prvkom ochrany počítača jeho zabezpečenie pomocou vhodného bezpečnostného programu, ktorý zabezpečí prístup len definovaným používateľom. Nejde len o zamedzenie vírusovej nákazy, ale aj o ochranu informácií uchovávaných v počítači. S pripojením počítača na Internet vyvstáva potreba chrániť sa aj proti nežiaducim prienikom zo siete.

- 4. Inštalujte včas všetky "záplaty" na používaný softvér!**

Existujú vírusy, ktoré používajú tzv. bezpečnostné diery v operačných systémoch a aplikáciách. Ak je taká chyba v programe zistená, jeho výrobca zvyčajne pripraví tzv. záplatu (patch), ktorú je možné na daný program aplikovať (nainštalovať) a tým chybu odstrániť. Tieto súbory sú zvyčajne k dispozícii na internete (bezplatne) na stránkach jednotlivých výrobcov softvéru. Je v záujme používateľa sledovať aktuálnu situáciu a nové záplaty čo najskôr aplikovať.

- 5. Ochraňujte svoj počítač pred Spyware!**

Spyware je označenie pre škodlivé programy, ktoré dokážu prebrať nad Vaším počítačom kontrolu bez toho, aby ste boli na to upozornení. Cieľom môže byť i odcudzenie citlivých údajov súkromného charakteru z Vášho počítača. Ak sa chcete týmto nepríjemným problémom vyhnúť, zariadte sa v súlade s bodom č.4 a neinštalujte do počítača programy, ktoré nie sú dôveryhodné. Samozrejme, aj pri vysokej opatrnosti sa môže stať, že k napadnutiu dôjde, preto je vhodné pravidelne kontrolovať svoj počítač aktualizovaným antispayware programom.

- 6. Vždy preverujte diskety a CD médiá predtým, ako ich použijete!**

Aj keď podľa dostupných údajov asi 90 % zaznamenaných vírusových útokov prichádza prostredníctvom e-mailu, nemôžeme podceňovať ani "tradičné" spôsoby ich šírenia. Je bezpečnejšie a finančne výhodnejšie investovať niekoľko minút času a médium otestovať dobrým antivírusovým softvérom, ako sa potom niekoľko hodín trápiť nad zavíreným počítačom, zaplatiť špecialistu, alebo dokonca prísť o obsah pevného disku.

- 7. S každým novým súborom (i z dôveryhodného zdroja) nakladajte s najväčšou opatrnosťou!**

Uvedené pravidlo platí nielen pre pirátsky softvér. Existujú dokonca prípady, keď inštalačné CD od známeho výrobcu tlačiarň obsahovalo vírus. Mnohonásobne väčšie je riziko v prípade súborov sťahovaných z Internetu. Nezáleží na tom komu stránky patria, aj na stránkach renomovanej firmy môžu byť súbory infikované vírusmi. Pripomeňme si napríklad prípad, kedy na stránkach najznámejšieho výrobcu nemenovaného operačného

systému bol niekoľko týždňov k dispozícii dokument nakazený makrovírusom.

#### 8. **Využívajte viac ako len jeden spôsob antivírusovej ochrany!**

Z hľadiska celkovej bezpečnosti nie je dostačujúce použiť len jednoduchý antivírusový program, ktorý vie na požiadanie preveriť daný súbor či adresár. Je žiaduce, aby antivírusový program vedel kombinovať niekoľko druhov ochrany. Medzi ne patrí:

- antivírusový monitor, ktorý vie na pozadí kontrolovať otvárané súbory,
- integrity checker (kontrolný súčet), ktorý vie zaznamenať modifikácie súborov a adresárov, ktoré môžu indikovať napadnutie vírusom,
- heuristická analýza, ktorá vyhľadáva vírusy pomocou analýzy ich správania a prejavov. Kombinácia týchto technológií môže efektívne ochrániť počítač pred väčšinou škodlivých kódov.

#### 9. **Vytvorte si zaručene "čistú" bootovaciu disketu a starostlivo ju uložte na bezpečné miesto!**

Môže nastať prípad, že na počítači, ktorý bol napadnutý vírusom, nie je možné spustiť operačný systém. Nemusí to však nutne znamenať, že by vírus dáta na pevnom disku počítača zmazal. V takom prípade je vhodné mať k dispozícii vopred vytvorenú tzv. bootovaciu disketu (samozrejme nezavírenú), ktorá súčasne obsahuje antivírusový program. Pomocou tejto diskety je možné napadnutý počítač spustiť a infikované súbory vyliečiť či prinajhoršom zmazať. Väčšina antivírusových programov ponúka možnosť takúto disketu vytvoriť jednoduchým spôsobom.

#### 10. **Pravidelne zálohujte!**

Aj keď toto pravidlo priamo nesúvisí s antivírusovou ochranou, jeho dodržovanie umožňuje minimalizovať prípadné škody spôsobené agresívnym vírusom, nespoľahlivým hardvérom apod. V porovnaní s cenou stratených dát je čas strávený zálohovaním celkom zanedbateľný. Vytvorené zálohy je vhodné uložiť na bezpečnom mieste (pre prípad požiaru či inej živelnéj katastrofy).

#### 11. **Nepodliehajte panike!**

Cieľom formulovania týchto pravidiel nie je strašiť používateľa počítačov. Počítačové vírusy sú vo svojej podstate len obyčajné programy vytvorené obyčajnými ľuďmi a nemôžu mať teda žiadne prehnané schopnosti. Jediným rozdielom, ktorý ich činí nebezpečnými je to, že svoju činnosť vykonávajú nezávisle na vôli používateľa. Väčšie straty spravidla napácha neskúsený používateľ, ktorý sa v panickom strachu snaží napadnutý počítač "vyliečiť".

Najlepším riešením je zveriť zavírený počítač do rúk profesionálov alebo sa s nimi aspoň poradiť. Základom všetkého však bolo, že a bude inštalácia kvalitného antivírusového riešenia, jeho správne nastavenie a dodržiavanie základných pravidiel antivírusovej ochrany.

#### 12. **Nedôverujte falošným e-mail správam!**

Rovnako nie je potrebné stresovať sa, pokiaľ dostanete e-mail upozorňujúci Vás na šírenie nového vírusu so žiadosťou, aby ste túto správu poslali čo najviac ľuďom. V úplnej väčšine prípadov ide o tzv. "hoax", čiže falošnú poplašnú správu. Takýto e-mail môžete ignorovať, ak však máte podozrenie, že je pravdivý, pošlite ho zamestnancovi firmy, ktorý má na starosti bezpečnosť IT. O jeho pravdivosti sa môžete presvedčiť aj sami na stránke niektorého výrobcu antivírusového softvéru.

#### 13. **Nedôverujte e-mail správam, vyzývajúcim od vás získať heslá či iné citlivé informácie!**

Jedným zo spôsobov, akým záškodníci získavajú citlivé informácie a prístup k rôznym systémom či dokonca k bankovým účtom cez internet, je tzv. phishing. (z angl. password fishing – doslova rybárčenie hesiel). Podvodníci sa snažia vylákať od používateľov rôzne heslá, napr. k bankovému účtu. Rozposielajú e-maily, ktoré buď priamo vyzývajú používateľov napríklad na zmenu hesla alebo jeho obnovenie, často v súvislosti "s úpravami systému" a pod., alebo e-mail obsahuje odkaz na falošnú webstránku, ktorá vyzerá ako kópia už existujúcej dôveryhodnej stránky, ale spravidla má nenápadne inú adresu. Meno a heslo zadané do phishingovej stránky sa odošle podvodníkovi, ktorý ho môže zneužiť. Najlepšia ochrana proti phishingu je nedôverovať stránkam a e-mailom, ktoré chcú vylákať citlivé údaje, hlavne heslá. Zároveň sa odporúča použiť rôzne prihlasovacie údaje pre rôzne stránky. Prevádzkovatelia internetových systémov a internet bankingu vo svojich technických oznamoch nikdy nevyzývajú k zaslaniu citlivých údajov. V prípade neistoty sa pre potvrdenie pravosti e-mailu obráťte priamo na prevádzkovateľa príslušného systému.