Desatero bezpečného internetu

1. Důležité jsou pravidelné aktualizace celého počítače. Ty je nutné stahovat pro operační systém, bezpečnostní bránu (firewall), antivirus i další programy.
2. Některé viry dokážou bezpečnostní software v PC zablokovat. Proto je vhodné pravidelně kontrolovat, zdali funguje.
3. Škodlivé programy se často šíří prostřednictvím nevyžádané pošty. Pokud nevíte, od koho e-mail je, nikdy nestahujte jeho přílohu a neklikejte na žádné odkazy.
4. Pozor je nutné dávat na e-maily, v nichž odesílatel požaduje, abyste se přihlásili na nějakou webovou stránku a aktualizovali informace o vašem účtu.
5. Při zadávání přístupových hesel na internetových stránkách je nutné kontrolovat, zda je web zabezpečený. To poznáte například podle ikonky zámečku na liště internetového prohlížeče, nebo tak, že adresa webové stránky začíná zkratkou https, kde „s“ znamená bezpečná.
6. Citlivé osobní informace zadávejte vždy pouze na internetových stránkách, které bezpečně znáte.
7. Do e-mailů nepatří důvěrné informace, jako je například číslo kreditní karty nebo heslo k bankovnímu účtu. Elektronickou poštu totiž může zachytit útočník.
8. Firewall dovoluje lépe zabezpečit operační systém. Méně zkušení uživatelé by jej rozhodně neměli vypínat. Při nedostatečných znalostech je vhodné jej nechat pracovat v automatickém režimu.
9. V internetových kavárnách a na cizích počítačích se nepřihlašujte do internetového bankovnictví. V počítači mohou být nainstalované keyloggery.
10. Obezřetnost je nutná při připojení k nezašifrovaným bezdrátovým sítím. Ty totiž může kdokoliv odposlouchávat a získat tak přístup ke všem datům v cizím počítači.