

Virusi, Viermi și Troieni

Virusii și viermii sunt programe periculoase ce se pot răspândi prin e-mail sau prin paginile de Internet. Virusii pot distruge fișiere sau programe software de pe computer.

Viermii se răspândesc mai repede decât virusii, direct de la un computer la altul. De exemplu, un vierme de e-mail se poate transmite singur la toate adresele de e-mail din agenda utilizatorului. Viermii de Internet caută computerele care sunt conectate la Internet, dar care nu conțin ultimele actualizări de securitate a PC-ului.

Caii troieni sau Troienii sunt programe periculoase care sunt create să pară inofensive, de exemplu, sub formă de joc, dar odată activate pot distruge fișiere fără ca utilizatorul să-și dea seama de aceasta.

Hackeri și crackeri

Hackeri și crackeri sunt termeni care denumesc persoane ce pătrund în sistemele de date. Aceștia pot intra într-un computer neprotejat prin intermediul Internetului și pot să abuzeze de el, să fure sau să copieze fișiere și să le utilizeze pentru activități ilegale.

Cea mai bună metodă de a proteja un computer împotriva acestor atacuri este utilizarea unui firewall sau păstrarea sistemului de operare actualizat.

Trimiterea de mesaje nesolicitate pe Internet

E-mailurile în masă sunt cunoscute ca mesaje nesolicitate sau spam. Acestea supraîncarcă programele de e-mail și pot bloca cutiile de poștă electronică. Cei care trimit mesaje nesolicitate folosesc uneori viermii de e-mail ca instrumente.

Cinci reguli pentru e-mail:

1. Nu deschideți niciodată mesaje suspecte sau atașamente de e-mail de la persoane pe care nu le cunoașteți. În schimb, ștergeți-le direct din meniul de mesaje.
2. Nu răspundeți niciodată la un mesaj nesolicitat.
3. Utilizați filtrul de spam al furnizorului dvs. de Internet sau al programului de e-mail, dacă acesta are unul.
4. Utilizați o adresă de e-mail nouă sau accesibilă întregii familii pentru întrebări pe Internet, forumuri de discuții etc.
5. Nu trimiteți niciodată mai departe e-mailuri în lanț. În schimb, ștergeți-le.

De asemenea, rețineți

Închideți ferestrele pop-up suspecte

Ferestrele pop-up sunt ferestre mici cu mesaje care vă încurajează să faceți click pe ele. Dacă o astfel de fereastră apare pe ecran, cel mai sigur lucru este să o închideți apăsând pe butonul X – de obicei se află în colțul din dreapta sus. Nu puteți fi niciodată siguri ce va face programul chiar dacă apăsați pe „Nu”.

Nu vă lăsați păcăliți

Ascunderea identității este ușor de realizat pe Internet. Este recomandat să verificați identitatea persoanei cu care comunicați (de exemplu, în grupuri de discuție). Ar trebui să nu dezvăluiți niciodată informațiile personale pe Internet, cu excepția persoanelor pe care le cunoașteți și în care aveți încredere. Dacă vi se cer datele personale pe un site, citiți înainte „Termenii de utilizare” sau „Politica de confidențialitate” a site-ului pentru a vă asigura că operatorul acestuia a explicat cum va utiliza aceste informații, precum și dacă le va transmite către alte persoane.

Discutați despre utilizarea Internetului

Cea mai mare parte din materialul de pe Internet nu este potrivită pentru minori. Discutați cu elevii și cu copiii dvs. despre utilizarea și navigarea în siguranță pe Internet.