

Fii atent pe internet

Informație selectată și reformulată
de Furculiță Andreea, elevă a
clasei a 10-a "C", IPLT "Spiru
Haret"

Profesor: Guțu Maria

Avantajele și dezavantajele navigării pe internet:

Avantaje:

- 1) Accesul rapid la informații din toate domeniile (este mult mai convenabil să deținem un calculator conectat la internet, datorită căruia putem obține rapid informații din orice sferă, decât să cumpărăm numeroase cărți scrise pe diferite teme.);
- 2) Comunicarea cu instituții publice și companii private și socializarea cu rude, prieteni prin intermediul rețelelor de socializare, precum Messenger, Skype, Viber, WhatsApp, etc. (instituțiile și companiile își dispun pe paginile oficiale diverse date de contact, precum adresa de e-mail sau chiar numele pe rețele de socializare, precum facebook) ;
- 3) Instruirea (poate avea loc prin intermediul cursurilor online, cărților și exercițiilor online, articolelor, dar și prin intermediul tutorialelor de pe youtube);
- 4) Comerțul electronic;
- 5) Publicitatea (fiecare poate face publicitate prin postările de pe rețelele de socializare);
- 6) Posibilitatea de a-ți face publică o părere (tot prin intermediul rețelelor de socializare, oamenii își pot expune opiniile, care vor fi citite de mai multe persoane);
- 7) Economia de timp (Exemplu: căutarea unui cuvânt într-un dicționar online este mult mai rapidă decât căutarea acestuia într-un dicționar sub formă de carte, întrucât în al doilea caz nu știi exact la ce pagină se află cuvântul dat).

Dezavantaje:

- 1) Calitatea și veridicitatea informației este nesigură (oricine are posibilitatea de a posta informație pe diferite site-uri, deci nu putem fi siguri de cunoștințele sursei în domeniul dat și de veridicitatea informației);
- 2) Tot ce ai în calculator este expus din momentul conectării la internet;
- 3) Informațiile de pe mail sau din orice alte conturi online, toate parolele, toate mișcările pe internet sunt stocate de către cei ce oferă serviciile respective și sunt accesibile acestora;
- 4) Infracțiunile/ ilegalitățile/ fraudele/ țepele;
- 5) Identitatea virtuală ar putea să nu coincidă cu cea reală;
- 6) Pierderea de timp (internetul poate fi o metodă de economisire a timpului, dar și una de pierdere a acestuia, atunci când este utilizat irațional, cum ar fi pentru jocuri);
- 7) Daunele aduse sănătății (ochii se deprind să privească de la o distanță mică și pierd capacitatea de a vedea de la o distanță mare);

10 reguli pentru o navigare sigură pe internet:

1. Limitează informația personală de pe rețelele de socializare.
2. Postează cu mare grijă fotografii cu tine sau cu familia ta.
3. Nu dezvălui parolele utilizate și alege parole formate din cel puțin 15 caractere și care nu conțin numele, prenumele tău sau data nașterii tale.
4. Nu da persoanelor întâlnite pe internet informații personale despre tine sau familia ta.
5. Dacă vrei să te întâlnești față în față cu persoane cunoscute pe internet, anunță-ți părinții pentru a te însoți, preferabil într-un loc public.
6. Nu tot ceea ce citești pe internet este adevărat.
7. Nu răspunde la mesajele care te supără sau care conțin cuvinte sau imagini nepotrivite și anunță părinții în cazul primirii unor astfel de mesaje.
8. Dă dovadă de respect, chiar dacă nu-i cunoști pe cei cu care comunică.
9. Actualizează-ți programul antivirus.
10. Ai grijă la ce descarci.

Ce este un Adware?

Este un virus orientat cu precădere spre **reclame publicitare**. Infectarea unui PC cu un virus adware va afișa **reclame bannere** sau de **tip pop-up** la deschiderea paginilor de internet. Așadar, un adware afectează direct internet browserele **Firefox, Google Chrome, Opera** și mai ales **Internet Explorer**. Sunt forme de adware ceva mai dezvoltate care nu au nevoie de un internet browser pentru a deschide o reclamă, aceasta fiind executată și lansată direct din fișierul creat de virus pe PC. În mod normal, un adware nu aduce daune serioase unui PC, el fiind doar stresant prin reclamele pe care le afișează și consumând mici resurse. Problema este că niciodată nu putem fi siguri că un astfel de virus se limitează numai la a lansa reclame. Un adware poate fi ușor transformat într-un **virus de tip spyware** care să culeagă **date confidențiale din calculatorul victima** și să le trimită către **destinații rău intenționate**.

Ce este spam-ul?

Spam-ul este definit ca acel mesaj al cărui expeditor nu se regăsește în lista de contacte (sau de cunoștințe) a destinatarului. O altă definiție pentru spam este cea de utilizare abuzivă a serviciilor de

poștă electronică în scopuri publicitare sau de inducere în eroare (înșelare) a destinatarului.

Principalele metode de evitare în totalitate a email-urilor SPAM sunt: să nu te înregistrezi pe site-uri necunoscute sau nesigure, să îți ascunzi adresa de email din profilurile publice de pe rețelele sociale sau de pe orice site pe care ești înregistrat, să protejezi calculatorul de viruși atât prin utilizarea precaută a internetului, cât și prin folosirea unui antivirus performant, să nu trimiți email-uri la adrese nesigure și, desigur, să folosești doar platforme web sigure de email precum GMail, Yahoo și altele, care au incorporate strategii de identificare și blocare a spam-ului. Un alt aspect ce trebuie luat în considerare atunci când vine vorba de evitarea spam-ului este și numele adresei de email, o adresă de mail scurtă sau prea simplă poate primi SPAM pur și simplu la nimereală, pe baza unor algoritmi ce folosesc sau compun diverse cuvinte populare (cum ar fi prenumele, numele de familie, ani, etc.) pentru a forma adrese de email către care să trimită mesaje nesolicitate.

Ce este un hacker?

HACKER-Persoană care încearcă să obțină, în mod ilegal, controlul unui sistem de securitate, computer sau rețea, cu scopul de a avea acces la informații confidențiale sau avantaje materiale.

Ce este Phishing-ul?

Phisingul constă în trimiterea de e-mailuri care au ca și expeditor fals diverse instituții cu care potențiala victimă are anumite relații (de ex: bănci, magazine on-line etc). Aceste e-mailuri de obicei direcționează userii către anumite site-uri unde sunt rugați să-și actualizeze diverse informații sau să introducă date personale.

Aceste site-uri imită foarte bine structura celor originale însă sunt găzduite de către persoane rău intenționate care urmăresc obținerea de foloase materiale.

Ce trebuie să știm despre phishing?

La prima vedere tentativele de phishing pot trece neobservate însă sunt câteva lucruri de care ar trebui să ținem cont atunci când

primim un e-mail ce pare a fi de la una din instituțiile cu care colaborăm. De regulă toate urmează aceeași structură.

Introducerea

Salutul este generic, de exemplu : “Stimate client”. De obicei companiile cu care colaborați, personalizează e-mailurile cu numele dumneavoastră.

Avertizarea

Vi se transmite faptul că în urma unor investigații au fost descoperite câteva nereguli la conturile dumneavoastră și vi se cer informațiile personale. Majoritatea companiilor nu procedează așa, este puțin probabil ca un colaborator de-al dumneavoastră să vă solicite informații confidențiale prin e-mail.

În cazul în care nu urmați instrucțiunile din e-mail într-un interval de timp destul de scurt sunteți amenințat cu dezactivarea conturilor, pierderea banilor, etc.

Redirecționarea

Vi se cere să intrați imediat pe o anumită pagină web, accesând un link din cadrul emailului. Pe pagina respectivă ar trebui să introduceți informații cu caracter general ca numele dumneavoastră însă și cele cu caracter privat: coduri pin, coduri numerice personale, adrese detaliate, numere de telefon etc.

Rețineți faptul că nu toate paginile care arată a fi “oficiale”, chiar sunt. Linkurile pe care ar trebui să dați click sunt mai lungi în comparație cu cele obișnuite și adesea conțin simbolul @.

Ce este un keylogger?

Un keylogger este un program de calculator sau un dispozitiv fizic (hardware) atașat la sistem care are rolul de a prelua și înmagazina caracterele tastelor apăsate de către utilizatori pe parcursul folosirii computerului, atâta timp cât programul rulează în sistem sau dispozitivul de keylogger este conectat la calculator.

Hărțuirea în mediul online se manifestă prin:

-mesaje care țin să denigreze imaginea unei persoane;

- comentarii răutăcioase la fotografii sau la alte postări;
- distribuire de fotografii sau informații personale distorsionate, ajunse întâmplător sau intenționat la persoanele care se implică în hărțuire;
- limbaj agresiv în timpul jocurilor online în perechi sau grup pe care le preferă atât copiii din ciclul primar, cât și adolescenții.