Fii atent pe internet

Informație selectată și reformulată de Furculiță Andreea, elevă a clasei a 10-a “C”, IPLT “Spiru Haret”
Profesor: Guțu Maria

Anul 2018

Avantajele și dezavantajele navigării pe internet:

Avantaje:

1)Accesul rapid la informaţii din toate domeniile (este mult mai convenabil să deţinem un calculator conectat la internet, datorită căruia putem obţine rapid informaţii din orice sferă, decât să cumpărăm numeroase cărţi scrise pe diferite teme.);
2)Comunicarea cu instituţii publice și companii private și socializarea cu rude, prieteni prin intermediul reţelelor de socializare, precum Messenger, Skype, Viber, WhatsApp, etc. (instituţiile și companiile își dispun pe paginile oficiale diverse date de contact, precum adresa de e-mail sau chiar numele pe reţele de socializare, precum facebook) ;
3)Instruirea (poate avea loc prin intermediul cursurilor online, cărţilor și exerciţiilor online, articolelor, dar și prin intermediul tutorialelor de pe youtube);
4)Comerţul electronic;
5)Publicitatea (fiecare poate face publicitate prin postările de pe reţelele de socializare);
6)Posibilitatea de a-ţi face publică o părere (tot prin intermediul reţelelor 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 dicţionar online este mult mai rapidă decât căutarea acestuia într-un dicţionar sub formă de carte, întrucât în al doilea caz nu știi exact la ce pagină se află cuvântul dat).

Dezavantaje:

1)Calitatea și veridicitatea informaţiei este nesigură (oricine are posibilitatea de a posta informaţie pe diferite site-uri, deci nu putem fi siguri de cunoștinţele sursei în domeniul dat și de veridicitatea informaţiei);
2)Tot ce ai în calculator este expus din momentul conectării la internet;
3)Informaţiile 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)Infracţiunile/ ilegalităţile/ fraudele/ ţepele;
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, cm ar fi pentru jocuri);
7)Daunele aduse sănătății (ochii se deprind să privească de la o distanţă mică și pierd capacitatea de a vedea de la o distanţă mare);

10 reguli pentru o navigare sigură pe internet:

1.Limitează informaţia personală de pe reţelele de socializare.
2.Postează cu mare grijă fotografii cu tine sau cu familia ta.
3.Nu dezvălui parolele utilizate şi alege parole formate din cel puţin 15 caractere şi care nu conţin numele, prenumele tău sau data naşterii tale.
4. Nu da persoanelor întâlnite pe internet informaţii personale despre tine sau familia ta.
5. Dacă vrei să te întâlneşti faţă în faţă cu persoane cunoscute pe internet, anunţă-ţi părinţii pentru a te însoţi, preferabil într-un loc public.
6. Nu tot ceea ce citeşti pe internet este adevărat.
7. Nu răspunde la mesajele care te supără sau care conţin cuvinte sau imagini nepotrivite şi anunţă părinţii în cazul primirii unor astfel de mesaje.
8. Dă dovadă de respect, chiar dacă nu-i cunoşti pe cei cu care comunici.
9. Actualizează-ţi 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 afişa **reclame bannere** sau de **tip pop-up** la deschiderea paginilor de internet. Aşadar, un adware afectează direct internet browserele **Firefox**, **Google Chrome**, **Opera** şi 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 şi lansată direct din fişierul 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 afişează şi 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 uşor transformat într-un **virus de tip spyware** care să culeagă **date confidenţiale din calculatorul victima** şi să le trimită către **destinaţii rău intenţionate**.

Ce este spam-ul?

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

poştă electronică în scopuri publicitare sau de inducere în eroare (înşelare) 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 obţină, în mod ilegal, controlul unui sistem de securitate, computer sau reţea, cu scopul de a avea acces la informaţii confidenţiale sau avantaje materiale.

Ce este Phishing-ul?

Phisingul constă în trimiterea de e-mailuri care au ca şi expeditor fals diverse instituţii cu care potenţiala victimă are anumite relaţii (de ex: bănci, magazine on-line etc). Aceste e-mailuri de obicei direcţionează userii către anumite site-uri unde sunt rugaţi să-şi actualizeze diverse informaţii sau să introducă date personale.

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

Ce trebuie să ştim despre phishing?

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

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

Introducerea

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

Avertizarea

Vi se transmite faptul că în urma unor investigaţii au fost descoperite câteva nereguli la conturile domneavoastră şi vi se cer informaţiile personale. Majoritatea companiilor nu procedeaza aşa, este puţin probabil ca un colaborator de-al dumneavoastră să vă solicite informaţii confidenţiale prin e-mail.

În cazul în care nu urmaţi instrucţiunile din e-mail într-un interval de timp destul de scurt sunteţi ameninţat cu dezactivarea conturilor, pierderea banilor, etc.

Redirecţionarea

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

Reţineţi faptul că nu toate paginile care arată a fi “oficiale”, chiar sunt. Linkurile pe care ar trebui să daţi click sunt mai lungi în comparaţie cu cele obişnuite şi adesea conţin simbolul @.

Ce este un keylogger?

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

Hărţuirea în mediul online se manifestă prin:

-mesaje care ţintesc să denigreze imaginea unei persoane;

-comentarii răutăcioase la fotografii sau la alte postări;
-distribuire de fotografii sau informaţii personale distorsionate, ajunse întâmplător sau intenţionat la persoanele care se implică în hărţuire;
-limbaj agresiv în timpul jocurilor online în perechi sau grup pe care le preferă atât copiii din ciclul primar, cât şi adolescenţii.