1)Citatul: Acasă este locul unde Wi-Fi-ul se conectează automat.(Comentarea citatului de catre elevi)

2)Ce este este retea wifi?

Wi-Fi este o tehnologie radio folosită deseori la implementarea rețelelor locale de calculatoare de tip rețea locală fără fir (*Wireless Local Area Network, WLAN*). Un WLAN este un sistem de comunicații implementat ca extensie la, sau ca alternativă pentru o rețea locală (LAN) cablată, într-o clădire sau campus, combinând conectivitatea la viteză mare cu mobilitatea utilizatorilor, într-o configurație mult simplificată. Avantajele evidente, cum ar fi mobilitatea, flexibilitatea, simplitatea în instalare, costurile de întreținere reduse și scalabilitatea, au impus Wi-Fi și WLAN ca o soluție tot mai mult utilizată.

Cele nestructurate constau în atacurile unor indivizi mai putin experimentati care folosesc instrumente de “hacking”, scripturi shell sau programe de spart parole destul de usor de gasit si de folosit. Atacurile structurate vin din partea unor hackeri mult mai motivati si mai pregatiti din punct de vedere tehnic. Acesti oameni cunosc vulnerabilitatile sistemului wireless, pot întelege si dezvolta coduri sursa, scripturi si programe. Amenintarile externe sunt reprezentate de indivizi din afara unei companii; ei nu au acces autorizat la reteaua wireless; accesul la retea este câstigat din afara cladirii, din parcari, cladiri apropiate. Pentru prevenirea acestor tipuri de atacuri oamenii investesc cel mai mult. Amenintarile interne au loc atunci când cineva are acces la resursele retelei cu un cont pe server sau acces la mediul fizic. Sunt responsabile pentru 60-80 % din atacurile raportate.

Reguli de siguranta pe Internet

1. Stabileste împreuna cu parintii tai regulile de folosire a calculatorului si a Internetului.

Poti face o lista cu site-urile pe care doresti sa navighezi sau pe care ti le propun parintii si hotarati de comun acord orele cand e cel mai potrivit sa utilizezi Internetul. Calculatorul te poate ajuta sa-ti faci temele sau sa-ti petreci timpul într-un mod placut. Parintii te pot învata cum sa gasesti mai repede informatiile utile, dar si tu le poti arata cat de priceput esti în folosirea calculatorului.

2. Nu da nici unei persoane întalnite pe Internet informatii personale despre tine sau familia ta.

Acestea pot fi numele, varsta, numarul de telefon, fotografii, adresa, scoala la care înveti, locul de munca al parintilor etc. Atunci cand aceste persoane necunoscute insista (prin email, pe chat sau telefonul mobil) sa afle cine esti si unde locuiesti, anunta-ti parintii imediat.

3. Parolele sunt secrete si îti apartin.

Ele sunt ca si cheile de la casa pe care nu le dai nimanui, nici macar cunoscutilor. Cu exceptia parintilor! Trebuie sa-i refuzi întotdeauna pe prietenii care îti cer parola, deoarece acestia pot folosi adresa ta de email pentru a trimite mesaje jignitoare altor persoane sau

pentru a intra pe site-uri interzise. Daca banuiesti ca parola ti-a fost divulgata, schimb-o imediat, singur sau cu ajutorul parintilor.

4. Daca vrei sa te întalnesti fata în fata cu persoanele cunoscute pe Internet sau de la care ai primit mesaje pe telefonul mobil, anunta-ti parintii pentru a te însoti, preferabil într-un loc public.

Nu accepta niciodata sa mergi singur. Oamenii pot fi foarte diferiti de ceea ce par a fi pe Internet. Nu de putine ori baietii se dau drept fete sau invers, ori varsta declarata nu este cea adevarata. Pentru a evita orice pericol, nu folosi telefonul personal pentru a suna pe cineva întalnit pe Internet. Discuta mai întai cu parintii tai acest lucru.

5. Posteaza cu mare grija fotografii cu tine sau cu familia ta!

Atunci cand doresti sa încarci (upload) fotografii sau filme pe site-urile pe care trebuie sa-ti creezi un profil sau cont (cum ar fi, Hi5, My Space etc.), selecteaza fisierele împreuna cu parintii. Învata sa creezi o lista cu persoanele care îti pot vedea profilul. Foloseste camera web numai cand sunt parintii alaturi de tine. Nu uita, fotografiile sau filmulete, odata postate, pot ramane pentru totdeauna pe Internet chiar daca le vei sterge!

6. Nu tot ceea ce citesti sau vezi pe Internet este adevarat.

Astazi, multe persoane, inclusiv copiii, pot sa creeze pagini web sau sa posteze texte, fotografii, stiri. În plus, fotografiile si filmele pot fi modificate pe calculator cu usurinta. Pentru a verifica daca ceea ce ai aflat pe Internet este adevarat, cere ajutorul parintilor sau profesorilor tai care îti pot oferi si alte surse de informare. Nu descarca si nu instala programe pirat sau pe care nu le cunosti; ele pot distruge datele de pe calculatorul tau.

7. Nu raspunde la mesajele care te supara sau care contin cuvinte sau imagini nepotrivite!

Pastreaza-le pentru a le arata parintilor, profesorilor sau, în cazuri grave, Politiei. Daca primesti e-mail-uri, fisiere, fotografii sau programe de instalare care ti se par suspecte de la cineva pe care nu-l cunosti si în care nu ai încredere, sterge-le din calculator. Ele pot avea virusi sau programe care îti vor citi toate datele de pe calculatorul tau. Cere ajutorul unei persoane de încredere.

8. Da dovada de respect, chiar daca nu-i cunosti pe cei cu care comunici.

Obligatia ta este de a-i proteja si tu pe altii. Nu trimite imagini jignitoare sau mesaje care ar putea sa le provoace frica sau sa-i puna în pericol.

9. Cumpararea produselor pe Internet este permisa doar parintilor.

Ei sunt singurii care au voie sa foloseasca cartile de credit. De aceea, anunta-ti parintii ori de cate ori ti-au fost trimise, pe email sau pe chat, oferte sau cereri de bani.

10. Poti oricand sa te opresti din navigarea pe Internet sau sa refuzi sa continui discutiile pe chat, daca s-a întamplat ceva care nu ti-a placut, te-a speriat sau, pur si simplu, nu ai înteles.

Vorbeste direct parintilor tai sau profesorilor si explica-le ce te-a îngrijorat. Poti scoate oricand din lista de contacte pe cei cu care nu mai vrei sa comunici.

Cum recunosc un computer virusat

1. *“Computerul vorbeste cu mine“* - Apar pe ecran tot felul de ferestre “pop-up” si mesaje publicitare, precizand ca PC-ul este infectat si ca are nevoie de protectie. Acesta este un exemplu tipic de infectare. Este vorba fie de un program spion (“spyware”) in computer sau de o infectare cu un antivirus fals (numit si “rogueware“).
2. *“Computerul meu functioneaza extrem de incet“* - Acesta poate fi un simptom pentru multe cauze, inclusiv infectarea cu un virus. In cazul in care s-a produs infectarea cu un virus, vierme sau troian, acestea pot consuma resursele calculatorului, facandu-l sa functioneze mai greu decat de obicei.
3. *“Am aplicatii care nu pornesc”* - De cate ori ati incercat sa porniti o aplicatie din meniul start sau de pe desktop si nimic nu se intampla? Uneori se poate deschide chiar un alt program. Ca si in cazul anterior, poate fi vorba de orice alta problema, insa este cel putin un simptom care va spune ca ceva nu este in regula.
4. *“Nu ma pot conecta la Internet sau acesta ruleaza extrem de incet“* -Pierderea accesului la Internet este un alt semn al infectarii, desi poate fi cauzat si de probleme legate de furnizorul de Internet sau router. Pe de alta parte, este posibil sa aveti o conexiune la Internet care functioneaza mult mai greu decat de obicei. Daca ati fost infectat, malware-ul se poate conecta la o anumita adresa de Internet sau poate deschide anumite conexiuni separate, limitand astfel viteza de accesare a Internetului sau chiar facand imposibila folosirea acestuia.
5. *“Cand ma conectez la Internet, mi se deschid pe ecran tot felul de ferestre sau pagini web nesolicitate”* - Acesta este cu siguranta un alt semn al infectarii cu malware. Multe fisiere virale sunt concepute special pentru redirectarea traficului de Internet catre anumite website-uri, fara consimtamantul utilizatorului, sau chiar sa imite anumite website-uri, creand impresia unui site legitim.
6. *“Unde au disparut fisierele mele?“* - Sa speram ca nimeni nu va pune aceasta intrebare, desi anumite atacuri sunt concepute special pentru criptarea sau stergerea anumitor fisiere si chiar mutarea documentelor dintr-un loc in altul. Daca va gasiti in aceasta situatie, este cazul sa incepeti sa va faceti griji.
7. *“Antivirusul meu a disparut, firewall-ul este dezactivat”* - O alta actiune tipica a amenintarilor de pe Internet este dezactivarea sistemelor de securitate (antivirus, firewall, etc) instalate pe calculator. Daca un singur program s-ar opri, poate ca ar fi vorba de o eroare de software, dar daca toate componentele de securitate s-ar dezactiva, aveti cu siguranta computerul infectat.
8. *“Computerul meu vorbeste in alta limba”* - Daca limba anumitor aplicatii se schimba, ecranul apare inversat, “insecte” ciudate incep sa “manance” ecranul, este posibil sa aveti un sistem infectat.
9. *“Imi lipsesc fisiere necesare pentru a rula jocuri, programe etc”* - Din nou, acest lucru ar putea fi un semn de infectare, desi este posibil sa fie vorba de o instalare incompleta sau incorecta a acelor programe.

10. *“Computerul meu, practic, a innebunit”* - In cazul in care computerul dumneavoastra incepe sa actioneze singur sau sa trimita email-uri fara sa stiti, daca aplicatii sau ferestre de Internet se deschid singure, in mod sporadic, sistemul ar putea fi compromis de malware.

Utilizarea protecției antivirus
Virușii, viermii și caii troieni sunt programe create de hackeri, care utilizează Internetul pentru a infecta computere vulnerabile. Virușii și viermii se pot reproduce de la computer la computer, în timp ce caii troieni intră întrun computer ascunzânduse întrun program aparent legitim, cum ar fi un economizor de ecran. Virușii, viermii și caii troieni destructivi pot să șteargă informații din hard disk sau să dezactiveze complet computerul. Alții nu cauzează daune directe, dar înrăutățesc performanța și stabilitatea computerului.

3. Internetul înregistrează și salvează (depozitează) totul – fotografii, comentarii, aprecieri, locuri, contacte etc. Internetul nu are butonul Ștergere. În baza informațiilor publicate aici, deseori oamenii își fac concluzii și își formează atitudini față de alți utilizatori.

Atunci când vorbim despre imaginea virtuală a unui copil, ne referim la toată informația publică online despre acesta – fotografiile sale care vorbesc despre mediul din care provine și instituțiile pe care le frecventează, familia copilului, felul lui de a se exprima în comentarii și aprecieri, distribuirile care le face. Deseori anume părinții sunt cei care le creează copiilor astfel de imagini prin postări de fotografii sau descrieri ce vizează copilul. Imaginea virtuală o creează și orice alte publicații despre copil, făcute de alte persoane, fie rude ale copilului, fie colegii și prietenii, îngrijitorii, educatorii sau profesorii instituțiilor pe care le frecventează. Imaginea virtuală contribuie la formarea unei reputații virtuale a copilului, care, în contextul siguranței sale, este foarte importantă.

Pentru un copil este esențial ca imaginea sa virtuală să fie una corectă, fie în scopul evitării riscului de a deveni victima hărțuirii în mediul online, ținta unor persoane cu intenții răuvoitoare, fie pentru succesul ulterior la admitere într-o instituție, acceptarea sa în activități de voluntariat sau chiar găsirea unui loc de muncă, unde tot mai frecvent un criteriu neoficial de analiză a candidatului sunt informațiile despre el obținute prin motoare de căutare în Internet.

Încă de la o vârstă fragedă copilul trebuie învățat că nu doar felul cum vorbește, se comportă în mediul real îl ajută să creeze o imagine despre sine, ci și orice alt pas pe care el îl face în Internet și pe care acesta îl înregistrează, păstrând astfel o urmă.

Dat fiind faptul că mulți copiii, utilizând rețelele sociale, nu cunosc și nu setează parametrii de confidențialitate, multe lucruri despre ei și activitățile lor în afara școlii sunt vizibile pentru foarte multă lume în mediul online. Profesorii pot deveni, la fel, voluntar sau involuntar, martori la evoluția imaginii virtuale a copilului.

7. Securitatea este un motiv de îngrijorare pentru dezvoltarea oricarui tip de aplicatie. Cu toate acestea, aplicatiile web dezvaluie anumite caracteristici care trebuie luate în considerare la proiectarea functionalitatilor de securitate si care solicita mai multe tehnici de securitate, comparativ cu alte tipuri de aplicatii. De exemplu, spre deosebire de programele care sunt instalate pe o singura masina gazda, aplicatiile web sunt accesibile publicului, pe Internet, pentru a ajunge la o numar mare de potentiali utilizatori. De exemplu, autentificarea si autorizarea utilizatorilor trebuie sa fie implementate în mod diferit pentru sistemele folosite de un singur utilizator.

8. Spam-ul reprezinta acele mesaje electronice (email-uri) nesolicitate, care apar in casuta de email fara ca posesorul contului sa autorizeze in prealabil aceasta actiune. In majoritatea cazurilor caracterul principal al email-urilor nesolicitate este comercial, de publicitate pentru produse sau servicii de regula indoielnice, sau de promovare a unor website-uri, actiuni sau ideologii. Alte caracteristici ale spamului includ:

- nu permite posesorului adresei de email sa se dezaboneze si sa nu mai primeasca alte email-uri de la sursa respectiva (privarea de dreptul la optiune);
- adresele de email carora li se va expedia mesaje spam sunt colectate fie prin intermediul unor formulare de inregistrare false care se prezinta ca apartinad de diverse site-uri populare, fie acestea sunt procurate contra cost de la organizatii sau persoane (hackari) care le obtin tot prin metode ilegale;
- este expediat automat de catre un program software;
- sursele de spam sunt greu de identificat, programele care trimit spam sunt plasate ilegal pe calculatoare aleatoare, iar acest proces se face folosind software de tip malware.

In plus, spam-ul ocupa spatiu de stocare din contul de email, efectueaza trafic de date in reteaua de internet care poate incetini trimiterea sau receptionarea de email-uri reale si inrautateste experienta utilizatorului pentru ca acesta este nevoit sa verifice si sa sorteze email-urile bune fata de cele spam, pentru ca apoi sa le stearga; iar acest lucru necesita atentia utilizatorului si un timp alocat pentru curatarea de spam a casutei de email.

Principalul mod de a evita in totalitate email-urile SPAM este sa nu te inregistrezi pe site-uri necunoscute sau nesigure, sa iti ascunzi adresa de email din profilurile publice de pe retelele sociale sau de pe orice site pe care esti inregistrat, sa protejezi calculatorul de virusi atat prin utilizarea precauta a internetului dar si prin folosirea unui antivirus performant (vezi si articolul Cum sa ramai in siguranta pe internet), sa nu trimiti email-uri la adrese nesigure si, desigur, sa folosesti doar platforme web sigure de email precum GMail,Yahoo si altele, care au incorporate strategii de identificare si blocare a spam-ului.

10. Un keylogger este un program care înregistrează fiecare bătaie de tastă pe o tastatură şi salvează aceste date într-un fişier. După ce colectează o anumită cantitate de date, le va transfera prin intermediul internetului unei gazde de la distanţă, predeterminată. De asemenea, poate captura capturi de ecran şi utiliza alte tehnici pentru a urmări activitatea utilizatorului. Un keylogger poate cauza pierderea parolelor, date de autentificare, şi alte informaţii similare. Ca şi concluzie, un keylogger este capabil de iniţierea următoarelor activităţi:

- Să înregistreze intrările de taste de pe tastatură.
- Să obţină capturi de ecran cu activitatea utilizatorului de pe internet la intervale de timp predeterminate.
- Să urmărească activitatea utilizatorului prin înregistrarea titlurilor ferestrelor, numele aplicaţiilor lansate, şi alte informaţii specifice.
- Să monitorizeze activitatea online a utilizatorului înregistrând adresele website-urilor vizitate, cuvintele cheie introduse şi alte date similare.
- Să înregistreze nume de autentificare, detalii a unor diverse conturi, numerele cardurilor de credit şi parole.
- Să captureze conversaţiile chat-urilor online de pe instant messengers.
- Să obţină copii neautorizate a emailurilor primite şi trimise.
- Să salveze toate datele colectate într-un fişier de pe hard disk, şi să trimită acest fişier unei adrese de email.
- Să îşi complice detectarea şi eliminarea.

12. Ce înseamnă activitatea de phishing

De obicei, activitatea de phishing se face prin e-mailuri, anunțuri sau prin intermediul unor site-uri care arată la fel ca site-urile pe care le folosești deja. De exemplu, e posibil ca cineva care practică phishing să îți trimită un e-mail care arată ca și cum a fost trimis de banca ta, astfel încât să îi transmiți informații despre contul tău bancar.

E-mailurile sau site-urile de tip phishing pot să îți ceară:

- nume de utilizator și parole, inclusiv modificări de parolă;
- codul numeric personal;
- numărul contului bancar;
- codurile PIN (numere de identificare personală);
- numărul cardului de credit;
- numele dinainte de căsătorie al mamei tale;
- data nașterii.

Important: Google sau Gmail nu îți va solicita niciodată să transmiți aceste informații prin e-mail.

Evită atacurile de phishing

Tratează cu atenție e-mailurile pe care le primești de la un site care îți solicită informații personale. Dacă primești astfel de e-mailuri:

1. nu da clic pe niciun link și nu transmite niciun fel de informații personale până când confirmi că e-mailul este real.
2. dacă expeditorul are o adresă Gmail, raportează abuzul din Gmail la Google.

Notă: Gmail nu îți va solicita niciodată prin e-mail informații personale precum parola.

Când primești un e-mail care pare suspect, iată câteva lucruri pe care e recomandat să le verifici:

- verifică dacă adresa de e-mail și numele expeditorului corespund;
- verifică dacă e-mailul este autentificat;
- plasează cursorul peste linkuri înainte de a da clic pe ele. Dacă adresa URL a linkului nu corespunde cu descrierea acestuia, e posibil să te direcționeze către un site de tip phishing.
- verifică antetele mesajelor pentru a te asigura că antetul „from” nu afișează un nume greșit.

  Important: în cazul în care crezi că adresa ta Gmail a fost piratată, recuperează-ți contul Gmail compromis înainte de a trimite sau de a deschide alte e-mailuri.