Proiect :Realizat de Nicoara Cristian si Cuciuc Loredana

Internetul reprezintă un spaţiu fascinant, în care comunicarea, informaţia şi divertismentul sunt beneficii pentru toţi oamenii, indiferent de vârstă şi de cultura căreia îi aparţin. **Cu toţii petrecem ore bune în faţa computerului, în fiecare zi, fie că citim, fie că socializăm online, fie că ne expunem viaţa pe retelele de socializare. Cu alte cuvinte, suntem în secolul IT, iar acest lucru are beneficii şi dezavantaje.**

-intrebari adresate clasei

-filmulet

1)10 reguli pentru o navigare sigura pe internet

1.Stabileste împreuna cu parintii tai regulile de folosire a calculatorului si a Internetului.
2.Nu da nici unei persoane întalnite pe Internet informatii personale despre tine sau familia ta.
3.Parolele sunt secrete si îti apartin.
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.
5.Posteaza cu mare grija fotografii cu tine sau cu familia ta!
6.Nu tot ceea ce citesti sau vezi pe Internet este adevarat.
7.Nu raspunde la mesajele care te supara sau care contin cuvinte sau imagini nepotrivite!
8.Da dovada de respect, chiar daca nu-i cunosti pe cei cu care comunici.
9.Cumpararea produselor pe Internet este permisa doar parintilor.
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.

2) Hartuirea online

Ce este hărţuirea online, numită în limbajul uzual cyber bullying**? Este un termen lansat de Bill Belsey, specialist canadian în educaţie, care l-a definit astfel: "*Cyber bullying-ul implică utilizarea tehnologiilor informaţionale şi comunicaţionale pentru a sprijini un comportament deliberat, repetat şi ostil desfăşurat de către un individ sau grup, care este destinat să aducă prejudicii altor persoane".Exemple:***

- **bârfa**
- **hărţuirea**
- **urmărirea online**
- **trolling**
- **comentarii**
- **profiluri false**

Aceste acţiuni constituie nişte abuzuri în adresa persoanei. În primul rând, este bine să ştim ce instrumente tehnice putem folosi pentru a opri un asemenea comportament din partea terţilor. Dacă hărţuirea se realizează pe o reţea de socializare ,trebuie să cunoaşteţi că aceste platforme au opţiuni de a raporta comentariile abuzive, hărţuirea sau aşa numitul spam. A nu se ignora această opţiune ce vi se pune la dispoziţie, ori ea chiar poate duce la închiderea contului de pe care sunteţi molestat.

Soluţii tehnice ar fi mai multe, de a vă seta contul în aşa fel încât să fie mai puţin accesibil persoanelor cu care nu sunteţi "prieteni".. În cazul în care hărţuirea se realizează în afara reţelelor de socializare, de exemplu pe anumite site-uri sau bloguri, primul pas ar fi să notificaţi proprietarul site-ului prin a solicita ştergerea informaţiei care vă defăimează.

3)Reputatia online

Managementul reputatiei online se ocupa de influentarea si controlul reputatiei unei organizatii/individ.
Reputatia online reprezinta poate cel mai de pret activ pentru o organizatie (fie ea afacere, institutie publica, organizatie non-profit, etc.) si/sau individ. O reputatie negativa poate avea efecte dintre cele mai neplacute la fel cum o reputatie pozitiva ne poate propulsa usor pe culmi inalte. Esti antrepenor si detii o afacere, ai o profesie liberala (avocat, medic, stomatolog, expert contabil, arhitect, etc.), esti managerul unei institutii publice, esti politician,asta inseamna ca cineva, undeva, pe internet comenteaza si scrie review-uri despre tine si/sau afacerea institutia pe care o conduci. In acest context ar trebui sa fii preocupat de **ORM**, sau, mai exact spus - de imaginea ta in mediul online. De cele mai multe ori aceasta imagine nu ti-o construiesti singur si din pacate nici nu mai detii controlul total asupra ei.

4)Cum recunoastem un calculator 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.

2. "*Computerul meu functioneaza extrem de incet*" -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*" - Daca ati fost infectat, virusul 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*" - 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.

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*" – Acest lucru ar putea fi 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.

5) Protectia antivirus

Protectia antivirus reprezinta programele de calculator concepute pentru a preveni, detecta si elimina virusii informatici.

SOLUTII

Exista multe solutii antivirus pe piata. Important in cazul unei astfel de solutii este nivelul de protectie pe care il ofera. Sunt mai multe metode de a identifica virusi, astfel in alegerea solutiei antivirus este important sa tinem cont de acest lucru. Un alt aspect important este frecventa cu care solutia antivirus isi face actualizarile privind semnaturile virusilor. Practic, exista o baza de date pentru fiecare produs antivirus care contine semnaturile virusilor informatici cunoscuti, iar aceasta se actualizeaza constant.

Un alt aspect important este pe ce echipamente folosim solutii antivirus. Este bine ca protectia antivirus sa fie pe mai multe nivele. Daca avem un echipament de retea prin care este filtrata antivirus toata informatia care vine din internet dar statiile de lucru nu au o solutie proprie antivirus este posibil ca un utilizator sa foloseasca un stick usb si sa infecteze toata reteaua.

Pentru echipamentele de retea care filtreaza traficul internet in si dinspre internet sunt solutiile oferite de Fortinet si Juniper. Pentru statiile de lucru si servere exista solutiile antivirus oferite de Bitdefender, Kaspersky, Microsoft Forefront

6) Securitatea informaţiei se ocupă cu protejarea informaţiei şi sistemelor informatice, de accesul neautorizat, folosirea, dezvăluirea, întreruperea, modificarea sau distrugerea lor. **Comisia Electrotehnică Internaţională** tratează securitatea informaţiilor prin cele trei componente principale: confidenţialitatea, integritatea şi disponibilitatea.Confidenţialitatea este asigurată prin criptarea informaţiei. Integritatea se obţine prin mecanisme şi algoritmi de dispersie. Disponibilitatea se asigură prin întărirea securităţii reţelei sau reţelelor de sisteme informatice şi asigurarea de copii de siguranţă.

Printre cele mai frecvente infracţiuni din domeniul securităţii informaţiei pot fi menţionate:

- Accesul nesancţionat la baze de date şi informaţii sensibile în scopul însuşirii lor, copierii şi utilizării ilegale.
- Utilizarea nesancţionată a resurselor informatice în scopul obţinerii unor beneficii sau a provocării unor prejudicii sistemelor informatice şi utilizatorilor acestora.
- Modificarea (falsificarea) intenţionată a datelor.
- Furturi de identitate, obţinerea nelegală a drepturilor la proprietate.
- Provocarea unor defecţiuni ale mijloacelor tehnice de prelucrare, transmitere şi stocare a informaţiei.

- Răspândirea viruşilor şi a programelor maliţioase, pentru a compromite sistemele informatice

7)Securitatea aplicatiilor

Un aspect important – dar care în cele mai multe cazuri este neglijat, din păcate – este cel al asigurării securităţii sitului/aplicaţiei Web. Orice aplicaţie software – poate fi victima unui incident de securitate. Acest incident reprezintă frecvent un eveniment apărut în cadrul reţelei, cu implicaţii asupra securităţii, provenind din interiorul sau din exteriorul organizaţiei.. La momentul crearii, multe protocoale Internet nu au luat în calcul posibilele vulnerabilităţi ce pot surveni. Vulnerabilitatea se referă la slăbiciunea unui sistem hardware sau software care permite utilizatorilor neautorizaţi să aibă acces asupra acestuia ,Niciun sistem informatic nu poate fi considerat 100% sigur, iar deseori vulnerabilităţile pot apărea datorită unei inadecvate administrări. La întrebarea "La ce nivel trebuie luate măsuri de securitate?", principalele acţiuni ar fi inhibarea ascultării mediilor de transmisie, interzicerea accesului fizic la server, instalarea zidurilor de protecţie (*firewall*-urilor), criptarea conexiunilor, monitorizarea şi actualizarea software-ului .

8)Securitatea in retelele WI-FI

 Securitatea informaţiei şi a reţelei poate fi înţeleasă ca abilitatea reţelei sau a sistemului informatic de a rezista evenimentelor accidentale sau acţiunilor maliţioase care compromit disponibilitatea, autenticitatea, integritatea şi confidenţialitatea datelor stocate sau transmise şi a serviciilor oferite sau accesibile prin aceste reţele.
 Sunt definite următoarele caracteristici de securitate:
- autentificarea,
- confidenţialitatea,
-integritatea,
-disponibilitatea, controlul accesului,
-administrarea cheilor,
-managementul (administrarea) securităţii.

Ameninţările la adresa securităţii unei reţele de calculatoare conectate prin cablu sau prin mijloace wireless, inclusiv prin Wi-Fi, pot avea

următoarele origini:
-defectări ale echipamentelor
-greşeli umane de operare sau manipulare
-fraude

9)Spam-urile

Spamming este procesul de expediere a mesajelor electronice nesolicitate, de cele mai multe ori cu caracter comercial, de publicitate pentru produse şi servicii dubioase,*Spam*-ul se distinge prin caracterul agresiv, repetat şi prin privarea de dreptul la opţiune.
Această metodă se foloseşte şi la colectarea adreselor de e-mail utilizând metode de ugenul *Citeşte şi dă mai departe*. Conţinutul acestor mesaje variază de la texte biblice, urări de bine cu îndemnarea de a trimite mai departe, în caz contrar vor urma evenimente neplăcute, până la mesaje cu caracter alarmant menite să atragă atenţia asupra unui fapt plauzibil, îndemnând cititorul să trimită mesajul şi altor persoane. Aceste mesaje rulează într-o anumită comunitate iar emitentul acestui mesaj foloseste diferite metode pentru a ajunge iar în posesia lui. Adresele de email colectate sunt cel mai adesea vândute cu scopul de a trimite alte mesaje SPAM cum ar fi cele comerciale.
Spamming-ul este o metodă foarte ieftină de a face reclamă pentru ceva în Internet; succesul campaniei este de obicei proporţional cu numărul de destinatari; de aceea mesajul respectiv este transmis la mii, chiar milioane de adrese simultan.

10)Spyware & Keyloggers

Programele spion sau ***spyware*** sunt o categorie de software rău intenţionat, ataşate de obicei la programe gratuite care captează pe ascuns date de marketing (prin analiza siturilor pe care le vizitează utilizatorul, de exemplu de modă, pantofi, cluburi de tenis, ş.a.m.d.) şi le folosesc apoi pentru a transmite utilizatorului reclame corespunzătoare dar nesolicitate.

Există programe spion care modifică modul de comportare a unor motoare de căutare (Google, Yahoo, MSN, etc.), pentru a trimite utilizatorul contra voinţei sale la situri (scumpe) care plătesc comisioane producătorului programului spion.

În general, chiar după ştergerea programelor gratuite care au instalat programul spion, acesta rămâne în continuare activ. Există şi numeroase programe anti-spion, dar atenţie:

unele dintre ele sunt *false antispyware* - inducând utilizatorul în eroare deoarece ele însele conţin programe spion mascate.

Multe programe de hackeri mascate pot găsi drumul pe computerul dvs. prin internet, iar un keylogger este unul dintre cele mai grave.Ex. Spyware care înregistrează activităţile dvs. **Un keylogger înregistrează fiecare tastă pe tastatură pe tastatura calculatorului** . Cu aceste informaţii, un hacker îţi poate elabora numele de utilizator şi parola pentru o serie de site-uri fără a vedea chiar ce apare pe ecran. Keylogger-urile nu vă încetinesc calculatorul şi nici nu veţi observa când vă aflaţi în funcţiune. Pe scurt, **există multe scenarii de funcţionare pentru keylogger-ele şi** multe locaţii diferite pe computerul în care ar putea fi difuzat programul si este deosebit de greu de scăpat de acesta.Cele mai bune şanse pe care le aveţi de a împiedica funcţionarea unui keylogger pe computerul dvs. trebuie să îl blocheze înainte de a fi instalat. Pentru aceasta, aveţi nevoie de un software antimalware foarte bun şi, de asemenea, un scepticism în ceea ce priveşte descărcarea de orice pe web.

Metoda tipică de intrare pentru un keylogger este ca parte a unui troian . Un troian este o bucată de software care pretinde a fi utilă. Când descărcaţi această aplicaţie gratuită şi o instalaţi, nu va funcţiona sau aplicaţia nu funcţionează aşa cum a promis.

11) Comunicarea pe retelele de socializare

Internetul a devenit un prieten pentru unii, un dusman pentru altii. Un lucru este cert, pe unii accesibilitatea la retelele de socializare ii ajuta sa-si creeze noi relatii, pe altii insa ii sustrage de la lucruri poate mai importante – viata reala. Procesul de comunicare virtuala prin intermediul retelelor de socializare precum Facebook sau Twitter, au transformat viata generatiei secolului XXI, intr-o viata mai mult virtuala decat un reala.

Savanţii au constatat că persoanele care sunt active pe reţelele de socializare se simt izolate de societatea în care trăiesc

Această problemă este una actuală, deoarece afectează într-un grad destul de mare tineretul, devenind o adevărată epidemie. Omul după natura sa este o fiinţă socială însă, cu părere de rău, modul de viaţă pe care îl avem astăzi ne determină să ne înstrăinăm unul de altul tot mai mult.
Dezavantaje

Atunci cand ai o comunicare virtuala cu o persoana, n-ai siguranta ca cel cu care discuti este cu adevarat cel care se pretinde. Nu poti identifica identitatea acestuia.

- Nu poti verifica cat este de sincer cu tine celalalt atunci cand aveti o comunicare virtuala.
- Avand o comunicare virtuala, nu poti urmari mesajele non-verbale si paraverbale – zambetul, privirea, tonul vocii.
- Poti fi tradat, in cazul in care ai prea multa incredere in prietenul cu care ai o comunicare virtuala.

12) Activitatea de phishing Un atac de tip phishing are loc atunci când cineva încearcă să te păcălească pentru a dezvălui informaţii personale online.

Ce înseamnă activitatea de phishing. De obicei, activitatea de phishing se face prin e-mailuri, anunţuri sau prin intermediul unor site-uri care arată la fel ca site-urile pe care le foloseşti deja. De exemplu, e posibil ca cineva care practică phishing să îţi trimită un e-mail care arată ca şi cum a fost trimis de banca ta, astfel încât să îi transmiţi informaţii despre contul tău bancar.

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

- nume de utilizator şi 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.

Raportează e-mailurile de tip phishing

Concluzie

Sperăm că această lecţie va fost de folos. E important să protejaţi calculatorul de viruşi pentru o funcţionare mai bună a acestuia. De asemenea, aveţi grijă când navigaţi pe internet, pe langă plăcerea pe care o primiţi, să ştiţi că puteţi fi şi în pericol.