Securitatea cibernetică

Proiect elaborat de:
Gandraman Milena
Chirtoca Andreea
Clasa a XI-a „C”
Profesoară:
Guțu Maria
Anul de studii:
2018

Introducere

1. 10 reguli pentru o navigare sigură pe Internet.
2. Hărțuirea în mediul Online.
3. Reputația Online.
4. Cum recunoaștem un calculator virusat?
5. Protecție antivirus.
6. Securitatea informațiilor.
7. Spam-urile.
8. Spyware & Keyloggers.
9. Comunicarea pe rețelele de socializare.
10. Adresele de e-mail pentru phishing.

10 reguli pentru o navigare sigură pe Internet

1. Foloseşte programe cu licenţă şi evită-le pe cele tip sharing.

10 reguli pentru o navigare sigură pe Internet

2. Foloseşte o soluţie antivirus actualizată zilnic.

Efectuează scanări periodice ale sistemului pentru a identifica posibile fişiere cu potenţial maliţios.

10 reguli pentru o navigare sigură pe Internet

3. Nu deschide ataşamentele aferente unor e-mailuri venite din partea unor expeditori necunoscuţi.

10 reguli pentru o navigare sigură pe Internet

4. Fii întotdeauna sceptic când primeşti o ofertă ce sună foarte tentant.

Multe tehnici de phishing încearcă să te păcălească în a oferi date personale.

10 reguli pentru o navigare sigură pe Internet

5. Rămâi cât mai anonim posibil.

Să nu faci publice informaţiile personale (numele complet, adresa, numărul de telefon, CNP-ul, parole, nume ale membrilor de familie, numere de cărţi de credit). Majoritatea oamenilor şi companiilor credibile nu îţi vor cere să le comunici astfel de date pe Internet.

10 reguli pentru o navigare sigură pe Internet

6. Fii cât se poate de discret

Datele personale şi pozele postate în mediul virtual s-ar putea să fie folosite împotriva ta. Oricine îţi poate vizualiza profilul de pe reţelele de socializare online, pentru a culege informaţii pe care le-ar putea folosi ulterior spre a-ţi provoca diverse neplăceri.

10 reguli pentru o navigare sigură pe Internet

7. Asigură-te că aplicaţiile Facebook acceptate sunt de încredere.

10 reguli pentru o navigare sigură pe Internet

8. Evită pe cât posibil căutările riscante

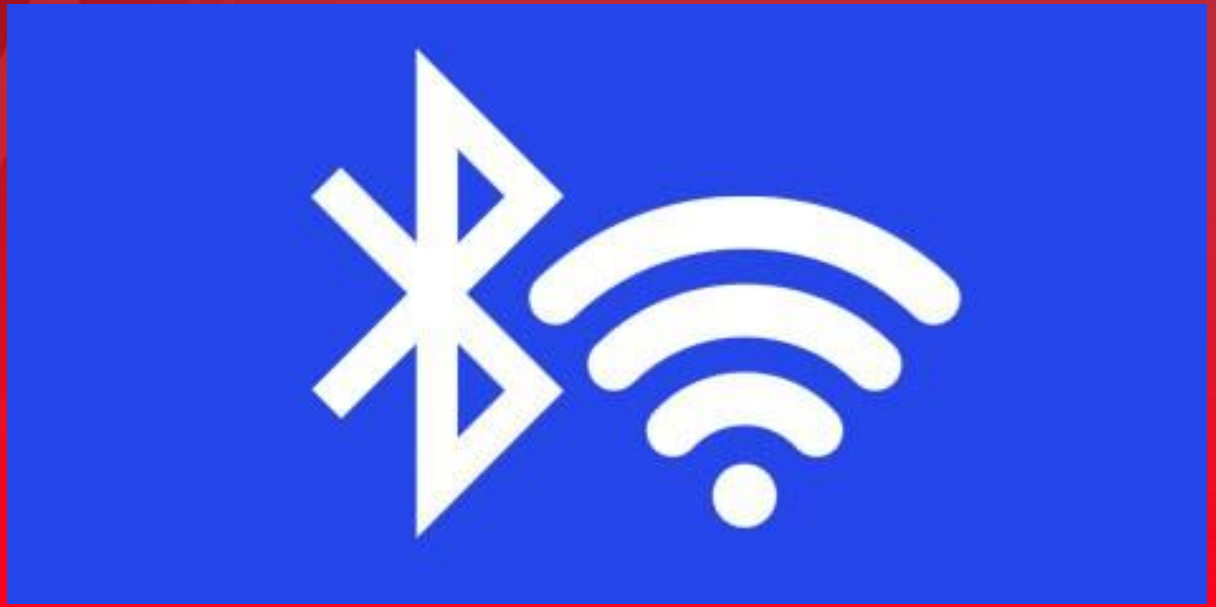
Rezultatele căutărilor voastre ar putea conţine link-uri către site-uri ce găzduiesc conţinut maliţios. Aceste site-uri pot instala aplicaţii maliţioase de tip spyware, viruşi etc. Dacă foloseşti aplicaţii de partajare a fişierelor, este foarte probabil să descarci un virus în loc de fişierul audio sau video pe care doreşti să îl preiei.

10 reguli pentru o navigare sigură pe Internet

9. Evită utilizarea reţelelor wi-fi publice pentru operaţiuni bancare, comerţ on-line sau afaceri personale.

10 reguli pentru o navigare sigură pe Internet

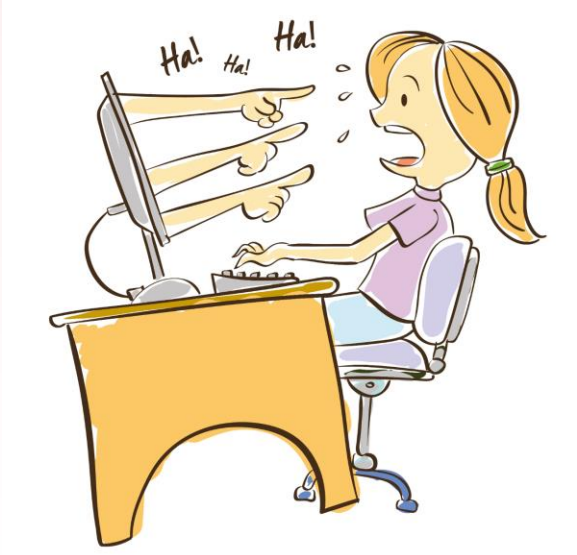
10. Dezactivează opţiunea Bluetooth atunci când nu o foloseşti.

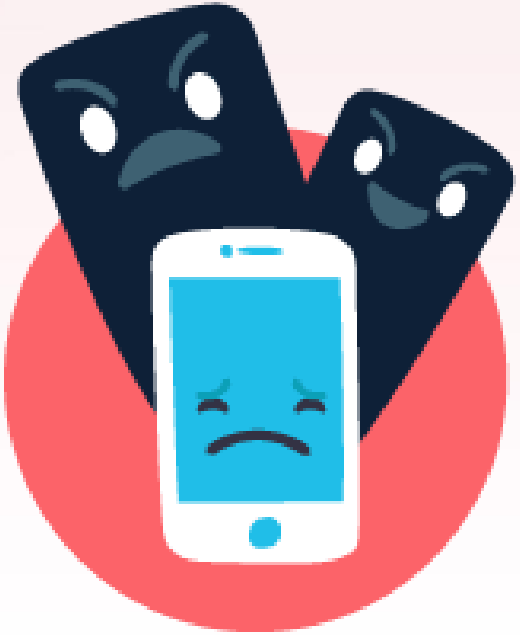


Hărțuirea în mediul Online

Cyberbullying-utilizarea tehnologiei pentru a hărțui, amenința, țintind o anumită persoană;

ACEASTA ESTE O CRIMĂ ȘI POȚI FI TRAS LA RĂSPUNDERE DE CĂTRE AUTORITĂȚILE LEGALE, ÎN UNELE CAZURI-PEDEAPSA CU ÎNCHISOARE.





Hărțuirea în mediul Online

Exemple de cyberbullying:

- Comentariu sau mesaj cu tentă agresivă și răutăcioasă
- Utilizarea datelor personale cum ar fi poze, video-uri pentru a umili o persoană
- Crearea paginilor false și a pretinde că ești altă persoană
- Etc.

Hărțuirea în mediul Online

Semne:

- Schimbarea bruscă a dispoziției după utilizarea internetului sau telefonului
- Ascunderea unor lucruri (mai ales ceea ce ține de viața online)
- Distanțarea față de membrii familiei și prieteni
- Schimbări de comportament, dispoziție, regimul de somn și pierderea poftei de mâncare
- Etc.

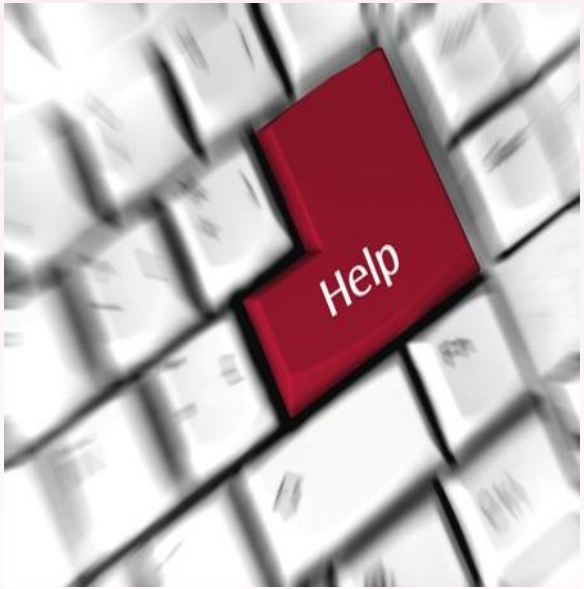
Hărțuirea în mediul Online

Consecințe:

- Anxietate
- Depresie
- Stres
- Gânduri sinucigașe
- Sinucidere

Depășirea situației:

- Blocarea agresorului
- Limitarea accesului la tehnologii
- Adresarea către organele specializate

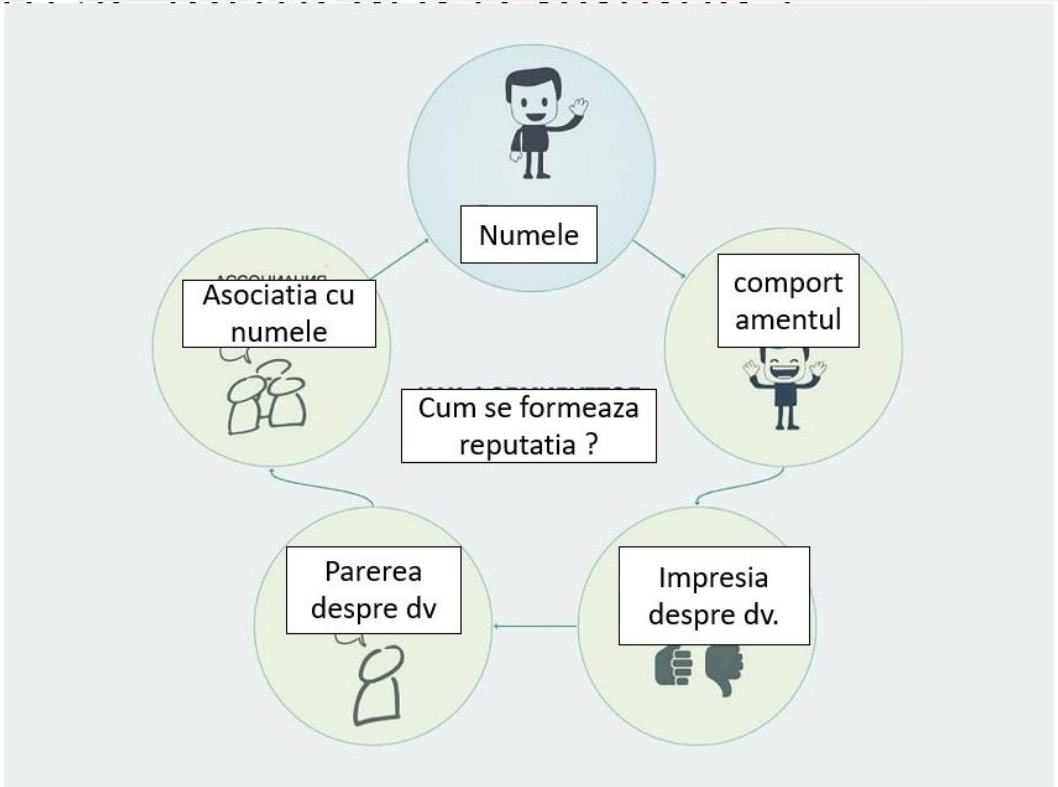


Reputația Online

Clasificare:

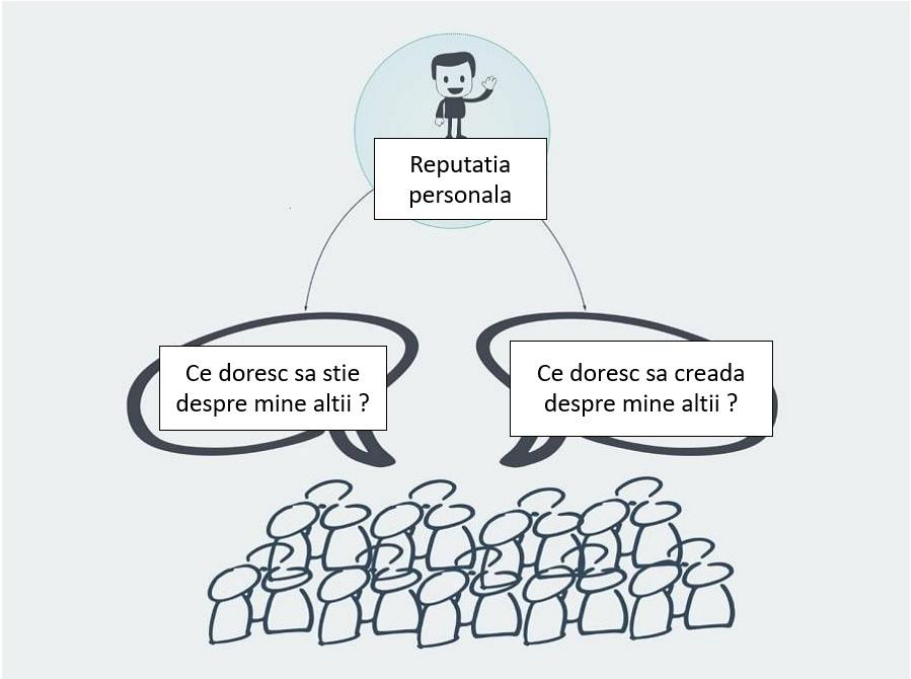
- Antreprenorii care își promovează ei înșiși și afacerea personală prin Internet.
- Personalități publice: scriitori, bloggeri, lideri de opinie, profesori, muzicieni, politicieni, sportivi.
- Oamenii care folosesc Internetul pentru a menține co ntacte cu prietenii, rudele și colegii.

Reputația Online



Reputația Online

Cum să formezi imaginea dorită a reputației tale?



Reputația Online

Ce doresc să se cunoască despre mine pe rețelele de socializare?

- Unde lucrez;
- În care domeniu sunt specialist;
- Ce beneficii aduc oamenilor;
- Ce proiecte desfășor;
- Care sunt alte interese decât cele profesionale;
- Fie că sunt gata să împărtășesc sau nu părți ale vieții mele personale; dacă da, care dintre ele?

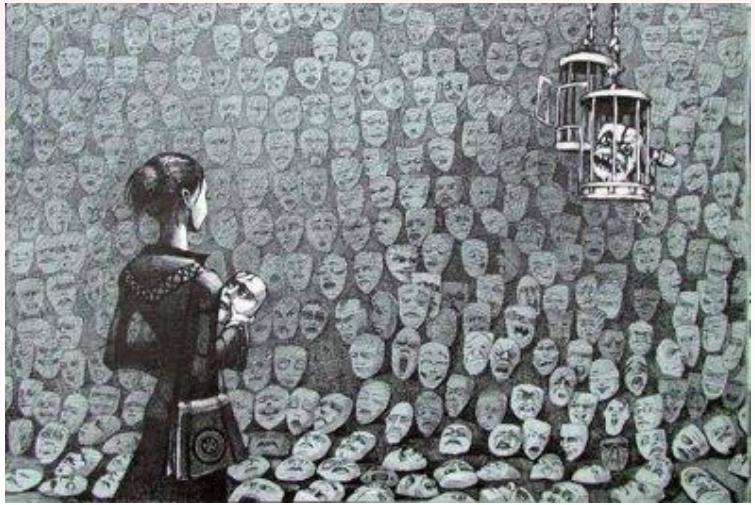
Reputația Online (Sfaturi)

1.Gândește-te ce vrei ca oamenii să creadă despre tine

- Exemple de formulare "Vreau să oamenii sa stie și să vorbesca despre mine urmatoarele lucruri ..."
- "Semyon este un profesor de limba engleză, el poate explica gramatica copiilor, astfel încât ei să nu mai o urască. El are un farmec, iar copii sunt atrași de el de la prima întâlnire. Modest, adecvat. "
- "Maria - scrie articole, articolele ei sunt editate de editori pentru prima dată și sunt în general gata sa accepte un articol de la ea pe orice subiect, pentru ca sunt încrezători in calitate. Întotdeauna răspunde la scrisori, clar în comunicare. Dragă spec ialist, dar merită banii ".

2. Luați în considerație trăsăturile personale

Nu este nevoie să inventezi o imagine artificială. Nu descrieți trăsături pe care nu le posedați. Dacă sunteți introvertit,
nu încercați să creați o reputație de persoană sociabilă.



Reputația Online (Sfaturi)

3. Determinați cercul persoanelor care sunt "proprietari" ai reputației dvs.

- Prietenii mei;
- Familia mea;
- Colegii mei;
- Conducătorii mei;
- Colegii mei din comunitatea mea profesională
- Clienții mei existenți;
- Partenerii și furnizorii mei existenți;
- Potențialii clienți;
- Potențiali parteneri și furnizori;
- Persoane aleatorii, etc.

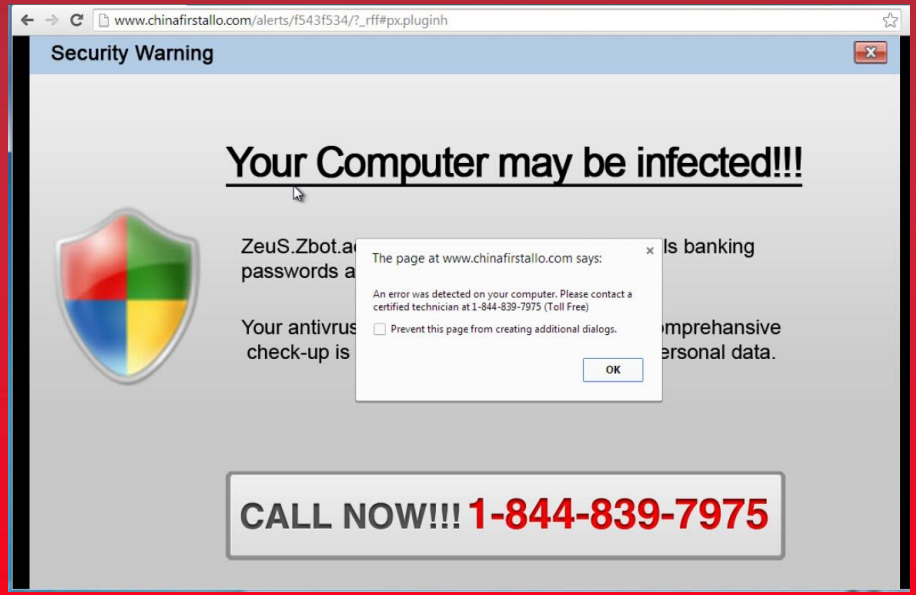
Reputația Online (Sfaturi)

4.Analizați unde și ce informații publicați,cum vă comportați:

- Ceea ce publicasem și voi continua să public.
- Exemplu: publicați fapte din viața dvs care pot aduce beneficii oamenilor, și anume (lista de exemple continuă).
- Ce voi începe sa public.
- Exemplu: Voi trimite un comentariu personal la acele linkuri către publicațiile pe care le împărtășesc.
- Că voi opri denpublicat.
- Exemplu: Voi înceta să public fotografii cu umor dubios, voi înceta să public fotografii din fiecare călătorie - numai cele mai neobișnuite.

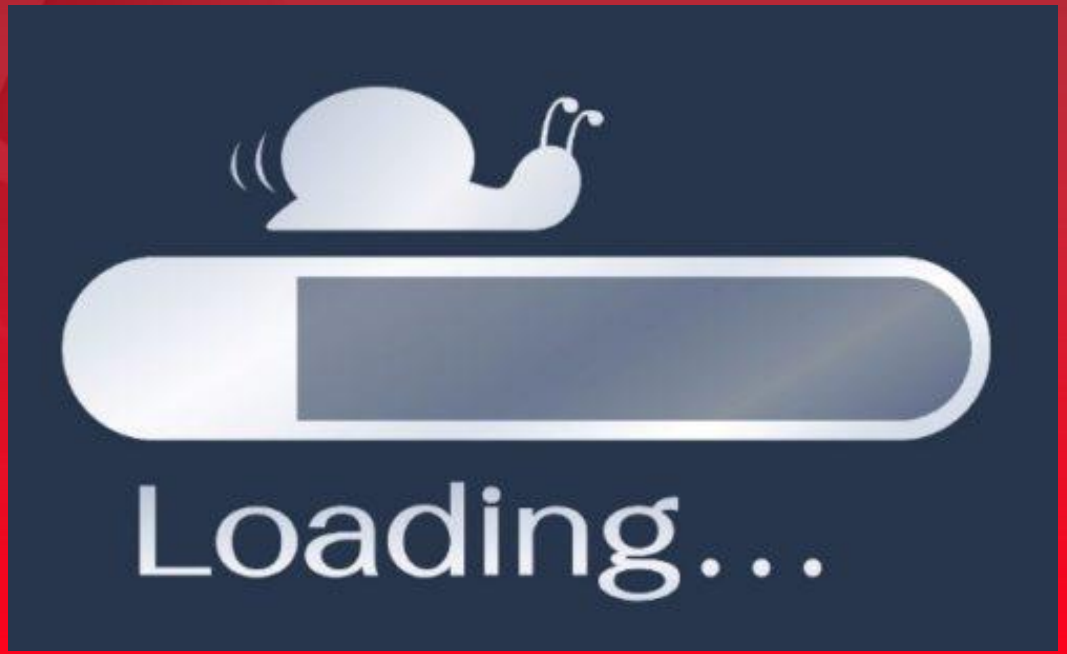
Cum recunoaștem un calculator virusat?

1. *“Computerul vorbeste cu mine“*



Cum recunoaștem un calculator virusat?

2. *“Computerul meu funcționează extrem de încet“*



Cum recunoaștem un calculator virusat?

3. *“Am aplicații care nu pornesc”*

Cum recunoaștem un calculator virusat?

4. *“Nu mă pot conecta la Internet sau acesta rulează extrem de încet“*

Cum recunoaștem un calculator virusat?

5. *“Când mă conectez la Internet, mi se deschid pe ecran tot felul de ferestre sau pagini web nesolicitate”*

Cum recunoaștem un calculator virusat?

6. *“Unde au disparut fișierele mele?“*

Cum recunoaștem un calculator virusat?

7.“Computerul meu vorbește în altă limbă”

Hà Nội là thủ đô, đồng thời là thành phố đứng đầu Việt Nam về diện tích tự nhiên và đứng thứ hai về diện tích đô thị sau thành phố Hồ Chí Minh, nó cũng đứng thứ hai về dân số với 6.913.161 người.

Cum recunoaștem un calculator virusat?

8. *“Îmi lipsesc fișiere necesare pentru a rula jocuri, programe etc”*

Protecție antivirus

TDL4 este cel mai periculos virus informatic din istorie, avertizează cei de la Kaspersky Labs, citați de atlantico.fr.
Catalogat drept "indestructibil', virusul ar fi patruns deja în 4,5 milioane de computere, potrivit sursei citate. Potrivit specialiștilor, virusul a făcut ravagii în Statele Unite, Marea Britanie Italia și Franța.

Protecție antivirus

Ce este un virus ?

Protecție antivirus

•Virusul informatic este în general un program care se instalează singur, fără voia utilizatorului, și poate provoca pagube atât în sistemul de operare cât și în elementele hardware (fizice) ale computerului.

•Modul de actiune difera de la un virus

la altul, astfel anumiti virusi distrug datele de pe disc prin coruperea program elor, stergerea fisierelor sau chiar prin reformatarea discului fix. Totusi, majori tatea virusilor doar se reproduc si afiseaza diverse mesaje.

Protecție antivirus

Virusii pot face urmatoarele lucruri:

- infecteaza fisiere executabile (de program), cum ar fi aplicatii de editare de text, calcul tabelar sau chiar fisiere ale sistemului de operare;
- infecteaza discurile atasandu-se la anumite programe speciale, in mod deosebit in zonele denumite de boot si master boot records;
- infecteaza fisiere atasate mesajelor transmise prin intermediul postei electronice, unor dispozitive de transfer al datelor (dischete, CD-uri) sau prin retea;

Protecție antivirus

Ce este protectia antivirus ?

- Protectia antivirus reprezinta programele de calculator concepute pentru a preveni, detecta si elimina virusii informatici. Un virus informatic reprezinta un program rau intentionat dezvoltat de un programator, care, precum un virus biologic, se multiplica si incearca sa se raspandeasca pe alte calculatoare prin diverse mijloace.

Securitatea informațiilor

Infracțiuni din domeniul securităţii informaţiei:

- 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.
- Atacuri de tipul DDOS (distributed denial of service) – refuz de prestare a serviciilor, în particular – atacurile asupra serverelor din reţea.
- Răspândirea viruşilor şi a programelor maliţioase, pentru a compromite sistemele informatice.

Securitatea informațiilor (Prevenire)

1. În timpul utilizării poștei electronice:

 Nu accesați imaginile sau link-urile din e-mailurile dubioase.

 Setați e-mailul dvs. în așa fel, încât acesta să vă afișeze e-mailurile în format de text simplu, și nu în format HTML.

 Aveți în vedere că este periculos să deschideți orice atașament, chiar și documentele Microsoft Word și PDF pot conține viruși, nu doar acele care au la sfârșit extensia de".exe".

 În cazul în care dvs. totuși doriți să deschideți documentul PDF sau Word: â
Pentru verificarea unui fișier suspect încărcați acesta pe site-ul online de verificare https://www.virustotal.com/

Securitatea informațiilor (Prevenire)

În timpul activităţii de lucru zilnice:

- fiţi precauţi referitor la apelurile telefonice nesolicitate, vizite, sau emailuri de la persoane care solicită informaţii despre angajaţi sau companie. În cazul în care o persoană necunoscută pretinde a fi de la o organizaţie legitimă, încercaţi să verificaţi identitatea acestuia, în raport cu organizaţia respectivă;
- nu oferiţi informaţii personale sau informaţii despre organizaţia dvs, inclusiv structura reţelei sale, dacă nu sunteţi sigur de autoritatea persoanei care solicită informaţiile;
- nu dezvăluiţi informaţii personale sau financiare prin e-mail;
- utilizaţi funcţii anti-phishing oferite de clientul de e-mail şi browser.

Securitatea informațiilor

Cum se crează o parolă?

Nu se recomandă:

- Utilizarea parolelor mai scurte de 6 caractere;
- Utilizarea numelui de familie sau prenumelui ca parolă sau diferite combinaţii ale lor;
- Utilizarea doar a literelor minuscule sau doar a cifrelor (de ex. data naşterii).

Se recomandă:

- Parole de tip 1, formate din registru mic [a-z] sau din cifre [0-9], lungimea minimă 20 caractere;
- Parole mixte, de tip 2, formate din registru mare mic [a-z][A-Z], lungimea minimă 14 caractere;
- Parole mixte, de tip 3, formate registru mic mare + cifre [a-z][A-Z][0-9], lungimea minimă 10 caractere;
- Parole mixte, de tip 4, formate din registru mic mare cifre + semne [a-z][A-Z][0- 9][!@$.-_], lungimea minimă de 8 caractere;
- Modificarea parolei cel puţin o dată la 3-6 luni.

Cum se creează o parolă de tip 4: Sa presupunem ca avem un cuvânt preferat “ACADEMICA”, transformat ar fi “Ac@d3m!ca.”

Spam-urile

Ce este un spam ?

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.

Spam-urile

Efectele negative ale spam-ului:

- nu permite posesorului adresei de email sa se dezaboneze si sa nu mai primeasca alte email-uri de la sursa respectiva
- este expediat automat de catre un program software
- 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

Spam-urile

Nu răspunde niciodată unui e-mail nesolicitat

Spam-urile

Nu da click pe link-urile din e-mail

Spam-urile

Dacă deschizi un e-mail nesolicitat ai grijă ca imaginile să fie blocate

Spyware & Keyloggers

Ce este Spyware?

Spyware este o categorie de ameninţări cibernetice, ce descrie programele maliţioase create pentru a infecta sistemele PC-urilor după care să iniţieze activităţi ilegale în acestea. Acestea sunt folosite pentru a urmări oamenii şi să le înregistreze cele mai vizitate website-uri precum şi acţiunile luate atunci când au fost vizitate. Această informaţie, în general, este utilizată de către diverse terţe în scopuri de marketing şi promovare, deci spyware-urile pot conduce şi la mărirea numărului de spam-uri.

Spyware & Keyloggers

Pentru ce pot fi utilizate amenințările de tip spyware:

- Pentru a fura informaţii sensibile.
- Să afişeze reclame nedorite.
- Redirecţionarea utilizatorilor către website-uri chestionabile sau maliţioase contrar dorinţei lor.
- Să creeze numeroase link-uri în rezultatele căutărilor efectuate de victimă şi să îl/o redirecţioneze către locurile dorite (site-uri spyware terţe, website-uri şi alte domenii asociate).
- Să cauzeze modificări esenţiale în setările sistemului.
- Conectarea la un calculator compromis utilizând backdoors.
- Degradarea performanţei generale a sistemului şi cauzarea instabilităţii acestuia.

Spyware & Keyloggers

Ce este keylogger?

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.

Spyware & Keyloggers

Un keylogger este capabil de iniţierea următoarelor activităţi:

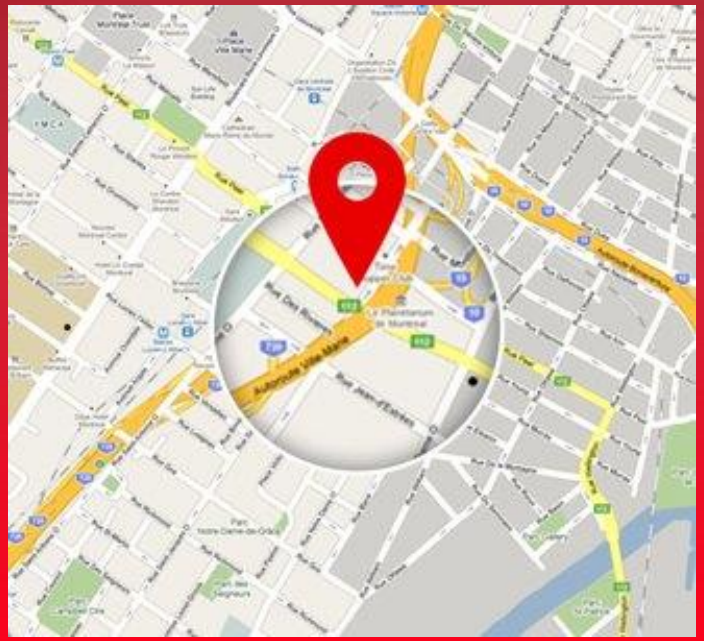
- Să înregistreze intrările de taste de pe tastatură.
- Să obţină capturi de ecran cu activitatea utilizatorului de pe internet la intervale de timp predeterminate.
- Să urmărească activitatea utilizatorului prin înregistrarea titlurilor ferestrelor, numele aplicaţiilor lansate, şi alte informaţii specifice.
- 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.

Comunicarea pe rețelele de socializare

- În New Hampshire, a existat un caz de jaf, care a adus victimei pierderi de 200 de mii de dolari. Motivul jafului a fost postul neglijent al unui bărbat în care el însuși a postat data plecarii în vacanță. Este bine ca săracul să nu s-a gandit să spună întregii lumi că a lăsat cheile la apartament sub covor ...

Comunicarea pe rețelele de socializare

Nu publicați pe rețelele de socializare locul în care vă aflați la moment



Comunicarea pe rețelele de socializare

Nu publicați date cu caracter personal

Comunicarea pe rețelele de socializare

Nu răspândiți informația despre alți oameni

Comunicarea pe rețelele de socializare

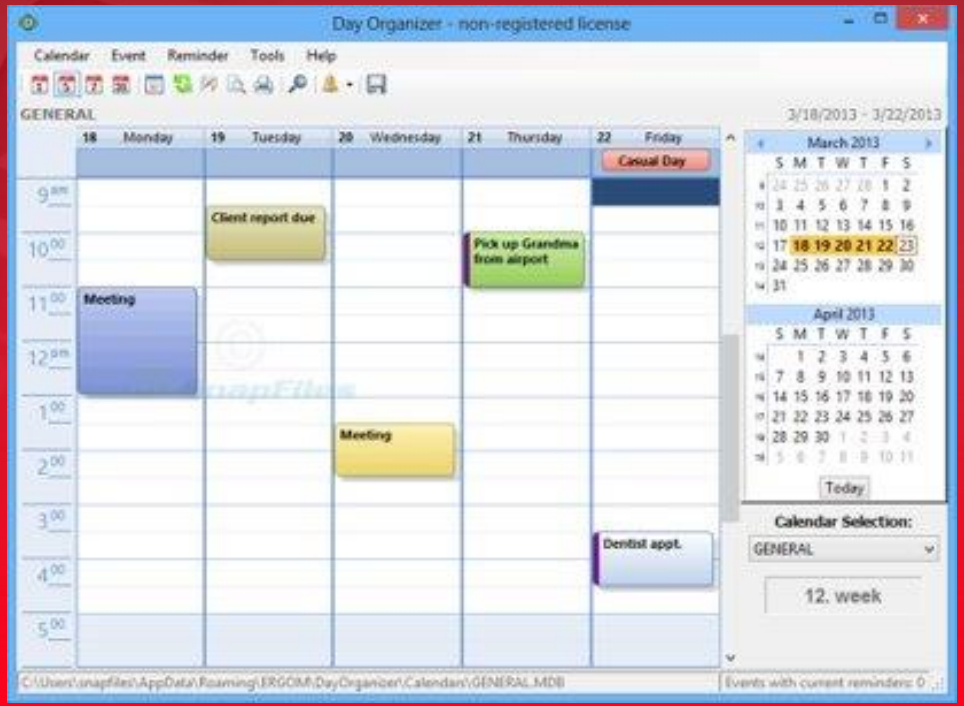
Nu divulgați informația despre lucrurile de preț pe care ați procurat

Comunicarea pe rețelele de socializare

Nu postați informație că nu veți fi acasă

Comunicarea pe rețelele de socializare

Nu publicați graficul vostru zilnic



Comunicarea pe rețelele de socializare

Întâlniți-vă cu prietenii noi din lumea virtuală doar în locuri populate

Comunicarea pe rețelele de socializare

Nu postați și nu scrieți nimic ce poate contribui la stricarea reputației

Comunicarea pe rețelele de socializare

Nu ofensați prietenii si cunoscuții voștri

Adresele de e-mail pentru phishing

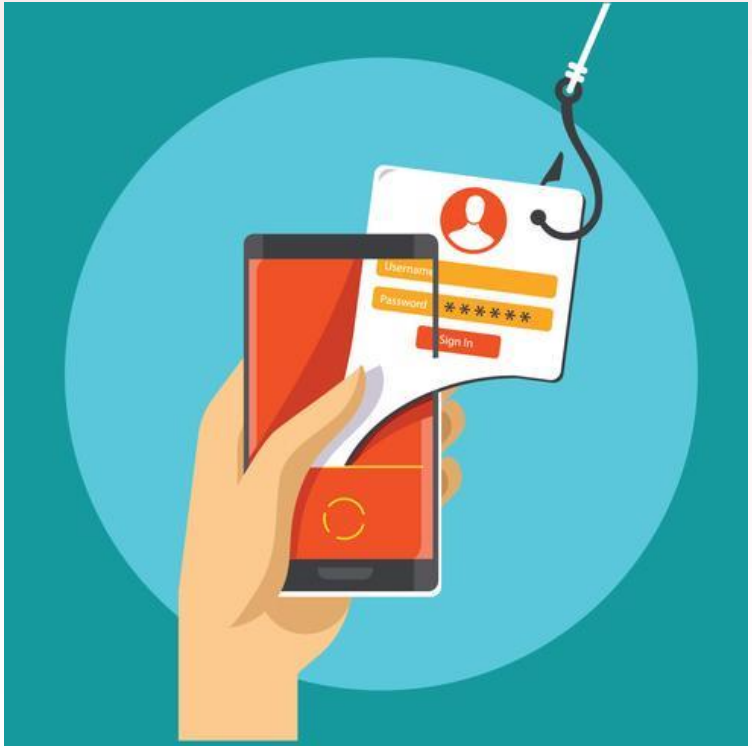
Ce înseamnă activitatea de phishing

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.

Adresele de e-mail pentru phishing

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.



Adresele de e-mail pentru phishing

Evită atacurile de phishing

Nu da clic pe niciun link și nu transmite niciun fel de informații personale până când confirmi că e-mailul este real.

Vă mulțumim pentru atenție!