

SECURITATEA PE INTERNET

Elaborat de : Carciumaru Marius
Diana Cernetchi
Elevi ai clasei a 10-a "C"
Anul elaborarii: octombrie 2018

Internet

- Internetul este o retea internationala formata prin conectarea tuturor retelelor din lume, facilitand schimbul de date si domenii in diferite domenii.

10 reguli importante pentru navigarea sigura pe Net

- 1. Stabileste împreuna cu parintii tai regulile de folosire a calculatorului si a Internetului.
- 2. Parolele sunt secrete si îți apartin.
- 3. Nu da nici unei persoane întâlnite pe Internet informatii personale despre tine sau familia ta.
- 4. Nu tot ceea ce citești sau vezi pe Internet este adevărat.
- 5. Nu raspunde la mesajele care te supara sau care contin cuvinte sau imagini nepotrivite!
- 6. Cumpararea produselor pe Internet este permisa doar parintilor.
- 7. Posteaza cu mare grija fotografii cu tine sau cu familia ta!
- 8. Dezactivează opțiunea Bluetooth atunci când nu o folosești.

- 6. Cumpararea produselor pe Internet este permisa doar parintilor.
- 7. Posteaza cu mare grija fotografii cu tine sau cu familia ta!
- 8. Dezactivează opțiunea Bluetooth atunci când nu o folosești.
- 9. Daca vrei sa te întâlnești fata în fata cu persoanele cunoscute pe Internet sau de la care ai primit mesaje pe telefonul mobil, anunta-ti parintii pentru a te însoți, preferabil într-un loc public.
- 10. Poti oricand sa te opresti din navigarea pe Internet sau sa refuzi sa continui discutiile pe chat, daca s-a întâmplat ceva care nu ti-a placut, te-a speriat sau, pur si simplu, nu ai înțeles.

Hartuirea in mediul Online

- Hartuirea online sau Cyber bullying-ul este un lucru des intalnit, din pacate, sunt multi oameni rau care vor incerca cu ajutorul Internetului sa te intimideze, supere sau ameninte. Hartuirea online poate fi prevenita daca vor fi urmate toate cele 10 reguli de utilizare sigura a Internetului.

Reputatia Online

Pe Internet pot aparea informatii sau poze cu tine, mai ales daca esti o persoana publica, multe din informatii pot sa nu fie adevarate. Reputatia pe Net tine de tine si de cum te porti, atat in viata reala cit si online.

Cum recunoastem un calculator virusat?

- 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 fizice ale computerului
- Dacă unele aplicații din computerul vostru nu se pornesc, apar pe ecran multe ferestre și imagini pe care nu le-ați accesat sau fișierele din calculator au disparut, e foarte probabil ca computerul e virusat
- Ca să scapăm de viruși e necesar să dăm computerul la mester, el știe ce să facă.

Protectie anti-virus

- Antivirusii ii putem instala in calculator prin internet, exista multe aplicatii si programe ce apara soft-ware-ul insa nu toate aceste aplicatii sunt de incredere, trebuie sa fim atenti cand descarcam in computer o astfel de programa.

Securitatea Informatiilor

- Fiti foarte atenti de informatiile pe care le publicati pe internet, nu e de dorit sa postati informatii peresonale despre voi sau familiile voastre. Multe din aceste date pot fi folosite de oameni cu scopuri rele si ne pot aduce pagube morale.

Ce sunt cookie-urile?

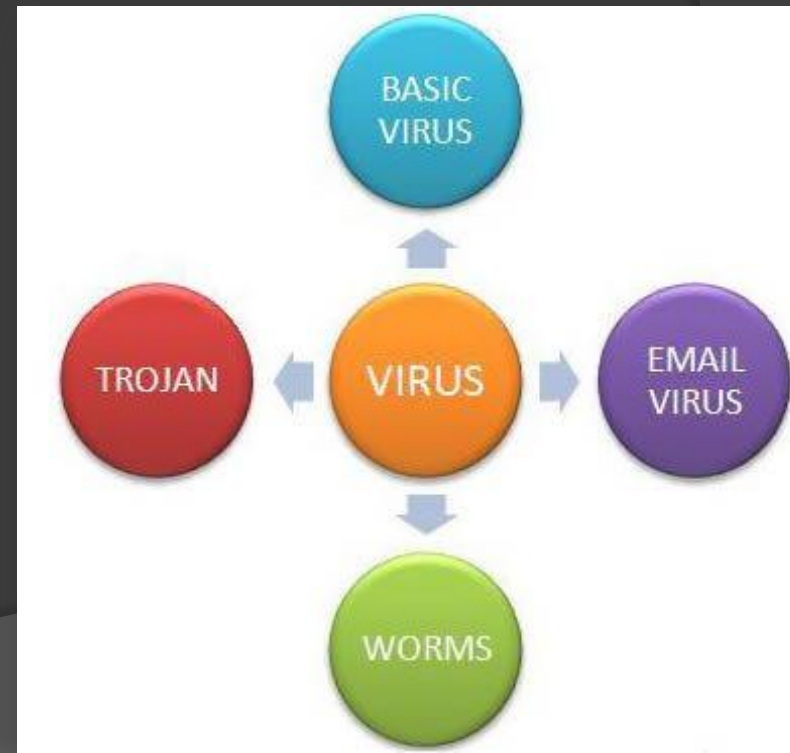
Un cookie sau un modul cookie este un text special, deseori codificat, trimis de un server unui navigator web și apoi trimis înapoi (nemodificat) de către navigator, de fiecare dată când accesează acel server. Cookie-urile sunt folosite pentru autentificare precum și pentru urmărirea comportamentului utilizatorilor; aplicații tipice sunt reținerea preferințelor utilizatorilor și implementarea sistemului de „coș de cumpărături”.

Cookie-urile au creat îngrijorare din cauză că ele permit strângerea de informații despre comportamentul utilizatorilor (în principiu, ce anume pagini web vizitează și când). Ca urmare, folosirea lor (și a informațiilor culese) sunt supuse în unele țări unor restricții legale, printre care [Statele Unite ale Americii](#) și țările [UE](#). Tehnicile de tip „cookie” au fost de asemenea criticate pentru faptul că identificarea utilizatorilor nu e întotdeauna precisă, ca și pentru faptul că prin intermediul lor se pot executa atacuri informatice.



Virusii, viermii si troienii

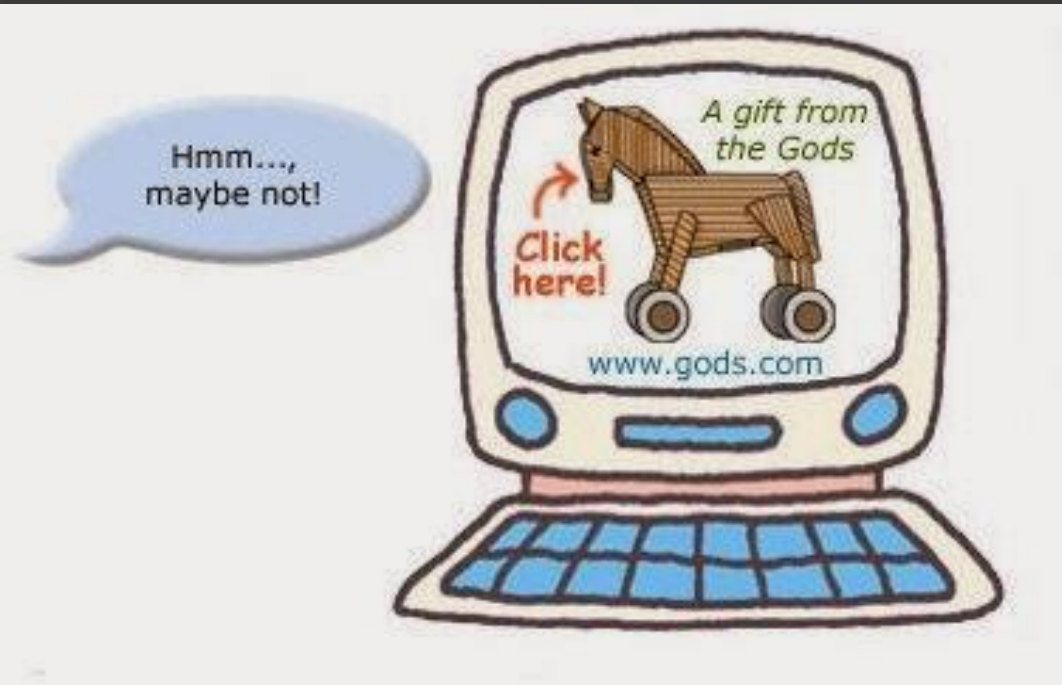
Viruși: virușii informatici sunt programe care se autocopiază pe sistemul compromis, fără știrea utilizatorului. Virusul va infecta astfel componente ale sistemului de operare sau alte programe informatice.



Viermi: programe care se pot auto-replica. Acestea folosesc rețeaua de calculatoare pentru a-și trimite propriile copii în alte noduri (calculatoare din rețea), reușind să facă acest lucru fără intervenția vreunui utilizator. Spre deosebire de un virus informatic, un vierme informatic nu are nevoie să fie atașat la un program existent. Viermii provoacă daune rețelei, chiar și prin simplul fapt că ocupă bandă, în timp ce virușii corup sau modifică aproape întotdeauna fișiere de pe computerul țintă.



Troieni: aceste programe se prezintă sub forma unor programe legitime, care, în realitate, sunt create cu scopul de a fura date confidențiale, sau de a permite unor utilizatori sau programe neautorizate accesul la sistemul infectat.



Securitatea aplicatiilor

Soluțiile software de securitate a sistemelor sunt instrumente cu rol în detectarea și eliminarea virușilor, lucrând activ la îmbunătățirea principiilor de apărare a computerelor. Cele mai importante module ale sistemelor de securitate sunt cele de scanare, diagnosticare și protejare împotriva programelor de tip spion, viruși, cai troieni sau multe altele.



Securitatea in rețelele Wi-Fi

Majoritatea utilizatorilor de internet folosesc conexiunea Wi-Fi , cu ajutorul unui laptop, telefon, etc. și în multe cazuri dacă aceste rețele nu sunt securizate oricine se poate conecta fără probleme

Obs: ar trebui să schimbați parola de acces pentru configurarea echipamentului cu una cât mai solidă, care să conțină minim 8 caractere, caractere speciale :\$#*&, cifre, litere mari și mici. Anumite echipamente Wi-Fi oferă posibilitatea administrării via wireless și cel mai bine ar fi să blocați acest feature pentru o securitate mai ridicată. securizat – fără parolă de acces).

Un alt sfat pentru o securitate mai bună a echipamentului Wi-Fi, ar fi poziționarea acestuia în casă cât mai central, cât mai departe de fereastră ca să nu poată fi accesat din exterior (semnalul să fie cât mai slab, sau inexistent)

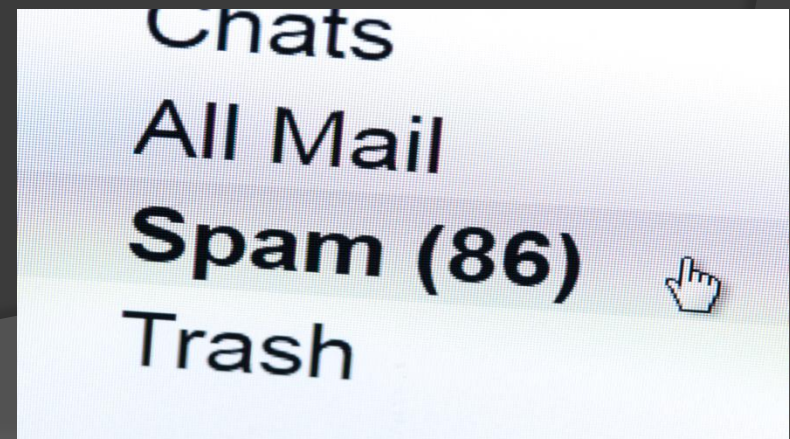
A logo with the text "FREE WiFi" in a bold, teal, sans-serif font. To the right of the word "FREE" is a green Wi-Fi signal icon consisting of three curved lines. The entire logo is enclosed in a thin teal rectangular border.

FREE
WiFi



SPAM

Spam: mesaje electronice nesolicitate, de cele mai multe ori cu caracter comercial, de publicitate pentru produse și servicii dubioase, folosite de industria emarketingului și de proprietarii de site-uri cu un conținut indecent. Mesajele spam sunt trimise cu ajutorul unor calculatoare infectate cu troieni, care fac parte dintrun botnet. Mesajele spam, deși nu sunt un program malițios în sine, pot include atașamente care conțin astfel de programe, sau trimit utilizatorii către pagini de internet periculoase pentru siguranța sistemului.



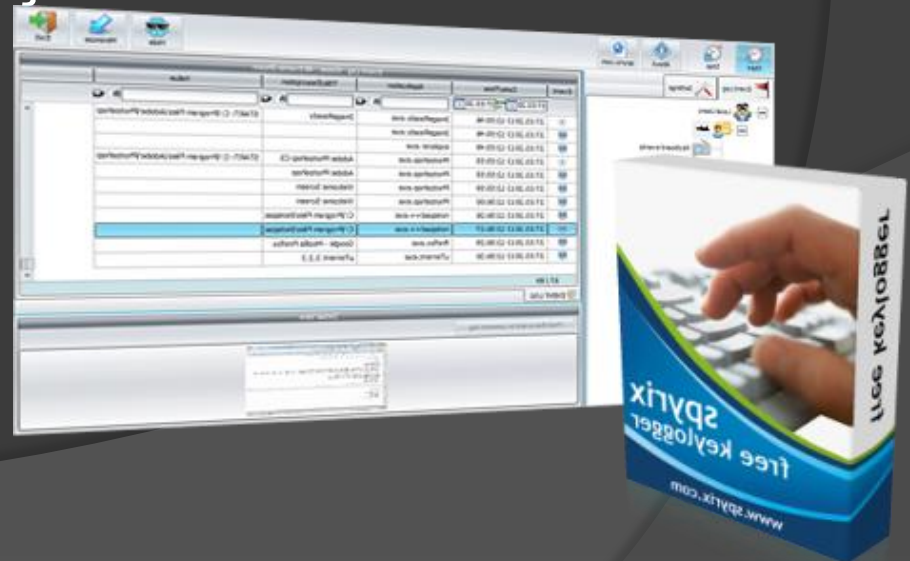
Spyware

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



Keyloggers

Un keylogger este un program care înregistrează fiecare bătaie de tastă pe o tastatură și salvează aceste date într-un fișier. După ce colectează o anumită cantitate de date, le va transfera prin intermediul internetului unei gazde de la distanță, predeterminată. De asemenea, poate captura capturi de ecran și utiliza alte tehnici pentru a urmări activitatea utilizatorului. Un keylogger poate cauza pierderea parolelor, date de autentificare, și alte informații similare.

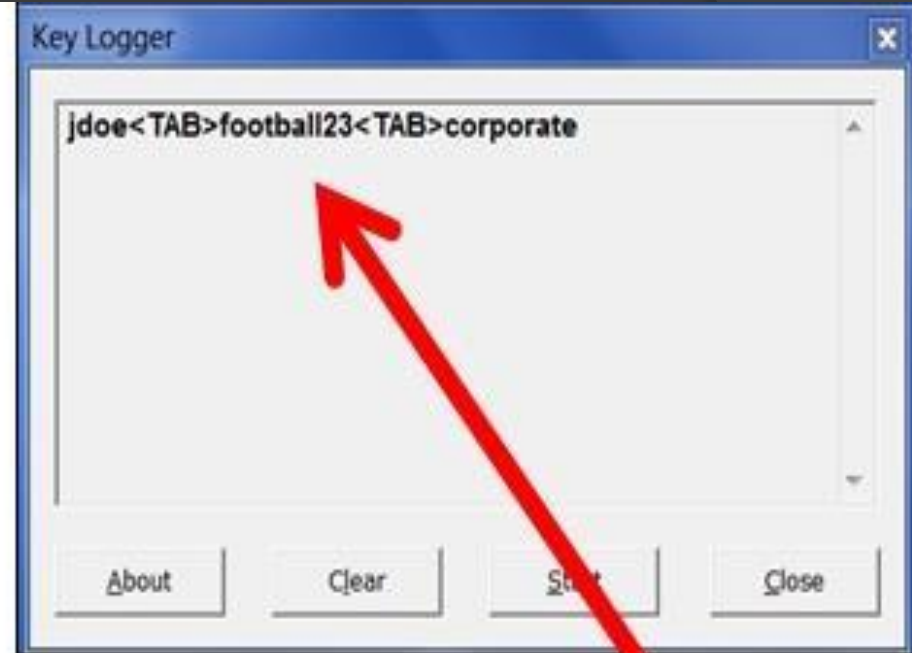


Keyloggers

Există două tipuri de keyloggeri: hardware și software. Keyloggerul de tip hardware este un dispozitiv fizic, mic care poate fi lăsat între cablul tastaturii și portul tastaturii din calculator. Un keylogger de tip hardware poate înregistra toate apăsările de pe tastatură și le salvează în propria memorie. Un astfel de dispozitiv nu se bazează pe un anumit software sau driver. Prin urmare, poate funcționa în diferite medii. Totuși, nu poate obține capturi de ecran și poate fi descoperit cu ușurință la inspectarea calculatorului. Keyloggerii de tip software sunt împărțiți în aplicații legitime și paraziți.



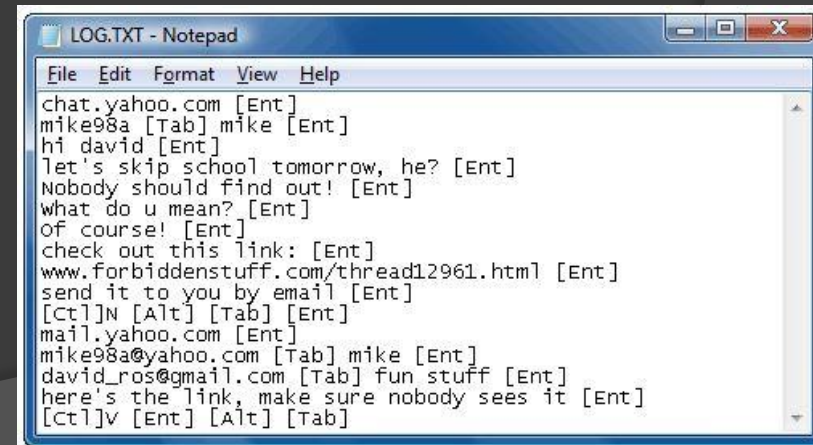
Keyloggers



**Image above shows Keylogger
Stealing VPN credentials**

Keyloggers

Keyloggerii malițioși sunt similari virușilor și troianilor. Aceștia sunt utilizați de către hackeri pentru a viola intimitatea utilizatorului. Keyloggerii legitimi, cunoscuți și ca unelte de monitorizare a calculatorului, sunt produse comerciale vizate în mod special de către părinți, angajatori și profesori. Aceștia permit să descopere ce fac online copiii și angajații. Totuși, chiar și programele legale lucrează fără știrea sau aprobarea utilizatorului. Acestea pot fi utilizate de către persoane malițioase și, prin urmare, nu sunt clasificate ca și mai puțin dăunătoare decât anumiți paraziți.



```
LOG.TXT - Notepad
File Edit Format View Help
chat.yahoo.com [Ent]
mike98a [Tab] mike [Ent]
hi david [Ent]
let's skip school tomorrow, he? [Ent]
Nobody should find out! [Ent]
what do u mean? [Ent]
of course! [Ent]
check out this link: [Ent]
www.forbiddenstuff.com/thread12961.htm [Ent]
send it to you by email [Ent]
[Ctrl]N [Alt] [Tab] [Ent]
mail.yahoo.com [Ent]
mike98a@yahoo.com [Tab] mike [Ent]
david_ros@gmail.com [Tab] fun stuff [Ent]
here's the link, make sure nobody sees it [Ent]
[Ctrl]V [Ent] [Alt] [Tab]
```

Reguli de securitate în cadrul rețelelor sociale

- Alegeți o parolă pentru contul dumneavoastră care să nu fie ușor de ghicit de către un alt utilizator sau program. În acest sens, evitați parolele generice, precum "123456789" sau "parola" sau o parolă identică cu numele de utilizator;
- Asigurați-vă că știți pe cine urmăriți și pe cine adăugați drept prieten;
- Evitați să accesați link-urile împărtășite de către alți utilizatori;
- Evitați să faceți publice informații personale, precum ziua de naștere, adresa de email sau adresa fizică;

Reguli de securitate în cadrul rețelelor sociale

- ⦿ Atunci când împărtășiți poze, asigurați-vă că o faceți doar cu persoanele cunoscute
- ⦿ Nu dezvăluiți niciodată informații referitoare la perioadele în care părăsiți locuința (mesaje precum: "plec la mare tot weekend-ul; "sunt singur acasă" trebuie evitate) ;
- ⦿ Utilizați o soluție de securitate specializată, care să scaneze mesajele și comentariile, și care să verifice nivelul de securitate al informațiilor confidențiale;

Phishing prin email

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

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.

Phishing prin email

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.

A golden fishing hook is positioned at the top center, with a small, irregularly torn piece of white paper hanging from its point. The paper has a rough, deckled edge. On the paper, there are two horizontal rectangular boxes for text input. The first box is preceded by the text 'USERNAME:' and the second box is preceded by 'PASSWORD:'. The entire scene is set against a solid, vibrant blue background.

USERNAME:

PASSWORD: