SECURITATEA CIBERNETICA

STOP – THINK - CONNECT

CUPRINS

OBIECTIVELE PROIECTULUI

Dupa studierea acestei prezentari, veti fi capabili:

- Sa recunoasteti un calculator virusat
- Sa instalati protectia antivirus
- Sa recunoasteti tipurile de programe maltioase
- Sa va protejati de fenomenul cyber-bullying
- Sa determinati modul de securizare a informatiilor si aplicatiilor software

BENEFICIILE SI RISCURILE NAVIGARII PE INTERNET

Beneficii. Internetul oferă:

- Informatii din toate domeniile (politica, administrație, sport, agricultură, vreme, informații juridice etc) prezentate sub tot felul de forme: știri, articole, imagini, videoclipuri etc.
- Comunicare rapidă cu oameni de oriunde de pe glob prin: mail, site-uri de socializare, messenger, skype etc;
- Acces la cursuri online, și alte informații/documente utile în pregătirea profesională și carieră
- Căutarea şi găsirea unui serviciu
- Posibilitatea de a lucra de acasă
- Comerț electronic – posibilitatea de a găsi și cumpăra sau comercializa produse
- Posibilitatea de a da anunturi referitoare la orice: cumpărări-vânzări, matrimoniale, evenimente, proteste etc
- Economie de timp

Riscurile navigării pe internet:

- Calitatea si veridicitatea informațiilor de pe internet este nesigura. Pentru că oricine are acces la internet, oricine poate posta informații pe internet, oricine poate spune neadevăruri, poate dezinforma, sau poate minți pe internet.
- Informatiile personale nu sunt in siguranța când folosim internetul. Această securitate a datelor personale pe care o promovează site-urile ce oferă de exemplu căsuță de mail, este falsă.
- Toate informațiile de pe mail sau din orice alte conturi online, toate parolele noastre, toate “mișcările” noastre pe internet sunt stocate si accesibile celor care oferă serviciile respective.
- Identitatea virtuală ce nu coincide cu cea reala. Atunci când vorbești cu cineva pe internet, indiferent în ce domeniu, habar nu ai cine este de fapt, ce fel de om este, cât de corect, cât adevăr spune sau cât minte.

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.**

CUM RECUNOASTEM UN CALCULATOR VIRUSAT

Cele mai raspandite semne de infectare :

- "Calculatorul 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.
- “Calculatorul meu functioneaza extrem de incet“ - acesta poate fi un simptom al infectarii cu un virus, vierme sau troian, care poate consuma resursele calculatorului, facandu-l sa functioneze mai greu decat de obicei.
- “Am aplicatii care nu pornesc” – simptom care va spune ca ceva nu este in regula.
- “Nu ma pot conecta la Internet“ – 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.
- “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.

- “Unde au disparut fisierele mele?“ - anumite atacuri sunt concepute special pentru criptarea sau stergerea anumitor fisiere si chiar mutarea documentelor dintr-un loc in altul.
- “Antivirusul meu a disparut, firewall-ul este dezactivat” – o actiune tipica a amenintarilor este dezactivarea sistemelor de securitate instalate pe calculator.
- “Calculatorul 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.
- “Calculatorul meu, practic, a innebunit” – daca calculatorul incepe sa actioneze singur sau sa trimita email-uri fara sa stiti, iar aplicatii sau ferestre de Internet se deschid singure, atunci sistemul ar putea fi compromis.

PROTECTIE ANTIVIRUS


Bitdefender
TOTAL SECURITY 2017
Avast
Internet Security
NITRO
Kaspersky
Internet Security
2018

CUM SA TE FERESTI DE VIRUSI, VIERMI, TROIENI

Virușii:

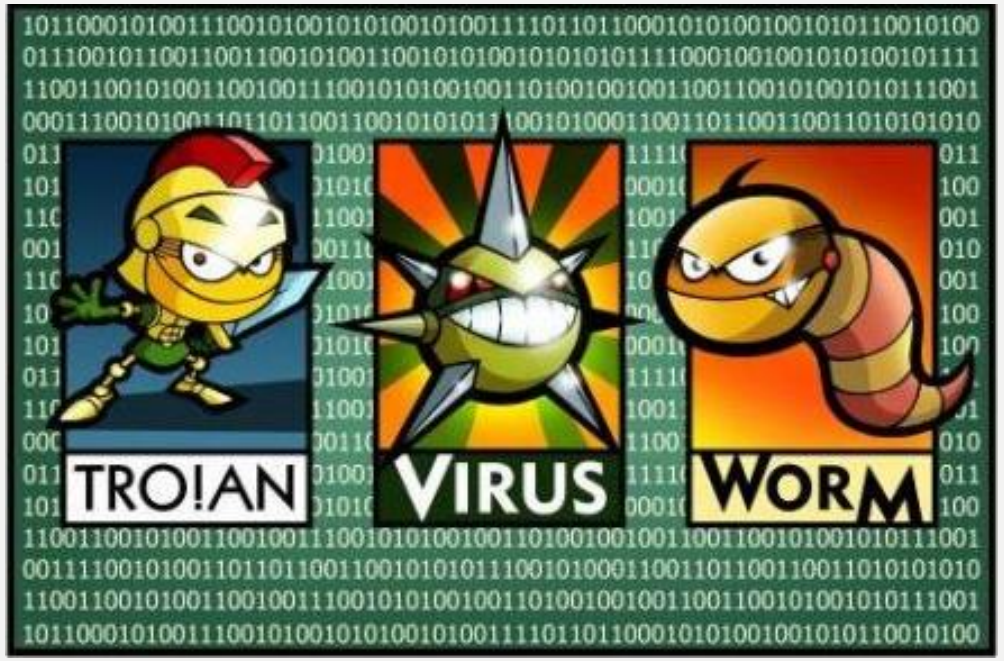
programe care se autocopiază pe sistemul compromis, fără știrea utilizatorului. Virusul va infecta astfel componentele sistemului de operare sau alte programe informatice.

Viermi:
programe care se pot auto-replica. Acestia 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.

Troieni:
programe ce 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.

În ceea ce privește securitatea calculatorului dumneavoastră, aveți în vedere următorii pași:

- 1. Verificați-vă calculatorul de infecții.
- 2. Instalați pachetele de servicii disponibile și actualizările de securitate pentru sistemul dumneavoastră. Activați actualizările automate.
- 3. Verificați regulat browser-ul de internet și plugin-urile încorporate (ex: Java, Flash, Shockwave, Quicktime).
- 4. Instalați un program antivirus și actualizați-l în mod regulat.
- 5. Folosiți un firewall, de exemplu Windows Firewall sau un router.



COOKIE-URILE

*__Cookie-urile__ sunt fișiere care stochează informații despre tine, browser-ul tău web și comportamentul tău pe internet. Ele sunt fișiere foarte mici păstrate pe dispozitivul tău, ce pot fi folosite de site-urile sau de aplicațiile web pentru a ajusta experiența ta online.

Ce fac cookie-urile?

- Un cookie este creat și interpretat de către expeditor, în timp ce destinatarul doar îl păstrează și îl trimite înapoi dacă expeditorul cere asta.
- Atunci când navighezi pe internet, expeditorul este serverul care găzduiește un site web și destinatarul este browser-ul web care vizitează acel site. Scopul lor este de a identifica utilizatorul, de a verifica activitatea lui din trecut pe acel site și de a oferi conținut specific bazându-se pe aceste date.

Cookie-urile conțin doar date, nu și instrucțiuni executabile: ele nu pot să șteargă sau să citească nimic de pe PC-ul utilizatorului. Totuși, ele permit detectarea paginilor vizitate de un utilizator pe unul sau mai multe site-uri.

HĂRȚUIREA ONLINE

Hartuirea se manifesta prin:

- **bârfa:** emiterea în mediul online a unor declarații speculative referitoare la o anumită persoană;
- **hărțuirea:** luarea în batjocură constant și deliberat o persoană, prin postarea de mesaje publice, poze ce pot afecta integritatea psihică a individului;
- **urmărirea online:** hărțuirea intimidantă cu scopul de a aduce conflictul și în viața reală (ex: de a solicita întrevederi în viața reală prin amenințare cu violență fizică);
- **trolling:** provocarea unor persoane să acționeze agresiv, prin insultarea implicită;
- **comentarii:** postarea de răspunsuri negative, denigrante la adresa unor persoane, la adresa unor fotografii, clipuri video sau mesaje lansate de o anumită persoană;
- **profiluri false:** crearea unor profiluri false de catre agresorii pe internet, ce împrumută identitatea altor persoane pentru a facilita comunicarea cu victimele lor;
- **sexting:** distribuirea de materiale pornografice minorilor, utilizând mijloacele electronice de comunicație.

"Cyber bullying-ul implică utilizarea tehnologiilor informaționale și comunicaționale pentru a sprijini un comportament deliberat, repetat și ostil desfășurat de către un individ sau grup, care este destinat să aducă prejudicii altor persoane".

Ce putem face pentru a opri un asemenea comportament?

1. Dacă hărțuirea se realizează pe o rețea de socializare (facebook, odnoklassniki, instagram, twitter etc.), trebuie să cunoașteți că :

- platformele au opțiuni de a raporta comentariile abuzive, hărțuirea sau spamul, ce pot duce la închiderea contului de pe care sunteți hărțuit.
- vă puteți seta contul în așa fel încât să fie mai puțin accesibil persoanelor cu care nu sunteți “prieteni”.

2. Dacă hărțuirea se realizează prin comentarii defăimătoare pe anumite site-uri sau bloguri, trebuie:

- să notificați proprietarul site-ului prin a solicita ștergerea informației care vă defăimează.
- să apelați la organele competente: poliție, procuratură, instanța de judecată.
- să apelați la un avocat sau un consultant juridic care să vă ajute să identificați și să elaborați o strategie de apărare, reieșind din circumstanțele particulare ale cazului dvs.

CUM ÎȚI CONSTRUIEȘTI REPUTATIA ONLINE

SPAM-URILE

*Spam-urile - mesajele nesolicitate trimise unui utilizator de servicii de mesagerie electronică (poşta electronică) sau de telefonie mobilă – în acest caz : spam prin SMS.

*Spam-ul este acel mesaj al cărui expeditor nu se regăseşte în lista de contacte (sau de cunoştinţe) a destinatarului, prin care are loc utilizarea abuzivă a serviciilor de poştă electronică în scopuri publicitare sau de inducere în eroare (înşelare) a destinatarului.

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.

Cum se pot feri utilizatorii de mesajele spam?

- Utilizatorii trebuie sa aiba un produs de Securitate complet, care sa contina si modulul Antispam. In lipsa lui, utilizatorul nu va fi niciodata protejat 100%.

CARE SUNT PRINCIPALELE CANALE DE RASPÂNDIRE A MESAJELOR DE TIP SPAM?

Spamurile se gasesc:

- pe e-mail, pentru ca majoritatea oamenilor detin o adresa de e-mail, folosita fie in scop professional, fie personal
- sub forma de comentarii la diverse bloguri (cu cat au o mai mare vizibilitate cu atat vor fi si mai mult targetate)
- sub forma de mesaje pe forumuri
- pe retelele sociale
- prin SMS - este dificil de detectat, pentru ca este foarte variat si localizat.

CARE SUNT PERICOLELE LA CARE SUNT EXPUSI UTILIZATORII CÂND DESCHID ASTFEL DE MESAJE? CELE MAI IMPORTANTE PERICOLE

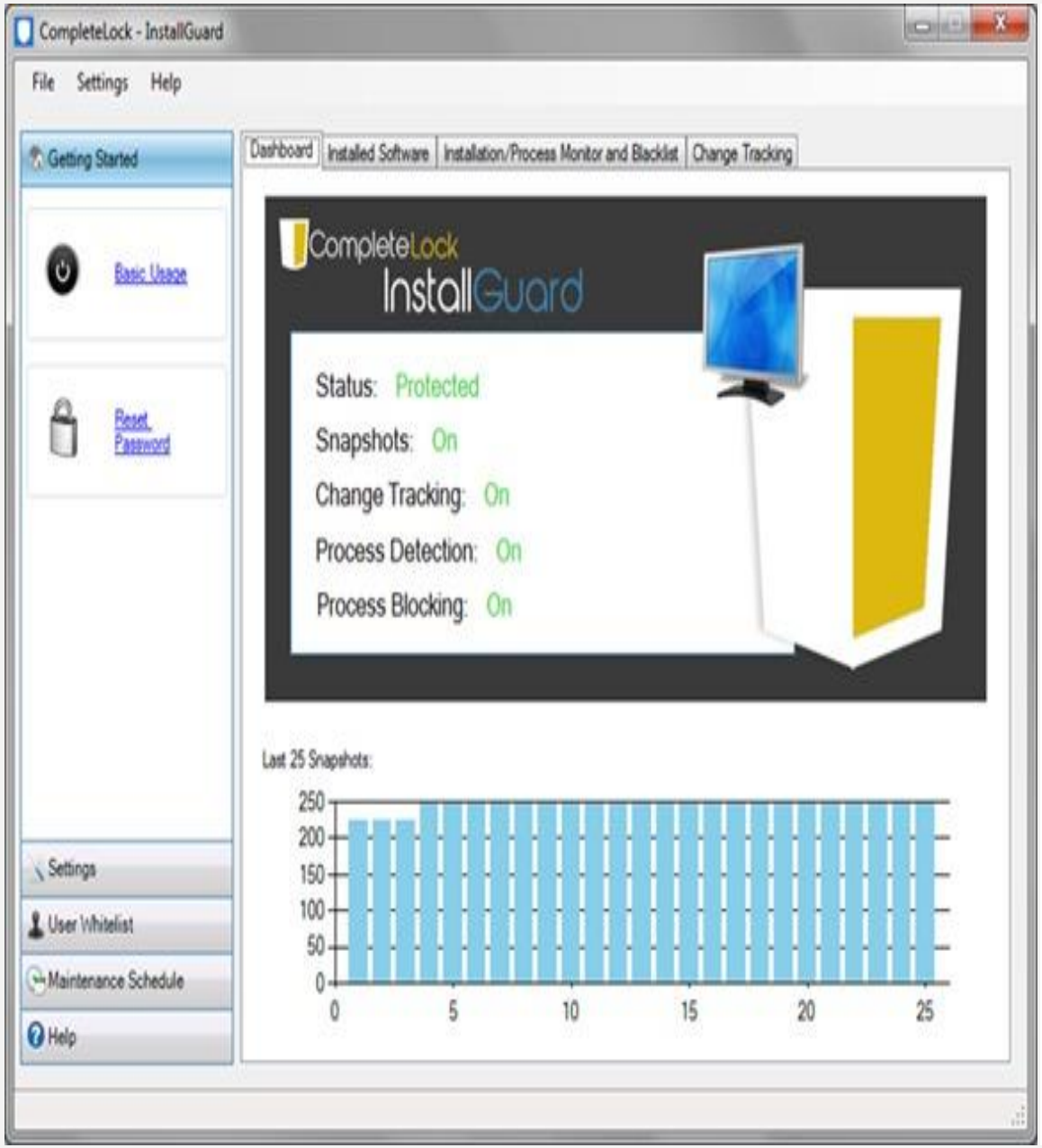
- Mesajele de tip phishing - pot fi extrem de daunatoare, pentru ca ele pretind a veni din partea unei institutii(uneori bancare, uneori nu) si de vreme ce mesajele de acest tip inca exista (si chiar creste numarul lor) inseamna ca sunt suficient de multe victime pentru ca afacerea sa aiba succes.
- Infectarea calculatorului prin deschiderea unui link periculos dintr-un spam, prin download-ul si rularea unui executabil, prin deschiderea unui eventual atasament infectat etc. Dupa infectarea calculatorului, pericolele pot sa capete forme variate in functie de tipul de malware cu care s-a infectat

SECURITATEA INFORMATIEI

- **Securitatea informației** se ocupă cu protejarea informației și sistemelor informatice, de accesul neautorizat, folosirea, dezvăluirea, întreruperea, modificarea sau distrugerea lor. ISO/**IEC27002/2013** tratează securitatea informațiilor prin cele trei componente principale: confidențialitatea, integritatea și disponibilitatea.
- Confidențialitatea este asigurată prin criptarea informației. Integritatea se obține prin mecanisme și algoritmi de dispersie. Disponibilitatea se asigură prin întărirea securității rețelei sau rețelelor de sisteme informatice și asigurarea de copii de siguranță.

SECURITATEA APLICATIILOR (SOFTWARE)

- Echipa noastră globală care se ocupă de securitatea software-ului depune mari eforturi pentru a proteja activele informaționale, serviciile și produsele Sony Mobile, precum și confidențialitatea informațiilor clienților. Dar suntem întotdeauna dornici de mai mult ajutor. Recunoaștem rolul important pe care comunitatea de cercetare îl joacă în consolidarea poziției noastre privind securitatea și salutăm oportunitatea de a colabora cu comunitatea respectivă.
- Programul Sony Mobile privind securitatea software-ului acceptă raportarea de erori care-i asigură unui potențial atacator capacitatea să compromită integritatea, disponibilitatea sau confidențialitatea produselor, a serviciilor sau a infrastructurii IT a Sony Mobile și care respectă **instrucțiunile noastre de remitere.**. În cazul în care considerați că ați descoperit o vulnerabilitate validă privind securitatea într-un produs sau site Web Sony Mobile, dorim să ne aduceți la cunoștință acest lucru.
- Dacă doriți să remiteți o vulnerabilitate, vizitați adresa **https://hackerone.com/sony.** Veți fi redirecționat la un site terț unde veți găsi mai multe informații privind instrucțiunile de remitere și veți putea remite un raport. Ne vom strădui să investigăm cu promptitudine informațiile primite.
- **Alte tipuri de asistență**
- Dacă întâmpinați dificultăți care nu au legătură cu securitatea software-ului, de exemplu, la descărcarea și instalarea de actualizări, sau dacă aveți nevoie de asistență suplimentară pentru telefon, contactați **asistența Sony Mobile.**
- 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.


CompleteLock - InstallGuard
File
Settings
Help
Getting Started
Basic Usage
Reset Password
Settings
User Whitelist
Maintenance Schedule
Help
Dashboard
Installed Software
Installation/Process Monitor and Blacklist
Change Tracking
CompleteLock
InstallGuard
Status: Protected
Snapshots: On
Change Tracking: On
Process Detection: On
Process Blocking: On
Last 25 Snapshots:
250
200
150
100
50
0
0
5
10
15
20
25


my Social Security
MESSAGE CENTER
SECURE CONNECTION TO SSA
INCREASED CONVENIENCE
DECREASED WAIT TIME
CHAT
TALK
VIDEO
SECURE MESSAGES

SPYWARE

* Spyware: o categorie de software malițios, atașate de obicei la programe gratuite (jocuri, programe de schimbat fișiere, programe de video chat etc.), care captează pe ascuns date de marketing (prin analiza site-urilor 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.
*În general, chiar după ștergerea programelor gratuite care au instalat programul spion, acesta rămâne în continuare activ. Există și numeroase programe anti-spion, dar atenție: unele dintre ele sunt false antispyware - inducând utilizatorul în eroare deoarece ele însele conțin programe spion mascate.
*Pentru înlăturarea programelor spion sunt folosite programele antispyware

Keyloggers

* Keyloggers: troieni care ruleaza in background si inregistreaza tot ceea ce se introduce de la tastatura, permitand unui utilizator extern sa aiba acces la continutul introdus. In majoritatea cazurilor este vorba despre conturi de e-mail si parole, conturi de instant messenger, carduri de credit, parole de la domeniul personal s.a.m.d.

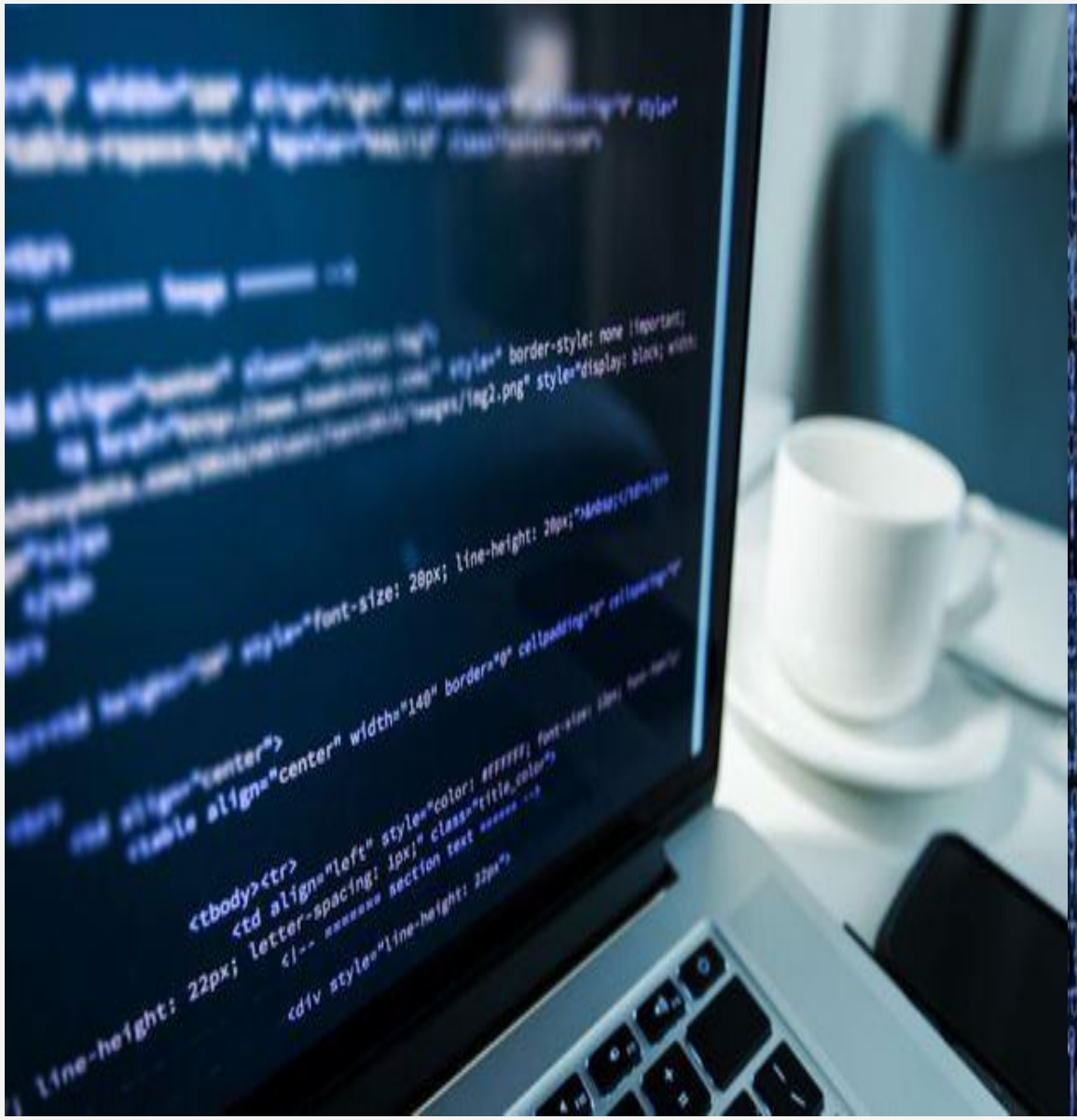
- Cum se detecteaza?

Cea mai simplă modalitate de a detecta orice software nedorit este să te uiți în Managerul de activități pentru a verifica procesele care rulează.

- Cum ne putem proteja de aceste programe „rau facatoare”?

Antrivirusi cu licenta sau versiuni open source actualizate la timp, un firewall cu licenta sau open source la fel cu update-urile la zi. Acest lucru va scadea rata dumneavoastra de infectare cu pana la 90% .

SECURITATEA IN REŢELELE WI-FI



COMUNICAREA PE REȚELE DE SOCIALIZARE

AVANTAJE

- Procesul de comunicare virtuala este avantajos in cazul persoanelor care se cunosc in lumea reala,intrucat nu ofera vreun risc.
- Poti comunica cu rude si prieteni ce se afla la o mare distanta
- Iti poti crea noi prietenii si relatii care ti-ar oferi noi oportunitati.
- Costurile comunicarii sunt mult reduse, singura plata fiind abonamentul la internet.
- Singur decizi daca vrei o astfel de comunicare virtuala.
- Singur alegi cu cine discuti si cat discuti

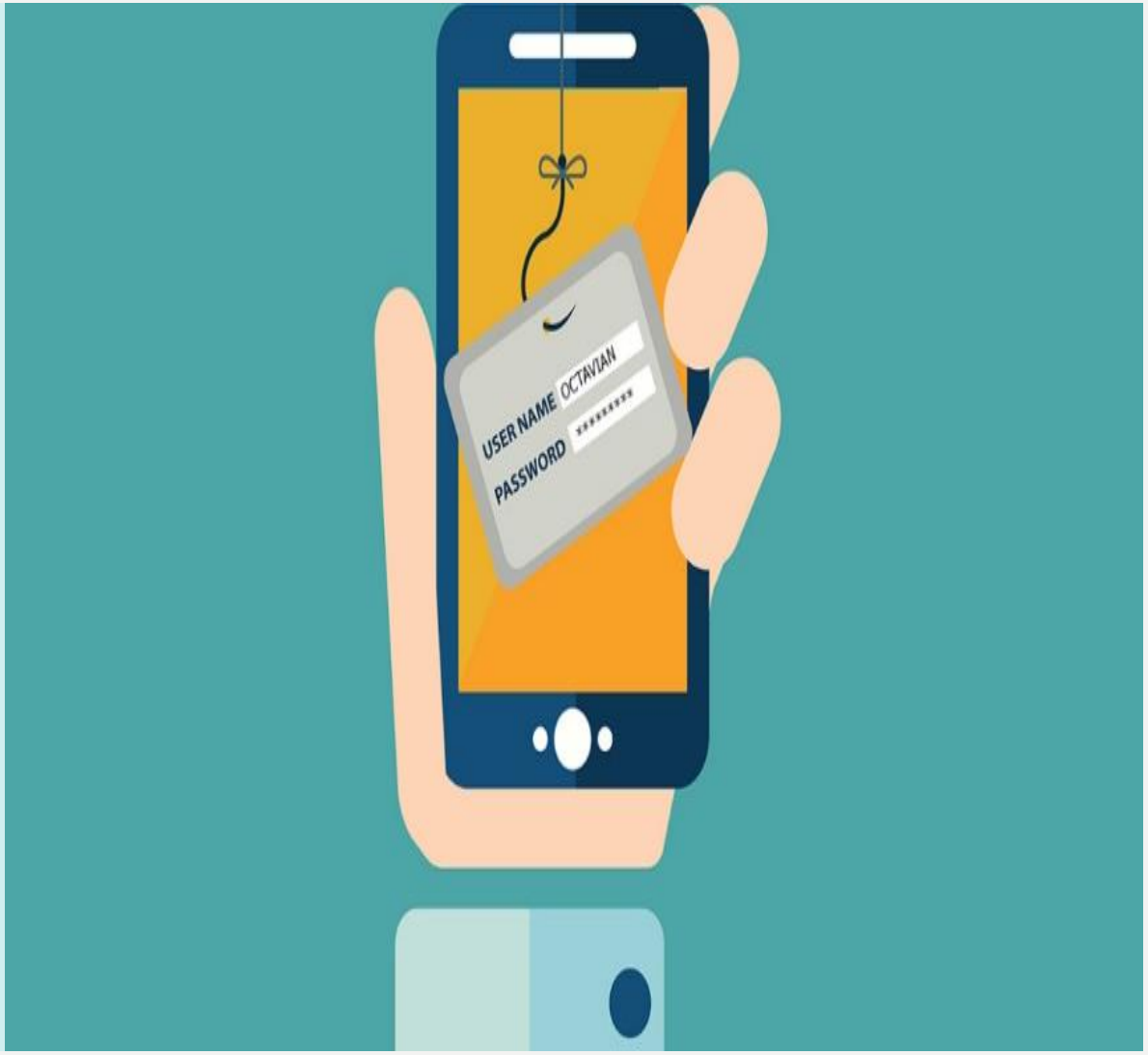
DEZAVANTAJE

- Nu 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 (ex. zambetul, privirea, tonul vocii).
- Poti fi tradat, in cazul in care ai prea multa incredere in prietenul cu care ai o comunicare virtuala.

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. 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 e-mail sau adresa domiciliului;
- 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;

CE ESTE PHISHINGUL?



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.

Va multumim pentru atentie!