



**SAFER  
INTERNET  
DAY**



# ZIUA EUROPEANĂ A SIGURANȚEI PE INTERNET

8 februarie 2017

cyberbullying

virusi

spamming

cal troian

hackeri

plagiarism

hărțuire

crackeri

rootkits

tranzacții  
online

terorism  
emoțional

phishing

jocuri  
agresive

furt de identitate

cookie-uri

Identitatea digitală





# Fii sigur on line!



Nu publica date personale: data nașterii, adresa, numele sau numărul de telefon - nici pe ale tale, nici pe ale apropiaților sau prietenilor tăi.



Parola: o știi doar tu, o schimbi frecvent, o restabilești cu ajutorul e-mail-ului sau telefonului mobil. Alege parole sigure. Deloghează-te de pe cont, revenind la pagina de start, în deosebi când folosești un calculator public.



Setează parametrii de confidențialitate, pentru a te asigura că informațiile și fotografiile postate sînt văzute doar de prieteni și persoane de încredere.



Nu accepta cereri de prietenie de la persoane pe care nu le cunoști în viața reală, decît dacă ți-au fost recomandate de persoane de încredere.



Nu pune like sau distribui mesaje/imagini/video/postări vulgare și nu plasa poze sau video cu tine sau prietenii tăi în ipostaze indecente. Nu replica la un mesaj menit să te hărțuiască, ci blochează-l pe cel care l-a trimis.



Raportează conținutul abuziv - evenimente nepotrivite, pagini, grupuri, precum și profiluri false. Raportarea este confidențială.

# „DOWNLOAD”, „COPY PASTE” și DREPTURILE DE AUTOR sau PLAGIARISMUL



**Pirateria software**, sancționată de legislație, presupune copierea și transmiterea neautorizată (fizică sau digitală) a lucrărilor protejate prin drepturile de autor ori a programelor software, cu sau fără scopuri comerciale, pe calculatorul personal sau pe cel utilizat la locul de muncă, sunt considerate infracțiuni și se pedepsește conform legii.

## Download

**Legal** (documentele oficiale aflate pe siteurile autorităților ori instituțiilor private, documentele, programele și jocurile educaționale gratuite - freeware, cum ar fi, softul de navigare Google Chrome, secvențe video ori audio de pe site-uri specializate – Youtube, documentele aflate pe website-urile școlilor etc.);

**Illegal**, atunci când este vorba de operele de creație (cărți, filme, muzică, software etc.) protejate prin drepturile de autor și care sunt copiate, utilizate sau distribuite fără autorizație (*piraterie*). În acest caz, de regulă, sunt folosite programe de partajare de fișiere de tipul **peer to peer** (*de la egal la egal*, prescurtat *P2P*) care permit realizarea unei conexiuni directe între două sisteme de calcul fără a fi necesar un server central.

„**copy paste**” sau **plagiatul** electronic. Este o practică folosită în ziua de astăzi de către persoanele de toate vârstele. Vina n-o poartă tehnologia, însă, de vreme ce conținutul digital poate fi reprodus cu atît de multă ușurință, tentația este foarte puternică. Pentru a evita problemele și pentru a încuraja publicul să folosească sursele de informații cu discernămint și respect pentru drepturilor de autor, trebuie să ne asigurăm că ei înțeleg diferența dintre „citare” și „copiere” și că știu să folosească regulile de citare.

## SFATURI DE SECURITATE WIRELESS:

- evitarea conectării la Wi-Fi publice, întrucât există hackeri care clonează locații de tip free Wi-Fi și accesează datele personale;
- folosirea, de către firme, a conexiunii de tip VPN (Virtual Private Network), prin care datele transmise sunt criptate;
- folosirea permanentă a firewall-ului, pentru a preveni eventuale intruziuni;
- accesarea de site-uri și servicii web care nu necesită date personale sau parole de acces personal.



## EFECTELE INFECTĂRII UNUI CALCULATOR:

- dezactivarea computerului;
- adăugarea, modificarea sau ștergerea unor fișiere;
- formatarea hard-diskului;
- furtul de informații (precum adresele de email) din computerul nostru pentru a trimite viruși prietenilor, colegilor tăi;
- trimiterea de mesaje spam către contactele noastre;





## REȚINE!

**Cyberbullying** - Diferite forme de abuz psihologic comis prin acte de hărțuire transmise prin tehnologiile de informare și comunicare, cum ar fi Internetul, telefonul mobil sau rețelele de tip wireless ori bluetooth;

**Cai troieni** – nu sunt viruși, ei sunt programe spion care, sub aparența utilității lor, realizează funcții malefice care permit accesarea neautorizată a unui calculator, respectiv copierea fișierelor și chiar controlarea comenzilor calculatorului;

**Crackerii** – creează programe care scanează porturile calculatoarelor pentru a verifica dacă sunt accesibile. În cazul în care calculatorul nostru apare pe una dintre aceste verificări, crackerul ar putea să decidă să intre în sistemul nostru informatic;

**Phishing** - bazat pe un tip de fraudă electronică, acest sistem constă, de exemplu, în trimiterea de emailuri prin care utilizatorului i se cere să introducă date personale pentru a se putea bucura în continuare de anumite servicii;

**Vierme informatic** este un program de calculator care se poate auto-replica. Acesta folosește 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.

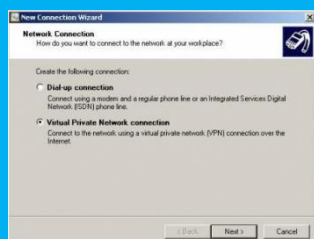
**Rootkit** - permite ca un intrus să ne acceseze sistemul și să preia controlul acestuia fără a putea fi detectat de metodele obișnuite de protecție, cum ar fi antivirusul. În una dintre cele mai întâlnite situații, rootkit-urile sunt folosite pentru a lansa mesaje spam în masă sau pentru a ataca alte computere sau rețele. O altă utilizare a rootkit-urilor este de a ascunde troieni, astfel încât să poată fi extrase informații din computer.

# 10 sfaturi pentru utilizarea în siguranța a internetului:



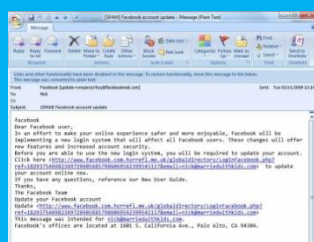
## 1. Utilizează motoarele de căutare care nu colectează date;

DuckDuckGo, singurul motor de căutare ce garantează siguranța utilizatorilor împotriva colectării datelor.



## 2. Folosește un serviciu VPN

Cele mai multe servicii VPN de calitate nu sunt gratuite, dar îți oferă o conexiune sigură la internet care previne colectarea informațiilor despre tine de către site-urile vizitate, dar și de către furnizorul de internet.



## 3. Vizualizează email-ul ca text

Elimina complet amenințările malware din email, ce se pot strecura și în poze, vizualizând toate mesajele email ca text.



## 4. Utilizează o adresă de mail secundară

Cele mai multe servicii online necesită o adresă de email, motiv pentru care este important să ai cel puțin două adrese de poșta electronică.



## 5. Dublează-ți siguranța cu un sistem de verificare în două etape - te vei conecta parola și un cod care îți va fi trimis pe telefon.



## 6. Limitează-ți tranzacțiile online

## 7. Nu lăsa computerul conectat la rețea când nu îl folosești

## 8. Gestionează-ți datele din contul Google

## 9. Ține "curioșii" la distanță de dispozitivul tău



## 10. Raportează conținutul deranjant sau spam;

<http://www.siguronline.md/rom/cum-sa-raportez#raport>



**Helpline**  
Cere un sfat!

Poți cere un sfat accesând:  
<http://helpline.sigur.info/>

Mai multe informații, despre siguranța on-line,  
sînt disponibile pe: [www.siguronline.md](http://www.siguronline.md)

