# Securitatea cibernetică

**Au elaborat: Gorgan Bogdan**
**Bondari Sofia**

**Chișinău 2018**

# Ce este internetul?

Prin Internet se înţelege o reţea globală, compusă din sisteme de calculatoare interconectate şi servicii computerizate, care permite utilizatorului, indiferent de locaţia sa geografică, să acceseze informaţia aflată oriunde în reţea.

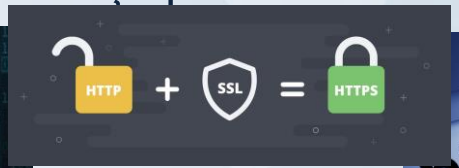
# REGULI PENTRU O NAVIGARE MAI SIGURĂ

✓ având în vedere că cele mai multe aplicaţii maliţioase afectează Microsoft Internet Explorer (utilizat de peste 50% dintre utilizatori), orientează-te şi spre alte tipuri de browser (ex. Google Chrome, Opera, Firefox, Safari etc.), mai ales când accesezi pagini web posibil nesigure;

✓ verifică secţiunea de contact a site-urilor web (adresă, număr de telefon, e-mail);

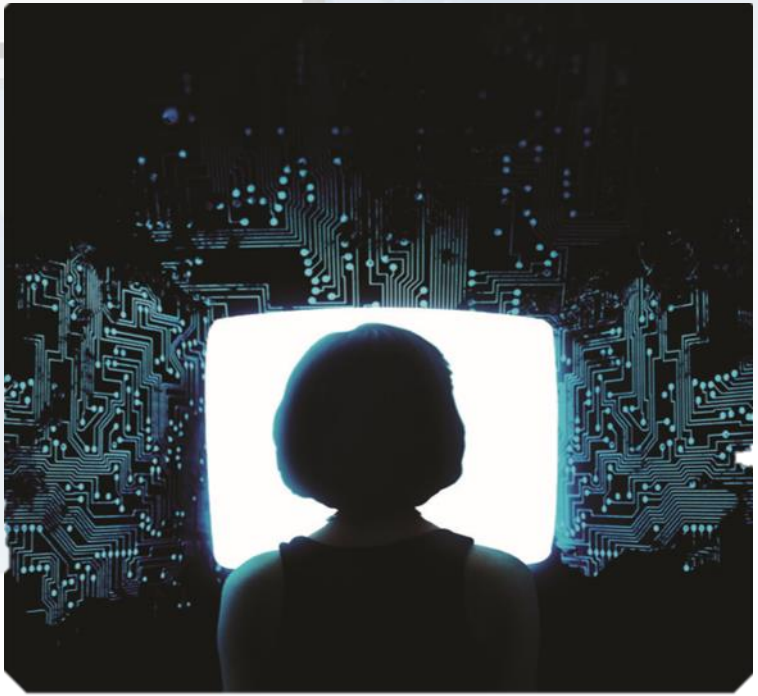
✓ nu apăsa pe link-urile din cadrul ferestrelor de tip pop-up;

✓ verifică existenţa „https://” în partea de început a adresei web, înainte de a introduce informaţii personale.




# DEZINSTALEZI APLICAȚIILE DE CARE NU MAI AI NEVOIE?

Daca nu mai ai nevoie de un anumit soft, dezinstalează-l! Astfel, vor fi mai uşor de urmărit aplicaţiile care necesită a fi actualizate, iar de multe ori acest lucru va permite o executare rapidă a sarcinilor de către calculator (sunt frecvente aplicaţiile de mici dimensiuni şi add-on-urile care se instalează împreună cu diverse softuri şi care pornesc odată cu computerul, ocupând memoria acestuia şi afectându-i performanţele).



Un element important în configuraţia de securitate cibernetică este **antivirusul**. Acesta este un program informatic conceput să detecteze, să prevină şi să elimine instalarea oricăror forme de malware (viruşi, troieni, adware, spyware etc.) pe sistemele de calcul. Actualizarea acestuia este deosebit de importantă pentru a putea face faţă celor mai noi (versiuni ale unor) programe maliţioase.


Un exemplu de malware este **troianul** (trojan horse), a cărui denumire provine din mitologia greacă. Acest tip de program pare a avea o funcţie utilă, legitimă, dar deţine şi una ascunsă, potenţial maliţioasă, care scapă mecanismelor de securitate, uneori exploatând vulnerabilităţi ale sistemelor vizate. Astfel, odată rulat, programul poate iniţia activităţi maliţioase, precum sustragerea de informaţii, afectarea calculatorului gazdă sau crearea unor căi disimulate de acces de la distanţă la sistemul infectat.

# ALTE EXEMPLE DE PROGRAME MALIȚIOASE:

- virusul informatic: program care se poate autoreplica în cadrul unui sistem şi propaga în alte calculatoare din reţea fără ştiinţa utilizatorului. Acesta poate afecta negativ funcţionalitatea, integritatea, disponibilitatea sistemului sau a datelor conţinute de acesta;
- viermele informatic: un malware ce dispune de capacitatea de a se autoreplica şi propaga într-o reţea de calculatoare şi dincolo de aceasta (alte sisteme sau reţele), folosind resursele reţelei, fără a se ataşa unui alt program sau proces.

# EŞTI ATENT LA DATELE TALE PERSONALE?

# RECOMANDĂM UN SET MINIM DE REGULI:

✓ cumpărăturile să se realizeze doar de pe site-uri web recunoscute şi securizate;

✓ contravaloarea unui produs achiziţionat nu trebuie transmisă înainte de verificarea existenţei şi funcţionalităţii acestuia, prin folosirea unui serviciu de escrow recunoscut;

✓ nu se folosesc servicii financiare de transfer rapid WesternUnion sau MoneyGram înainte de recepţionarea produsului achiziţionat, mai ales când această operaţiune este solicitată de vânzător;

✓ verificarea site-ului web (există magazine online fictive care au ca scop atragerea de clienţi şi reţinerea datelor bancare ale acestora).

✓ respectarea unei simple metode de verificare, respectiv compararea link-urilor receptate prin mesaje de tip „spam“ cu cele legitime ale instituţiilor bancare.

# FOLOSIREA ÎN SIGURANȚĂ A TELEFONULUI SAU A TABLETEI

# Telefoanele au un nivel de securizare scăzut.

- ✓ nu instala decât aplicaţii necesare şi verifică la ce date au acces înainte de le descărca (poziţionare geografică, contacte, apeluri telefonice etc;
- ✓ în plus faţă de codul PIN care protejează cartela SIM, foloseşte o parolă sau un cod pentru a securiza accesul la telefon;
- ✓ instalează software-uri de securitate special concepute pentru dispozitive mobile; acestea pot detecta şi elimina viruşii, bloca mesajele spam multimedia sau alte ameninţări cibernetice;
- ✓ criptează memoria internă a telefonului sau tabletei dacă aceastea conţin informaţii sensibile; dacă dispozitivul mobil este pierdut, persoana care intră în posesia acestuia nu va putea accesa datele respective;
- ✓ realizează salvări periodice ale datelor pe un suport extern pentru a le putea restaura;
- ✓ nu permite salvarea parolelor, în special pentru aplicaţiile bancare sau cele puse la dispoziţie de furnizorii de servicii pentru gestionarea consumului şi plata facturilor;
- ✓ aplică, periodic, actualizările de securitate furnizate de producătorii software-urilor instalate pe dispozitivele mobile.


# PLATFORMELE SOCIALE ŞI COPIII


# SE RECOMANDĂ:

✓ evitarea publicării informaţiilor personale, precum ziua de naştere, adresa de e-mail sau adresa fizică;

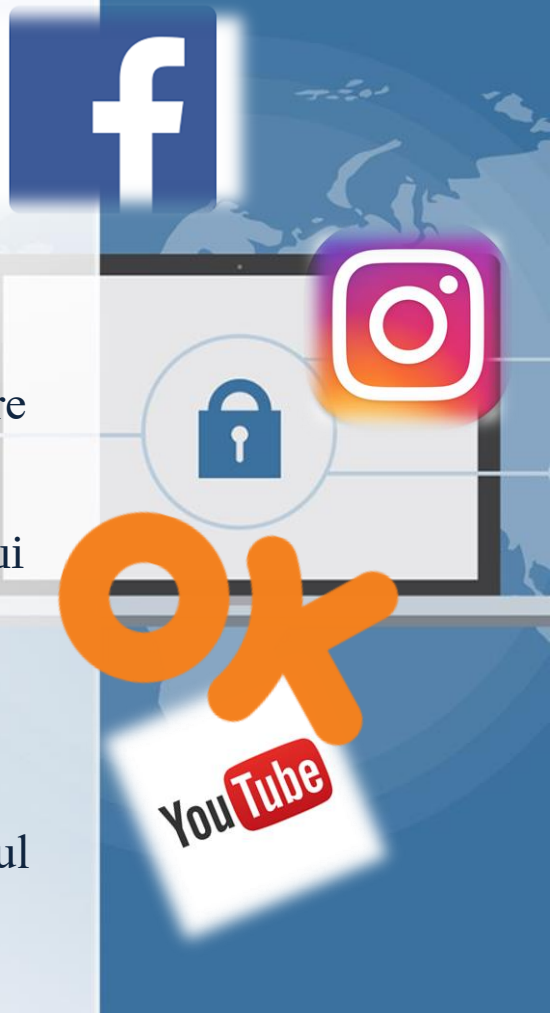
✓ atunci când postezi fotografii, asigură-te că o faci doar cu persoanele cunoscute, iar acestea nu surprind locaţii exacte (ex.: adrese de domiciliu);

✓ nu dezvălui niciodată informaţii referitoare la perioadele în care părăsiţi locuinţa;

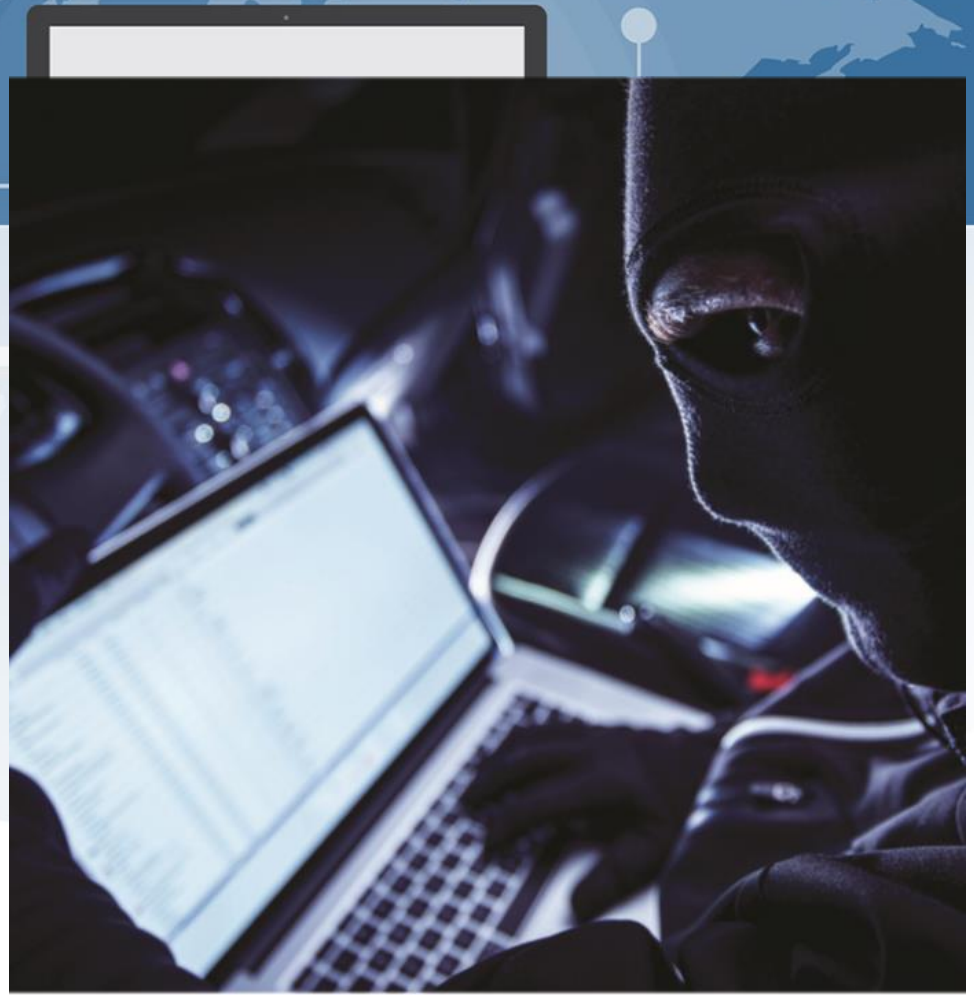
✓ în cazul în care ai copii care au voie să folosească calculatorul familiei, nu le oferi privilegii de administrator asupra respectivului computer;

✓ instalează o soluţie antivirus cu control parental, filtru de conţinut şi filtru pentru reţelele sociale. Dată fiind ponderea conţinutului pornografic şi a violenţei online, este de datoria părinţilor să îşi păstreze copilul în siguranţă;

✓ informează-te despre cyber-bullying şi poartă discuţii cu copilul tău.



*Utilizatorul reprezintă primul zid de apărare împotriva ameninţărilor din spatele monitorului, primul şi uneori ultimul în identificarea pericolelor şi, în funcţie de caz, semnalarea acestora unui matur. Utilizatorul este, totodată, cel care poate preveni crearea unor daune atât pentru sine, cât şi pentru mediul inconjurator.*



- ✓ utilizează ID-uri şi parole unice şi nu le comunica altor utilizatori;
- ✓ lungimea parolei şi complexitatea acesteia trebuie alese astfel încât să fie dificil de ghicit dar uşor de ţinut minte;
- ✓ schimbarea periodică a parolelor (la un interval de 1-3 luni); 3 utilizarea unor parole diferite, pentru aplicaţii diferite;
- ✓ utilizarea unor metode multiple de autentificare (PIN, amprentă, mesaje alertă, etc);
- ✓ evitarea utilizării unor parole similare acasă şi la locul de muncă

# Vă mulțumim pentru atenție