**Trăim într-o lume digitală în care Internetul are rolul principal. Chiar dacă te afli printre persoanele care nu fac tranzacții bancare online, care nu-și cumpără nimic din magazinele virtuale și nici nu faci greșeala de a comunica date personale unor necunoscuți, există situații în care navigarea ta pe Internet este nesigură. Asigurarea securităţii informaţionale este un proces continuu, ce constă în aplicarea celor mai raţionale forme, metode,  căi de creare şi perfecţionare a mijloacelor de securitate.Pentru a naviga sigur si placut pe Internet, este necesar ca fiecare dintre voi sa respecte o serie de reguli de baza.**

1. Prima regulă a navigatului pe Internet este să rămâi cât mai anonim posibil. Aceasta înseamnă să nu faci publice prea multe 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.
2. Păstrați cu grijă informațiile personale. Dacă un site Web vă cere un număr de carte de credit, informații bancare sau alte informații personale, asigurați­vă că site­ul Web este de încredere și verificați dacă sistemul său de tranzacție este unul sigur.
3. **Foloseşte pentru navigare un browser ce beneficiază de actualizări şi asigură-te că acestea sunt aplicate imediat ce devin disponibile.**
4. **Fiți atenți atunci când faceți clic pe hyperlinkuri în mesaje de poștă electronică. Hyperlinkurile (legături care deschid site­uri Web atunci când faceți clic pe acestea) sunt utilizate adesea în cadrul unor trucuri pentru înșelătorie sau programe spion, dar pot transmite și viruși. Faceți clic numai pe linkurile din mesajele de poștă electronică în care aveți încredere.**
5. Instalați programe de completare numai din site­uri Web în care aveți încredere. Programele de completare pentru browserul Web permit paginilor Web să afișeze elemente cu ar fi bare de instrumente, cotații bursiere, clipuri video și animație. Totuși, programele de completare pot instala și un program spion sau alt software rău intenționat. Dacă un site Web vă cere să instalați un program de completare, asigurați­vă că site­ul este de încredere înainte de a face acest lucru.
6. **Fiți precauți atunci când deschideți atașări de poștă electronică. Atașările de poștă electronică (fișiere atașate mesajelor de poștă electronică) sunt o sursă principală de infectare cu viruși. Nu deschideți niciodată o atașare primită de la o persoană necunoscută. În cazul în care cunoașteți expeditorul, dar nu așteptați o atașare, verificați dacă expeditorul chiar v­a trimis atașarea, înainte de a o deschide.**
7. Utilizați un paravan de protecție. Un paravan de protecție este un software sau un hardware care verifică informațiile venite de pe Internet sau dintr­o rețea, apoi fie le îndepărtează, fie le permite să treacă în computer, în funcție de cum ați setat paravanul de protecție. Astfel, un paravan de protecție ajută la împiedicarea hackerilor și a software­ului rău intenționat să aibă acces la computer. Paravanul de protecție Windows este inclus în Windows și este activat automat. Spre exemplu, dacă executați un program, cum ar fi un program de schimb instantaneu de mesaje sau un joc de rețea cu mai mulți jucători care are nevoie să primească informații de pe Internet sau dintro rețea, paravanul de protecție vă întreabă dacă blocați sau deblocați (permiteți) conexiunea.
8. **Utilizați protecție antivirus. Virușii, viermii și caii troieni sunt programe create de hackeri, care utilizează Internetul pentru a infecta computere vulnerabile. Virușii, viermii și caii troieni destructivi pot să șteargă informații din hard disk sau să dezactiveze complet computerul. Alții nu cauzează daune directe, dar înrăutățesc performanța și stabilitatea computerului. Programele antivirus scanează mesajele electronice și alte fișiere de pe computer pentru detectarea virușilor, viermilor și cailor troieni. Dacă este găsit unul, programul antivirus fie îl pune în carantină (izolează), fie îl șterge în întregime înainte de a deteriora computerul și fișierele.**
9. Utilizați protecția antispyware. Programele spion sunt acele tipuri de software care pot să afișeze reclame, să colecteze informații despre dvs. sau să modifice setările din computer, de obicei fără a avea aprobarea dvs. De exemplu, programele spion pot să instaleze bare de instrumente nedorite, linkuri sau preferințe în browserul Web, pot să modifice pagina de pornire implicită sau să afișeze frecvent reclame pop­up. Unele programe spion nu afișează niciun indiciu pentru a le detecta, dar colectează în secret informații sensibile, cum ar fi site­urile Web pe care le vizitați sau textul pe care îl tastați. Majoritatea programelor spion sunt instalate prin intermediul unui software gratuit pe care îl descărcați, dar în unele cazuri simpla vizitare a unui site Web poate duce la o infectare cu programe spion. Pentru a ajuta la protejarea computerului de programe spion, utilizați un program antispyware.
10. **Urmăreşte indiciile unor măsuri de securitate. Site-urile securizate folosesc „https://” în cadrul adreselor web, litera „s” semnificând faptul că datele trimise şi primite către/de la site-ul respectiv sunt protejate prin criptare. Niciodată să nu furnizezi informaţii personale pe un site web ce are adresa web prefixată cu „http://”.**

Respectarea acestor măsuri poate reduce considerabil riscul de incidente cibernetice, precum infiltrarea softurilor malițioase în calculatorul și conturile Dvs. online, captarea informațiilor personale, furtul de bani sau identitate.  
Cu siguranţă, cunoaşterea riscurilor din mediul online va constitui cel mai important pas în evitarea şi contracararea lor.

**Pe Internet răspândirea zvonurilor, postarea fotografiilor sau altor informaţii personale, trimiterea unui mesaj răuvoitor sau postarea comentariilor răuvoitoare se face uşor. Atunci când una sau mai multe persoane încearcă în mod repetat și intenționat să rănească o altă persoană putem vorbi în mod clar despre hărţuire. Pe Internet se întâmplă la fel.**

**Această problemă există şi nu toţi oamenii sunt imuni la comentarii răutăcioase. Cei care agresează online trebuie să se gândească de două ori înainte să fie răutăcioși, iar cei care trec prin asta trebuie să ştie că pot să ceară şi să primească ajutorul cuiva, fie că e vorba de prieteni apropiaţi sau familie.**

„Cyber-bullying” sau hărţuirea cibernetică este termenul folosit pentru definirea diverselor forme de abuz psihologic pe internet (hărţuire, ameninţare, intimidare, adresare de injurii, transmiterea de mesaje obscene, uneori ajungându-se chiar şi la şantaj), cu scopul de a ataca în mod deliberat, repetat şi ostil o persoană sau un grup de persoane.

Hărțuirea online este un fenomen complex ce se realizează în mediul virtual cu ajutorul tehnologiilor și serviciilor electronice de comunicare. Ceea ce face ca hărţuirea online sa fie şi mai periculoasă este faptul că odată Informaţiile deranjante despre tine, postate pe Internet, acestea sunt foarte greu de eliminat definitiv pentru că mereu altcineva s-ar putea să le copie și posteze altundeva iar ritmul multiplicării acestor postări este şi mai mare decât în viaţa reală.

Să fie hărţuit i se poate întâmpla oricui și oricând.

**Acțiuni și manifestări care cad sub incidența acestui fenomen:**

* **bârfa: emiterea în mediul online a unor declarații speculative ce denigrează o persoană sau instigă un grup de persoane în a adopta un comportament restrictiv;**
* **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. De exemplu, de a solicita întrevederi în viața reală prin a amenința cu răfuială 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 create de agresorii pe internet, ce împrumută identitatea altor persoane pentru a facilita comunicarea cu victimele lor; sub protecția anonimatului, agresorii își amenință victimele sau, aleatoriu, folosesc identitatea victimei în raport cu alte persoane;
* sexting: distribuirea de materiale pornografice minorilor, utilizând mijloacele electronice de comunicație.

### **(nu stiu daca vom spune asta) Pentru început, însă:**

* Nu răspunde comportamentelor agresive într-o manieră similară cu cea a agresorului;
* Evită situația sau persoana agresivă. Blochează online agresorii;
* Dacă indiferența nu funcționează, reacționează. Spune-i calm, dar ferm să înceteze;
* Spune prietenilor să înceteze hărțuirea online a altei persoane și spune că nu eşti de acord cu acest comportament, atunci când îl observi;
* Dacă ai postat un video în care cineva este agresat sau ai distribuit un video postat de altcineva, este important să-l elimini de pe contul tău pentru a opri distribuirea în continuare;
* Cere ajutor de la colegii sau profesorii în care ai încredere, mai ales dacă situaţia neplăcută are legătură cu școala;
* Dacă ești îngrijorat(ă) povestește-i unui adult tot ce ți se întâmplă. Alege o persoană de încredere: părinte, frate, sora mai mare, antrenor etc.;
* Încearcă [să ștergi comentariile utilizatorului](https://support.google.com/youtube/answer/111870) și [să-l blochezi](https://support.google.com/youtube/answer/56113), dacă acesta face ceva ce te deranjează. Astfel, i se va interzice să-ți viziteze profilul. În plus, poți să dezactivezi comentariile la videoclipul tău sau poți să setezi aşa ca înainte de postare, comentariile să fie aprobate de tine;
* Respectă opiniile altor persoane, dar recunoaște când depășesc limita bunului simț. Utilizatorii de Internet nu trebuie să se simtă intimidați sau amenințați;
* Nu distribui, comenta sau aprecia postările în care cineva este hărţuit;
* Raportează conținutul și utilizatorii abuzivi folosind instrumentele de raportare;
* Dacă agresorul te urmărește, te amenință și insistă să-ți facă un rău - salvează dovada hărțuirii, precum screenshot-urile conversației. Păstrează email-urile.

**În primul rând, este bine să știm ce instrumente tehnice putem folosi pentru a opri un asemenea comportament din partea terților. Dacă hărțuirea se realizează pe o rețea de socializare (*facebook, odnoklassniki, instagram, twitter* etc.), trebuie să cunoașteți că aceste platforme au opțiuni de a raporta comentariile abuzive, hărțuirea sau așa numitul spam. A nu se ignora această opțiune ce vi se pune la dispoziție, ori ea chiar poate duce la închiderea contului de pe care sunteți molestat.**

Soluții tehnice ar fi mai multe, de a vă seta contul în așa fel încât să fie mai puțin accesibil persoanelor cu care nu sunteți “prieteni”. Acestea nu sunt măsuri de ordin legal, dar cel puțin vă protejează și nu vă expune atât de mult riscului de a fi hărțuit în mediul online. În cazul în care hărțuirea se realizează în afara rețelelor de socializare, de exemplu prin comentarii defăimătoare pe anumite site-uri sau bloguri, primul pas ar fi să notificați proprietarul site-ului prin a solicita ștergerea informației care vă defăimează.

**Atunci când mijloacele tehnice nu v-au permis să soluționați problema apărută, iar hărțuirea continuă, în mod sigur, ați putea  apela la organele competente: poliție, procuratură, instanța de judecată într-un final. Pentru a ne apăra drepturile ar exista două căi:**

* **fie prin depunerea unei plângeri penale, contravenționale;**
* **fie prin înaintarea unei acțiuni civile în instanța de judecată.**

**Identitatea digitală**este modul cum te văd ceilalți pe Internet. Postările tale, fotografiile postate de tine sau cele în care apari, comentariile pe care le scrii, grupurile din care faci parte, numărul de prieteni, aplicațiile pe care le accesezi şi paginile favorite sunt numai câteva dintre elementele care conturează imaginea ta pe rețelele de socializare. Toate acestea te definesc.

Profilurile pe rețelele sociale constituie cărți de vizită pe care le oferim altor utilizatori. Fii autentic şi prudent! Felul tău real de a fi e mai bun decât orice te-ai putea preface a fi.

**Ce pot afla alții despre tine online**

**Ai încercat vreodată să-ți tastezi numele în motoarele de căutare, de exemplu pe Google? Informația pe care o găsești este pozitivă sau trimite către site-uri cu care nu ți-ai dori să fii asociat?**

**Fii  selectiv în legătură cu persoanele pe care le adaugi în lista de prieteni, deoarece acea persoană, în continuare îți va putea vedea fotografiile şi datele personale. Niciodată nu ştii dacă vârsta, numele, adresa sau fotografiile persoanei cu care vorbești pe Internet sunt adevărate.**

## **5 pași pentru a-ți construi reputația online:**

1. Fii foarte atent la informațiile care le postezi pe un profil online. Asigură-te că ceea ce postezi te reprezintă și nu te va face să roşeşti peste ani. Nu posta nimic din ceea ce n-ai vrea să vadă părinții, profesorii sau eventualii tăi colegi de muncă pe viitor;
2. Ține cont că o fotografie, odată postată, va rămâne pe Internet și după ce o ștergi. Ea poate fi copiată de oricine și folosită oriunde, fără știrea și voia ta;
3. **Ai grijă ce fotografii postezi și în ce ipostaze apari atunci când ești fotografiat sau filmat. De asta depinde imaginea ta online;**
4. **Ai grijă ca ceea ce postezi să nu fie ofensator sau deranjant pentru ceilalți;**
5. **Fii atent/ă la exprimarea publică a sentimentelor tale personale. Ceea ce îți poți permite într-o corespondență privată cu o prietenă sau un prieten, în majoritatea cazurilor nu este pentru uz public.**

### **Postează online doar:**

* Lucruri utile prietenilor tăi;
* Informații de interes public, precum evenimente, știri etc.;
* Mesaje de recomandare pentru un produs sau un serviciu de care ești mulțumit. Nu le confunda cu postările comerciale, acelea au un scop de a promova un produs și nu calitatea;
* **Materiale cu caracter pozitiv și de motivare din domeniile care te interesează sau în care activezi;**
* **Îndemnuri de participare la proiecte sociale;**
* **Alte informaţii, după bunul tău simț și plac.**

### *****Reţine!******Dacă astăzi ai grijă de imaginea ta, mâine ea va avea grijă de tine.*