Utilizarea în siguranță a Internetului

4.2. Rețele sociale

4.2.1. Înțelegerea importanței nedezvăluirii informațiilor confidențiale în cadrul site-urilor de rețele sociale

- O rețea socială virtuală reprezintă un serviciu disponibil pe Internet, creat cu principalul scop de a conecta utilizatori cu aceleași interese, activități, hobby-uri.
- Pe baza unui cont creat pe aceste site-uri, utilizatorii pot completa profiluri cu informații personale, domenii de interes, educație, locul de muncă, date de contact etc. Au la dispoziție instrumente de mesagerie (chat), de adăugare a fotografiilor, a conținutului video, diferite jocuri online și sisteme de comentarii și recomandări.

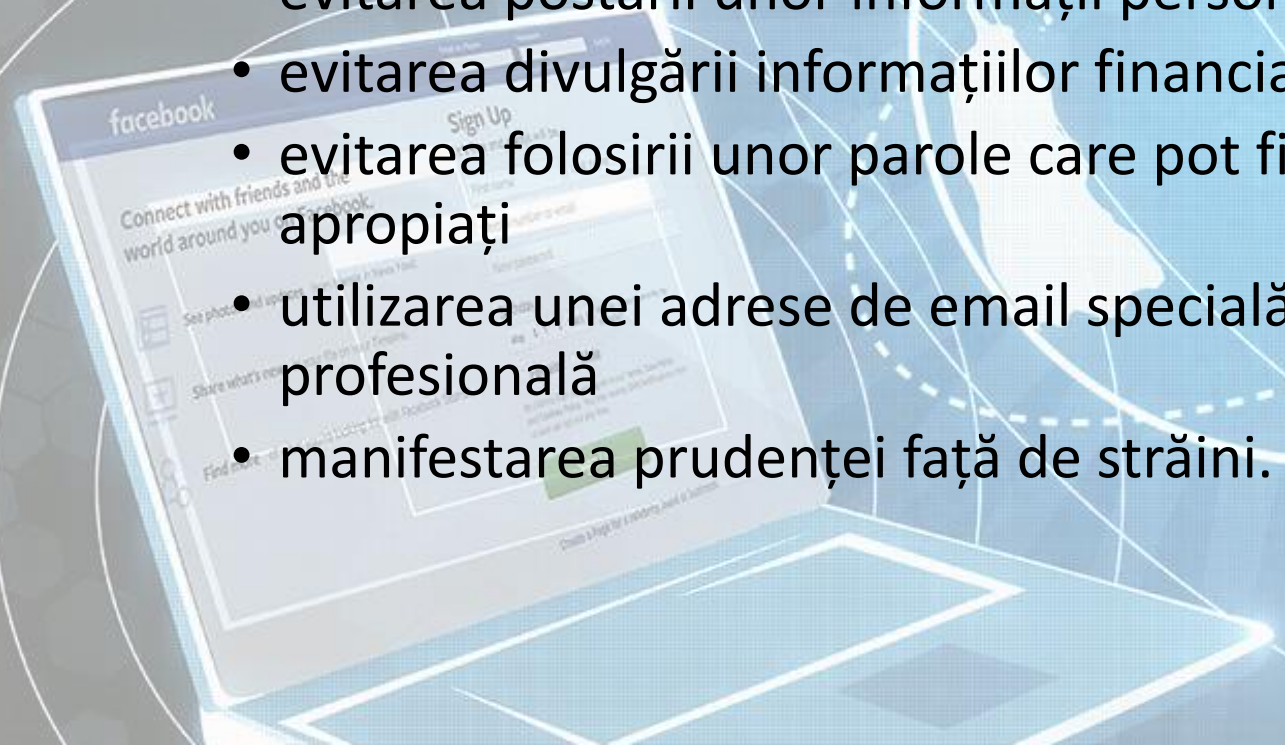
- Se creează astfel comunități de **utilizatori cu interese specifice**:
- Rețele sociale de **afaceri** Linkedin, Talkbiznow
- Rețele sociale de **prietenii**: Facebook;
- Rețele sociale de **partajare de fotog**rafii: Flickr;
- Comunități pentru **ecologiști**: Care2;
- Comunități de **blogging**: Blogster, Twitter
- **Un blog** se referă la o publicație web (un text web) ce conține articole periodice, cu actualizare continuă, care are de obicei un caracter personal (web log = jurnal pe internet).
- Ca regulă, actualizarea blogurilor constă în adăugări de texte noi, asemenea unui jurnal de bord, toate contribuțiile fiind afișate în ordine invers cronologică în partea de sus, la vedere. Acest gen de publicații sunt în principiu accesibile publicului larg, ce poate să scrie comentarii, creându-se astfel o comunitate de cititori în jurul blog-ului.

- Comunități pentru pasionați ai **jocurilor online**: Avatars United.
- **Forumuri** de discuții (site-uri de discuții online, unde oamenii pot conversa prin Intermediul mesajelor postate): Forum Softpedia.
- Datorită interactivității acestui serviciu putem enumera câteva avantaje:
  - sunteți la curent cu ultimele știri, evenimente, noutăți;
  - căuta în aceste rețele prieteni, cunoștințe, colegi de școală;
  - puteți partaja conținut audio-video;
  - puteți comenta, vota și recomanda mesajele text, pozele, videoclipurile adăugate de ceilalți utilizatori,
- Altă metodă de a partaja conținut audio-video o reprezintă podcast Aceasta este o metodă de distribuție a fișierelor în format multimedia (de obicei fișiere audio și video). Materialele pot fi descărcate și redate pe echipamente mobile sau calculatoare ce acceptă formatul în care acestea au fost create.
- Siturile de **podcasting** pot oferi fișierele spre descărcare și ascultare off-line sau pentru redare directă on-line. Multe site-uri, pe baza unui abonament, vă permit să descărcați manual, conținut podcast. Dacă doriți ca acest conținut sa fie actualizat si descărcat automat, atunci folosiți un program (client) de podcasting. Exemple de clienți podcast Happyfish, Doppler, iTunes etc.

- Utilizate pe scară largă la nivel mondial, site-urile de rețele sociale reprezintă spațiul în care oamenii interacționează on-line, conversează, fac schimb de fotografii sau muzică ori își împărtășesc experiențe.
- Dezvoltarea accelerată a acestei forme de comunicare, a dat naștere anumitor îngrijorări legate de siguranța utilizării Internetului pentru dezvăluirile anumitor date personale.

- În ultima vreme au apărut din ce în ce mai multe avertismente din partea companiilor care se ocupă cu securitatea online în legătură cu pericolul la care se expun utilizatorii rețelelor sociale atunci când publică prin intermediul acestora informații private cum ar fi numărul de telefon, adresa de e-mail sau chiar adresa unde locuiesc.
- Informațiile obținute de hackeri prin intermediul Facebook, MySpace sau LinkedIn pot compromite atât identitatea online a utilizatorilor inconștienți, cât și bazele de date ale companiilor la care aceștia lucrează în cazul în care aceștia afișează online locul de muncă și/sau date despre angajatori.
- De exemplu, dacă un cont al unui angajat la o anumită companie este compromis, acest lucru va însemna invariabil mai mult spam și/sau malware îndreptat spre conturile de e-mail ale corporației respective, ceea ce poate duce la pierderea sau coruperea de date vitale pentru compania în cauză.
- În plus, folosind informațiile personale ale userilor, hackerii pot obține în mod fraudulos permise de conducere sau pașapoarte, pot pune la cale fraude bancare sau pot obține ilegal transferuri de bani.

- Astfel, se recomandă celor care utilizează site-urile de rețele sociale:
  - afișarea unui profil privat
  - limitarea persoanelor care pot vizualiza informațiile personale postate
  - evitarea postării unor informații personale ca adresa și numărul de telefon
  - evitarea divulgării informațiilor financiare (detalii card credit, cod PIN)
  - evitarea folosirii unor parole care pot fi identificate ușor, chiar și de cei apropiați
  - utilizarea unei adrese de email specială, diferită de cea strict personală sau profesională
  - manifestarea prudenței față de străini.

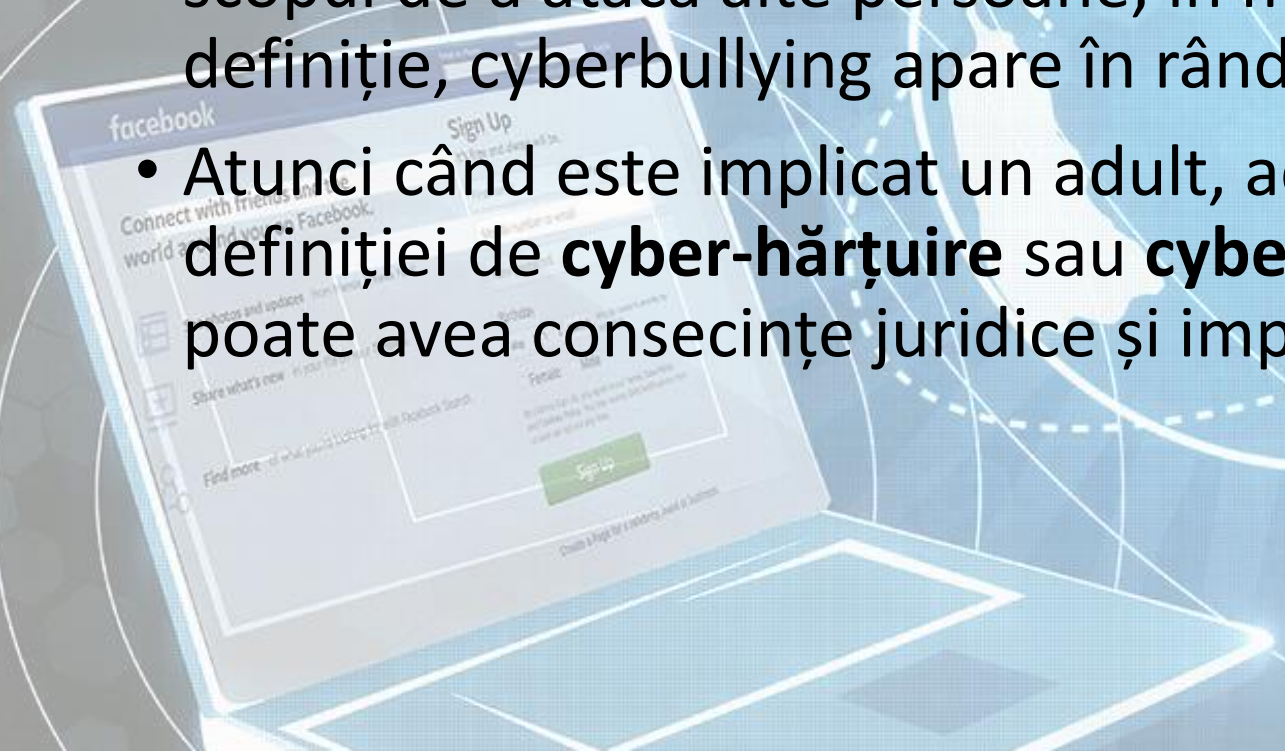


4.2.2. Conștientizarea necesității aplicării setărilor de securitate corespunzătoare conturilor existente pe rețelele sociale

- Furtul de date personale este principalul pericol la care se expun zilnic utilizatorii rețelelor sociale. Regula numărul unu, care se aplică pentru orice rețea de socializare este alegerea unei parole complexe, diferită pentru fiecare cont în parte.
- Recomandările cu privire la setările de securitate ale conturilor de pe diverse rețele sociale sunt:
  - înainte de a instala o aplicație, verifică permisiunile pe care aceasta le solicită, precum și datele la care are acces această aplicație, odată instalată
  - limitează numărul celor care au acces la datele tale personale (adresa de e- mail, locație, vârstă, listă de prieteni sau alte date care se pot folosi în scopuri frauduloase)
  - folosește opțiunile de setare a vizibilității mesajelor postate
  - setează-ți profilul astfel încât doar prietenii să îți poată vedea informațiile și fotografiile
  - acceptă prietenia doar a persoanelor apropiate, pe care le cunoști în viața reală și în care ai încredere
  - raportează / blochează persoanele care te deranjează
  - activează navigarea securizată sau opțiunea de urmărire a calculatoarelor de pe care se accesează contul tău
  - activează monitorizarea tag-urilor astfel încât să afli dacă cineva te-a etichetat într-o fotografie, înainte ca aceasta să devină publică.

4.2.3. Înțelegerea pericolelor potențiale asociate utilizării site-urilor de rețele sociale

- **Cyberbullying** (agresiune online sau hărțuire cibernetică) implică utilizarea tehnologiilor de telecomunicații (e-mail, rețele sociale, telefoane mobile, site-uri web defăimătoare, forumuri, blog-uri) cu scopul de a ataca alte persoane, în mod deliberat, repetat și ostil. Prin definiție, cyberbullying apare în rândul tinerilor.
- Atunci când este implicat un adult, aceasta poate corespunde definiției de **cyber-hărțuire** sau **cyber urmărire**, o infracțiune care poate avea consecințe juridice și implică închisoare.



- Cyberbulling este termenul folosit pentru a defini diverse forme de abuz psihologic realizate prin Internet și poate include:
  - trimiterea de conținut obscen și ofensator (atât text, cât și imagini) prin email, mesagerie instantanee sau SMS/MMS în vederea intimidării unei personae
  - trimiterea de amenințări
  - batjocorirea repetată a unei persoane
  - publicare online a unor informații sau fotografii personale, fără acordul persoanei în cauză
  - folosirea de conținut obscen în timpul discuțiilor online
  - ridiculizarea unei persoane prin crearea unui profil sau blog fals, conținând informații umilitoare.

- Cyberbulling-ul se manifestă în cadrul aplicațiilor de mesagerie instantanee și rețelelor de socializare. De asemenea, SMS-urile și MMS-urile pot fi utilizate pentru hărțuirea persoanelor.
- Pentru a te feri de cyberbulling, recomandările sunt următoarele:
  - Nu divulga informații personale (nume, vârstă, adresă, telefon)
  - Nu divulga parolele
  - Nu deschide mesaje de la necunoscuți
  - Nu posta nimic pe Internet din ceea ce nu vrei ca alții să vadă. Odată postată pe Internet, o informație poate fi preluată ușor
  - Dacă primești un mesaj de amenințare, nu răspunde la el. Salvează mesajul și arată-l părinților
  - Fii mereu politicos
  - Respectă-i pe ceilalți utilizatori, chiar dacă au altă etnie sau rasă
  - Raportează orice ilegalitate observată
  - Nu discuta online cu persoane necunoscute.

- **Grooming** implică acțiuni deliberate în vederea împrietenirii și stabilirii unei conexiuni emoționale cu un copil pentru a-l determina să accepte un comportament inadecvat. Pedofilii online folosesc camere de chat, site-uri de jocuri și servicii de rețele sociale pentru a lua contact cu tinerii, cu intenția de a-i atrage în activități sexuale On-line sau Off-line.
- ”Grooming on-line", este o infracțiune, întrucât aparatele foto digitale, telefoanele cu cameră web și webcam-urile devin tot mai populare, tinerii ar putea fi în pericol sporit în cazul în care postează online imagini sexuale, provocatoare sau dacă le partajează cu alții de exemplu prin intermediul unui telefon mobil. În unele cazuri, ar putea face acest lucru la cererea unei persoane pe care au întâlnit-o online.
- Pentru a proteja tinerii de grooming online, aceștia trebuie să știe că foarte multe persoane de pe Internet își asumă identități false și furnizează informații false despre ei înșiși pentru a fi mai convingători în diferite contexte. De aceea, nu trebuie divulgate informații cu caracter personal pe Internet.

- În unele cazuri, infractorii pot trimite diferite link-uri înșelătoare către diverse site-uri, pretinzând că puteți ajuta un nevoiaș sau un bolnav apăsând click pe un buton sau completând un formular.
- În alte situații, pretextul este câștigarea unui telefon, tablete PC sau chiar a unui laptop. Se recomandă atenție sporită la aceste link-uri întrucât vă pot conduce spre site-uri virusate ce au ca scop în general furtul de informații confidențiale din calculatorul dumneavoastră.