

Protecția datelor personale în Internet

- **Internetul** este o rețea formată din mii de rețele de calculatoare conectate între ele, situate în diferite țări și continente folosind regulile de comunicație (*protocolul*) *TCP/IP*.

- informațiile postate în Internet sunt publice.

- **datele personale** (d.p.) sunt cele cu care o persoană poate fi recunoscută (nume, CNP, poză, amprente, număr telefon, adresă, vârstă, ocupația, unele date despre familie sau rude etc.)

- **identitatea virtuală** a unei persoane este *urma lăsată de activitatea sa* în Internet (căutări, postări) sau felul în care apare *într-un anumit cont* din Internet (o rețea de socializare, joc, program de comunicare, site multimedia).

- **furtul de identitate** este o faptă dăunătoare pedepsită de legi prin care o persoană folosește d.p. ale altcuiva pentru a obține foloase necuvenite (furt de bani, recompense etc).

- realizarea furtului de identitate :

- publicarea voluntară a d.p. pe rețele de socializare
- mesaje înșelătoare pe telefon și Internet
- folosirea parolelor slabe
- folosirea d.p. în rețele wifi publice.

- pentru siguranța conturilor trebuie să folosim **parole puternice** și să respectăm anumite reguli:

- folosim parole lungi
- evitam cuvinte ușor de ghicit
- folosim parole diferite la conturi diferite
- schimbăm periodic parolele
- putem crea parole după o propoziție sau prin înlocuirea unor litere (o 0, I !,s \$)

- **GDPR** (*Regulamentul pentru protecția datelor personale*) are rolul să protejeze d.p. atunci când sunt prelucrate de diferiți operatori (firme, instituții, persoane) din Uniunea Europeană.

- persoanele au anumite drepturi cu privire la folosirea datelor lor personale (pag 13)

Programele rău intenționate

- programele rău intenționate (malware) sunt pericole din Internet : viruși, viermi, cai troieni, spyware, adware, ransomware

- *Virusul* acționează când pornim programul care îl conține. El caută alt program de care să se atașeze.
- *Viermele* se răspândește prin rețea sau pe suporturi fără acțiunea utilizatorului
- *Cal troian* oferă acces de la distanță la calculatorul pe care rulează
- *Spyware* transmite (spionează) spre un centru de control parole, adrese folosite, cuvinte tastate
- *Adware* aduce reclame pe calculator
- *Ransomware* blochează accesul la calculator sau fișiere în schimbul unei plăți

-transmiterea malware :

- prin soft deja infectat,
- prin stickuri infectate,
- prin Internet (siteuri, jocuri)

-măsurile de protecție :

- programele anti-virus (protejează calculatorul de acțiunea malware),
- evitarea site-urilor nesigure și a jocurilor,
- nu folosim stickuri neverificate,
- nu instalăm programe nesigure sau inutile,
- soft actualizat