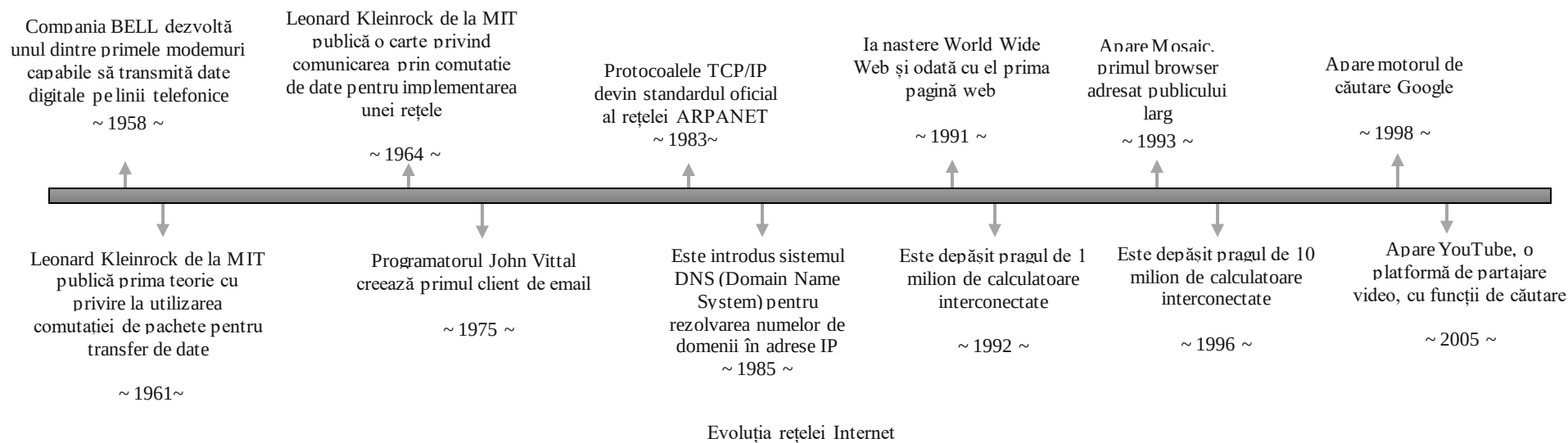




Ghid de bune practici pentru navigarea în Internet

Introducere

Internetul reprezintă un sistem global de rețele de calculatoare interconectate care utilizează anumite protocoale pentru a comunica între ele. Este o rețea formată din mai multe rețele (publice, private, guvernamentale etc.) iar scopul acesteia a fost de a facilita comunicarea și de a permite oamenilor să acceseze rapid informații, indiferent de poziția geografică.

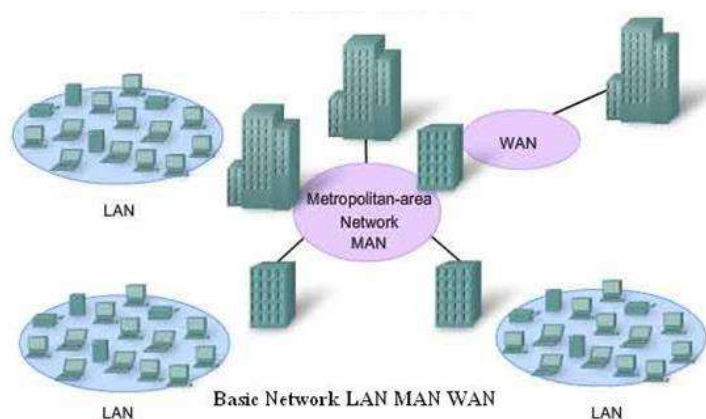


⚡ Notă: Teoria lui Leonard Kleinrock privind comunicarea prin comutația de pachete la nivel de rețea se numește "**Information Flow in Large Communication Nets**" și poate fi accesată la adresa <http://www.nobbyville.com/Internet/Kleinrock61.pdf>.

Modul de funcționare al Internetului

Furnizarea acestui serviciu se face prin intermediul organizațiilor de tip ISP (Internet Service Provider), iar accesarea Internetului din punct de vedere fizic se poate face prin diverse metode: linie dedicată, conectare prin cablu de rețea Ethernet, fibră optică, conectare prin rețeaua electrică, conectare wireless și conexiune mobilă.

Din punctul de vedere al acoperirii geografice, rețelele de calculatoare sunt clasificate în:

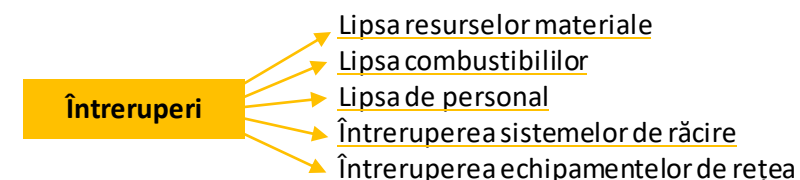
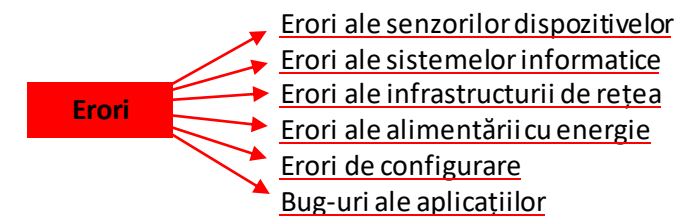
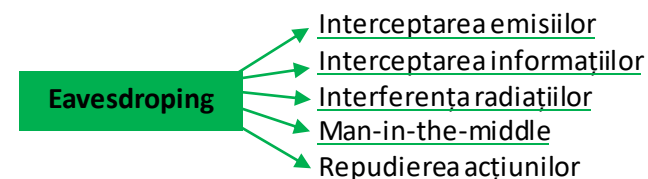
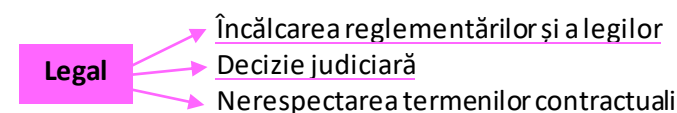
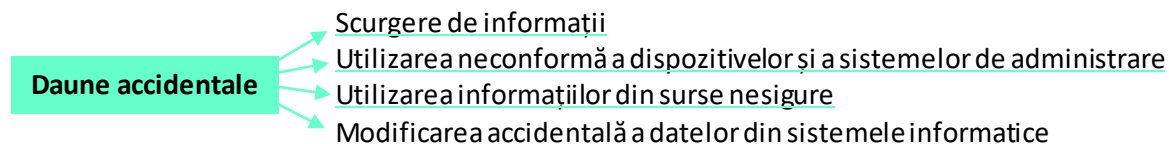
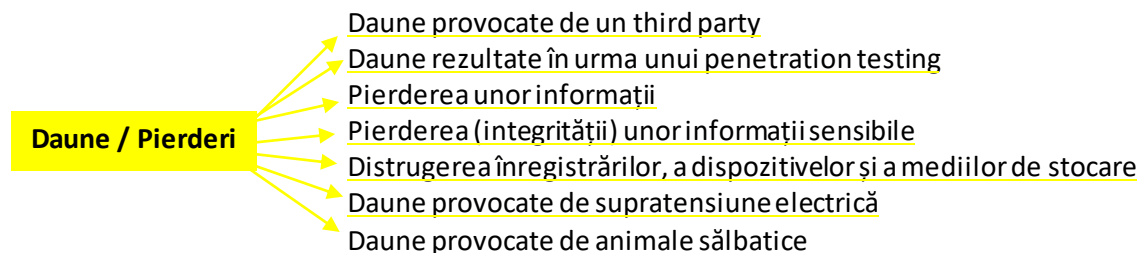
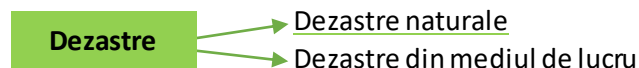
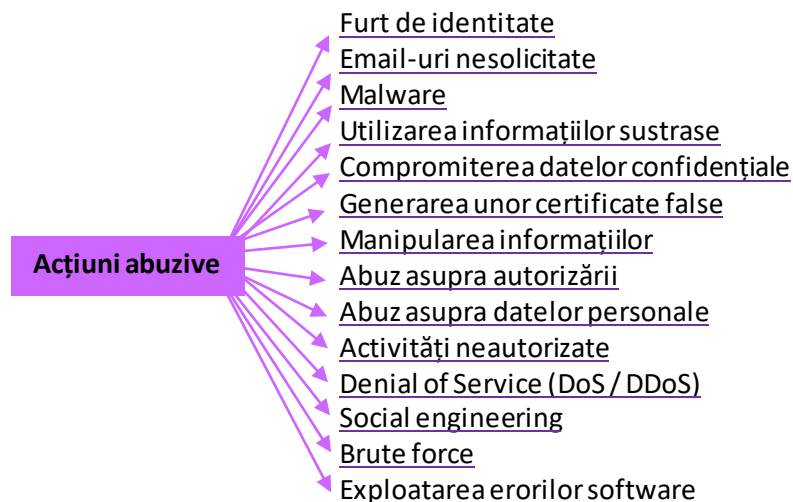


- PAN-uri (Personal Area Network)
- LAN-uri (Local Area Network)
- WLAN-uri (Wireless Local Area Network)
- CAN-uri (Campus Area Network)
- SAN-uri (Storage Area Network)
- MAN-uri (Metropolitan Area Network)
- WAN-uri (Wide Area Network)

Notă: Pentru ca un sistem informatic să poată comunica în rețea și să poată fi identificat ușor printre milioanele de dispozitive conectate, fiecărui dispozitiv îi este asignată o adresă IP unică formată din 32 de biți.

Tipuri de amenințări în spațiul cibernetic

În prezent, Internetul face parte activ din cotidianul multora dintre noi. Navigarea în Internet este de cele mai multe ori utilă, informativă și distractivă, însă fără o protecție adecvată acesta poate fi și deosebit de periculoasă. Atunci când navigăm în Internet, accesarea anumitor pagini web ne poate pune în pericol identitatea, imaginea și resursele financiare.



Bune practici de securitate privind navigarea în Internet

➤ Utilizați o conexiune VPN

Tehnologia VPN sau Virtual Private Network permite unui utilizator să își securizeze conexiunea la Internet prin criptarea traficului de rețea dintre dispozitivul său și serverul VPN, crescând nivelul de confidențialitate și protecție a datelor.



O altă modalitate de protecție a datelor în mediul online este folosirea unui server proxy.

➤ Stabilirea și configurarea browser-ului

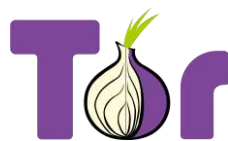
Browser-ul web reprezintă interfața prin care un utilizator poate accesa resursele existente în spațiul cibernetic. În prezent, cele mai cunoscute browsere sunt Microsoft Edge, Google Chrome, Mozilla Firefox, Opera și Safari. Atunci când alege browser-ul, utilizatorul trebuie să ia în considerare nivelul de protecție și de confidențialitate pe care acesta îl oferă, dar și dacă acesta este actualizat constant. Odată ales, se recomandă ca setările de securitate și confidențialitate permise de browser să fie stabilite la cel mai înalt nivel.



Google Chrome



Mozilla Firefox



Tor



Microsoft Edge



Opera



Safari



IceCat

Pe lângă browserele menționate anterior, există și browsere precum Iridium, Tor și GNU IceCat, orientate spre confidențialitate. Acestea oferă funcții suplimentare de protecție a datelor, precum blocarea urmăririi și limitarea colectării informațiilor, iar nivelul de criptare al traficului depinde de protocoalele utilizate (de exemplu: HTTPS). Browserul Tor utilizează rutarea traficului prin mai multe noduri pentru a crește nivelul de anonimitate.

Utilizarea acestor browsere este legală și are ca scop principal protejarea confidențialității utilizatorilor, însă nivelul de anonimitate și politicile aplicabile pot varia în funcție de legislația fiecărei țări.

Este esențială actualizarea în permanență a browser-ului utilizat pentru a fi protejat de ultimele amenințări apărute în spațiul cibernetic.

➤ **Alegeți motorul de căutare**

Motorul de căutare este modalitatea prin intermediul căreia pot fi căutate informații din Internet. În momentul în care un utilizator caută o frază sau un cuvânt, motorul de căutare va accesa bazele de date și, în funcție de anumite criterii, va afișa o listă de rezultate.

Pe lângă Google, există și alte motoare de căutare precum Bing, Yahoo, Ask, AOL sau DuckDuckGo. Trebuie menționat că atunci când un utilizator realizează o anumită căutare, acesta furnizează datele de căutare către compania care deține motorul de căutare, date ce pot fi utilizate ulterior în campanii de marketing. Totuși există alternative, mai puțin cunoscute, centrate pe confidențialitate prin criptarea datelor introduse și ștergerea istoricului de căutare la un interval de timp mult mai mic.



➤ **Managementul plugin-urilor**

Pentru a extinde funcționalitatea browserului, utilizatorii pot instala extensii sau componente suplimentare. Acestea sunt mici aplicații care adaugă funcții ce nu sunt incluse în mod implicit în browser, precum blocarea reclamelor sau gestionarea parolelor. În prezent, majoritatea browserelor moderne pot deschide fișiere PDF nativ, fără a necesita plugin-uri dedicate

Atunci când se dorește utilizarea unui plugin este recomandat ca înainte de instalare să fie verificate cu atenție funcționalitățile acestuia. De asemenea recenziile celorlalți utilizatori pot reprezenta o bună sursă de documentare despre cât de bine este optimizată aplicația, dar și dacă este de încredere sau nu.

➤ **Utilizați doar protocolul HTTPS**

Verificați în permanență ca adresa URL a site-ului pe care îl accesați să aibă înainte *https://* sau o pictogramă de forma unui lacăt. Aceasta este confirmarea că site-ul web accesat este protejat și criptat.



➤ **Activați setările de confidențialitate**

Specialiștii în marketing, dar și persoanele rău-intenționate, obișnuiesc să adune cât mai multe informații despre utilizatori. Aceștia țin cont de interogările din motoarele de căutare, de paginile web accesate și de lucrurile urmărite pe platformele de socializare pentru a furniza ulterior diferite reclame și oferte la produsele vizualizate.

Pentru a limita acest lucru, atât browser-ele web cât și sistemele de operare mobile au disponibile diferite setări pentru a vă proteja confidențialitatea. De multe ori aceste setări sunt greu de găsit, deoarece marile companii doresc obținerea a cât mai multe informații personale despre utilizatori datorită valorii acestora în marketing.

➤ **Blocați ferestrele pop-up și scripturile**

Ferestrele de tip *pop-up* sunt adesea forme de publicitate menite să atragă atenția utilizatorilor. Accesarea acestora poate duce la deschiderea de noi pagini în cadrul browser-elor pentru a afișa reclame sau pentru a instala programe de tip spyware și obține informațiile personale.

Este recomandată dezactivarea acestor ferestre fie prin configurațiile browser-ului, fie prin instalarea unei extensii de tip [AdBlock](#). De asemenea, pentru a bloca scripturile și adware-urile malițioase poate fi instalat un program precum [NoScript](#).



➤ **Nu stocați niciodată parolele în cadrul browser-ului**

Multe browsere moderne oferă funcții de salvare și completare automată a parolelor, acestea fiind protejate prin mecanisme de criptare și autentificare. Cu toate acestea, pentru un nivel sporit de securitate, se recomandă utilizarea unui manager de parole dedicat, protejat printr-o parolă principală sau autentificare biometrică. Evitați folosirea aceleiași parole pentru mai multe conturi.

Dacă salvați parolele, protejați-le corespunzător și folosiți un manager de parole sigur.



➤ **Acordați atenție fișierelor descărcate**

Un obiectiv principal al infractorilor cibernetici constă în păcălirea utilizatorilor astfel încât aceștia să descarce programe malware. De cele mai multe ori aceste programe vin ascunse sub forma unor aplicații legitime precum jocuri, aplicații meteo sau aplicații financiare.

Nu se recomandă descărcarea fișierelor sau aplicațiilor care provin din surse nesigure.



DOWNLOAD

➤ **Acordați atenție persoanelor cu care comunicați în mediul online**



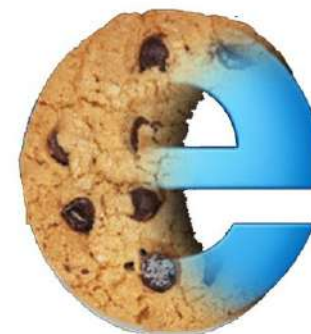
Persoanele întâlnite în spațiul virtual nu sunt întotdeauna ceea ce pretind a fi, uneori s-ar putea ca nici măcar să nu existe. Conform statisticilor efectuate, profilurile false de pe rețelele sociale sunt o modalitate populară prin care infractorii cibernetici încearcă să câștige încrederea viitoarelor victime.

Atunci când comunicați cu o persoană necunoscută din mediul online, rămâneți la fel de precaut ca și în viața reală.

➤ Managementul cookie-urilor

Cookie-urile stochează informațiile introduse de utilizator, astfel încât la următoarea accesare a paginii acesta să nu mai fie nevoit să reintroducă datele. Cu toate acestea, cookie-urile pot fi folosite de către persoane rău intenționate și pentru a urmări și analiza interesele utilizatorilor fiind încălcată confidențialitatea acestora.

Configurați browser-ul pentru a vă solicita permisiunea de a accepta sau nu cookie-uri. De asemenea puteți utiliza o aplicație de tip *anonymous cookies*. Acest software vă va menține dispozitivul fără cookie-uri sau poate limita accesul la acest tip de fișiere.



➤ Folosiți parole complexe și autentificarea multi-factor acolo unde este posibil



Parolele reprezintă în continuare unul dintre cele mai vulnerabile puncte din întreaga structură de securitate a Internetului, neexistând nici o modalitate de a le ocoli. Cea mai mare problemă este că oamenii tind să își configureze parole foarte ușor de reținut, precum *1234567* sau chiar *parola*.

Se recomandă configurarea unor parole unice și complexe care să nu aibă legătură cu evenimentele sau oamenii din viața personală. O parolă puternică trebuie să fie compusă din minim 8 caractere și să aibă litere mici, litere mari, cifre și caractere speciale.

➤ **Actualizați în permanență programele antimalware instalate**

Chiar dacă sunteți prudent de cele mai multe ori, uneori se poate întâmpla ca o anumită amenințare să ocolească măsurile de securitate implementate în browser și să ajungă pe dispozitivul dumneavoastră. În acest sens, pentru a fi protejat, se recomandă instalarea și actualizarea în permanență a unui program antimalware (antivirus, firewall).

➤ **Avertizare conexiuni securizate**

Configurați browser-ul pentru a afișa o alertă de fiecare dată când accesați o pagină nesecurizată din Internet. Există programe software speciale numite *sniffer* care monitorizează traficul de rețea și care au capacitatea de a recunoaște modele specifice de numere, precum numerele cardurilor de credit. Nu ignorați niciodată alertele generate de browser sau de programele antimalware.



Your connection is not private

Attackers might be trying to steal your information from **expired.badssl.com** (for example, passwords, messages or credit cards). [Learn more](#)

NET::ERR_CERT_DATE_INVALID

Conexiunea este securizată

Informațiile tale (de exemplu, parolele și numerele cardurilor de credit) sunt private când sunt trimise la acest site. [Află mai multe](#)



➤ **Supravegheați copiii atunci când aceștia navighează în Internet**

Copiii se confruntă cu riscuri speciale de confidențialitate pe Internet. Uneori, personajele de desene animate din mediul online pot părea că îi adresează copilului dumneavoastră întrebări directe sau îl îndeamnă să facă anumite acțiuni. Personajele pot pune întrebări cu recompense atrăgătoare, astfel încât copilul dumneavoastră să fie tentat să ofere detalii personale, ceea ce poate duce la încălcarea confidențialității sau la alte abuzuri grave.

Se recomandă supravegherea copiilor și activarea funcțiilor de *control parental*. De asemenea, asigurați-vă că aceștia înțeleg riscurile, chiar și în mică măsură, și nu furnizează informații sensibile necunoscuților.

➤ **Tranzacții online**

De fiecare dată când un utilizator dorește să facă o achiziție online, acesta trebuie să furnizeze informațiile cardului sau contului bancar. Acestea sunt niște informații foarte sensibile, tocmai de aceea se recomandă furnizarea acestor date numai în cadrul site-urilor web de încredere, securizate în mod corespunzător (utilizează protocolul HTTPS).



Referințe

<https://radio-waves.orange.com/ro/cum-functioneaza-un-telefon-mobil/>

<https://calculatorescu.ro/ce-este-internetul-istoria-internetului/>

https://ro.wikipedia.org/wiki/Istoria_Internetului

<https://www.lifewire.com/lan-wans-and-other-area-networks-817376>

<https://vivadifferences.com/lan-vs-man-vs-wan/>

<https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online>

<https://resources.infosecinstitute.com/topic/best-practices-web-browser-security/>

https://www.pcpd.org.hk/english/publications/files/internet_e.pdf



Agenția de Apărare Cibernetică