

# SUPORT ONLINE DE BUNE PRACTICI DE SECURITATE CIBERNETICĂ

**Autori: Denis Mihai CSEKE<sup>1</sup>,**  
[deniscseke@yahoo.com](mailto:deniscseke@yahoo.com)

**Coordonator: Conf. Univ. Dr. Ing. Simona RIUREAN<sup>2</sup>**

<sup>1</sup> *Universitatea, Facultatea, specializarea: Calculatoare, anul III*

<sup>2</sup> *Universitatea, Facultatea, Departamentul: ACIEE*

## Rezumat

Lucrarea de față prezintă un blog realizat cu suport AI pe care îl consider util în eforturile mele de educare și conștientizare a utilizatorilor (de orice vârstă, nivel de educație sau cunoștințe tehnice în domeniul IT) în privința amenințărilor de securitate cibernetică. Prin intermediul acestui blog, utilizatorii au acces la informații actualizate și sfaturi utile pentru a-și proteja datele personale și dispozitivele în mediul online. Blogul conține o serie de bune practici și trimiteri către știri de actualitate prin hiperlegături către surse legitime de informare. Un aspect important al blog-ului este interactivitatea, deoarece oferă utilizatorilor posibilitatea de a interacționa cu conținutul și de a-și testa cunoștințele prin completarea unui chestionar referitor la cunoștințele minime necesare de securitate cibernetică. În plus, are un design atractiv, este ușor de navigat și are un limbaj accesibil ceea ce face ca informațiile să fie ușor de înțeles și de aplicat în practică de orice tip de utilizator indiferent de nivelul de cunoștințe în domeniul tehnologic.

## Cuvinte cheie

conștientizare, phishing, smishing, vishing quishing

### 1. Introducere

De-a lungul timpului, amenințările cibernetice au devenit din ce în ce mai frecvente dar și mai sofisticate odată cu apariția aplicațiilor de inteligență artificială (AI). Întrucât tehnologia devine o parte integrantă a vieții noastre, este important ca oamenii să fie informați și să înțeleagă riscurile pe care le implică navigarea pe internet, de aceea, educația și conștientizarea privind amenințărilor de securitate online este esențială într-o lume digitală în continuă schimbare [1].

În urma unei cercetări amănunțite, am constatat că, deși există câteva bloguri informative referitoare la securitatea cibernetică, cele mai multe se adresează companiilor [2-5], copiilor și adolescenților [6-9] sau persoanelor care au cunoștințe în domeniul IT [10,11] dar nu am găsit surse digitale informative care să se adreseze tuturor utilizatorilor de internet, inclusiv seniorilor și care să fie utile, să fie simple conceptual și care să conțină exemple practice și indicații tehnice ușor de înțeles și aplicat, chestionare cu scop educativ și link-uri către surse legitime.

În figura 1 este prezentat blogul realizat de mine cu instrumentul AI Durable, AI Blog builder [12].



**Fig. 1. Blogul Upet Cybersecurity**

### 2. Tipuri de atacuri cibernetice și amenințări de securitate privind datele personale și echipamentele digitale

Cele mai frecvente forme de atacuri cibernetice și amenințări de securitate privind datele personale și echipamentele digitale sunt cele care au la bază ingineria socială și anume cele de tip phishing, smishing, vishing, quishing, shoulder surfing, credential Harvester/Harvesting, scam-uri, juice jacking precum și, eavesdropping, man in the middle. Toate aceste forme de atacuri cibernetice au ca scop obținerea neautorizată a datelor personale sensibile.

Phishing-ul este o formă de atac cibernetic care încearcă să înșele utilizatorii să dezvăluie informații sensibile, cum ar fi parolele și numerele cardurilor de credit. Atacurile de phishing provin de la escroci deghizați ca surse de încredere și pot facilita accesul la toate tipurile de date confidențiale [13].

Smishing-ul este o formă de phishing care utilizează mesaje text (SMS). Atacatorii trimit mesaje text false, într-o încercare de a obține datele personale ale victimelor. Aceste mesaje false pot părea că provin din surse în care persoanele atacate ar avea încredere, precum familia, prietenii, șefii, IRS sau banca [14].

Vishing-ul, sau voice phishing, este o formă de phishing care utilizează apeluri telefonice. Atacatorii se deghizează în entități de încredere pentru a păcăli victimele să dezvăluie informații sensibile<sup>3</sup>. Aceste atacuri pot fi foarte eficiente atunci când sunt folosite „live” la telefon [15].



**Fig. 2.** Secțiunea Tipuri de atacuri cibernetice și amenințări de securitate privind datele personale și echipamentele digitale din Blogul Upet Cybersecurity

Quishing, sau QR code phishing, este o formă de phishing care utilizează coduri QR. Atacatorii creează coduri QR false care, atunci când sunt scanate, conduc la site-uri web frauduloase sau solicită descărcarea de software dăunător [16].

Shoulder surfing este o tehnică în care un atacator observă sau înregistrează de la distanță datele de autentificare (cum ar fi parolele sau PIN-urile) ale unei persoane în timp ce aceasta le introduce pe un dispozitiv, cum ar fi un telefon mobil sau un ATM. Acest lucru poate fi realizat simplu, privind peste umărul victimei sau prin utilizarea camerelor video sau a dispozitivelor de înregistrare.

Un credential harvester (sau harvesting) este o tehnică utilizată în cadrul unui atac cibernetic în care atacatorii încearcă să obțină informații de autentificare (cum ar fi numele de utilizator și parola) ale victimelor. Aceste atacuri pot fi efectuate prin diferite mijloace, inclusiv prin intermediul site-urilor web false sau prin mesaje de phishing. Aatacatorii creează adesea pagini web sau alte mijloace care par a fi autentice (de exemplu, o pagină de conectare la un serviciu online), dar care în realitate sunt controlate de ei. Când utilizatorii introduc informațiile lor de autentificare pe aceste pagini false, atacatorii le capturează informațiile și le folosesc pentru a accesa conturile victimelor sau pentru a le vinde pe piața neagră.

Scam-urile (escrocheriile) sunt diverse scheme frauduloase utilizate pentru a înșela oamenii și a le fura bani sau informații personale. Credential harvesting este doar una dintre multele tactici pe care le pot folosi escrocii pentru a păcăli oamenii să dezvăluie informații sensibile sau să facă plăți înșelătoare prin intermediul e-mailuri false, site-uri web false, apeluri telefonice sau alte mijloace. De cele mai multe ori, scam-urile sunt elaborate pentru a părea credibile și pentru a induce în eroare victimele nevinovate. Este important să fim vigilenți și să fim conștienți de astfel de tacticile pentru a ne proteja împotriva lor. Cu această tehnică de atac cibernetic infractorii cibernetici colectează în masă acreditările utilizatorilor - cum ar fi ID-urile de utilizator, adresele de e-mail, parolele și alte informații de autentificare pentru a accesa sisteme și a colecta date sau alte informații sensibile, pentru a le vinde sau a le împărtăși pe dark web, și/sau pentru a avansa un atac mai sofisticat [17].

Juice Jacking este un atac cibernetic în care atacatorii folosesc stații publice de încărcare sau porturi USB pentru a fura date de pe dispozitivul propriu sau pentru a instala programe malware [18].

Eavesdropping (ascultarea ilegală) implică interceptarea și ascultarea comunicațiilor electronice sau vocale între două sau mai multe părți, fără ca acestea să fie conștiente de acest lucru. Această interceptare poate avea loc în diverse medii, cum ar fi rețelele Wi-Fi nesecurizate, telefoanele mobile sau telefoanele fixe. Scopul poate fi de a obține informații sensibile, cum ar fi date personale, parole sau informații comerciale [19].

Man-in-the-middle attack (MiTM) este un tip de atac cibernetic în care un atacator interceptează comunicările dintre două părți (de exemplu, între un utilizator și un site web sau între două dispozitive) fără ca acestea să fie conștiente de aceasta. Atacatorul poate să fure sau să modifice datele transmise între părți, astfel încât să poată accesa informații sensibile sau să manipuleze comunicările într-un mod care să le avantajeze. Acest tip de atac este adesea folosit în încercările de a obține informații de autentificare sau date financiare [20].

### 3. Conștientizarea pericolelor de securitate în mediul online

Conștientizarea pericolelor de securitate în mediul online este un aspect crucial în protejarea datelor și a vieții private a utilizatorilor în era digitală. Pericolele pot fi diverse și pot include phishing-ul, malware-ul, cyberbullying-ul, furtul de identitate, violarea confidențialității personale în urma expunerii datelor sensibile personale și multe altele. Prin înțelegerea acestor riscuri și a modului în care acestea pot afecta viața lor online și offline, utilizatorii devin mai vigilenți și mai proactivi în adoptarea măsurilor de protecție adecvate. Conștientizarea poate fi promovată prin educație și formare, campanii de conștientizare, materiale informative și exemple concrete [21].

Furnizarea de informații detaliate despre diferitele amenințări cibernetice și modul în care acestea pot afecta utilizatorii, precum și instruirea lor în privința practicilor de securitate cibernetică, organizarea de campanii publice și evenimente de conștientizare a securității cibernetice pentru a atrage atenția asupra riscurilor și a promova comportamente sigure online, crearea și distribuirea de materiale informative, care să prezinte riscurile de securitate cibernetică și modalitățile de protecție, prezentarea de exemple concrete și studii de caz despre incidentele de securitate

cibernetică pentru a evidenția impactul acestor amenințări și importanța protejării datelor personale precum și folosirea tehnologiei pentru a monitoriza și a detecta potențialele amenințări cibernetice și pentru a oferi notificări și sfaturi de securitate utilizatorilor sunt câteva din cele mai importante metode de conștientizarea populației în ceea ce privește amenințările de securitate online [22].

Un studiu realizat de Poliția Română a arătat că, deși majoritatea utilizatorilor sunt activi pe internet și manifestă un nivel decent de precauție, există încă o serie de vulnerabilități și comportamente nesigure care necesită o atenție sporită. De exemplu, un procent semnificativ de utilizatori consideră că postarea de fotografii personale pe rețelele de socializare sau descărcarea de conținut piratat nu prezintă riscuri majore [23].

Există resurse disponibile, cum ar fi "Ghidul utilizării în siguranță a Internetului", [24] care ajută utilizatorii să înțeleagă mai bine aceste riscuri și să navigheze în siguranță în mediul online. Acestea oferă sfaturi și strategii pentru a se proteja împotriva amenințărilor online și pentru a naviga în mod responsabil și etic în peisajul digital. Prin creșterea nivelului de conștientizare a pericolelor de securitate în mediul online, utilizatorii pot lua măsuri proactive pentru a-și proteja datele și a-și reduce expunerea la riscuri cibernetice. Această conștientizare este esențială pentru a promova un mediu online mai sigur și mai securizat pentru toți utilizatorii [25].

#### 4. Sfaturi utile pentru protejarea datelor personale și dispozitivelor precum și o navigare online în siguranță

##### 4.1. Importanța parolelor puternice

Importanța unei parole puternice în securitatea online este crucială pentru protejarea datelor și a conturilor personale împotriva accesului neautorizat. O parolă puternică este unul dintre cei mai eficienți factori de protecție împotriva atacurilor cibernetice, deoarece dificultățile în ghicirea sau spargerea unei parole pot descuraja potențialii infractori. O parolă puternică este caracterizată de o combinație de litere majuscule și minuscule, cifre, caractere speciale și o lungime adecvată, ceea ce face aproape imposibilă ghicirea sau forțarea ei prin metode brute sau algoritmice. Ea trebuie să conțină minim 8 caractere, majuscule, litere mici, numere și un caracter special (!@#\$%^&\*()) și să nu conțină detalii personale. Prin urmare, alegerea și utilizarea unei parole puternice pentru conturile online este esențială pentru a proteja informațiile personale și financiare, precum și pentru a preveni eventualele consecințe negative ale accesului neautorizat la date.

Un studiu privind comportamentul adulților din România în mediul online derulat în 2024 arată că doar 21% dintre respondenți schimbă periodic parolele pentru toate conturile personale (figura 3) [26].

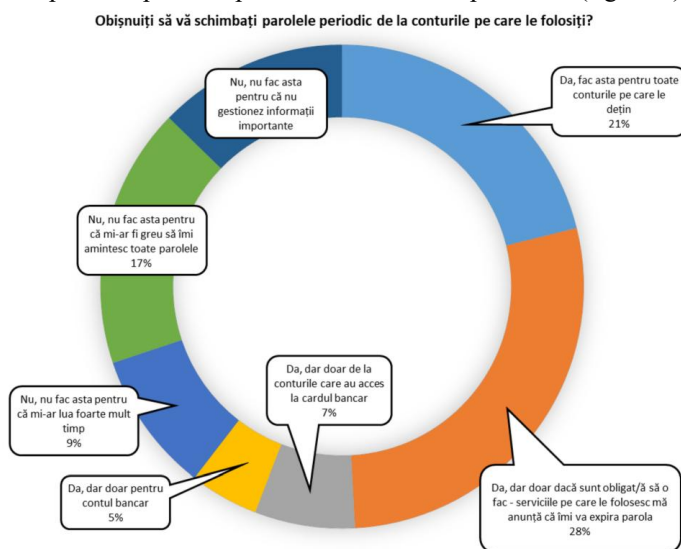


Fig. 3. Rezultatul sondajului Institutului de Cercetare și Prevenire a Criminalității, 2024 Sursa: [26]

Este importantă utilizarea unui manager de parole. Alegerea unui manager de parole depinde de preferințele personale, nivelul de securitate dorit și bugetul disponibil. Se pot utiliza oricare din instrumentele NordPass, LogMeOnce, KeePass, Avira Password Manager sau Bitwarden [27].

NordPass este un serviciu simplu de gestionare a parolelor dezvoltat de echipa din spatele NordVPN, are acces securizat la parole prin aplicații desktop, mobile sau pe web. Ca dezavantaj, al acestei aplicații, versiunea gratuită deconectează utilizatorul atunci când schimbă dispozitivele și nu permite partajarea de parole [28].

LogMeOnce oferă o soluție de gestionare a parolelor pentru întreprinderi, cu o versiune gratuită disponibilă pentru afaceri mici, are autentificare multi-factor (MFA) iar versiunea gratuită are restricții, dar poate fi utilă pentru utilizatorii individuali [29].

KeePass este un manager de parole gratuit și sigur, dar poate fi mai dificil de utilizat decât majoritatea și nu este potrivit pentru utilizatorii non-tehnici. Stochează parolele într-o bază de date criptată local și are posibilitatea de personalizare și control complet asupra datelor utilizatorilor [30].

Avira Password Manager este o soluție simplă în care versiunea gratuită oferă stocarea parolelor și are o interfață ușor de utilizat [31].

Bitwarden este un manager de parole global, open-source, cu o versiune gratuită și una plătită. Are criptare puternică și sincronizare între dispozitive. Versiunea gratuită oferă funcționalități de bază, iar versiunea plătită adaugă funcționalități avansate [32].

#### **4.2 Politica unui birou curat**

Prin promovarea acestei mentalități de organizare, curățenie și securitate în mediul digital, utilizatorii își protejează mai bine datele personale și reduc expunerea la riscuri de securitate cibernetică atât acasă, cât și la locul de muncă sau pe dispozitivele lor mobile [33]. Principiile politicii unui birou curat pot fi cele de organizare și structurare, curățenie digitală și cele de confidențialitate și securitate. La fel cum organizăm documentele și obiectele importante într-un birou curat, ar trebui să organizăm și să structurăm datele digitale într-un mod similar. Acest lucru înseamnă să utilizăm instrumente de stocare și gestionare a datelor care să ofere protecție, precum servicii de stocare în cloud cu autentificare în doi pași sau aplicații de gestionare a parolelor. La fel cum aruncăm hârtiile și obiectele inutile din birou pentru a menține un mediu curat, ar trebui să eliminăm datele și fișierele digitale neutilizate sau nefolositoare pentru a reduce riscul de expunere la atacuri cibernetice. La fel cum ne asigurăm că documentele importante sunt păstrate într-un loc sigur și accesibil doar persoanelor autorizate, ar trebui să ne asigurăm că parolele și datele sensibile sunt protejate printr-o securitate adecvată, precum parole puternice și autentificare în doi pași [34].

#### **4.3. Navigarea pe internet în siguranță**

Navigarea pe internet se poate face în siguranță utilizând VPN, cunoscând diferența dintre HTTP și HTTPS, evitarea opțiunii "Keep me signed in", cunoașterea și evitarea tehnicii de hacking "cookie hijacking", ștergerea memoriei cache a browser-ului.

VPN (Virtual Private Network) este o rețea privată virtuală care asigură confidențialitatea datelor prin criptare și schimbarea adresei IP. Acesta este un instrument care oferă un nivel superior de securitate cibernetică. Conectarea la un VPN, permite conectarea la un server îndepărtat oferit de furnizorul de internet. Astfel, datele sunt protejate și se creează acces la conținut geo-blocat, chiar și pe conexiuni Wi-Fi publice. VPN-urile sunt esențiale pentru protecția datelor, mai ales când se realizează conexiunea la un Wi-Fi public [35,36].

HTTP (Hypertext Transfer Protocol) este un protocol la nivel de aplicație din suita de protocoale Internet utilizat ca principal sistem de transmitere a informațiilor pe World Wide Web. În schimb, HTTPS (Hypertext Transfer Protocol Secure) este o extensie a protocolului HTTP care oferă mai multă securitate datelor transmise printr-un Secure Socket Layer (SSL). Principala diferență între HTTP și HTTPS este certificatul SSL3. Website-ul care se încarcă pe HTTPS îl folosește pentru a trimite și primi informațiile în stare criptată. În schimb, pe HTTP, datele sunt trimise în format text, care poate fi citit ușor de oricine [37].

Opțiunea "Keep me signed in" (rămâi autentificat) este o caracteristică comună pe multe site-uri web și aplicații care permite menținerea statusului autentificat pe dispozitivul propriu, chiar și după s-a închis browser-ul sau aplicația. Aceasta este o caracteristică convenabilă care economisește timp, deoarece nu va trebui introdus din nou numele de utilizator și parola de fiecare dată când se vizitează site-ul sau se utilizează aplicația. Cu toate acestea, există și unele riscuri de securitate asociate cu utilizarea acestei opțiuni. Dacă dispozitivul este pierdut sau furat, oricine îl găsește va avea acces la conturile personale [38].

Cookie Hijacking este o tehnică de hacking prin care se fură o sesiune de la un utilizator pentru a accesa contul acestuia. Atacatorii folosesc atacurile de tip Cookie Hijacking pentru a compromite contul personal atunci când utilizatorul se autentifică, de exemplu pe contul propriu de pe rețelele sociale, cum ar fi LinkedIn, Meta sau Instagram. Un atac de tip Cookie Hijacking implică, de obicei, injectarea de cod JavaScript într-un site web prin încorporarea acestuia în HTML-ul unui e-mail sau al unei reclame care pare autentice. Acest cod rău intenționat este apoi executat de browser atunci când utilizatorul vizitează site-ul infectat. Acceptarea fiecărei solicitări de cookie nu este necesară sau benefică. Unele cookie-uri sunt plasate de către părțile principale, cum ar fi site-urile vizitate, pentru a te ajuta să navighezi mai ușor, să setezi preferințe, să salvezi articole într-un coș de cumpărături etc. Alte tipuri de cookie-uri sunt plasate de către terțe părți, cum ar fi "advertiser-ii". Acestea pot urmări comportamentul de navigare și pot colecta date despre acesta, trimițându-le înapoi site-urilor web [39,41].

Ștergerea memoriei cache a browser-ului implică eliminarea informațiilor temporare stocate de browser pentru a îmbunătăți viteza de încărcare a paginilor web. Aceste informații pot include imagini, stiluri CSS și JavaScript de pe site-urile pe care le-ai vizitat. După ce goliți memoria cache și ștergeți cookie-urile, anumite setări ale site-urilor sunt șterse. În Chrome, se poate accesa opțiunea de ștergere a datelor de navigare prin meniul "Mai multe" din dreapta sus iar în Microsoft Edge, din meniul "Setări și multe altele" din colțul din dreapta sus al browser-ului [42].

#### **4.4. Securizarea rețelei de acasă, soluții antivirus, anti-malware și actualizarea SO și apps**

Un LAN (Local Area Network) este un grup de computere sau alte dispozitive interconectate într-o singură zonă limitată, de obicei prin Ethernet sau Wi-Fi. Dispozitivele dintr-o rețea LAN, de obicei computerele personale și laptop-urile, pot partaja fișiere și pot fi accesate între ele utilizând o conexiune la Internet. Securizarea rețelei de acasă presupune schimbarea credențialelor default ale router-ului deoarece hackerii încearcă în mod constant să obțină acces la dispozitive, folosind aceste informații cunoscute public, utilizarea de parole diferite pentru Wi-Fi și router pentru a preveni accesul neautorizat la setările router-ului dacă parola Wi-Fi este compromisă, actualizarea regulată a firmware-ului router-ului deoarece patch-urile de securitate și remedierile de erori vor fi inserate în cel mai recent firmware pentru a remedia problemele rețelei [43-51].

Utilizarea soluțiilor antivirus este esențială pentru a proteja dispozitivele personale împotriva amenințărilor cibernetice. Acestea pot include viruși, troieni, ransomware și alte tipuri de malware care pot compromite securitatea datelor și performanța sistemului. Există pe piață o serie de soluții antivirus gratuite Bitdefender Antivirus Free Avast Free Antivirus AVG AntiVirus Free și cu plată Norton Antivirus Bitdefender Antivirus Plus sau McAfee Total Protection [52-60].

Actualizările pot îmbunătăți performanța software-ului, făcându-l mai rapid și mai eficient. Este important să menținem dispozitivele personale actualizate și patch-uite pentru a rezolva vulnerabilităților de securitate, a îmbunătăți performanța și a stabilitatea dispozitivelor și a preveni expunerea la amenințările noi, pentru că, lansarea constantă de noi amenințări cibernetice necesită o vigilență continuă din partea utilizatorilor. Este esențial să menținem sistemele de operare și soft-urile actualizate pentru a ne asigura că dispozitivele personale sunt protejate, eficiente și în pas cu cele mai recente inovații tehnologice [61-68].

## 5. Conținut interactiv

Blogul conține de asemenea, o serie de trimeri (hiperlegături) către surse de informații legitime (cum sunt DNSC sau Microsoft) dar și un chestionar (realizat în Google Forms) de testarea cunoștințelor minime de protecția datelor personale și dispozitivelor utilizatorilor (figura 4.).



Fig. 4. Sondaj și sfaturi legitime cu hiperlegături

## Concluzii

Blogul realizat evidențiază faptul că siguranța datelor personale și a dispozitivelor în mediul online trebuie să fie o preocupare importantă pentru toți utilizatorii de dispozitive inteligente care accesează rețeaua internet. Este important să ne amintim că navigarea sigură pe internet necesită mai mult decât doar cunoașterea riscurilor. Necesită și aplicarea constantă a măsurilor de protecție adecvate, cum ar fi schimbarea periodică a parolelor, evitarea deschiderii link-urilor din e-mailuri necunoscute și furnizarea cu precauție a datelor personale pe internet. În continuare îmi propun să dezvolt blogul prin postarea de exemple de e-mail-uri de tip phishing și e-mail-uri ce impersonează entități legitime (bănci, provider de internet, centre de sănătate, etc) pentru ca utilizatorii să facă diferența dintre un e-mail legitim și un atac din oricare din categoria menționată la tipurile de atacuri cibernetice și amenințări de securitate privind datele personale și echipamentele digitale.

## Bibliografie

1. <https://support.microsoft.com/ro-ro/windows/proteja%C8%9Bi-v%C4%83-%C3%AEmpotriva-atacurilor-de-tip-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44>
2. <https://www.thc.ro/blog/securitatea-cibernetica-ce-este-si-de-ce-este-importanta-pentru-securitatea-afacerii/>
3. <https://fotc.com/ro/blog/practici-securitate-cibernetica/>
4. <https://blog.eset.ro/cybersecurity/construirea-unei-lumi-digitale-mai-sigure-de-ce-conteaza-securitatea-cibernetica/>
5. <https://www.microsoft.com/ro-ro/security/business/security-101/what-is-cybersecurity>
6. <https://www.bitdefender.ro/blog/hotforsecurity/de-ce-ar-trebuie-sa-iti-inveti-copiii-despre-securitatea-cibernetica/>
7. <https://www.blog.bloomcoding.ro/2021/11/02/securitatea-cibernetica-si-siguranta-in-mediul-online/>
8. <https://blog.eset.ro/how-to/game-on-6-jocuri-care-ajuta-ca-invatarea-despre-securitatea-cibernetica-sa-fie-distractiva/>
9. <https://www.edupedu.ro/cursuri-online-despre-siguranta-in-spatiul-virtual-pentru-elevi-si-adulti-lansate-gratuit-de-directoratul-pentru-securitate-cibernetica-copiii-pot-invata-ce-inseamna-dependenta-de-internet-si-sa-is/>
10. <https://www.nav.ro/blog/7-inovatii-tehnologice-in-securitate-cibernetica/>
11. <https://teachbit.ro/blog/securitate-cibernetica-cum-sa-incepi/> <https://ramonnastase.ro/blog/curs-securitate-cibernetica/>

12. <https://durable.co/>
13. <https://www.microsoft.com/ro-ro/security/business/security-101/what-is-phishing>
14. <https://useit.ro/digital/ce-e-smishing-si-cum-functioneaza-inselatoria-poate-fi-extrem-de-periculoasa-pentru-victime-17655.html>
15. <https://blog.eset.ro/malware/vishing-ce-este-si-cum-evit-acest-scam/>
16. <https://useit.ro/digital/ce-e-quishing-si-cum-functioneaza-inselatoria-poate-fi-extrem-de-periculoasa-pentru-victime-32510.html>
17. <https://www.crowdstrike.com/cybersecurity-101/cyberattacks/credential-harvesting/>
18. <https://securitypatch.ro/juice-jacking-ce-este-si-cum-functioneaza/>
19. <https://itigic.com/ro/wi-fi-eavesdropping-attacks-when-using-public-networks/>
20. <https://www.bitdefender.ro/blog/hotforsecurity/tabelul-lui-malwareev-elementul-man-middle-mitm/>
21. <https://dnsc.ro/vezi/document/ghid-securitate-cibernetica-2021>
22. <https://bit-sentinel.com/ro/4-lucruri-de-facut-in-cazul-unui-incident-de-securitate/>
23. <https://revista.universuljuridic.ro/drepturile-digitale-si-protectia-lor-mediul-online-reprezentarea-cetatenilor-ue/>
24. <https://oradenet.ro/wp-content/uploads/2023/10/ghidul-sigurantei-in-mediul-online-digital-1.pdf>
25. <https://socialweb.ro/10-sfaturi-utile-pentru-a-fi-in-siguranta-pe-internet/>
26. [https://www.politiaromana.ro/files/pages\\_files/Siguranta\\_pe\\_internet.pdf](https://www.politiaromana.ro/files/pages_files/Siguranta_pe_internet.pdf)
27. <https://www.pcmag.com/picks/the-best-free-password-managers>
28. <https://nordpass.com/>
29. <https://logmeonce.com/>
30. <https://keepass.info/>
31. <https://passwords.avira.com/login>
32. <https://bitwarden.com/>
33. <https://xontech.md/news/cele-12-elemente-ale-unei-politici-de-securitate-a-informatiilor/>
34. <https://kitgdpr.ro/wp-content/uploads/2018/01/kit-gdpr-politica-birou-curat---ecran-curat.pdf>
35. <https://nerdist.ro/ce-este-un-vpn/>
36. <https://www.digitalcitizen.ro/cum-creezi-si-configurazi-o-conexiune-vpn-windows-10/>
37. <https://omulbun.com/care-este-diferenta-dintre-http-si-https/>
38. [https://answers.microsoft.com/en-us/outlook\\_com/forum/all/turn-on-keep-me-signed-in-option/fdde7ca3-1d5f-4fbc-b619-5c6090a6cfl1e](https://answers.microsoft.com/en-us/outlook_com/forum/all/turn-on-keep-me-signed-in-option/fdde7ca3-1d5f-4fbc-b619-5c6090a6cfl1e)
39. <https://securityintelligence.com/articles/guide-to-cookie-hijacking/>
40. <https://www.geeksforgeeks.org/what-is-cookie-hijacking/>
41. <https://keepnetlabs.com/blog/what-is-cookie-hijacking-aka-session-hijacking>
42. <https://us.norton.com/blog/privacy/should-i-accept-cookies>
43. Riurean S.M., Concepte si tehnologii noi de comunicatii in arhitecturi de retele, Ed.Universitas Petrosani, 2023
44. <https://www.makeuseof.com/do-you-really-need-accept-all-cookies/>
45. <https://cyberguy.com/security/a-beginners-guide-to-cookies-accept-or-reject/>
46. <https://www.33rdsquare.com/is-it-ok-to-accept-all-cookies/>
47. <https://support.google.com/accounts/answer/32050?hl=ro&co=GENIE.Platform%3DDesktop>
48. <https://www.bitdefender.ro/consumer/support/answer/21852/>
49. <https://ik4.es/ro/cum-s%C4%83-%C8%99terge%C8%9Bi-memoria-cache-a-browserului-web/>
50. <https://help.webex.com/ro-ro/article/WBX9000035442/Clear-Cache-and-Cookies-in-Microsoft-Edge>
51. <https://blog.hostx.ro/utile/ce-este-o-retea-lan-local-area-network/>
52. <https://www.tp-link.com/ro/blog/79/ce-reprezinta%C4%83-securitatea-re%C8%9Belei-de-acas%C4%83-%C8%99i-cum-%C3%AEmi-pot-securiza-routerul-wi-fi/>
53. <https://www.nav.ro/blog/10-sfaturi-pentru-a-fi-in-siguranta-pe-internet-in-2019/>
54. <https://calculatorescu.ro/ce-inseamna-lan/>
55. <https://gadgetreport.ro/ai-router-wireless-10-masuri-esenitale-de-securitate/>
56. <https://ro.safetydetectives.com/blog/cele-mai-bune-programe-cu-adevarat-gratuite-antivirus-pentru-windows/>
57. <https://ro.safetydetectives.com/blog/cel-mai-bun-antivirus-gratuit/>
58. <https://netitworks.ro/blog/2024/importanta-actualizarii-firmware-ului-si-a-patch-urilor-de-securitate/>
59. <https://fixthephoto.com/ro/antivirus-gratuit.html>
60. <https://ro.safetydetectives.com/best-antivirus/windows/>
61. <https://support.microsoft.com/ro-ro/topic/important-actualiz%C4%83ri-de-securitate-windows-%C8%99i-antivirus-software-4fbc7b34-b27d-f2c4-ee90-492ef383fb9c>
62. <https://ro.safetydetectives.com/>
63. <https://quantumdatascience.ro/ce-inseamna-actualizare-software/>
64. <https://itigic.com/ro/ways-to-update-major-operating-systems/>
65. <https://support.microsoft.com/ro-ro/windows/>
66. <https://www.isidors.ro/actualizare-software/>
67. <https://www.networld.ro/actualizare-software-la-zi/>
68. <https://news.microsoft.com/ro-ro/2022/09/21/versiunea-actualizata-a-sistemului-de-operare-windows-11>