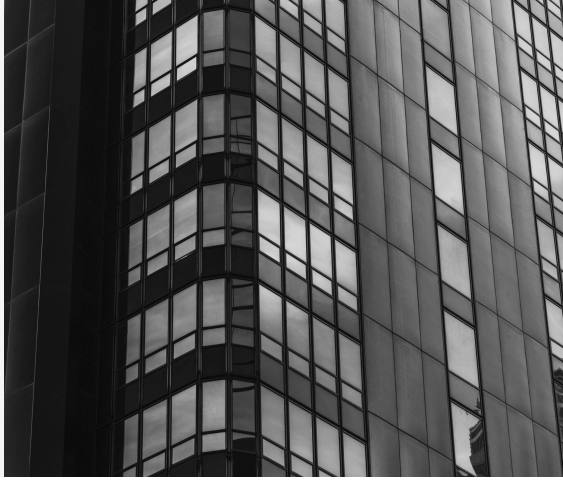
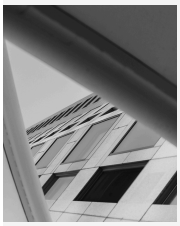
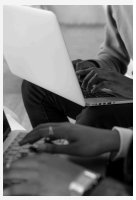
Cum să te protejezi în mediul digital ?





Siguranța în mediul online este esențială, mai ales pentru copii și adolescenți.
Acest ghid oferă măsuri practice pentru a proteja identitatea, datele personale și securitatea financiară în mediul virtual.



Reguli esențiale pentru protecția identității și securitatea online

1. Protejarea identității personale
Nu folosi numele tău real pe rețelele de socializare; este mai sigur să alegi un nickname pentru a-ți proteja identitatea. Creează conturi de social media utilizând o adresă de e-mail care nu conține numele tău real, astfel încât să fie mai dificil pentru alte persoane să te identifice. Nu dezvălui pe internet informații personale, precum adresa casei tale, numărul de telefon sau alte date care ar putea fi utilizate împotriva ta. De asemenea, evită să postezi fotografii sau videoclipuri care arată locația exactă a locuinței tale, deoarece acestea pot oferi indicii despre unde locuiești.

2. Protecția conturilor online
Pentru a-ți proteja conturile, folosește parole puternice și unice pentru fiecare platformă pe care o utilizezi. Activează autentificarea în doi pași (2FA) oriunde este posibil, pentru un nivel

suplimentar de securitate. Schimbă parolele periodic, ideal la fiecare 3-6 luni, și nu le împărtăși cu alte persoane, chiar dacă ai încredere în ele.

3. Atenție la interacțiunile online
Nu accepta cereri de prietenie de la persoane necunoscute și fii precaut atunci când primești mesaje suspecte, mai ales dacă cineva îți cere informații personale. Dacă o persoană insistă să afle detalii despre tine sau încearcă să te manipuleze, discută imediat cu un adult de încredere.

4. Evitarea expunerii excesive
Nu publica informații despre programul tău zilnic, cum ar fi când ești acasă sau când pleci în vacanță, deoarece acest lucru te poate face vulnerabil în fața infractorilor. De asemenea, evită să postezi imagini cu obiecte de valoare, bani sau gadgeturi scumpe, deoarece acestea pot atrage atenția hoților. Nu dezvălui locul unde înveți sau locurile pe care le frecventezi des, pentru a preveni situațiile în care cineva ar putea încerca să te urmărească.

5. Siguranța la plățile online
Atunci când cumperi produse online, utilizează un card de unică folosință sau un cont bancar separat pentru plăți, pentru a minimiza riscul în cazul unei fraude. Înainte de a introduce datele cardului, verifică dacă site-ul este securizat (trebuie să aibă conexiune „https” și recenzii pozitive de la alți utilizatori). De asemenea, evită să salvezi datele cardului pe platformele online, deoarece acestea pot fi compromise în cazul unui atac cibernetic.

6. Verificarea informațiilor înainte de a le distribui
Nu crede orice citești pe internet și asigură-te că verifici sursa informațiilor înainte de a le distribui. Evită să răspândești știri false sau conținut dubios, deoarece acest lucru poate contribui la dezinformare și poate afecta alte persoane.

7. Protecția împotriva atacurilor informatice
Nu descărca fișiere sau aplicații din surse necunoscute, deoarece acestea pot conține viruși sau programe malițioase. Instalează un antivirus de încredere și menține-l actualizat pentru a te proteja împotriva amenințărilor cibernetice. De asemenea, evită să dai click pe linkuri suspecte primite prin e-mail sau mesaje, deoarece acestea pot fi încercări de phishing pentru a-ți fura datele personale.

8. Prevenirea cyberbullying-ului
Dacă ești victima hărțuirii online, nu răspunde provocărilor și blochează imediat persoana respectivă. Păstrează dovezi, cum ar fi capturi de ecran, și anunță un adult de încredere sau autoritățile competente pentru a lua măsurile necesare.

9. Protejarea locației
Dezactivează funcția de geolocalizare în postările și aplicațiile care nu au nevoie de această opțiune, pentru a preveni divulgarea involuntară a locației tale. De asemenea, nu distribui locația ta în timp real pe rețelele sociale, deoarece acest lucru poate pune în pericol siguranța ta.

10. Gestionarea timpului petrecut online
Stabilește limite clare pentru timpul petrecut pe internet, astfel încât să ai un echilibru sănătos între activitățile online și cele offline. Implică-te în activități care nu necesită utilizarea ecranelor, cum ar fi sportul, lectura sau întâlnirile cu prietenii și familia, pentru a menține o viață echilibrată și sănătoasă.
11. Utilizarea unei adrese de e-mail separate pentru conturile importante – Creează și folosește adrese de e-mail diferite pentru rețelele sociale, servicii bancare și conturile de muncă sau școală. Astfel, dacă una dintre ele este compromisă, celelalte rămân în siguranță.

12. Evitarea folosirii aceleași poze de profil pe mai multe platforme – Persoanele rău intenționate pot folosi căutarea inversă a imaginilor pentru a descoperi alte conturi legate de tine.

Căutarea inversă a imaginilor este o tehnică prin care cineva poate încărca o fotografie pe un motor de căutare, precum **Google Images**, **TinEye** sau **Yandex**, pentru a găsi alte site-uri unde apare aceeași imagine.

De exemplu, dacă folosești aceeași poză de profil pe mai multe platforme (Meta, Instagram, LinkedIn etc.), cineva poate descărca acea imagine și o poate folosi pentru a găsi toate conturile tale asociate. Astfel, un necunoscut ar putea afla mai multe informații despre tine, inclusiv numele real, locul de muncă, interesele sau cercul social.

Pentru a preveni acest lucru, este recomandat să folosești poze de profil diferite pe fiecare platformă sau să folosești imagini editate (de exemplu, decupate, cu un filtru aplicat) pentru a îngreuna identificarea automată a acestora prin căutare inversă.

13. Folosirea unui VPN de încredere – Un VPN (Virtual Private Network) îți protejează datele criptând conexiunea și ascunzând adresa IP. Evită VPN-urile gratuite, care pot colecta date despre tine. Câteva opțiuni sigure includ **NordVPN**, **ExpressVPN**, **ProtonVPN** .

Securitatea online

14. Evitarea conectării la rețele publice de Wi-Fi – Rețelele Wi-Fi gratuite din cafenele, aeroporturi sau hoteluri sunt nesigure și pot fi exploatate de hackeri pentru a intercepta datele transmise de dispozitivul tău. Dacă trebuie să te conectezi, folosește un VPN pentru protecție.

15. Folosirea unui manager de parole securizat – Un manager de parole îți generează și stochează în siguranță parole complexe pentru fiecare cont. Evită să le notezi în browser sau pe hârtie. Opțiuni sigure includ **Bitwarden, 1Password, NordPass** sau **KeePass**.

16. Verificarea permisiunilor aplicațiilor – Multe aplicații cer acces la camera, microfon sau contacte fără un motiv justificat. Revizuiește și restricționează permisiunile pentru a evita expunerea inutilă a datelor tale.

17. Monitorizarea activității conturilor – Verifică periodic activitatea conturilor tale și activează alertele de securitate pentru a fi notificat în cazul unor logări suspecte. Unele servicii, precum Google și Microsoft, oferă opțiuni de verificare a dispozitivelor conectate.

18. Ștergerea regulată a istoricului de navigare și a cookie-urilor – Site-urile web colectează multe informații despre tine prin cookie-uri. Curăță periodic istoricul și cookie-urile din browser pentru a preveni urmărirea activității tale online.

19. Atenție la aplicațiile de tip "free" sau "gratis"
Multe aplicații gratuite sau jocuri pentru copii pot conține reclame intruzive sau pot solicita permisiuni excesive pentru a colecta datele utilizatorilor. Este important să verifici cu atenție permisiunile aplicațiilor înainte de a le descărca și să citești recenziile altor utilizatori pentru a te asigura că aplicația este sigură. În plus, părinții ar trebui să monitorizeze aplicațiile pe care le descarcă copiii și să folosească setările de control parental pentru a preveni accesul la aplicații sau jocuri neadecvate.

20. Înțelegerea și prevenirea phishing-ului
Phishing-ul este o metodă prin care atacatorii încearcă să obțină informații sensibile (parole, date bancare, nume de utilizator) prin e-mailuri sau mesaje false, care par să provină de la o sursă de încredere (ex. bancă, site de cumpărături, platforme sociale). Atunci când primești mesaje care solicită date personale sau linkuri pentru a-ți "verifica contul" sau "recupera parola", fii foarte atent! Nu da click pe linkuri din mesaje dubioase și, în schimb, deschide site-ul direct în browser pentru a verifica dacă este o solicitare reală.

21. Verificarea unui site înainte de a face achiziții sau a introduce informații personale
Înainte de a introduce orice informație personală sau de a efectua o achiziție online, asigură-te că site-ul este legitim și sigur. Verifică următoarele elemente:

- **Adresa URL**: Asigură-te că site-ul are o conexiune securizată (URL-ul trebuie să înceapă cu „https” și nu „http”). Litera „s” semnifică faptul că datele tale sunt criptate.
- **Certificat SSL**: Căută un simbol de lacăt în bara de adrese din browser, ceea ce indică un certificat SSL valid, care protejează datele tale.
- **Recenzii și feedback**: Verifică recenziile altor utilizatori și căută recenzii externe despre site-ul respectiv. Site-urile de încredere de obicei au recenzii pozitive și un istoric clar.
- **Detalii de contact**: Un site legitim trebuie să aibă informații de contact clare și accesibile (adresă fizică, număr de telefon, e-mail). Dacă acestea sunt absente sau vagi, ar trebui să fii precaut.
- **Design-ul și navigarea**: Fii atent la aspectul site-ului. Dacă pare ieftin, greu de navigat sau plin de reclame dubioase, este un semn că ar putea fi nesigur.

22. Instalează și actualizează un antivirus de încredere

Este esențial să instalezi un software antivirus, cum ar fi **Bitdefender**, pe toate dispozitivele tale (computer, smartphone, tabletă) pentru a proteja împotriva virușilor, malware-ului și altor amenințări cibernetice. Asigură-te că antivirusul este întotdeauna actualizat, astfel încât să poți detecta cele mai noi tipuri de atacuri. Multe dintre aceste soluții antivirus, cum este Bitdefender, includ și protecție suplimentară pentru navigarea pe internet, blocarea site-urilor periculoase și protejarea plăților online.

Bitdefender este o companie globală de securitate cibernetică, care oferă soluții pentru protejarea dispozitivelor împotriva amenințărilor informatice, cum ar fi viruși, malware, ransomware și atacuri de tip phishing. Bitdefender dezvoltă software antivirus și soluții de securitate care protejează computerele, smartphone-urile și alte dispozitive conectate la internet.

Printre cele mai populare produse Bitdefender se numără:

- **Bitdefender Antivirus**: Oferă protecție împotriva virușilor și malware-ului.
- **Bitdefender Internet Security**: Include protecție suplimentară pentru securitatea rețelei, firewall și protecție pentru plăți online.
- **Bitdefender Total Security**: Oferă o protecție completă pentru toate dispozitivele (Windows, Mac, Android, iOS), inclusiv protecție pentru identitatea online și copii.
- **Bitdefender Mobile Security**: Protejează dispozitivele mobile de amenințările cibernetice.

Bitdefender utilizează tehnologii avansate de detecție, precum inteligența artificială și analiza comportamentală, pentru a identifica și preveni amenințările cibernetice în timp real, fără a afecta performanța dispozitivelor. Este considerat unul dintre cele mai bune programe antivirus disponibile pe piață.

Acest ghid oferă pași simpli, dar esențiali, pentru a naviga în siguranță pe internet. Protejează-te și fii responsabil în mediul online!