
AGENȚIA DE APĂRARE CIBERNETICĂ

# GHID DE BUNE PRACTICI PENTRU UTILIZAREA PLATFORMELOR SOCIALE ȘI SECURIZAREA CONTURILOR DIN CADRUL ACESTORA

# CUPRINS

Social Media

# DEFINIȚIE

Termenul de social media definește un ecosistem de platforme digitale (site-uri, aplicații și servicii online) care permit crearea, distribuirea și interacțiunea cu conținut generat de utilizatori (text, imagini, video sau audio). Aceste platforme folosesc algoritmi de recomandare pentru a personaliza conținutul afișat utilizatorilor și facilitează comunicarea în timp real între utilizatori, comunități și instituții.

Rețelele sociale oferă utilizatorilor o comunicare rapidă pentru a împărtăși conținut media, informații personale, documente, fotografii, videoclipuri, etc.

Blogurile, forumurile, rețelele sociale (Facebook, Instagram, LinkedIn, TikTok), platformele de conținut video (YouTube, Twitch), aplicațiile de mesagerie (WhatsApp, Messenger, Telegram, Discord), platformele de comunități (Reddit), precum și platformele de conținut scurt sau algoritmic (TikTok, Instagram Reels, YouTube Shorts) sunt exemple de instrumente de social media.

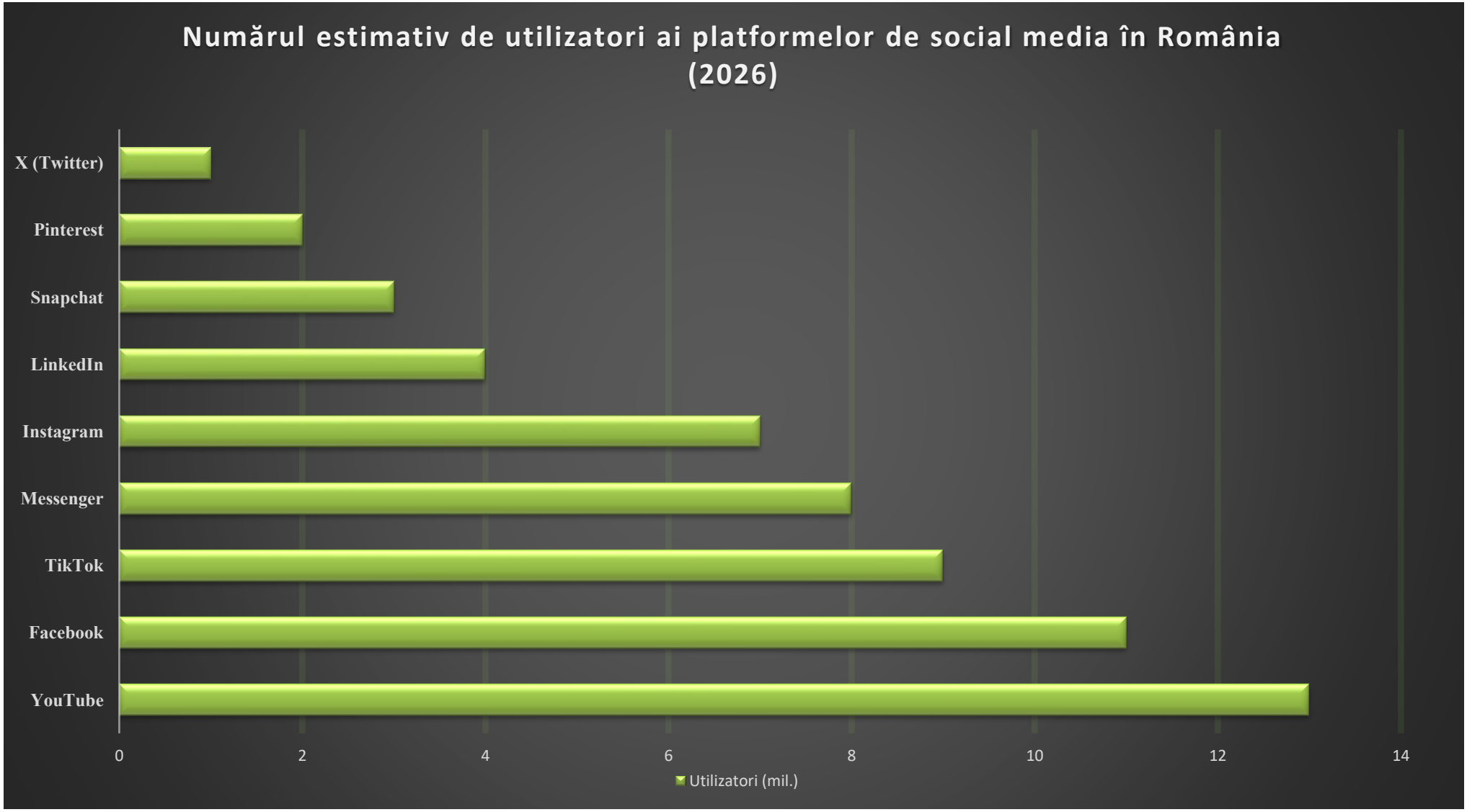
# SOCIAL MEDIA ÎN ROMÂNIA

Devenit un trend la nivel global, peste jumătate din populația planetei este activă pe cel puțin o platformă de social media. Conform statisticilor, în medie, un utilizator normal petrece în fiecare zi aproximativ 145 de minute pe o astfel de platformă.

În România, platforma Facebook, fondată în anul 2004, a fost vârful de lance al conceptului de social media. Facebook a adus interacțiunea socială la un nou nivel, iar oamenii au fost imediat atrași. Acest lucru s-a văzut imediat în cifrele înregistrate. În ianuarie 2010, platforma înregistra 500.000 de conturi de utilizatori, iar un an mai târziu, numărul de conturi a ajuns la 2,4 milioane.

În 2026, numărul utilizatorilor de social media din România este estimat la aproximativ **15 milioane**, reprezentând peste **78%** din populația țării. Utilizarea rețelelor sociale a crescut constant, iar platformele dominante sunt cele bazate pe conținut

**video** și algoritmi de recomandare.



# BENEFICIILE SOCIAL MEDIA

Platformele de social media au devenit un instrument important în viața de zi cu zi, fiind utilizate atât pentru comunicare, cât și pentru informare, divertisment sau dezvoltare profesională. Acestea oferă numeroase avantaje, atât pentru utilizatorii individuali, cât și pentru instituții.

## Posibilități de comunicare 24/24


Platformele de socializare permit comunicarea rapidă și eficientă între utilizatori, indiferent de locația geografică. Mesajele, apelurile video sau grupurile online facilitează colaborarea, schimbul de idei și menținerea relațiilor personale și profesionale.

## Acces rapid la informații

Rețelele sociale oferă acces imediat la o cantitate mare de informații din diverse domenii. Utilizatorii pot urmări evenimente în timp real, pot accesa știri sau pot învăța lucruri noi prin conținut educațional distribuit de instituții, specialiști sau creatori de conținut.

## Divertisment și conținut personalizat

Platformele moderne utilizează algoritmi pentru a furniza conținut adaptat preferințelor utilizatorilor. Astfel, utilizatorii pot accesa videoclipuri, transmisiuni live sau alte forme de divertisment într-un mod rapid și personalizat.

## Oportunități de angajare și dezvoltare profesională

Social media joacă un rol important în procesul de recrutare și în dezvoltarea carierei. Platforme precum LinkedIn permit crearea unui profil profesional, identificarea oportunităților de angajare și interacțiunea directă cu angajatori sau specialiști din domeniu.

## Dezvoltarea și promovarea afacerilor

Instituțiile utilizează rețelele sociale pentru promovarea produselor și serviciilor, interacțiunea cu clienții și construirea unei imagini de brand. Aceste platforme permit targetarea publicului și adaptarea strategiilor de marketing în funcție de comportamentul utilizatorilor.

## Educație și învățare online

Platformele de social media sunt utilizate tot mai frecvent pentru educație și formare profesională. Utilizatorii pot accesa tutoriale, cursuri sau materiale explicative într-un format accesibil și ușor de urmărit.

## Construirea unei identități profesionale

Social media oferă posibilitatea dezvoltării unei identități digitale, prin care utilizatorii își pot exprima opiniile, își pot prezenta activitatea sau pot contribui la comunități online.

# RISCURILE DIN SPATELE SOCIAL MEDIA

Pentru a maximiza beneficiile oferite de platformele de social media, utilizatorii ar trebui să recunoască și să ia măsurile adecvate împotriva riscurilor asociate utilizării acestora.

## Feedback negativ, hărțuire și cyberbullying

Oamenii folosesc platformele de social media pentru a distribui conținut, dar și pentru a-și exprima nemulțumirea cu privire la o postare, o imagine sau un videoclip anume. De asemenea, aceste platforme sunt folosite de către persoanele publice pentru a-și ține la curent urmăritorii cu ultimele acțiuni întreprinse. Cu toate acestea, nu toate persoanele abonate la paginile respective apreciază acțiunile întreprinse și drept consecință apar comentariile negative și mesajele de hărțuire la adresa persoanei respective.

În cazul în care vă simțiți agasat sau amenințat de anumite persoane nu uitați că puteți să le restricționați accesul la postările dumneavoastră sau le puteți bloca contul. Totodată, aveți posibilitatea de a raporta aceste conturi sau diverse postări din motive precum: cont fals, nume fals, informații false, conținut neadecvat, instigare la violență, etc.

O categorie aparte care trebuie monitorizată atent sunt copiii. Mesajele de intimidare pe care aceștia le pot primi îi pot afecta profund din punct de vedere emoțional și le pot provoca traume. Este recomandat ca aceștia să nu fie lăsați singuri să navigheze în Internet, cel puțin la început, și să le fie explicate pe larg pericolele pe care le pot întâlni în spațiul cibernetic.

## Furt de identitate

Lipsa confidențialității este una dintre caracteristicile platformelor de social media. Utilizatorii ar trebui să acorde o deosebită atenție informațiilor pe care aleg să le posteze deoarece sunt foarte multe persoane rău intenționate care pot prelua aceste date pentru a le folosi în diverse scopuri.

Zi de zi sunt create zeci de conturi false, care arată identic cu cele originale, însă în urma unei analize amănunțite se dovedesc a fi nelegitime. Spre exemplu, compania Facebook declara în anul 2020 că numărul conturilor false create pe această platformă este estimat undeva la 1,5 miliarde, aproximativ 5% din numărul total de conturi create.

Multe persoane rău intenționate folosesc diferite tehnici de inginerie socială pentru a câștiga încrederea unei persoane pentru ca, ulterior, să obțină acces la informațiile personale ale acesteia. Fiți precauți atunci când primiți mesaje, deoarece se poate întâmpla ca uneori, conturile prietenilor sau cunoștințelor să fie compromise. Dacă o conversație vi se pare ciudată, iar interlocutorul dumneavoastră devine foarte curios despre viața dumneavoastră personală sau vă solicită din senin o sumă de bani, este foarte posibil ca acel cont să fie compromis și o persoană rău intenționată să se folosească de el în scopuri ilicite.

## Informații false (Fake news)

Când vine vorba de răspândirea unei informații, rețelele de social media sunt un instrument puternic, atât pentru companii, cât și pentru persoanele fizice. Cu toate acestea, nu toate informațiile încărcate sunt reale. Termenul de informații false sau fake news se referă la dezinformări care acoperă o gamă variată de subiecte precum sănătatea, mediul, economia, politica etc.

Sunt mai multe tipuri de informații false. Acestea se pot clasifica în:

- **Clickbait** – Sunt articole care folosesc titluri senzaționale pentru a atrage atenția a cât mai mulți cititori, astfel încât venitul din reclame al site-ului web să fie cât mai mare. De cele mai multe ori aceste articole prezintă informații eronate sau lipsite de acuratețe.
- **Propagandă** – Reprezintă articolele care sunt create pentru a induce în mod deliberat publicul în eroare prin promovarea unui punct de vedere părtinitor sau pentru o anumită cauză politică.


- **Satiră / Parodie** – Sunt foarte multe site-uri web și conturi pe rețelele sociale care publică știri false doar pentru amuzament.
- **Jurnalism neglijent** – Uneori, reporterii sau jurnaliștii pot publica o poveste cu informații neverificate care pot induce publicul în eroare.
- **Titluri false** – Acest tip de știri se pot răspândi rapid pe platformele de social media, acolo unde sunt afișate doar titlurile sau mici fragmente scoase din context existent în articol.
- **Știri părtinitoare** – Multe persoane sunt atrase de știri sau povești care le confirmă propriile convingeri, iar știrile false sunt modul ideal de distribuție a acestor informații. Fluxurile de știri afișate pe platformele de social media sunt personalizate în funcție de căutările recente ale utilizatorilor.

Cum putem identifica informațiile false?

- **Analizați conținutul** – Verificarea sursei poveștii sau a site-ului reprezintă primul pas pentru a combate răspândirea de informații false. În mod normal, pentru transparență, la secțiunea *Despre* a unui site se pot găsi mai multe informații despre autor, scop etc.
- **Treci dincolo de titlu** – Se recomandă parcurgerea întregului articol deoarece multe știri folosesc titluri senzaționale sau șocante pentru a atrage atenția. Adesea, titlurile de povești false folosesc majuscule sau semne de exclamare
- **Verificați informația și din alte surse** – Pentru a fi sigur de corectitudinea informației, verificați dacă sunt și alte știri despre același subiect sau alte trusturi de presă care prezintă această informație. Dacă există surse citate în cadrul articolului verificați dacă acestea sunt de încredere.
- **Acordați atenție datelor cronologice** – De foarte multe ori, informațiile false conțin date incorecte sau modificate din punct de vedere cronologic. De asemenea, ar putea fi utilă verificarea datei publicării articolului, deoarece știrea

prezentată ar putea fi de fapt un eveniment desfășurat cu mult timp în urmă.

- **Prea amuzant pentru a fi adevărat** – Site-urile satirice sunt populare în mediul online și de multe ori nu este clar dacă povestea prezentată este reală sau este o glumă / parodie. Verificați dacă site-ul accesat este cunoscut pentru satiră

## Conținut manipulat cu inteligență artificială (Deepfake)

Odată cu dezvoltarea inteligenței artificiale, a devenit posibilă generarea de imagini, videoclipuri sau înregistrări audio false, dar extrem de realiste. Acestea sunt cunoscute sub numele de „deepfake". Astfel de materiale pot fi utilizate pentru manipularea opiniei publice, pentru șantaj sau pentru răspândirea de informații false.

Utilizatorii trebuie să fie atenți la materialele video sau audio care par neobișnuite și să verifice informațiile din mai multe surse înainte de a le distribui.

## Scam-uri și fraude financiare pe social media

Platformele de social media sunt utilizate frecvent pentru diverse tipuri de înșelătorii financiare. Printre cele mai întâlnite se numără:

- investiții false în criptomonede;
- concursuri sau giveaway-uri frauduloase;
- conturi false care se dau drept persoane publice;
- mesaje care solicită transferuri urgente de bani.

Este recomandat ca utilizatorii să nu trimită bani persoanelor necunoscute și să verifice autenticitatea conturilor înainte de a

interacționa.

### Utilizarea excesivă a platformelor sociale

Utilizarea excesivă a rețelelor sociale poate duce la scăderea productivității, la tulburări de concentrare sau la afectarea sănătății mentale. Algoritmii platformelor sunt concepuți pentru a menține utilizatorii conectați cât mai mult timp, ceea ce poate crea dependență de consumul constant de conținut.

## ÎMBUNĂTĂȚIREA SECURITĂȚII CONTURILOR DE SOCIAL MEDIA

### Setări de confidențialitate și complexitatea parolei

Majoritatea utilizatorilor folosesc setările implicite de confidențialitate atunci când își creează un nou profil sau o nouă pagină. Potrivit unei statistici realizate în anul 2017 de către Statista, utilizatorii au declarat că nu au încredere că setările de confidențialitate alese funcționează așa cum ar trebui.

Pentru un plus de securitate este necesară setarea unei parole complexe și unice pentru fiecare cont din mediul online. Aceasta ar trebui să aibă **cel puțin 12-16 caractere** și să includă litere mari, litere mici, cifre și caractere speciale. Totodată, nu este recomandată includerea informațiilor personale, precum numele părinților, data nașterii sau numele animalului de companie.

De asemenea parola ar trebui schimbată periodic și, acolo unde este posibil, introducerea autentificării multifactor. Dacă utilizați un dispozitiv partajat cu alte persoane pentru a accesa platformele de social media, se recomandă să vă deconectați de fiecare dată când nu mai utilizați sistemul, utilizând funcția Sign out.

Se recomandă utilizarea **aplicațiilor de autentificare** (Google Authenticator, Microsoft Authenticator, Authy) în locul

codurilor primite prin SMS, deoarece acestea oferă un nivel mai ridicat de securitate.

Managerii de parole sunt aplicații care permit generarea și stocarea în siguranță a parolelor complexe. Utilizarea unui astfel de instrument reduce riscul reutilizării parolelor și crește securitatea conturilor online.

## Aplicații third-party vulnerabile

Chiar și atunci când conturile de social media sunt securizate corespunzător, acestea pot fi compromise prin intermediul unor aplicații third-party nesigure instalate pe dispozitiv. Se recomandă descărcarea și instalarea aplicațiilor doar din surse sigure, precum și actualizarea în mod constant a sistemului de operare și a aplicațiilor instalate.

Este recomandată verificarea periodică a aplicațiilor și serviciilor conectate la conturile de social media și revocarea accesului celor care nu mai sunt utilizate.

## Atacuri malware, scam și phishing

Înșelătoriile și atacurile malware sunt foarte frecvente în cadrul platformelor și rețelelor de social media. Fie că vorbim de campanii de phishing sau de infectarea dispozitivului prin simpla accesare a unui site web, toate aceste acțiuni au de cele mai multe ori același scop și anume furtul credențialelor de autentificare, a datelor bancare ale utilizatorilor sau alte informații private.

## Geotagging

Funcția de geotagging este o caracteristică implementată pe majoritatea dispozitivelor mobile. Aceasta constă în adăugarea datelor de identificare geografică în cadrul tuturor fotografiilor, videoclipurilor sau mesajelor text realizate. Menținerea activă a acestei funcții poate duce la încălcarea confidențialității, deoarece poate dezvălui locația utilizatorilor în timp real, oferind astfel informații precum adresa exactă a locuinței sau a locului de muncă.

# CONȘTIENTIZAREA RISCURILOR DE IMAGINE DIN SPAȚIUL SOCIAL MEDIA

Este posibil ca postările publicate pe platformele de social media să devină virale într-un timp foarte scurt. Audiența, respectiv persoanele care urmăresc aceste postări, analizează atent conținutul distribuit. În acest context, publicarea unor informații sau materiale nepotrivite poate avea consecințe asupra imaginii personale sau profesionale.

Un alt aspect important este capacitatea de a identifica rapid mesajele de tip spam, tentativele de phishing sau alte amenințări de securitate și de a le raporta administratorilor platformelor sau autorităților competente. Se recomandă limitarea audienței la un cerc restrâns de persoane cunoscute și acceptarea cererilor de conectare sau prietenie doar din partea persoanelor pe care le cunoașteți.

Analizați cu atenție informațiile pe care intenționați să le publicați în mediul online, deoarece ulterior acestea pot fi dificil sau imposibil de eliminat complet. Chiar dacă platformele oferă opțiunea de ștergere a conținutului publicat, copiile de rezervă generate automat pot păstra aceste informații, fără ca utilizatorul să aibă control asupra gestionării lor.

Informațiile publicate pe internet pot rămâne disponibile pentru perioade îndelungate, chiar și după ștergere. Conținutul poate fi salvat sau redistribuit de alți utilizatori.

# RECOMANDĂRI GENERALE DE SECURITATE

Utilizarea platformelor de social media implică expunerea unor informații cu caracter personal și interacțiunea cu un număr mare de utilizatori. Din acest motiv, adoptarea unor bune practici de securitate este importantă pentru protejarea conturilor și a datelor personale. Respectarea unor reguli simple poate reduce semnificativ riscul compromiterii conturilor, al furtului de identitate sau al expunerii la diverse tipuri de atacuri cibernetice.

În continuare sunt prezentate câteva recomandări generale care pot contribui la utilizarea în siguranță a platformelor de social media:

- activați autentificarea multifactor (MFA) pentru conturile utilizate;
- utilizați parole complexe și diferite pentru fiecare cont;
- evitați accesarea linkurilor sau fișierelor provenite din surse necunoscute;
- evitați furnizarea informațiilor personale sau financiare prin canale de mesagerie private;
- verificați periodic setările de confidențialitate ale conturilor;
- utilizați doar aplicații din surse oficiale și actualizați constant aplicațiile deja instalate;
- evitați conectarea la conturi personale prin intermediul rețelelor Wi-Fi publice nesecurizate;
- raportați conturile sau mesajele suspecte administratorilor platformelor.

# SECURIZAREA CONTURILOR CREATE ÎN CADRUL PLATFORMELOR DE SOCIAL MEDIA

Securizarea conturilor de social media reprezintă o responsabilitate individuală esențială, având în vedere riscurile asociate expunerii informațiilor personale în mediul online. Adoptarea unor măsuri de securitate adecvate poate preveni accesul neautorizat la conturi și utilizarea abuzivă a acestora.

Pentru a reduce riscurile de securitate, se recomandă respectarea următoarelor măsuri:

**Protejarea accesului la cont:**

- nu divulgați datele de autentificare altor persoane;
- evitați salvarea parolelor pe dispozitive partajate;
- utilizați doar aplicații oficiale pentru accesarea platformelor;
- deconectați-vă de pe dispozitivele pe care nu le controlați.

**Gestionarea setărilor de confidențialitate:**

- limitați vizibilitatea informațiilor personale (număr de telefon, adresă, locație);
- restricționați accesul la postări doar pentru persoane cunoscute;
- dezactivați opțiunile de localizare automată (geotagging), acolo unde este posibil;
- analizați periodic permisiunile acordate aplicațiilor terțe.

**Identificarea și prevenirea accesului neautorizat:**

- acordați atenție notificărilor privind autentificări din locații necunoscute;
- nu accesați linkuri suspecte primite prin mesaje sau e-mail;
- verificați autenticitatea conturilor înainte de a interacționa cu acestea;

- raportați imediat orice activitate suspectă către platforma utilizată.

**Recomandări specifice pentru conturi instituționale:**

- desemnați persoane responsabile pentru administrarea conturilor;
- evitați utilizarea conturilor personale în scop profesional;
- utilizați adrese de e-mail instituționale pentru crearea conturilor;

- limitați accesul la cont doar personalului autorizat;
- actualizați periodic datele de acces și drepturile utilizatorilor.

# REFERINȚE


- https://www.investopedia.com/terms/s/social-media.asp
- https://www.webroot.com/us/en/resources/tips-articles/online-activities-internet-security
- https://blog.loomly.com/social-media-risks/
- https://www.doads.ro/cele-mai-utilizate-retele-sociale-in-romania-2020/
- https://datareportal.com/reports/digital-2026-romania
- https://www.financierworldwide.com/risks-associated-with-use-of-social-media#.Yqwa7HZBxPY
  https://businessdegrees.uab.edu/blog/social-media-risks/
- https://www.webfx.com/social-media/learn/social-media-marketing-advantages-and-disadvantages/
- https://www.webwise.ie/teachers/what-is-fake-news/


# AGENȚIA DE APĂRARE CIBERNETICĂ