DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Ghid de protejare și recuperare conturi social media

SEPTEMBRIE 2025

TLP:CLEAR

Introducere

Rețelele sociale sunt acum o parte integrantă a vieții cotidiene, fiind folosite pentru comunicare, acces la informații și promovarea ideilor personale sau profesionale. Acest tip de interacțiune digitală aduce, însă, și riscuri semnificative, mai ales din cauza volumului mare de date personale partajate online. Atacatorii cibernetici folosesc tehnici din ce în ce mai sofisticate pentru a compromite conturile, utilizând adesea metode bazate pe inteligența artificială (IA). Prin urmare, protejarea identității digitale nu mai este doar responsabilitatea platformelor, ci necesită o implicare activă din partea fiecărui utilizator.

În acest sens, acest ghid oferă recomandări clare pentru prevenirea incidentelor, precum și pași concreți pentru recuperarea conturilor afectate. Este destinat atât utilizatorilor individuali, cât și persoanelor responsabile cu administrarea conturilor instituționale sau profesionale în mediul online.

Riscuri și amenințări cibernetice în social media

Preluarea neautorizată a contului (Account Takeover – ATO)

Unul dintre cele mai frecvente riscuri în social media este ca altcineva să îți acceseze contul fără permisiune. Acest lucru se poate întâmpla dacă folosești o parolă compromisă, ai fost victima unui atac de tip phishing, contul tău a fost implicat într-o breșă de securitate sau atacatorii au exploatat o problemă tehnică. Odată ce obțin accesul, aceștia pot trimite mesaje în numele tău, pot vedea informații personale sau pot încerca să păcălească alte persoane din lista ta de contacte pentru a obține bani sau date.

Phishing și Vishing

Ai primit vreodată un e-mail, un SMS sau o notificare, care părea să vină de la bancă, o autoritate publică sau o platformă cunoscută, dar ceva ți s-a părut ciudat? Este posibil să fi fost o tentativă de phishing - un tip de atac cibernetic care încearcă să îți fure parolele sau alte date personale. Uneori, atacatorii merg și mai departe, te pot suna direct (acesta e vishing-ul), imitând vocea unui funcționar pentru a părea cât mai convingători. În astfel de cazuri, pot folosi chiar IA pentru ca mesajele sau apelurile să pară cât mai reale. Printre instituțiile cel mai des imitate se numără Banca Națională a României (BNR), Agenția Națională de Administrare Fiscală (ANAF), Inspectoratul General al Poliției Române (IGPR) și altele.

Infectarea cu programe malițioase

Dacă dai click pe un link compromis sau instalezi aplicații din surse neoficiale, dispozitivul tău (telefon, tabletă, calculator) riscă să fie infectat cu programe malițioase. Acestea pot accesa datele tale sensibile, îți pot monitoriza activitatea pe dispozitiv sau îți pot compromite conturile de social media.

Inginerie socială

Atacatorii pot încerca să te păcălească pretinzând că sunt prieteni, rude sau angajați ai unor companii cunoscute. Prin manipulare psihologică, urmăresc să-ți câștige încrederea și să obțină parole, informații sensibile sau chiar bani. Cu ajutorul IA, pot crea profiluri false extrem de convingătoare, ceea ce face aceste atacuri și mai greu de detectat.

SIM Swap

Prin acest tip de atac, cineva poate transfera numărul tău de telefon pe o altă cartelă SIM, pe care o controlează. Asta înseamnă că poate primi SMS-urile tale, inclusiv codurile de autentificare. Astfel, chiar dacă ai activată autentificarea în doi pași (2FA) prin SMS, conturile tale pot fi accesate fără permisiune.

Manipularea conținutului audio-video

Atacatorii pot folosi tehnologii precum deepfake sau imitarea vocii (voice cloning) pentru a crea videoclipuri și mesaje audio false, dar foarte convingătoare. Aceste materiale pot fi folosite pentru a te păcăli să oferi date personale, să trimiți bani sau să crezi informații care nu sunt adevărate.

Aplicații externe suspecte

Unele aplicații pot solicita acces la contul tău de social media și la informațiile personale. Dacă nu provin din surse oficiale, acestea pot colecta date sau publica în numele tău. Pentru siguranță, instalează aplicații doar din magazine oficiale și verifică cu atenție ce permisiuni îți cer înainte să le oferi acces.

Lipsa politicilor de securitate în mediul profesional

Dacă administrezi conturi de social media pentru o instituție sau companie, este important să existe reguli clare privind accesul, securitatea conturilor și răspunsul la incidente. Lipsa unor astfel de politici poate

duce la conturi compromise, scurgeri de date sau daune de imagine. Asigură-te că organizația ta are politici de securitate digitală bine definite și aplicate.

Măsuri proactive de combatere a amenințărilor

Pentru a-ți păstra conturile și datele în siguranță, este important să aplici câteva măsuri simple:

Folosește parole puternice și diferite pentru fiecare cont

- Creează parole lungi (de cel puțin 12 caractere), care conțin litere mari și mici, cifre și simboluri. Cu cât o parolă este mai lungă și include o varietate de caractere, cu atât este mai greu de ghicit de către atacatori, chiar și cu ajutorul programelor specializate;
- Evită parole ușor de ghicit, cum ar fi numele tău, data nașterii sau combinații simple. Atacatorii încearcă adesea să ghicească parolele folosind informații despre tine (care sunt publice sau ușor de aflat). O parolă personală simplă este cel mai ușor de spart și te expune rapid riscurilor;
- Folosește un manager de parole pentru a crea și salva parole sigure, fără să fii nevoit să le memorezi. Un manager de parole este ca un seif digital care generează și reține pentru tine parole unice și complicate pentru fiecare cont. Tu vei memora doar o singură parolă, cea a managerului, iar el se va ocupa de restul, simplificându-ți viața și sporindu-ți considerabil securitatea online;
- La întrebările de securitate, nu folosi informații reale. Scrie răspunsuri greu de intuit, ca și cum ar fi o parolă suplimentară. Întrebările de securitate (precum „numele de fată al mamei” sau „prima școală”) sunt adesea ușor de ghicit de către atacatori, mai ales dacă informațiile tale sunt publice online. Pentru a te proteja, inventează răspunsuri false, dar pe care doar tu le știi și pe care le poți nota într-un manager de parole. Gândește-te la ele ca la o a doua parolă, la fel de importantă.

Activează autentificarea multifactor

- Activează autentificarea în doi pași (2FA) oriunde este posibil, pe rețele sociale, adresa de e-mail, aplicații bancare sau alte servicii importante. Această funcție adaugă un strat suplimentar de securitate conturilor tale. Chiar dacă un atacator îți află parola, nu va putea accesa contul fără al doilea pas de verificare, de obicei un cod trimis pe telefonul tău sau generat de o aplicație;
- Folosește metode mai sigure, cum ar fi aplicațiile mobile care generează coduri de securitate (de tip autentificator, ex. Google Authenticator) sau dispozitive fizice (chei de securitate) care se conectează prin USB sau NFC (Near-Field Communication). Aceste opțiuni sunt considerabil mai sigure decât codurile trimise prin SMS, care pot fi interceptate în cazul unor atacuri de tip SIM Swap;
- Evită autentificarea prin SMS, pentru că este mai ușor de compromis. Deși pare la îndemână, metoda SMS poate fi ocolită de atacatori prin tactici precum SIM Swap. Cu toate acestea, dacă nu ai altă opțiune, este totuși mult mai bine să folosești 2FA prin SMS decât să nu ai nicio metodă suplimentară de autentificare activată;
- Păstrează codurile de rezervă (backup codes) într-un loc sigur, în cazul în care pierzi accesul la telefon sau la aplicația de autentificare. Aceste coduri reprezintă o „cheie de rezervă” care te ajută să recuperezi accesul la conturile tale dacă nu mai poți folosi metoda principală de 2FA (ex: îți pierzi telefonul). Asigură-te că le notezi și le stochezi într-un loc foarte sigur, la care ai acces doar tu.

Revocă accesul aplicațiilor terțe

- Verifică periodic aplicațiile conectate la conturile tale. Caută în setările de securitate secțiunea „Aplicații conectate”, „Aplicații și site-uri web” sau „Permisiuni acordate”. Multe aplicații, jocuri sau quiz-uri pe care le folosești o singură dată primesc acces la profilul tău de social media. Este important să verifici regulat aceste permisiuni și să vezi ce informații pot accesa;
- Elimină accesul aplicațiilor pe care nu le mai folosești, pe care nu le recunoști sau care solicită permisiuni excesive. Fiecare aplicație reprezintă un potențial punct de intrare pentru atacatori, iar eliminarea celor inutile reduce semnificativ riscul de scurgeri de date sau acces neautorizat;
- Citește cu atenție ce permisiuni cere o aplicație înainte să-i acorzi acces. Permite doar ce este strict necesar pentru funcționarea ei. Când instalezi o aplicație nouă, ea îți poate cere permisiunea de a accesa diverse date, cum ar fi lista de prieteni, locația sau chiar postările tale. Acordă acces doar la informațiile indispensabile pentru funcționarea aplicației.

Ține totul actualizat și verifică periodic activitatea conturilor

- Instalează întotdeauna actualizările pentru aplicații și sistemul de operare, acestea corectează vulnerabilități care pot fi exploatate de atacatori;
- Monitorizează activitatea conturilor tale, verifică dacă există conexiuni suspecte, locații neobișnuite sau acțiuni pe care nu le-ai făcut (postări, mesaje, modificări);

- Dacă observi ceva ciudat, schimbă imediat parola și deconectează sesiunile pe care nu le recunoști;
- Fii atent la notificările de securitate primite de la platforme, ele te pot avertiza despre încercări de acces neautorizat sau modificări importante în contul tău.

Fii atent la linkuri și mesaje suspecte

- Nu da click pe linkuri sau atașamente din mesaje care par suspecte sau vin de la persoane necunoscute, pot ascunde programe malițioase ori te pot direcționa către pagini false;
- Verifică întotdeauna adresa site-ului (URL-ul) înainte să introduci date personale. Asigură-te că este scrisă corect – de exemplu, „facebook.com” și nu „faceb00k.com”. În plus, verifică dacă adresa începe cu „https://” și dacă vezi o iconiță cu un lacăt închis lângă ea. Acel „s” de la „https” și lacătul înseamnă că site-ul este securizat și că informațiile pe care le trimiți (cum ar fi parolele) sunt criptate, adică protejate;
- Dacă un mesaj pare ciudat, chiar dacă vine de la cineva cunoscut, confirmă întotdeauna cu persoana respectivă printr-un alt mijloc (cum ar fi un apel telefonic sau o discuție față în față). Atacatorii pot prelua conturile prietenilor tăi și pot trimite mesaje false în numele lor, profitând de încrederea pe care o ai. O simplă verificare directă te poate salva de o înșelătorie;
- Evită să oferi date personale unor persoane necunoscute, indiferent de cât de convingător sau „oficial” ar părea mesajul. Fii extrem de precaut atunci când ți se cer informații sensibile (cum ar fi CNP-ul, datele de pe cardul bancar sau parole) prin e-mail, SMS sau telefon, chiar dacă expeditorul susține că este o bancă, o instituție publică sau o companie cunoscută. Aceste entități nu îți vor cere niciodată astfel de date prin mesaje nesolicitate. Verifică întotdeauna legitimitatea cererii contactând direct instituția, folosind date de contact oficiale (nu cele din mesajul suspect).

Controlează ce informații postezi

- Gândește-te bine înainte să distribui informații personale, cum ar fi data nașterii, adresa, locul de muncă sau planurile de vacanță. Aceste detalii aparent inofensive pot fi adunate de atacatori și folosite împotriva ta în diverse scenarii de fraudă sau inginerie socială. Odată publicate online, ele sunt dificil de șters și pot fi exploatate oricând;
- Setează nivelul de confidențialitate al contului astfel încât doar persoanele în care ai încredere să-ți poată vedea postările, fotografiile și detaliile personale. Verifică setările de confidențialitate și asigură-te că informațiile tale nu sunt publice pentru oricine. Astfel, reduci riscul ca datele tale să fie colectate și folosite în scopuri malițioase;
- Verifică periodic setările de securitate și șterge informațiile sau conturile pe care nu le mai folosești. Este o bună practică să faci o „curățenie” digitală regulată. Elimină datele vechi, fotografiile sau postările pe care nu le mai vrei online și închide conturile pe care nu le mai utilizezi. Mai puține informații expuse înseamnă mai puține riscuri pentru tine.

Ai grijă de dispozitivele tale

- Blochează accesul la telefon și computer folosind un cod PIN, o parolă sau metode biometrice, cum ar fi amprenta sau recunoașterea facială. Blocarea ecranului este prima linie de apărare împotriva accesului neautorizat la informațiile tale. Dacă dispozitivul tău ajunge pe mâini greșite, aceste măsuri simple pot împiedica pe cineva să-ți acceseze datele personale stocate local;
- Evită să te conectezi la conturile tale de social media de pe dispozitive publice sau ale altor persoane, pot fi nesigure și îți pot compromite datele;
- Instalează un antivirus și un firewall și actualizează-le constant, pentru a detecta și bloca amenințările cibernetice. Antivirusul detectează și elimină virușii și alte programe periculoase, în timp ce firewall-ul blochează accesul neautorizat la computerul tău din exterior;
- Când folosești rețele Wi-Fi publice, protejează-ți conexiunea printr-un VPN (Virtual Private Network), pentru a preveni interceptarea datelor. Rețelele Wi-Fi publice (din cafenele, aeroporturi) sunt adesea nesigure și permit oricui să-ți intercepteze datele. Un VPN criptează traficul tău de internet, creând un tunel securizat care îți protejează informațiile de ochii curioși și de potențialii atacatori.

Cum îți poți recupera contul de social media compromis

Dacă bănuiești că ți-a fost compromis contul de social media, e important să acționezi rapid și să urmezi pașii recomandați de platformă. Ignorarea semnelor de compromitere poate avea consecințe grave, cum ar fi furtul de identitate, distribuirea de conținut malițios sau chiar pierderi financiare.

FACEBOOK

Semne ale compromiterii contului de social media

- Schimbări neautorizate: numele, parola, e-mailul sau numărul de telefon asociat contului au fost înlocuite fără acordul tău;
- Activitate străină: postări, mesaje sau cereri de prietenie trimise de pe contul tău pe care nu le recunoști;
- Notificări suspecte: primești alerte de la Facebook despre conectări de pe dispozitive sau din locații necunoscute sau schimbări de parolă pe care nu le-ai inițiat;
- Acces blocat: nu te poți autentifica, iar parola ta nu mai funcționează;
- Verificare rapidă: accesează *Setări* > *Securitate și conectare* > *Unde te-ai conectat*. Deconectează imediat orice sesiune activă pe care nu o recunoști.

Notă: Hackerii folosesc tactici noi, inclusiv videoclipuri generate de AI, fișiere malițioase (update-uri false), spyware sau extensii de browser periculoase pentru a obține acces. Fii extrem de precaut cu link-urile și fișierele suspecte.

Pași concreți de recuperare

Recuperează-ți contul de pe un dispozitiv pe care l-ai folosit anterior (telefon/laptop personal):

1. *Accesează pagina oficială de recuperare*: mergi la *facebook.com/hacked*. Acesta este punctul de plecare principal, chiar dacă nu te poți autentifica:
   - urmează instrucțiunile pentru a-ți identifica contul (e-mail, număr de telefon sau nume de utilizator);
   - dacă hackerul a schimbat datele de contact, Facebook poate trimite un link de recuperare la adresa de e-mail anterioară.
2. *Resetează parola:* alege o parolă nouă, puternică și unică (peste 10 caractere, combinând litere mari/mici, cifre și simboluri). Nu o mai folosi pe alte platforme;
3. *Verificarea identității (dacă este solicitată):* Facebook poate cere dovezi ale identității tale:
   - Aceasta poate include un *video selfie* (folosind recunoașterea facială avansată) sau încărcarea unei fotografii a unui *act de identitate oficial* (pașaport, buletin, permis de conducere, etc.), sau a unor *documente non-guvernamentale* (card de student, adeverință de muncă).
4. *Deconectează-te de pe toate dispozitivele necunoscute:* după ce ai recăpătat accesul, mergi la *Setări* > *Securitate și conectare* și alege *Deconectează-te de pe toate dispozitivele* sau verifică manual și deconectează sesiunile suspecte;
5. *Verifică setările și activitatea:* examinează *Jurnalul de activități*, postările recente, mesajele trimise și setările de confidențialitate. Șterge sau corectează orice modificare pe care nu ai făcut-o tu;
6. *Ajutor de la prietenii de încredere: d*acă ai setat *Contacte de Încredere* (*Trusted Contacts*) în prealabil, îi poți ruga să te ajute. Facebook le va trimite părți dintr-un cod de recuperare.

Atenție: Există escrocherii care se folosesc de această funcție pentru a păcăli utilizatorii să dezvăluie coduri. Prietenii tăi ar trebui să înțeleagă procesul și să nu îți ceară codul direct.

Linkuri oficiale utile

- Recuperare cont compromis: *facebook.com/hacked*;
- Centrul de ajutor Facebook: *facebook.com/help/* (articole despre conturi sparte, resetare parolă și securitate);
- Centrul de conturi Meta: *accountscenter.meta.com/* (verifică activitatea de conectare pentru toate conturile Meta – necesită autentificare).

INSTAGRAM

Semne ale compromiterii contului de social media

- Schimbări neautorizate: parola, numele de utilizator, adresa de e-mail sau numărul de telefon asociat contului s-au modificat fără acordul tău;
- Activitate străină: postări, povești, comentarii sau mesaje (DM-uri) trimise de pe contul tău pe care nu le recunoști;
- Notificări suspecte: primești alerte de la Instagram despre conectări de pe dispozitive sau locații necunoscute sau schimbări de parolă pe care nu le-ai inițiat;
- Acces blocat: nu te poți autentifica, iar parola ta nu mai funcționează sau ești deconectat brusc din cont fără motiv;
- Verificare rapidă: accesează *Profil* > *Meniu* (trei linii orizontale) > *Setări și confidențialitate* > *Centrul de Conturi* > *Parolă și securitate* > *Unde ești conectat*. Deconectează imediat orice sesiune activă pe care nu o recunoști.

Notă: Hackerii folosesc tactici precum: campanii de phishing (mesaje false prin SMS, e-mail sau mesaje private care solicită date de autentificare sau amenință cu blocarea contului), aplicații malițioase (care imită instrumente legitime și pot fura date sau suprapune ecrane false de conectare) și inginerie socială (manipulare psihologică pentru a obține informații sensibile). Fii precaut cu linkurile și fișierele suspecte, mai ales cele care par urgente sau provin din surse necunoscute.

Pași concreți de recuperare

Recuperează-ți contul de pe un dispozitiv pe care l-ai folosit anterior (telefon/laptop personal):

1. *Accesează pagina oficială de recuperare*: mergi la *instagram.com/hacked/*. Acesta este punctul de plecare principal, chiar dacă nu te poți autentifica. Alternativ, de pe ecranul de conectare al aplicației, atinge *Ai uitat parola?* sau *Obține ajutor la conectare*;
2. *Resetează parola:*
   - Pe ecranul de conectare, atinge *Ai uitat parola?;*
   - Introdu numele de utilizator, adresa de e-mail sau numărul de telefon asociat contului;
   - Atinge *Trimite link de conectare* sau *Continuă*;
   - Completează testul *Captcha*;
   - Verifică-ți e-mailul (inclusiv dosarele Spam/Promoții/Social) sau mesajele SMS pentru un link de conectare sau un cod de resetare a parolei de la Instagram;
   - Urmează instrucțiunile pentru a crea o nouă *parolă puternică și unică*.
3. Verificarea identității (dacă este solicitată): Instagram poate cere dovezi ale identității tale:
   - Aceasta poate include un *video selfie* (dacă ai fotografii cu tine în cont). Acesta ajută Instagram să confirme că ești o persoană reală și proprietarul contului, deoarece fotografiile și actele de identitate pot fi modificate digital. Procesul de revizuire poate dura până la două zile lucrătoare;
   - Încărcarea unui *act de identitate* emis de guvern;
   - Pentru conturile comerciale, pot fi necesare dovezi suplimentare, cum ar fi actele companiei.
4. *Deconectează-te de pe toate dispozitivele necunoscute*: după ce ai recăpătat accesul, mergi la *Profil* > *Meniu* (trei linii orizontale) > *Setări și confidențialitate* > *Centrul de Conturi* > *Parolă și securitate* > *Unde ești conectat*. Elimină conexiunile către toate dispozitivele necunoscute;
5. *Verifică setările și activitatea*: restaurează toate modificările făcute de hackeri, reintrodu numărul de telefon și adresa ta de e-mail, actualizează numele de profil și alte date personale. Verifică *Centrul de conturi* și elimină orice conturi pe care nu le recunoști. Verifică setările de e-mail pentru reguli de redirecționare și șterge-le pe cele neautorizate. Examinează dosarele *Trimise* și *Șterse* din e-mail pentru activitate suspectă. Verifică lista de conturi blocate din setările Instagram.

Linkuri oficiale utile

- Recuperare cont compromis: *instagram.com/hacked/*;
- Centrul de ajutor Instagram: *help.instagram.com* (pentru articole despre conturi sparte, resetare parolă și securitate);
- Centrul de conturi Meta: *accountscenter.meta.com* (verifică activitatea de conectare pentru toate conturile Meta – necesită autentificare).

TIKTOK

Semne ale compromiterii contului de social media

- Schimbări neautorizate: parola sau numărul de telefon asociat contului au fost modificate fără acordul tău;
- Modificări de profil: numele de utilizator (username) sau pseudonimul a fost schimbat fără permisiunea ta;
- Conținut neautorizat: videoclipuri au fost șterse sau publicate fără ca tu să le fi aprobat;
- Mesaje suspecte: din contul tău au fost trimise mesaje directe (DM-uri) pe care nu le-ai scris tu.

Pași concreți de recuperare

1. Resetați-vă parola:
   - În aplicația TikTok, atingeți *Profil* în partea de jos;
   - Atingeți butonul *Meniu* ☰ din partea de sus, apoi selectați *Setări și confidențialitate*;
   - Atingeți *Cont*;
   - Atingeți *Parolă*;
   - Schimbați-vă parola.
2. Conectați-vă numărul de telefon:
   - În aplicația TikTok, atingeți *Profil* în partea de jos;
   - Atingeți butonul *Meniu* ☰ din partea de sus, apoi selectați *Setări și confidențialitate*;
   - Atingeți *Cont*;
   - Atingeți *Informații cont*;
   - Atingeți *Număr de telefon*;
   - Conectați-vă numărul de telefon.
3. Eliminați dispozitivele suspecte:
   - În aplicația TikTok, atingeți *Profil* în partea de jos;
   - Atingeți butonul *Meniu* ☰ din partea de sus, apoi selectați *Setări și confidențialitate*;
   - Atingeți *Securitate și permisiuni*;
   - Atingeți *Gestionați dispozitivele* și examinați dispozitivele listate;
   - Eliminați dispozitivele nedorite sau suspecte.

Linkuri oficiale utile

- Recuperare cont compromis (cont piratat, probleme de autentificare): *tiktok.com/hacked*;
- Resetare parolă TikTok (instrucțiuni pentru schimbarea parolei uitate sau compromise): *tiktok.com/reset-password*;
- Gestionarea informațiilor contului (adăugare/verificare e-mail și număr de telefon): *tiktok.com/update-account-info*;
- Autentificare în doi pași (2FA): *tiktok.com/2step*;
- Gestionare dispozitive conectate (vizualizare și închidere sesiuni suspecte): *tiktok.com/manage-devices*.

WHATSAPP

Dacă bănuiești că o altă persoană îți folosește contul de WhatsApp, este foarte important să îți informezi imediat membrii familiei și prietenii.

- Atacatorii ar putea profita de încrederea generată de contul tău pentru a cere bani sau informații personale în conversații și grupuri;
- Nu comunica nimănui codul de verificare WhatsApp primit prin SMS, nici măcar prietenilor;
- Fără acest cod, nimeni nu îți poate prelua contul sau înregistra numărul tău de telefon în aplicație.

Semne ale compromiterii contului de social media

- Modificări neautorizate ale numărului de telefon sau ale parolei de securitate (se referă la PIN-ul pentru verificarea în doi pași);
- Alerte în aplicație, cineva încearcă să înregistreze numărul tău;
- Primirea codului SMS de verificare fără să îl fi solicitat;
- Convorbiri inițiate în grupuri sau în privat pe care nu le recunoști.

Pași pentru recuperare

Reînregistrează-te cu numărul tău de telefon, aceasta este cea mai rapidă metodă de a-ți recupera contul și de a deconecta orice alt utilizator neautorizat:

1. Deschide aplicația WhatsApp;
2. Introdu numărul tău de telefon *și apasă Înainte* (sau *Next*);
3. Vei primi un *cod SMS de 6 cifre* pentru verificare;
4. Introdu-l imediat în aplicație;
5. Odată autentificat, orice alt utilizator care ți-a preluat contul este automat deconectat.

Activează verificarea în doi pași (2FA)

Verificarea în doi pași adaugă un nivel critic de securitate contului tău:

1. Deschide aplicația WhatsApp;
2. Apasă pe *Setări* (pictograma roată dințată sau cele trei puncte/linii verticale), apoi pe *Cont*;
3. Apasă pe *Verificare în doi pași* > *Activează și creează un PIN de 6 cifre*;
4. *Adaugă o adresă de e-mail pentru recuperare* în cazul în care uiți PIN-ul. Această adresă de e-mail este importantă pentru a reseta PIN-ul fără a aștepta 7 zile.

Notă: Verificarea în doi pași (2FA) pe WhatsApp este o măsură de securitate distinctă de codul SMS primit la prima înregistrare. Chiar dacă un atacator ar obține codul SMS, nu-ți va putea activa contul dacă tu ai deja 2FA activată și el nu cunoaște PIN-ul tău.

Dacă PIN-ul 2FA este uitat, contul poate fi recuperat după cele 7 zile fără PIN, însă doar dacă ai configurat o adresă de e-mail de recuperare. În lipsa acesteia și a PIN-ului, recuperarea poate fi mai dificilă.

Linkuri oficiale utile

- Recuperare cont compromis: *whatsapp.com/recover*;
- Verificare în doi pași (2FA): *whatsapp.com/2step*;
- Criptare end-to-end: *whatsapp.com/encryption*;
- Backup criptat în cloud: *whatsapp.com/encrypted-backup*.

YOUTUBE

Înainte de a lua măsuri, este important să verifici dacă există semne clare că ți-a fost compromis canalul YouTube. Reține că fiecare canal YouTube este asociat cel puțin unui cont Google, așadar, dacă un canal YouTube este compromis, înseamnă că și cel puțin unul dintre conturile Google asociate este compromis.

Semne ale compromiterii contului de social media

Modificări neautorizate în setările contului, cum ar fi:

- Schimbări la fotografia de profil, descrierea contului sau alte informații despre canal;
- Modificări la setările de notificare prin e-mail sau la preferințele de comunicare;
- Schimbări la contul AdSense asociat canalului tău.

Conținut suspect încărcat pe canal:

- Videoclipuri postate pe care nu le recunoști;
- Notificări de la YouTube privind încălcări ale regulilor comunității sau avertismente legate de drepturile de autor, pentru conținut pe care nu l-ai încărcat tu.

Modificări în informațiile de securitate ale contului Google:

- Schimbări neautorizate ale numelui de utilizator, parolei sau adreselor de e-mail de recuperare;
- Dispozitive necunoscute conectate la contul Google.

Activitate neobișnuită pe canalul YouTube:

- Comentarii, playlist-uri sau activități suspecte pe canalul YouTube pe care nu le recunoști.

Pașii pentru recuperare

Recuperează și securizează contul Google (fundamental pentru securitatea YouTube):

1. Mergi la pagina de recuperare a contului Google - *accounts.google.com/signin/recovery*;
2. Introdu adresa ta de e-mail;
3. Completează cât mai corect întrebările de verificare, care pot include:
   - Parole vechi sau dispozitive folosite;
   - Locurile din care te-ai conectat/autentificat în trecut.
4. Resetează parola imediat ce ai acces din nou. Asigură-te că folosești o parolă puternică și unică.

Dacă te poți conecta la contul Google, dar bănuiești o compromitere

1. Intră în *Verificarea securității* Google: *myaccount.google.com/security*;
2. Verifică *Evenimentele recente de securitate* pentru orice activitate suspectă;
3. Revizuiește *dispozitivele conectate*: dacă vezi dispozitive necunoscute, selectează-le și alege *Deconectează-te;*
4. *Schimbă parola*;
5. *Activează Verificarea în doi pași (2FA)*, preferabil cu o aplicație Authenticator (ex. Google Authenticator) sau dispozitive fizice (chei de securitate) care se conectează prin USB sau NFC.

Securizează-ți contul de YouTube (după ce ai securizat contul Google)

1. Șterge videoclipurile, comentariile sau playlist-urile neautorizate încărcate sau create de atacator;
2. Verifică și ajustează permisiunile pentru editori sau manageri în canalul tău, dacă este cazul:
   - Accesează *YouTube Studio* > *Setări*, apoi *Permisiuni*;
   - Asigură-te că doar persoanele de încredere au acces la gestionarea canalului tău.

Linkuri oficiale utile

- Recuperare cont Google compromis: *google.com/recover*;
- Verificare activitate și securitate cont Google: *myaccount.google.com/security-checkup*;
- Activare verificare în doi pași (2FA): *google.com/2step*;
- Gestionare permisiuni în canalul YouTube: *youtube.com/permissions*;
- Revocare acces aplicații terțe la contul Google: *myaccount.google.com/permissions*.

LINKEDIN

Semne ale compromiterii contului de social media

- Acces blocat sau date modificate: nu te mai poți conecta sau observi modificări neautorizate în profilul tău (fotografie, e-mail, experiență profesională);
- Notificări suspecte: primești alerte privind activitate de conectare de pe dispozitive sau locații necunoscute;
- Solicitări ciudate către contacte: prietenii sau colegii îți semnalează mesaje neobișnuite, solicitări sau linkuri suspecte trimise de pe contul tău;
- Modificări de securitate: au fost schimbate parola, adresa de e-mail sau alte setări de acces fără acordul tău.

Pași pentru recuperare

1. Raportează compromiterea contului completând formularul oficial LinkedIn: *Formular de contact*;
2. Confirmă-ți identitatea, poți fi rugat să trimiți *o fotografie a unui act de identitate, un selfie sau o declarație notarială*:
   - LinkedIn îți poate bloca temporar contul, pentru verificări de securitate;
   - Procesul poate dura până la 2 săptămâni, în funcție de complexitatea cazului.
3. Dacă ai acces la cont:
   - *Schimbă parola* cu una unică și puternică;
   - *Activează verificarea în doi pași* (2FA) din *Setări și confidențialitate* > *Securitate* > *Verificare în doi pași*;
   - *Verifică* cererile de conectare și mesajele trimise recent pentru *activitate neautorizată*;
   - *Analizează istoricul conectărilor* și *dispozitivele asociate contului*.

Alte măsuri de securitate

- Verifică periodic alertele de conectare și activitatea din cont;
- Fii atent la tacticile de inginerie socială, atacatorii pot pretinde că oferă locuri de muncă, colaborări sau oportunități de afaceri;
- Nu da click pe linkuri suspecte și nu descărca fișiere a căror proveniență nu a fost verificată.

Linkuri oficiale utile

- Raportare cont compromis: *linkedin.com/hacked*;
- Verificarea identității: *linkedin.com/verify*;
- Resetare parolă LinkedIn: *linkedin.com/reset*;
- Activare verificare în doi pași (2FA): *linkedin.com/2step*.

SIGNAL

Semne ale compromiterii contului de social media

Signal este considerată una dintre platformele de mesagerie cele mai sigure disponibile astăzi. Spre deosebire de conturile tradiționale de social media care pot fi compromise prin atacuri de parole sau atacuri online, Signal funcționează cu un model de securitate fundamental diferit. Un atacator necesită acces fizic la dispozitivul tău sau la numărul de telefon pentru a obține controlul contului Signal, făcând-o inerent mai sigură împotriva atacurilor online comune.
Dacă totuși ai impresia că o persoană necunoscută a accesat aplicația fără știrea ta, urmează instrucțiunile următoare pentru a consolida securitatea contului:

1. Reinstalează Signal (dacă este necesar): dacă întâmpini probleme cu aplicația, *dezinstalează și reinstalează Signal exclusiv din magazinul oficial* de aplicații al telefonului tău, din surse oficiale;
2. Introdu numărul de telefon: deschide aplicația Signal și urmează pașii pentru a-ți înregistra numărul de telefon. Asigură-te că introduci numărul corect, inclusiv prefixul de țară;
3. Verifică numărul de telefon: vei primi un SMS cu un *cod de verificare*. Introdu acest cod în aplicație pentru a-ți autentifica numărul și a-ți recupera accesul la cont.

Atenție: Dacă nu primești codul, verifică semnalul, corectitudinea numărului de telefon și dacă nu ai blocat SMS-urile de la numere necunoscute.

4. Introdu PIN-ul Signal: dacă ai avut un PIN Signal setat (*ar trebui să ai*), ți se va cere să-l introduci:
    - Acesta este esențial pentru a-ți recupera lista de contacte, grupurile și setările. *Fără PIN, vei începe cu un cont nou*;
    - Dacă ai uitat PIN-ul, poți încerca opțiunea *„Am uitat PIN-ul”*. Aceasta va reseta contul și îți va permite să setezi un PIN nou, dar *vei pierde toate conversațiile și datele anterioare* (deoarece Signal nu stochează mesajele pe serverele sale).
5. Restaurarea backup-ului local: pe Android, *dacă ai activat backup-ul local*, Signal îți va oferi opțiunea de a-ți restaura istoricul conversațiilor de pe dispozitiv. Asigură-te că ai fișierul de backup și parola de restaurare.

Linkuri oficiale utile

- Informații generale Centrul de Suport Signal: *support.signal.org/*;
- Informații despre PIN-ul Signal și resetare: *support.signal.org/pin*;
- Deconectare dispozitive și Signal Desktop: *support.signal.org/devices*;
- Backup local și restaurare: *support.signal.org/backup*.

TELEGRAM

Semne ale compromiterii contului de social media

- Acces pierdut: nu te mai poți autentifica, chiar dacă primești codul SMS sau ai aplicația instalată;
- Coduri nesolicitate: primești coduri de autentificare fără să le fi cerut;
- Activitate necunoscută: conținut sau mesaje pe care nu le recunoști;
- Nu mai ai acces la contul asociat cu numărul tău, dar contul pare activ pe alte dispozitive.

Pași pentru recuperare

1. Reinstalează aplicația Telegram din magazinul oficial;
2. Deschide aplicația și introdu numărul tău de telefon complet (cu prefix internațional);
3. Primește și introdu codul de autentificare:
   - Dacă ai alte sesiuni active, codul va fi trimis acolo (ex. Telegram Desktop);
   - Dacă nu, codul va veni prin SMS. Verifică și cere re-expediere dacă e nevoie.
4. Dacă ai activat verificarea în doi pași *(2FA)*, introdu parola PIN (Parola Cloud);
5. Dacă ai uitat PIN-ul, folosește opțiunea *Am uitat parola?*:
   - Dacă ai un e-mail de recuperare, vei primi un link de resetare;
   - Fără e-mail de recuperare, vei putea reseta contul complet doar după 7 zile, dar toate datele se vor pierde.

Scenarii de recuperare și soluții

1. Dacă ai pierdut accesul la numărul de telefon:
   - Telegram nu oferă un proces de recuperare a contului fără acces la codul SMS trimis pe numărul de telefon înregistrat sau la aplicațiile active pe alte dispozitive;
   - Nu există un proces oficial de recuperare a contului Telegram fără acces la numărul de telefon asociat;
   - În astfel de cazuri, singura opțiune este *crearea unui cont nou*, folosind același număr (dacă reușești să îl recuperezi de la operatorul tău) sau un număr de telefon nou. Toate datele asociate vechiului cont *vor fi pierdute*.
2. Dacă ai activat verificarea în doi pași (2FA) și ai codul PIN:

Telegram folosește un cod PIN suplimentar pentru autentificare atunci când este activată opțiunea *Verificare în doi pași*. Acest cod este diferit de codul primit prin SMS.

Dacă ai asociat un e-mail atunci când ai activat verificarea în doi pași:

- Apasă pe opțiunea *Am uitat parola?* în ecranul de autentificare;
- Vei primi un *e-mail de resetare* (verifică și folderul spam);
- *După confirmarea* prin e-mail, îți vei putea *seta un nou cod PIN*;
- Avantaj - datele tale din cloud (chat-uri, contacte, grupuri, canale) vor fi păstrate.

Dacă nu ai setat un e-mail de recuperare sau nu mai ai acces la el:

- Telegram nu permite accesul la cont, nici măcar dacă ai codul SMS primit pe telefon;
- Poți opta pentru resetarea completă a contului, dar acest proces presupune:
  - Ștergerea tuturor datelor asociate contului (mesaje, fișiere, canale, grupuri);
  - Să aștepți 7 zile, timp în care nu poți folosi acel număr de telefon pe Telegram;
  - După cele 7 zile, vei putea crea un cont nou cu același număr, dar acesta va fi complet gol.

Linkuri oficiale utile

- Recuperare cont Telegram: *telegram.org/faq#recover*;
- Verificare în doi pași și resetare PIN: *telegram.org/faq#2fa*;
- Informații despre securitatea contului Telegram: *telegram.org/faq#security*.

Notificare incidente

Incidentele de securitate cibernetică pot fi raportate prin Platforma Națională pentru Raportarea Incidentelor de Securitate Cibernetică (PNRISC), accesibilă la adresa: pnrisc.dnsc.ro. De asemenea, este disponibil 1911, numărul unic național de urgență dedicat raportării incidentelor cibernetice.

Securitatea conturilor tale nu ține doar de platformele pe care le folosești, ci și de deciziile pe care le iei. Dacă aplici măsuri simple și le respecți constant, poți reduce considerabil riscul ca datele tale personale sau conturile din social media să fie compromise.

Disclaimer

Pașii specifici pentru resetarea parolei, activarea funcțiilor de securitate sau recuperarea contului pot varia în funcție de platforma utilizată, tipul de dispozitiv (mobil sau desktop), precum și de modificările aduse interfeței aplicațiilor în urma actualizărilor.

Informațiile prezentate în acest ghid reflectă metodologia generală și cele mai frecvent întâlnite proceduri valabile la momentul redactării. Pentru instrucțiuni exacte și actualizate, se recomandă consultarea secțiunilor oficiale de Asistență sau Ajutor ale platformelor respective.

Autori: Daniel Abotezătoaei, Cristian Nistor, Radu Adrobotoaei

TLP:CLEAR se poate folosi atunci când informațiile prezintă un risc minim de utilizare abuzivă, în conformitate cu normele și procedurile aplicabile pentru publicare. Sub rezerva regulilor standard ale drepturilor de autor, informațiile TLP:CLEAR pot fi partajate fără restricții.

https://www.dnsc.ro/