Ghid de protejare și recuperare conturi social media

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Riscuri și amenințări

Măsuri de combatere

Facebook

Instagram

TikTok

WhatsApp

YouTube

Notificare incidente

Scanează-mă!

TLP:CLEAR

Riscuri și amenințări

Conturile de social media sunt expuse la diverse riscuri cibernetice, iar utilizatorii ar trebui să fie conștienți de amenințările potențiale pentru a-și proteja informațiile personale și prezența online. Iată câteva riscuri cibernetice comune asociate conturilor de social media:

Preluarea controlului asupra contului (Account Takeover Attack - ATO): Atacatorii cibernetici pot încerca să obțină acces neautorizat la conturile tale de social media prin utilizarea de parole furate sau exploatare de vulnerabilități. După ce au obținut controlul, ei pot să-ți fure identitatea, să posteze informații false ori conținut malițios sau să acceseze informații sensibile.

Atacuri de phishing: Phishing-ul implică inducerea în eroare a utilizatorilor pentru a furniza informații sensibile, cum ar fi date de autentificare, personale sau financiare. Atacatorii reușesc să le extragă de la utilizatori prin prezentarea unor scenarii și pretexte diverse, în care potențiala victimă este încurajată să furnizeze datele. Atacatorii fac uz de tehnici de inginerie socială și de elemente de identitate vizuală care au rolul de a oferi o doză de încredere și legitimitate acțiunii. Un exemplu ar fi site-urile clonă, care arată similar cu cel original, dar care este accesibil pe un domeniu diferit. Utilizatorii sunt contactați prin e-mail, sms, social media ori platforme de tip chat. Mesajele includ linkuri malițioase cu rolul de a redirecționa potențiala victimă către pagini de autentificare frauduloase, controlate de atacatori și menite să le captureze credențialele.

Distribuția de malware: Atacatorii cibernetici pot utiliza platformele de social media pentru a distribui malware. Acest lucru se poate întâmpla prin link-uri sau atașamente malițioase în mesaje sau postări. Făcând clic pe aceste link-uri, se poate instala malware pe dispozitivul tău.

Inginerie socială: Atacatorii cibernetici pot folosi tehnici de inginerie socială pentru a manipula utilizatorii și a-i determina să dezvăluie informații sensibile. Acest lucru ar putea implica deghizarea atacatorilor în prieteni, cunoștințe sau persoane de încredere, pentru a obține acces la informații sensibile.

Măsuri de combatere

Protejarea conturilor tale de social media este esențială pentru a-ți păstra informațiile personale în siguranță și a preveni accesul neautorizat. Câteva sfaturi:

Parole puternice: Creează parole puternice, cu o combinație de litere mici și mari, cifre și caractere speciale. Evită parolele evidente, cum ar fi datele de naștere sau numele de familie.

Autentificare în doi pași (2FA): Activează autentificarea în doi pași pentru un strat suplimentar de securitate. Acest lucru implică furnizarea unui cod generat pe dispozitivul tău mobil sau prin e-mail, în plus față de parolă.

Actualizări regulate ale parolelor: Schimbă parolele periodic și evită folosirea aceleiași parole pentru mai multe conturi. Parola trebuie să fie distinctă pentru fiecare cont.

Revizuirea setărilor de confidențialitate: Verifică și ajustează regulat setările de confidențialitate pentru a controla cine poate vedea informațiile tale și cine poate interacționa cu conținutul tău.

Evitarea linkurilor suspecte: Fii precaut în privința link-urilor și atașamentelor primite prin mesaje sau e-mail. Nu accesa link-uri suspecte sau provenite de la surse necunoscute.

Atenție la încercările de phishing: Fii conștient de posibile încercări de phishing și nu furniza niciodată informații personale sau date de conectare, în urma unor solicitări suspecte.

Actualizări regulate ale aplicațiilor: Asigură-te că aplicațiile de social media și cele asociate sunt actualizate la ultima versiune, pentru a beneficia de cele mai recente opțiuni de securitate.

Verificarea sesiunilor active: Monitorizează sesiunile active și dispozitivele conectate la contul tău de social media. Deconectează sesiunile neautorizate.

Folosirea unui VPN: Dacă te conectezi la conturile tale de social media pe rețele publice, utilizează o rețea privată virtuală (VPN) pentru a securiza conexiunea.

Evitarea aplicațiilor neoficiale: Descarcă aplicațiile oficiale ale platformelor de social media și evită utilizarea aplicațiilor neoficiale sau dubioase.

Cum îți poți recupera contul de Facebook

În cazul în care nu mai poți să îți accesezi contul de Facebook, este posibil ca cineva să îți fi schimbat datele de acces și contul să fi fost compromis. *Ce ai de făcut?*

1. Intră la adresa https://www.facebook.com/login/identify
2. Introdu adresa de e-mail cu care te-ai înregistrat sau numărul de telefon
3. Urmează pașii de pe ecran pentru a reseta parola contului

Poți cere ajutorul unui prieten. *Ce ai de făcut ?*

1. Roagă-l pe prietenul tău să caute contul tău
2. Intră pe contul tău. În partea dreaptă ai să vezi trei puncte (...)
3. Fă clic pe ele și o să apară un meniu
4. De acolo alegi **Primește ajutor sau raportează**
5. Aici alegi una din variante și urmezi pașii

Activități suspecte în contul tău

Dacă vezi orice activitate pe care nu o recunoști în contul tău, este un indiciu că acesta ar fi putut fi compromis, iar atacatorii au acces la el. *Dacă observi schimbări:*

- Numele, ziua de naștere, adresa de e-mail sau parola se schimbă brusc
- Solicitările de prietenie din contul tău sunt trimise persoanelor pe care nu le cunoști
- Mesajele pe care nu le-ai scris sunt trimise din contul tău
- Postări pe care nu le-ai creat apar pe cronologia ta

Dacă ai descoperit genul acesta de activități pe contul tău, dar încă poți accesa contul, urmează acești pași:

1. Accesează profilul tău de Facebook și caută **Setări și confidențialitate,** apoi **Setări**
2. Apasă pe **Parolă și securitate** pentru a vedea **Schimbă parola**
3. Introdu parola actuală, apoi introdu o parolă nouă (de minim 6 caractere, care sa cuprindă litere, cifre și caractere speciale)
4. Ar fi bine să folosești mai mult de 10 caractere. Un exemplu bun de parolă: !miplac35am3rglaMare (Îmi place Să merg la Mare)
5. Apasă pe **Schimbă parola**

Verifică dacă contul tău de Facebook a fost piratat

Cum poți verifica dacă ai fost piratat? Urmează acești pași pentru a afla dacă altcineva s-a conectat la contul tău de Facebook:

1. Accesează profilul tău de Facebook și caută **Setări și confidențialitate** apoi **Setări**
2. Apasă pe **Parolă și securitate** pentru a vedea **Unde te-ai conectat** apoi **Vedeți tot** (pe mobil) și verifică dacă recunoști dispozitivele care apar în listă
3. Dacă vezi un dispozitiv pe care nu îl recunoști, apasă pe numele dispozitivului, apoi pe **Selectează dispozitivele de pe care vrei să te deconectezi**
4. Bifează dispozitivele pe care vrei să le deconectezi, apoi click pe **Deconectare**

Cum îți poți recupera contul de Instagram

Dacă ai suspiciuni legate de contul tău de Instagram sau nu te mai poți conecta la el, accesează pagina oficială a centrului de ajutor Instagram (https://www.instagram.com/hacked/) pentru a începe demersurile de recuperare. Pentru a identifica contul de Instagram, este nevoie de **numele de utilizator, numărul de telefon** sau **adresa de e-mail.**

Verifică dacă adresa de e-mail asociată contului a fost schimbată

Dacă ai primit un e-mail de la **security@mail.instagram.com** prin care ești înștiințat că adresa ta de e-mail a fost schimbată, poți anula această modificare selectând **Securizează contul** din mesaj. Dacă au fost modificate și alte informații (parola, numele de utilizator) și nu poți schimba adresa de e-mail, solicită un link de conectare sau un cod de securitate de la Instagram.

Solicită un link de conectare de la Instagram

Poți solicita un link de conectare pe adresa de e-mail sau la numărul tău de telefon urmărind pașii de mai jos:

- Pe ecranul de conectare, atinge **Obține ajutor** pentru conectare
- Introdu numele de utilizator, adresa de e-mail sau numărul de telefon asociat contului tău, apoi accesează opțiunea **Trimite linkul de conectare**. Dacă nu ai acces la numele de utilizator, la adresa de e-mail sau la numărul de telefon asociat contului tău, vizitează această pagină și urmează instrucțiunile de pe ecran. Finalizează verificarea **captcha** pentru a confirma că ești o persoană reală, apoi apasă pe **Continuare**
- Apasă pe linkul de conectare din e-mail sau din mesajul text primit (SMS) și urmează instrucțiunile

Solicită un cod de securitate sau asistență de la Instagram:

Dacă nu reușești să-ți recuperezi contul folosind linkul de conectare, poți solicita asistență pe un dispozitiv mobil. Asigură-te că introduci o adresă de e-mail sigură, la care doar tu ai acces. După ce trimiți solicitarea, ar trebui să primești de la Instagram un e-mail care conține pașii ce trebuie urmați. Află mai multe despre ce poți face dacă nu-ți cunoști numele de utilizator.

Confirmă-ți identitatea

Dacă soliciți asistență pentru **un cont care conține fotografii cu tine**, ți se va cere să înregistrezi un selfie video cu tine întorcând capul în direcții diferite, pentru a verifica dacă ești o persoană reală. După ce trimiți selfie-ul video, vei primi un e-mail de la Instagram la adresa de e-mail pe care ai menționat-o. Acest clip video va fi folosit pentru a-ți confirma identitatea.

Dacă ai trimis o cerere de asistență pentru **un cont care nu conține fotografii cu tine**, ar trebui să primești prin e-mail un răspuns automat de la echipa de asistență Meta. Va trebui să menționezi adresa de e-mail sau numărul de telefon cu care te-ai înscris și tipul de dispozitiv pe care l-ai folosit în momentul înscrierii.

Dacă te poți conecta în continuare la contul de Instagram:

În cazul în care ti-a fost spart contul, dar te poți conecta în continuare la el, iată câteva lucruri pe care le poți face pentru a încerca să-ți păstrezi contul în siguranță:

- Asigura-te că numărul de telefon și adresa de e-mail din setările contului sunt corecte
- Schimbă-ți parola sau trimite-ți un e-mail de resetare a parolei
- Activează autentificarea cu doi factori pentru securitate sporită
- Accesează Administrare conturi și șterge conturile asociate pe care nu le recunoști
- Revocă accesul oricărei aplicații terțe suspecte

Cum îți poți recupera contul de TikTok

Dacă observi oricare dintre următoarele comportamente suspecte, contul tău cel mai probabil a fost compromis:

- Parola contului sau numărul de telefon au fost schimbate
- Numele de utilizator sau pseudonimul contului tău a fost schimbat
- Videoclipurile au fost șterse sau postate fără permisiunea ta
- Mesajele pe care nu le-ai scris au fost trimise din contul tău

Trebuie să raportezi incidentul:

1. Atinge **Profil** în dreapta jos
2. Atingeți **pictograma cu 3 linii** din dreapta sus
3. Atingeți **Setări și confidențialitate**
4. Atingeți **Raportați o problemă**
5. Selectează un subiect de raport

De asemenea, poți urma acești pași pentru a securiza contul:

Schimbarea parolei

- În cazul în care consideri că este posibil să-ți fi fost compromis contul, schimbă parola cât mai curând posibil. Alege o parolă memorabilă pentru tine, dar dificil de ghicit de alți utilizatori.
- Află cum să-ți resetezi parola TikTok

Activează verificarea în 2 pași

- Verificarea în 2 pași adaugă un nivel suplimentar de securitate contului tău, în cazul în care parola este compromisă. De asemenea, te ajută să-ți protejezi contul de dispozitive nerecunoscute/neautorizate sau de aplicații terțe. Află cum să activezi verificarea în 2 pași

Verifică dispozitivele pe care ești conectat

- Poți vizualiza telefoanele și alte dispozitive mobile care utilizează în prezent sau care ți-au accesat recent contul TikTok. Află cum să accesezi dispozitivele conectate

Verifică alertele de securitate

- Pentru a examina alertele de securitate, accesează setările aplicației TikTok, apasă **Securitate și conectare**, după care apasă **Alerte de securitate**

Cum îți poți recupera contul de WhatsApp

Este bine să îți informezi prietenii și membrii familiei dacă bănuiești că o altă persoană îți folosește contul de WhatsApp, deoarece atacatorii ar putea folosi identitatea și încrederea generată de acel cont în conversații și grupuri. Reține că WhatsApp este criptat integral și că mesajele se stochează pe dispozitivul tău, așa că, dacă cineva îți accesează contul de pe alt dispozitiv, **această persoană nu îți poate citi conversațiile anterioare.**

Nu comunica nimănui codul de verificare WhatsApp primit prin SMS, nici măcar prietenilor sau membrilor familiei! Fără acest cod, niciun utilizator care încearcă să îți verifice numărul nu va putea finaliza procesul de verificare și nu îți va putea folosi numărul de telefon pe WhatsApp.

Dacă cineva îți obține codul în mod fraudulos, iar tu îți pierzi accesul la contul WhatsApp, urmează instrucțiunile de mai jos pentru a-l recupera:

- Conectează-te la WhatsApp cu numărul de telefon, apoi verifică-ți numărul introducând codul din 6 cifre pe care îl primești prin SMS
- După ce introduci codul din 6 cifre primit prin SMS, **persoana care îți folosește contul va fi deconectată automat**
- Este posibil să ți se ceară să introduci și codul pentru verificarea în doi pași. Dacă nu știi acest cod, probabil persoana care ți-a folosit contul a activat verificarea în doi pași
- Trebuie să **aștepți 7 zile** până să te poți conecta fără **codul de verificare în doi pași.** Indiferent dacă știi sau nu acest cod de verificare, persoana care ți-a folosit contul este deconectată în momentul în care introduci codul din 6 cifre primit prin SMS

WhatsApp oferă asistență utilizatorilor, aceasta fiind disponibilă pe telefon, în aplicație, în secțiunea **WhatsApp > Setări > Ajutor > Contactați-ne** sau site-ul oficial al aplicației, în secțiunea Contactați-ne.

Dacă ți-ai pierdut sau ți s-a furat telefonul, asistența WhatsApp nu poate face nimic. Nu se poate dezactiva contul WhatsApp, deoarece nu există posibilitatea de a verifica dacă ești proprietarul numărului de telefon asociat contului respectiv.

Cum îți poți recupera contul de YouTube

Înainte de a lua măsuri, este important să verifici încă o dată dacă există semne că ți-a fost compromis canalul. Fiecare canal YouTube este asociat cel puțin unui cont Google. Când un canal YouTube este compromis, înseamnă că este compromis și cel puțin unul dintre conturile Google asociate canalului.

Dacă observi oricare dintre activitățile de mai jos în contul Google, s-ar putea ca acesta să fi fost piratat sau compromis:

- Modificări pe care nu le-ai făcut: fotografia de profil, descrierile, setările pentru e-mail, asocierea cu contul AdSense sau mesajele trimise sunt diferite
- Videoclipuri încărcate care nu-ți aparțin: cineva a postat videoclipuri de pe contul tău Google. S-ar putea să primești notificări prin e-mail despre aceste videoclipuri pentru penalizări sau avertismente pentru conținut neadecvat

Pentru a recupera un canal YouTube compromis, este necesar mai întâi să recuperezi contul Google compromis, asociat canalului YouTube. Trei pași pentru a-ți recupera canalul YouTube:

1. Recuperează și securizează contul Google compromis, asociat canalului YouTube
2. Anulează imediat modificările nedorite de pe canalul YouTube pentru a evita repercusiunile privind politicile, cum ar fi regulile comunității sau avertismentele privind drepturile de autor
3. Redu riscul de acces neautorizat la contul Google folosind cele mai bune practici privind securitatea pentru toți utilizatorii canalului asociat

Recuperează-ți contul Google

Dacă încă te poți conecta la contul Google este important să actualizezi parola și să securizezi contul Google. Dacă nu te poți conecta la contul Google:

1. Urmați pașii ca să vă recuperați contul Google sau Gmail. Vi se vor pune câteva întrebări pentru a confirma că este contul dumneavoastră și răspundeți corect la ele. Dacă întâmpinați probleme, urmați sfaturile pentru finalizarea pașilor de recuperare a contului
2. Resetați parola când vi se solicită. Alegeți o parolă puternică pe care nu ați mai folosit-o pentru acest cont. Aflați cum să creați o parolă puternică
3. Solicită-le managerilor / proprietarilor de canal să urmeze aceiași pași pentru a-și securiza contul Google

Notificare incidente

Raportarea se poate face prin formularul online de pe pagina de web www.dnsc.ro, alerts@dnsc.ro sau apelarea la 1911, care este numărul unic de urgență la nivel național dedicat raportării incidentelor de securitate cibernetică.

- Dacă ați primit un **e-mail suspect**, trimiteți-l către alerts@dnsc.ro sau apelați 1911
- Dacă ați primit un **mesaj text suspect**, raportați-l prin formularul online de pe pagina de web www.dnsc.ro, trimiteți-l către alerts@dnsc.ro sau apelați 1911
- Dacă ați primit apeluri telefonic suspecte, închideți, blocați utilizatorul și contactați furnizorul dvs. de telefonie.

Acest ghid a fost realizat de următorii experți ai DNSC:

Mihai Rotariu, Daniel Abotezătoaei, Dan Andrieș, Mihaela Dan, Irina Nemoianu, Cristian Nistor