



Ghid informativ privind recuperare conturilor online compromise

INTRODUCERE

Fie ca este vorba de contul de poștă electronică, conturile de pe rețele sociale, internet banking, pierderea accesului la un cont digital poate fi stresantă și să aibă impact atât social cât și financiar.

Acest ghid explică ce acțiuni pot fi întreprinse pentru minimalizarea prejudiciul provocat și cum poate fi restabilit accesul la conturile online.

Indicatori de compromitere a contului

Verifică conturile online pentru a analiza dacă nu a avut loc o activitate neautorizată precum :

- imposibilitatea de a te loga la conturile tale;
- schimbări la setările de securitate;
- mesaje sau notificări trimise de pe contul tău pe care tu nu le recunoști;
- conectări sau încercări de conectare de la locații ciudate și la o ore neobișnuite;
- transferuri bănești sau cumpărături neautorizate de la conturile tale online.

Acțiunile necesare în cazul în care contul tău a fost compromis

1.Contactează furnizorul contului – Accesează pagina web a furnizorului și caută rubrica dedicată ajutor sau suport. Acolo îți se vor oferi instrucțiuni detaliate a procesului de recuperare a contului (acestea pot fi diferite pentru fiecare cont). Dacă nu poți găsi ce ai nevoie pe website folosește un motor de căutare (de exemplu: *"Cum îmi pot recupera contul Twitter"*) și urmează link-ul.

2.Verifică contul tău de e-mail – Verifică filtrele și regulile de redeționare. O tactică specifică folosită de infractorii cibernetici este de a configura regulile de redeționare, ceea ce înseamnă ca automat se vor transmite câte o copie a tuturor email-urilor trimise de pe contului tău (ceea ce le va permite lor ca să-ți reseteze parola). Din nou, poți găsi instrucțiuni detaliate pe website-ul furnizorului sau poți folosi motoarele de căutare.

3.Schimbarea parolelor – După ce v-ați asigurat că nu există reguli nedorite de redeționare a email-urilor trebuie să:

- Să schimbi parola pentru orice cont care a fost compromis
- Să schimbi parola pentru orice cont care utilizează aceeași parolă.

Ambii pașii sunt importanți, deoarece infractorii cibernetici știu că foarte mulți oameni folosesc aceeași parolă pentru diferite conturi, și vor încerca parola sustrasă la mai multe conturi.

4.Dezloghează toate dispozitivele și aplicațiile de la contul tău – După ce ai schimbat parola trebuie să te asiguri că orice dispozitiv și aplicație (care încă mai pot fi logate) sunt dezlogate de la contul în cauză. Acesta de obicei poate fi făcut din meniul **Setări** ale aplicațiilor sau website-urilor Pentru instrucțiunile specifice cum să realizezi acest punct trebuie să accesezi pagina de suport a serviciului relevant. După acesta oricine va încerca să acceseze contul tău i se va cere noua parolă.

5.Setați verificarea în doi pași (2FA) – Multe conturi și servicii online îți permit să setezi autentificare în doi pași, ceea ce înseamnă că chiar dacă infractorii îți cunosc parola oricum nu vor putea accesa conturile tale. 2FA de obicei lucrează prin trimiterea a unui cod PIN, de obicei prin SMS sau email, care va trebuie să-l introduci ca să demonstrezi că ești tu cu adevărat.

Acțiunile necesare în cazul în care contul tău a fost compromis

6.Actualizează-ți dispozitivul – Trebuie să-ți aplici actualizările de program la aplicațiile și dispozitivele tale imediat ce sunt accesibile. Actualizările conțin protecția împotriva virusilor și des conțin îmbunătățiri și noi caracteristici. Aplicarea actualizărilor este unul din cele mai importante (și rapide) acțiuni ce pot fi întreprinse ca să previi compromiterea conturilor. La fel trebuie să acorzi permisiunea în setări a ”actualizărilor automate” dacă sunt disponibile, aceasta va înseamna că nu trebuie să memorizezi că dispozitivul sau aplicația trebuie actualizată.

Notă: actualizările dispozitivului îți vor lua ceva timp și pot cere o conexiuni de internet rapidă, de aceea e bine ca acesta să fie făcută de acasă unde poți să accesezi Wi-Fi-ul (și să-ți păstrezi dispozitivul conectat).

7.Notificați persoanele dvs de contact – Contactați contactele dvs, prieteni, urmăritor, lăsați să cunoască că ați fost piratat și sugerați-le să trateze mesajele recent primite de la contul compromis. Acesta îi va ajuta pe ei să evite compromiterea conturilor personale, sau să devină victime ale escrocheriilor desfășurate prin inginerie socială prin impersonalizarea dvs de către atacatori.

8.Verificați extrasele din cont și conturile pentru cumpărăturile online – Deseori conturile de email compromise pot duce la compromitere și în altă parte. Fiți atenți la achizițiile neautorizate sau verificați extrasele bancare pentru a vedea orice tranzacție neautorizată. Puteți contacta banca dumneavoastră pentru suport. Mereu folosiți un website autorizat, un canal social media autorizat sau introduceți adresa direct în browser. Nu folosiți linkurile din mesajele trimise.

9.Contactați organele specializate – Dacă ați pierdut bani anunțați banca și raportați la organele de drept specializate (ex. poliția). Așa veți contribui la reducerea activității infracționale sau măcar pe viitor să se prevină apariția unor noi victime.

! În unele cazuri nu este posibil recuperare contului cu ajutorul serviciilor online, în acest caz veți fi nevoit să creați un nou cont dacă doriți pe viitor să utilizați aceste servicii. Dar dacă faceți acesta este important să dați contactelor dvs noile detalii și să-i informați că ați abandonat contul vechi.