Cardul dvs. de credit sau detaliile bancare au fost furate?

Zilnic, tot mai mulți oameni se bucură de experiența cumpărăturilor online. Cumpărătorii trebuie să rămână prudenți întrucât escrocii sunt mereu în căutare de modalități de a fura datele cardurilor sau detaliile bancare!

Aceștia folosesc site-uri web false, se prezintă ca vânzători pe site-urile de licitații sau pot trimite, de asemenea, e-mailuri frauduloase (phishing) susținând că provin de la site-uri de plată sau de vânzare cunoscute.

Ce e de făcut?

Dacă contul dvs. bancar a fost compromis sau observați o activitate neobișnuită pe contul cardului dvs., iată câțiva pași pe care îi puteți face:

1. **Contactaţi-vă banca** imediat pentru ca aceasta să vă blocheze contul şi/sau respectiv cardul bancar. Este posibil să vă puteţi revendica banii şi să preveniţi furturile ulterioare.

3. **Actualizaţi** software-ul antivirus pentru a lupta împotriva viruşilor noi şi a vă proteja dispozitivul.

63%

2. În momentul accesării site-ului comerciantului de unde doriți sa achiziționați bunuri sau servicii, verificați tipul conexiunii. Accesați doar site-uri care folosesc **tehnologia SSL** (Secure Socket Layer).

Cum ştiți că este un site securizat? Dacă adresa afișată în bara browser-ului începe cu HTTPS:// (în loc de HTTP://), iar în bara de adrese sau pe bara de la baza paginii, este afișată o mică imagine a unui lacăt închis, inseamnă că acel site este unul securizat (schimbul de informații între calculatorul dvs. şi site este criptat, securizat).

Achizitionați de la comercianți cu reputație. **Nu cumpărați de pe site-uri care nu pot oferi condiții de securitate a plății.** Aceste condiții sunt întrunite în programele Verified by **VISA** şi **MasterCard SecureCode** marcate cu pictograme dedicate.

Vă recomandăm să **nu salvați datele cardului** în contul de client deschis la comerciant, chiar dacă exista inconvenientul de a introduce de fiecare dată informațiile despre card.

4. **Reportaţi frauda**.
Informațiile dvs. pot ajuta la identificarea mai rapidă a escrocilor şi preveni astfel apariţia altor victime.

5. Asigurați-vă că păstrați orice **dovadă** a furtului, de ex. e-mailuri, facturi, chitanțe, sms-uri, extrasuri bancare etc.

7. **Împărtășiți-vă experiența şi lecțiile învățate** cu familia şi prietenii pentru a-i proteja de experiențe similare.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

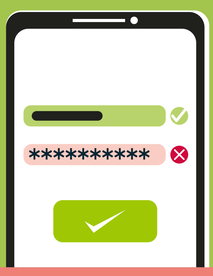
EUROPEAN CYBER SECURITY MONTH

#CyberSecMonth #ThinkB4UClick

I.P „Serviciul Tehnologia Informației şi Securitate Cibernetică”

V-a fost spart contul de socializare?

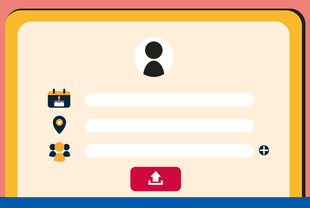
Semne de identificare



• Aveţi probleme la conectarea la contul dvs.
• Veţi primi un mesaj care vă informează că parola contului a fost schimbat, dar nu aţi făcut-o;
• Vedeţi postări pe care nu le-aţi scris;
• Urmăriţi brusc mulţi oameni pe care nu îi cunoaşteţi sau nu îi urmăreaţi anterior;
• Vedeţi o autentificare dintr-o locaţie neobişnuită;
• Primeşti o mulţime de reclame tip spam.

Ce semnifică asta?

Consecinţele de pe urma spargerii sau furtului contului dvs. personal depind de cât de multe informaţii personale aţi partajat în cadrul acestuia, de ex. data naşterii, adresa, locul de muncă, nr.de telefon, numele membrilor de familie - informaţiile dvs. ar putea fi utilizate pentru a accesa alte conturi sau a vă fura identitatea şi comunica cu alte persoane.



Ce e de făcut?

Dacă încă puteţi accesa contul

• **Schimbaţi-vă parola .** Atacatorul deţine vechea parolă aşa că, actualizaţi prin una mai puternică: din minim 15 caractere inclusiv cifre, litere minuscule, majuscule şi semne speciale, dacă permite sistemul.

• De asemenea, ar trebui să modificaţi **datele de conectare** pentru oricare dintre celelalte conturi care folosesc acelaşi numele de utilizator şi parola sau ceva similar. Aceasta include aplicaţii care sunt legate de logarea prin contul de socializare.

• Utilizaţi **parole unice** pentru fiecare cont personal.

• Asiguraţi-vă că sunteţi securizat la maxim. Verificaţi setările din rubricile **security and privacy settings** unde puteţi activa toate instrumentele oferite de platforma de socializare (de ex. autentificare dublă, drept de acces restricţionat după locaţie etc).

Dacă nu mai puteţi accesa contul:

- Urmaţi **paşii de recuperare** a contului recomandaţi de furnizor. Contactaţi centrul de suport sau ajutor a platformei pentru sfaturi.
-

Totodată:

• **Raportaţi contul.** Dacă furtul contului vă afectează imaginea sau are un impact negativ asupra altor utilizatori, contactaţi furnizorul şi raportaţi pagina sau solicitaţi prietenilor din cadrul platformei să o facă, pentru un răspuns cât mai rapid.

· **Anunţaţi lista dvs. de contact** că, contul dvs. a fost compromis. Aceştia pot primi mesaje sau pot vedea postări trimise din contul dvs., care conţin frauduloase link-uri sau informaţii înşelătoare. Anunţă-i că nu sunteţi responsabil de acel conţinut pentru ca ei să nu acceseze link-uri riscând să devină noi victime de atac.

• **Împărtăşiţi-vă experienţa şi lecţiile învăţate** cu familia şi prietenii pentru a-i proteja de experienţe similare.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

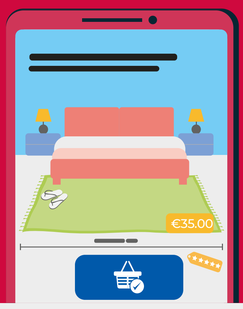
EUROPEAN CYBER SECURITY MONTH
#CyberSecMonth #ThinkB4UClick

I.P „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică”

Aţi devenit victima înşelăciunilor online?

Încă aşteptaţi ceva achiziţionat online? Sau produsul pe care l-aţi primit nu se potriveşte cu ceea ce aţi comandat? Atunci este posibil că aţi devenit victima unei înşelătorii online.

Escrocheriile sunt din ce în ce mai sofisticate şi cu toţii greşim. O înşelătorie de cumpărături online este atunci când efectuezi o achiziţie online, fără să ştii, de pe un site web fals sau dintr-un anunţ fals pe un site real. Este posibil ca produsul să nu existe într-adevăr, să fie contrafăcut sau de calitate inferioară.



Ce e de făcut?

1. Încercaţi să contactaţi **comerciantul cu amănuntul**, poate există un motiv real al problemei.

2. Contactaţi imediat banca dvs. dacă:

- contul dvs. bancar a fost compromis;
- observaţi activitate neobişnuită pe cardul dvs. de cont;
- nu primiţi un răspuns sau
- nu sunteţi mulţumit de răspunsul de la comerciantul cu amănuntul

Este posibil să preveniţi astfel un furt ulterior.

3. Schimbaţi parolele. Escrocul poate avea parola dvs., aşa că schimbaţi-o într-o **parolă puternică**, cu cel puţin **15** caractere, inclusiv litere mari şi mici, cifre şi simboluri.

O **expresie de acces** poate fi mai uşor de reţinut. Asta ar putea fi o propoziţie care include cuvinte neobişnuite sau cuvinte din diferite limbi.

Ar trebui, de asemenea, să schimbaţi **detaliile de conectare** pentru oricare dintre alte conturi ale dvs. care utilizează acelaşi nume de utilizator şi parolă, întrucât acestea ar putea fi uşor compromise.

Utilizaţi **parolă unică** pentru fiecare cont personal.

4. **Actualizaţi** software-ul antivirus pentru a lupta împotriva viruşilor noi şi a vă proteja dispozitivul

5. **Raportaţi frauda**. Informaţiile dvs. pot ajuta la prinderea escrocilor şi preveni alte incidente similare.

6. Asiguraţi-vă că păstraţi orice **dovadă** a furtului, de ex. e-mailuri, facturi, chitanţe, copie a publicităţii etc.

7. Împărtăşiţi-vă **experienţa şi lecţiile învăţate** cu familia şi prietenii pentru a-i proteja de experienţe similare.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBER SECURITY MONTH

#CyberSecMonth #ThinkB4UClick

I.P „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică”