Salut, avem un mesaj important pentru tine

În ultima perioadă, au fost identificate mai multe acţiuni de tip phishing şi alte fraude, care par a fi autentice. Acest ghid te va ajuta să recunoşti şi să eviţi aceste capcane online şi telefonice.

Care sunt tipurile de fraude?

Fraude online

a. Phishing

Infractorii trimit e-mailuri care par reale şi cer informaţii personale. De obicei, aceste mesaje includ link-uri către site-uri false. – (ex. Not Secure | bankabt.com , capital2#partners.com etc)

b. Vishing

Phishing prin apeluri telefonice, unde escrocii pretind că sunt de la bancă şi cer informaţii confidenţiale.

c. Malware

Programe maliţioase instalate pe dispozitivele tale care fură informaţii bancare.

d. Reţele Sociale

Infractorii folosesc rețele sociale (Facebook, LinkedIn, Instagram, TikTok etc) pentru a aduna informaţii şi a accesa conturi bancare.

Fraude telefonice

a. Apeluri falsificate

Infractorii folosesc numere false, pretinzând că sună de la bancă şi cer informaţii personale.

b. SMS-uri false (Smishing)

Mesaje text false care par să fie de la bancă şi cer informaţii sau accesarea unor link-uri nesigure.

c. Aplicaţii de control la distanţă

Infractorii cer instalarea unor aplicaţii de tip remote control, precum Anydesk sau BIZ Daemon, pentru a accesa dispozitivele victimei şi a prelua controlul asupra conturilor bancare.

Exemple de fraude recente

- Campanii publicitare false care par a fi lansate de companii din Grupul Financiar Banca Transilvania sau de intermediari autorizaţi de Autoritatea de Supraveghere Financiară (A.S.F.) şi promit câştiguri semnificative din investiţii.
- Apeluri telefonice/email-uri neautorizate, de la persoane care pretind că sunt reprezentanţi ai companiilor menţionate şi promovează investiţii, cer informaţii personale
- Apeluri telefonice, de la persoane care pretind că sunt reprezentanţi ai companiilor menţionate şi solicită instalarea de aplicaţii de control la distanta prin care reuşesc să acceseze conturi şi tranzacţii.

Aceste campanii publicitare sunt FRAUDE!

Societăţile din Grupul Financiar Banca Transilvania şi intermediarii autorizaţi de A.S.F. nu iniţiază astfel de demersuri nici prin email, nici telefonic, nu oferă sfaturi de investiţii, nu solicită sume de bani şi nici date cu caracter personal.

Cum să te protejezi?

Online

- Nu divulga informaţii personale prin e-mail sau text.
- Verifică adresa URL - asigură-te că site-ul este sigur (simbol de lacăt şi https).
- Actualizează software-ul - menţine programele şi aplicaţiile la zi.

Telefonic

- Nu divulga informaţii personale la telefon - băncile nu cer informaţii sensibile prin telefon(ex. CNP, domiciliu, parole, cod PIN etc).
- Verifică identitatea apelantului - sună banca la numărul oficial dacă ai dubii.
- Nu accesa link-uri din mesaje text suspecte.

Dacă consideri că eşti pus şi tu în situaţia fraudelor recente, ai în minte următoarele:

- Abordează cu precauţie orice telefon sau email.
- Verifică întotdeauna adresele şi numerele de telefon de la care eşti contactat.
- Nu furniza datele de pe cardul bancar - **BT CAPITAL PARTNERS şi companiile din Grupul Financiar Banca Transilvania nu solicită niciodată numărul sau codul CVV/CVC al cardului**.
- Vizitează doar paginile oficiale - asigură-te că vizitezi paginile oficiale ale companiilor şi intermediarilor autorizaţi de A.S.F. pentru a evita site-urile false.

Cum îţi dai seama că eşti contactat în mod fraudulos?

- Primeşti apeluri telefonice de la numere internaţionale.
- Primeşti emailuri de la conturi de tip Hotmail, Yahoo, Gmail etc.
- Mesajele care ajung la tine au greşeli gramaticale sau de ortografie.
- Adrese de website şi conturi de reţea socială cu mici modificări faţă de cele oficiale.
- În cadrul discuţiilor telefonice ţi se fac promisiuni de câştiguri rapide cu investiţii minime.
- Ţi se spune să îţi instalezi aplicaţii de tip remote control (ex. Anydesk, BIZ Daemon etc).

Ce să faci dacă eşti victima unei fraude?

Contactează imediat banca şi BT Capital Partners fie telefonic şi discută următorii paşi, fie scrie un mail la risc@btcapitalpartners.ro pentru a lua măsurile necesare şi a redirecţiona mesajele către reprezentanţii companiilor din cadrul Grupului
Nu uita să îţi schimbi parolele.

Reţine: Fraudele bancare sunt un risc real. Fii informat, ia măsuri preventive şi raportează orice activitate suspectă. Fii vigilent şi protejează-ţi datele personale şi financiare!
Te invităm să urmăreşti următoarele materiale despre siguranţa online:
Siguranţă online by BT - YouTube

Îţi mulţumim!