



## Salut, avem un mesaj important pentru tine

În ultima perioadă, au fost identificate mai multe acțiuni de tip phishing și alte fraude, care par a fi autentice. Acest ghid te va ajuta să recunoști și să eviți aceste capcane online și telefonice.

Societățile din Grupul Financiar Banca Transilvania și intermediarii autorizați de A.S.F. nu inițiază astfel de demersuri nici prin email, nici telefonic, nu oferă sfaturi de investiții, nu solicită sume de bani și nici date cu caracter personal.

### Cum să te protejezi?

#### Online

- Nu divulga informații personale prin e-mail sau text.
- Verifică adresa URL - asigură-te că site-ul este sigur (simbol de lacăt și https).
- Actualizează software-ul - menține programele și aplicațiile la zi.

#### Telefonic

- Nu divulga informații personale la telefon - băncile nu cer informații 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 ești pus și tu în situația fraudelor recente, ai în minte următoarele:

- Abordează cu precauție orice telefon sau email.
- Verifică întotdeauna adresele și numerele de telefon de la care ești contactat.
- Nu furniza datele de pe cardul bancar – **BT Asset Management și 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 și intermediarilor autorizați de A.S.F. pentru a evita site-urile false.

### Cum îți dai seama că ești contactat în mod fraudulos?

- Primești apeluri telefonice de la numere internaționale.
- Primești emailuri de la conturi de tip Hotmail, Yahoo, Gmail etc.
- Mesajele care ajung la tine au greșeli gramaticale sau de ortografie.
- Adrese de website și conturi de rețea socială cu mici modificări față de cele oficiale.
- În cadrul discuțiilor telefonice ți se fac promisiuni de câștiguri rapide cu investiții minime.



- Ți se spune să îți instalezi aplicații de tip remote control (ex. Anydesk, BIZ Daemon etc).

### **Ce să faci dacă ești victima unei fraude?**

Contactează imediat banca și BT Asset Management SAI fie telefonic și discută următorii pași, fie scrie un mail la [conformare@btam.ro](mailto:conformare@btam.ro) pentru a lua măsurile necesare și a redirecționa mesajele către reprezentanții companiilor din cadrul Grupului.

Nu uita să îți schimbi parolele.

### **Care sunt tipurile de fraude?**

#### **Fraude online**

a. Phishing

Infractorii trimit e-mailuri care par reale și cer informații 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 și cer informații confidențiale.

c. Malware

Programe malițioase instalate pe dispozitivele tale care fură informații bancare.

d. Rețele Sociale

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

#### **Fraude telefonice**

a. Apeluri falsificate

Infractorii folosesc numere false, pretinzând că sună de la bancă și cer informații personale.

b. SMS-uri false (Smishing)

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

c. Aplicații de control la distanță

Infractorii cer instalarea unor aplicații de tip remote control, precum Anydesk sau BIZ Daemon, pentru a accesa dispozitivele victimei și 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 autorizați de Autoritatea de Supraveghere Financiară (A.S.F.) și promit câștiguri semnificative din investiții.

- Apeluri telefonice/email-uri neautorizate, de la persoane care pretind că sunt reprezentanți ai companiilor menționate și promovează investiții, cer informații personale
- Apeluri telefonice, de la persoane care pretind că sunt reprezentanți ai companiilor menționate și solicită instalarea de aplicații de control la distanță prin care reușesc să acceseze conturi și tranzacții.

**Retine:** Fraudele bancare sunt un risc real. Fii informat, ia măsuri preventive și raportează orice activitate suspectă. Fii vigilent și protejează-ți datele personale și financiare!

Te invităm să urmărești următoarele materiale despre siguranța online:

[Siguranță online by BT - YouTube](#)

Îți mulțumim!