ProCredit Bank

ProB@nking

Informații privind securitatea online

ProCredit Bank se angajează să protejeze integritatea tranzacțiilor dumneavoastră și detaliile contului bancar. De aceea, ProCredit Bank utilizează cel mai modern software de securitate și proceduri pentru protecția tranzacțiilor dumneavoastră online. Cu toate acestea, ar trebui să conștientizați faptul că Internetul și e-mail-ul pot fi oricând utilizate ca vehicule pentru activități ilegale, drept pentru care vă recomandăm să luați următoarele măsuri de precauție pentru a vă asigura securitatea.

Măsuri de securitate online

Asigurați-vă că știți cu cine aveți de-a face

Întotdeauna accesați serviciul Internet banking prin introducerea adresei de internet a băncii în browser-ul dumneavoastră http://www.procreditbank.ro/. Nu accesți niciodată site-ul dintr-un link trimis prin e-mail și nu vă introduceți datele personale. Dacă aveți dubii, contactați ProCredit Bank la numărul: 0372.100.200.

Păstrați-vă parolele, token-urile și PIN-urile în siguranță

Fiți circumspecți cu e-mail-urile sau apelurile telefonice nesolicitate prin care vi se cere să dezvăluiți orice detalii personale sau numere de card. Păstrați această informație secretă. Aveți grijă când furnizați orice informații personale unor persoane pe care nu le cunoașteți. Banca dumneavoastră și poliția nu v-ar contacta niciodată pentru a vă cere să le furnizați informații despre PIN sau despre parole.

Protejați-vă calculatorul

Utilizați programe anti-virus actualizate și un firewall personal și, dacă folosiți sistemul de operare Microsoft Windows, mențineți-l actualizat prin intermediul site-ului Microsoft. Întotdeauna utilizați cea mai nouă versiune a browser-ului de Internet, care include actualizările de securitate. Luați-vă măsuri suplimentare de siguranță în cazul în care folosiți calculatoare de la Internet cafe-uri, biblioteci, sau orice alt calculator care nu vă aparține și asupra căruia nu dețineți nici un control.

Păstrați-vă banii în siguranță!

Nu vă lăsați păcăliți de e-mailuri aparent sincere prin care vi se oferă șansa să câștigați ușor niște bani. Dacă pare prea frumos ca să fie adevărat, probabil chiar așa și este. Aveți grijă în special la e-mailurile nesolicitate din afara țării – este mult mai greu de verificat dacă sunt cine pretind că sunt.

Pentru informații suplimentare, puteți apela la site-uri specializate, cum ar fi:
http://www.banksafeonline.org.uk/faq.html

Măsuri suplimentare de protecție

- Întotdeauna memorați-vă parola și alte informații de securitate, după care distrugeți nota care conține aceste informații cât mai repede posibil.
- Nu notați sau înregistrați niciodată parola sau alte informații de securitate, decât dacă este protejat bine.
- Asigurați-vă că urmați întotdeauna termenii și condițiile băncii.
- Luați întotdeauna măsurile corespunzătoare pentru a că păstra parola și alte informații de securitate secrete în permanență – nu le dezvăluiți prietenilor sau familiei.
- Nu folosiți aceeași parolă pe care o aveți pentru online banking pe niciun alt site, nebancar.
- Dacă vă schimbați parola, alegeți una care nu poate fi ghicită cu ușurință.
- Nu dezvăluiți nimănui detaliile contului dumneavoastră sau informațiile de securitate. În cazul în care sunați la bancă, fiți atenți la tipul de informații care vi se cer: în mod normal nu vi se va cere parola completă.
- Asigurați-vă că utilizați întotdeauna **serviciul securizat ProCredit Bank e-banking.** Întotdeauna accesați direct site-ul, introducând adresa http://www.procreditbank.ro/. Asigurați-vă că în colțul dreapta jos al ferestrei de browser apare imaginea unui lacăt închis sau a unei chei înainte de a accesa site-ul băncii. Partea de început a adresei de Internet a băncii se va schimba din 'http' în 'https' în momentul în care se realizează o conexiune securizată.
- Verificați ca simbolul conexiunii securizate să fie vizibil.
- Puteți verifica **Certificatul de Securitate** al site-ului ProCredit Bank, dacă apăsați pe lacătul care apare în browser-ul dumneavoastră.

Internet Explorer 9

Internet Explorer 8

Firefox 4

- **Orice** excepții de la rutina normală privind Internet banking trebuie privită ca suspectă. În cazul în care aveți dubii, vă rugăm să contactați ProCredit Bank, vizitând cea mai apropiată sucursală, contactându-că administratorul cont, sau telefonând la linia de asistență: 0372.100.200.
- Nu vă lăsați niciodată calculatorul nesupravegheat în timp ce sunteți conectați la Internet banking.

- Asigurați-vă că vă deconectați în mod corespunzător în momentul în care ați terminat activitatea bancară online.

Informații suplimentare privind securitatea online

Ce înseamnă phishing?

Phishing este numele dat practicii de transmitere prin sondaj a unor e-mailuri care par a fi trimise de o companie reală care operează pe Internet, in scopul de a-i face pe clienții acelei companii să își dezvăluie informațiile pe un site fictiv, administrat de persoane frauduloase. De regulă, aceste email-uri pretind că este necesară "actualizarea" sau "verificarea" informațiilor cuprinse în contul de client pe care îl deținești și vă îndeamnă să apăsați pe un link din e-mail, care vă duce la site-ul fictiv. Orice informație introdusă pe respectivul site va fi capturată de infractori pentru scopurile lor frauduloase.

Cum pot evita să devin o victimă a phishing-ului?

Elementul cheie este să rămâneți circumspecți la orice e-mail-uri neașteptate pe care le primiți, chiar dacă par că provin dintr-o sursă de încredere. E-mail-urile sunt trimise absolut la întâmplare în speranța de a ajunge în căsuța de mail a unui client cu cont la banca ce face obiectul atacului de phishing.

Cu toate că ProCredit Bank vă poate contacta prin e-mail, ProCredit Bank nu vă va contacta niciodată prin e-mail solicitându-vă să vă introduceți parola sau orice alte informații sensibile prin accesarea unui link și vizitarea unui site. Considerați modul în care banca dumneavoastră comunică în mod normal cu dumneavoastră și nu dezvăluiți niciodată parola completă sau alte informații personale.

Cum să identificați un e-mail de phishing

1 – De la cine este e-mailul?

E-mail-urile de phishing pot arăta ca și cum ar fi fost trimise de la o adresă de e-mail reală a ProCredit Bank. Din păcate din cauza setărilor de e-mail de pe Internet, este relativ simplu pentru phisher-i să creeze o înregistrare falsă în câmpul "From:" („De la:”).

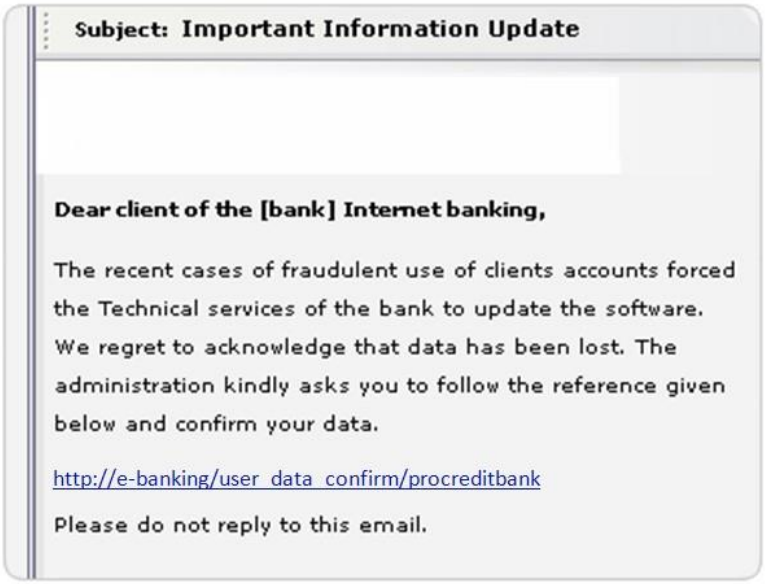
Adresa de e-mail care apare în câmpul "From:" al unui e-mail NU garantează faptul că acesta provine de la persoana sau organizația menționată în adresa de e-mail. Aceste e-mail-uri nu au fost trimise cu ajutorul sistemelor proprii ale băncii.

2 – Cui îi este destinat e-mail-ul?

E-mail-urile sunt trimise la întâmplare către liste de e-mail, fiind aproape sigur că infractorii nu vă cunosc numele real sau orice altceva despre dumneavoastră, adresându-vi-se în termeni vagi, precum "Stimate client".

3 – Observați e-mailul în detaliu - pare "suspect de phishing"?

Primul lucru de reținut este că băncile nu vă vor scrie niciodată pentru a vă solicita parola sau orice alte informații sensibile, prin e-mail. Mesajul mai poate conține "GRAF11" sau mAjusculE ciudate in câmpul "Subject:" („Subiect:”) (aceasta este o încercare de a ocoli programul de filtrare a e-mailurilor nesolicitate – spam), precum și greșeli gramaticale sau de scriere.



Exemplu de e-mail fraudulos

Nu vă conectați **niciodată** la contul dumneavoastră de online banking prin accesarea unui link dintrun e-mail. Deschideți **întotdeauna** browser-ul de Internet și tastați personal adresa web a site-ului de Internet banking al ProCredit Bank.

În cazul în care aveți dubii privind validitatea unui e-mail care pare că provine de la ProCredit Bank, vă rugăm să informați ProCredit Bank imediat, prin vizitarea celei mai apropiate sucursale, contactarea administratorului cont, sau prin apelarea numărului de telefon 0372.100.200. Puteți, de asemenea, să transmiteți mai departe e-mail-ul suspect la următoarea adresă de e-mail headoffice@procreditbank.ro.

4 – Unde vă duce hyperlink-ul?

Din păcate este foarte ușor să se ascundă destinația reală a unui link, astfel că link-ul afișat și orice altceva care apare în bara de status a programului dumneavoastră de e-mail poate fi falsificat cu ușurință.

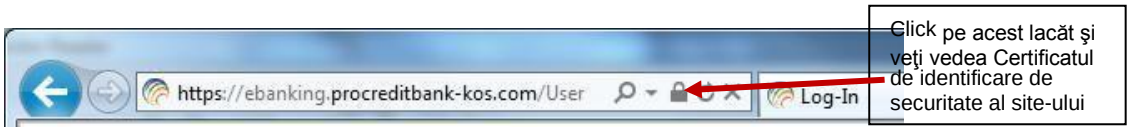
Cum depistați un site de Phishing

Care este adresa site-ului?

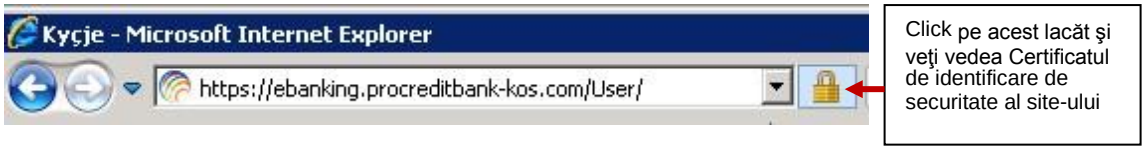
Dacă vizitați un site după ce ați apăsat pe un link dintr-un e-mail, rețineți că există multe modalități în care se poate acoperi locația reală a unui site fals in bara de adrese. Adresa site-ului poate începe cu numele real al domeniului site-ului, însă aceasta nu reprezintă o garanție că duce spre un site real. Alte trucuri includ utilizarea de adrese numerice, înregistrarea unei adrese similare (precum www.mybank-verify.com), sau chiar inserarea unei bare de adrese falsă în fereastra de browser. Multe dintre link-urile din aceste pagini pot duce chiar la site-ul real, însă nu vă lăsați păcăliți.

Puteți confirma că sunteți pe site-ul oficial securizat ProCredit Bank prin compararea simbolului pentru conexiunea securizată.

Internet Explorer 9



Internet Explorer 8



Firefox 4

Puteți verifica **Certificatul de Securitate** al paginii web a ProCredit Bank apăsând pe lacătul care apare pe browser-ul dumneavoastră.

Feriți-vă de ferestre pop-up frauduloase

În loc să afișeze un întreg site fals, persoanele care comit frauda pot încărca site-ul real în fereastra principală de browser și apoi pot suprapune propria lor fereastră pop-up falsă peste mare parte din aceasta. Dacă este afișată astfel, veți putea vedea bara de adrese a site-ului real in fundal, cu toate că orice informație pe care o tastați în fereastra pop-up va fi colectată de persoanele frauduloase pentru propriile lor scopuri.

Pentru a accesa contul dumneavoastră de online banking, tastați chiar dumneavoastră adresa în noua fereastră. Adresa site-ului real de online banking va începe cu "https" și va include un mic lacăt în partea de jos a ferestrei browser-ului.

Raportarea e-mail-urilor suspecte

Dacă primiți un e-mail suspect, vă rugăm să informați ProCredit Bank imediat, vizitând cea mai apropiată sucursală, contactând administratorul cont, sau telefonând la următorul număr 0372.100.200. De asemenea puteți transmite e-mail-ul mai departe la următoarea adresă headoffice@procreditbank.ro.

Rețineți:

- Băncile nu vă vor trimite niciodată e-mail-uri prin care vă solicită să „confirmați" sau să „actualizați" parola, sau orice alte informații personale prin accesarea unui link și vizitarea unui site web.
- Tratați orice e-mail-uri nesolicitate cu precauție și nu accesați niciodată link-urile din astfel de email-uri, respectiv nu vă introduceți niciodată informațiile personale
- Pentru a accesa Internet banking, deschideți browser-ul de Internet și tastați singuri adresa
- În cazul în care aveți dubii în privința validității unui e-mail, sau dacă considerați că e posibil să fi dezvăluit informații confidențiale, vă rugăm să informați ProCredit Bank imediat, vizitând cea mai apropiată sucursală, contactând administratorul cont, sau telefonând la următorul număr 0372.100.200. De asemenea, puteți transmite e-mail-ul mai departe la următoarea adresă headoffice@procreditbank.ro.

De reținut:

- **Tratați toate e-mail-urile nesolicitate (în special cele din surse necunoscute) cu circumspecție și nu accesați niciodată link-urile din astfel de e-mail-uri pentru a vizita siteuri necunoscute**
- **Instalați un program anti-virus, mențineți-l actualizat și efectuați scanări de securitate regulate**
- **Instalați și învățați cum să utilizați un firewall personal**
- **Instalați cele mai recente actualizări de securitate, denumite și patch-uri**