Part of the ProCredit Group

ProCredit Bank

Securitatea informațiilor

ProCredit Bank se angajează să protejeze securitatea dumneavoastră financiară prin asigurarea confidențialității și integrității informațiilor personale și tranzacționale. În acest sens, ProCredit Bank utilizează un set de tehnologii avansate pentru atingerea acestui obiectiv. Pentru a spori nivelul de siguranță și comfort în utilizarea serviciilor online, respectați măsurile de precauție de mai jos.

Măsuri de securitate online

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

Accesați serviciul Internet Banking prin introducerea adresei de internet a Băncii în browser-ul dumneavoastră (https://www.procreditbank.ro). În urma accesării prin această metodă, pagina web poate fi salvată la favorite pentru o accesare facilă. Nu accesați site-ul dintr-un link trimis prin e-mail.

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

Fiți prudent cu e-mail-urile sau apelurile telefonice nesolicitate prin care vi se va cere să dezvăluiți detalii confidențiale. Păstrați aceste informații secrete. Aveți grijă când furnizațiorice informații personale unor persoane pe care nu le cunoașteți. Banca şi poliția nu vor cere să le furnizați informații despre PIN, parole sau cod token.

Păstrați-vă banii în siguranță!

Nu vă lăsați păcăliți de e-mailuri aparent sincere prin care vi se oferă şansa să câştigați uşor bani sau bunuri. Dacă pare prea frumos să fie adevărat, probabil chiar aşa şi este. Aveți grijă în special la e-mailurile nesolicitate din afara țării – este mult mai dificil de verificat autenticitatea acestora.

Protejați-vă calculatorul

Asigurați securitatea calculatorului dumneavoastră prin utilizarea unei soluții anti-virus și firewall. De asemenea, este foarte important ca soluția anti-virus, browser-ul folosit și sistemul de operare să fie actualizate în mod automat pentru a beneficia de ultimele actualizări de securitate. Evitați utiliziarea calculatoarelor necunoscute și a rețelelor de tip WiFi gratuite, pentru că acestea pot avea mecansime de capturare a informațiilor.

Part of the ProCredit Group

ProCredit Bank

Măsuri suplimentare de protecție

1. Luați măsurile corespunzătoare pentru a păstra parola şi alte informații de securitate permanent în siguranță – nu le dezvăluiți nimănui. Nu notați sau înregistrați parola și alte informații de securitate, decât dacă sunt protejate corespunzător (ex: folosind o aplicație de centralizare a parolelor, protejată la rândul ei de o altă parolă).

2. Folosiți o parolă dedicată pentru serviciul Internet Banking, nu o utilizați pentru alte conturi. Alegeți o parolă ce nu poate fi ghicită cu ușurință. O parolă adecvată va fi compusă din **litere mici, litere mari, cifre și caractere speciale.** Nu folosți elemente ce pot fi deduse ușor (ex: nume/prenume propriu sau al unui membru din familie, data de naștere proprie sau a unui membru din familie, informații personale publicate pe site-uri de socializare, cuvinte comune găsite în dicționar, cifre succesive sau repetate, etc.)

3. Asigurați-vă că în colțul stânga sus al ferestrei de browser apare imaginea unui lacăt închis înainte de a accesa site-ul băncii. Verificați dacă simbolul conexiunii securizate este vizibil. Puteți verifica certificatul de securitate al site-ului ProCredit Bank, dacă apăsați pe lacătul care apare în browser-ul dumneavoastră.

4. Nu vă lăsați 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.

5. Nu folosiți aplicații ilegitime sau piratate. Acestea pot conține viruși cibernetici capabili de a lansa o gamă largă de atacuri (ex: exfiltrarea datelor confidențiale, efectuarea de tranzacții neautorizate, preluarea controlului asupra calculatorului, etc.)

6. Orice excepții de la rutina normală privind Internet Banking trebuie privită ca fiind suspectă. În cazul în care aveți dubii, vă rugăm să contactați ProCredit Bank, prin administratorul de cont, sau apelând linia de asistență: **0372.100.200.**

Part of the ProCredit Group

ProCredit Bank

Phishing

Ce înseamnă phishing?

Phishing-ul este încercarea frauduloasă de a obține informații sau date sensibile, cum ar fi nume de utilizator, parole și detalii despre cardul de credit. Desfășurat în mod obișnuit prin intermediul e-mail-ului, phishing-ul îndrumă adesea utilizatorii să introducă informații personale pe un site fals care imită aspectul site-ului legitim.

De regulă, aceste email-uri pretind că este necesară "actualizarea" sau "verificarea" informațiilor cuprinse în contul de client pe care îl dețineți şi 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?

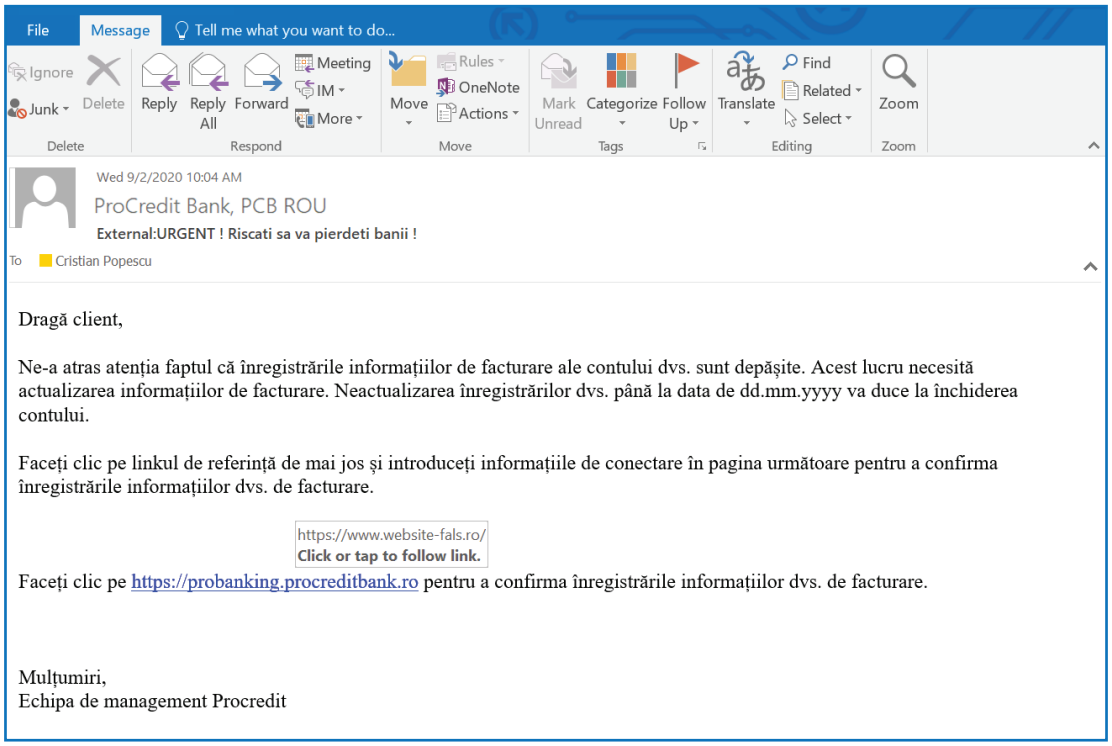
Elementul cheie este să fiți prudenți cu e-mail-uri neașteptate pe care le primiți, chiar dacă par a proveni dintr-o sursă de încredere. E-mail-uri ce conțin link-uri către pagini web, atașamente sau întrebări referitoare la date confidențiale, trebuie tratate cu o atenție deosebită.

Cum pot identifica un e-mail de phishing?

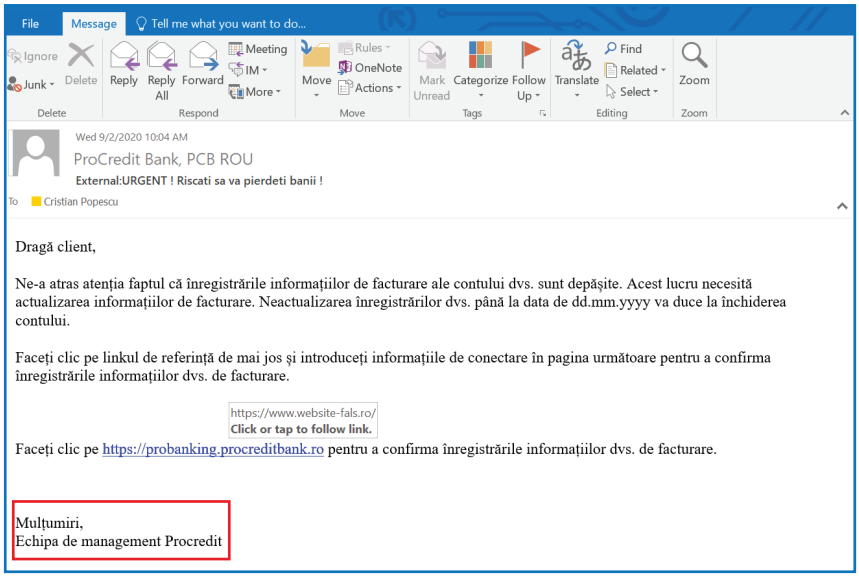
E-mail-urile de tip phishing pot arăta ca şi cum ar fi fost trimise de la o adresă de e-mail reală a ProCredit Bank. Din păcate este relativ simplu pentru infractorii cibernetici să manipuleze informația din câmpul "From" și să o înlocuiască după bunul plac.

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 sunt trimise cu ajutorul sistemelor proprii ale băncii. Pentru a identifica dacă un e-mail a fost într-adevar transmis de către ProCredit Bank, este important să acordați atenție la modul în care este redactat:

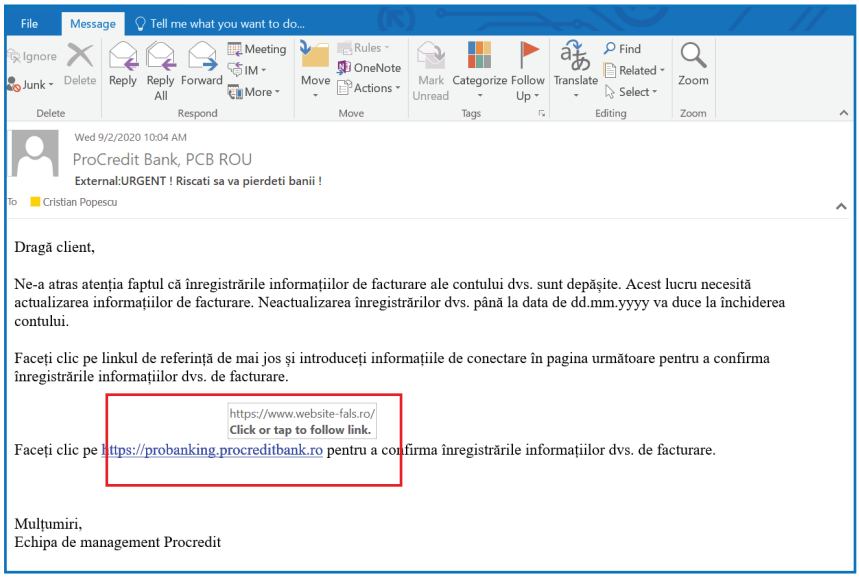
- Majoritatea e-mail-urilor de tip phishing sunt traduse folosind o unealtă automată iar în lipsa cunoștințelor despre limba maternă a potențialelor victime, infractorii cibernetici deseori nu au posibilitatea de a îmbunătății calitatea mesajului transmis. Probabilitatea de greșeli gramaticale este scăzută (cuvinte incorecte), însă modul în care sunt construite propozițiile va fi incorect din punct de vedere al formulării.



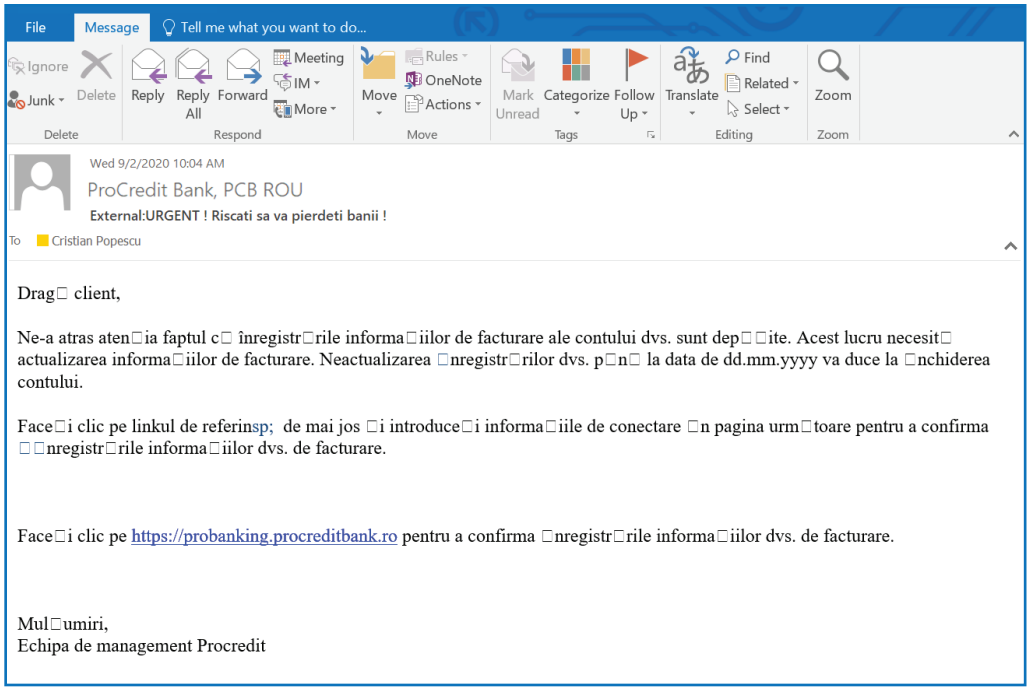
- Procredit Bank va include la sfarşitul e-mail-ului semnătura, sigla companiei şi un disclaimer. Lipsa acestor elemente sau prezența lor într-un format neprofesional indică probabilitatea crescută de phishing.



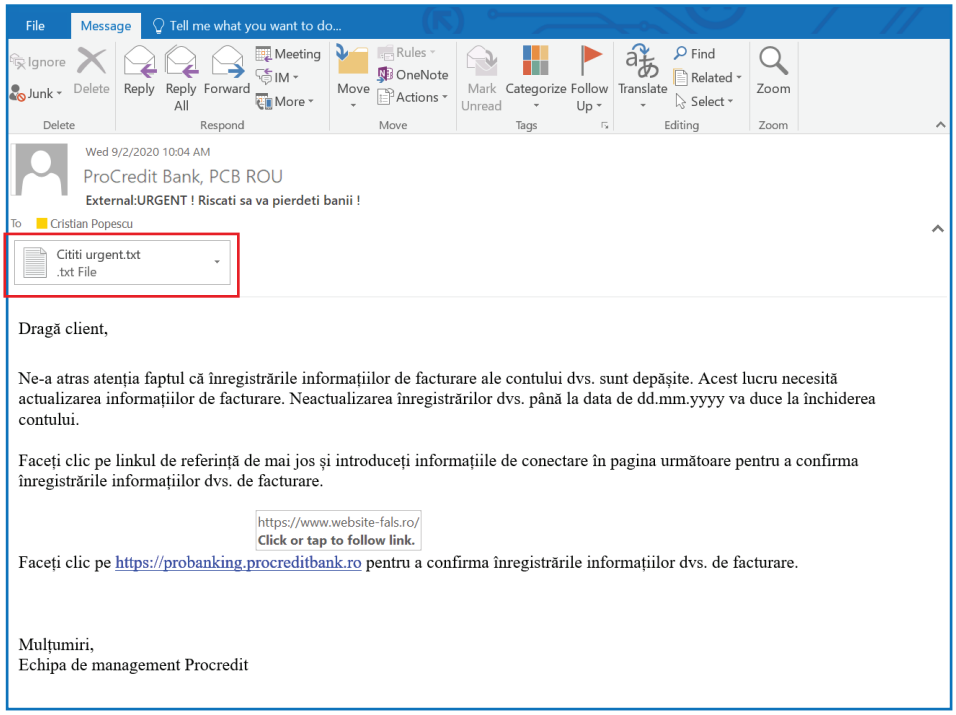
• Din păcate este foarte uşor să se ascundă destinația reală a unui link. Pentru a descoperi care este aceasta, mențineți cursorul deasupra link-ului câteva secunde fără a da click.



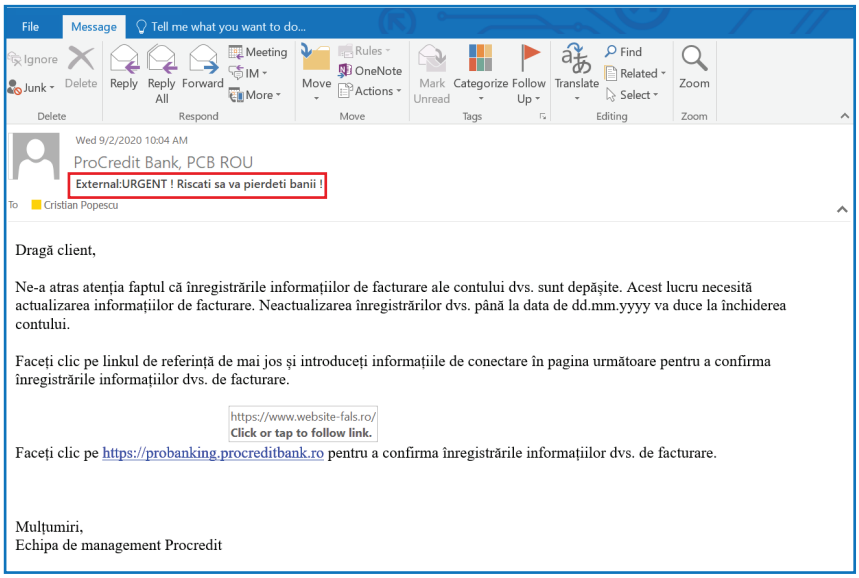
• Prezența unor simboluri sau caractere ciudate este un semn care indică, de obicei, faptul că infractorul cibernetic a încercat să folosească diacritice însă a eşuat.



• Atașamente nesolicitate, fonturi nefolosite în mod uzual și poze de calitate redusă indică posibilitatea unui phishing.



• Infractorii cibernetici vor încerca să genereze o stare de panică sau grabă. Atenție la cuvinte sau propoziții menite să cauzeze astfel de stări.



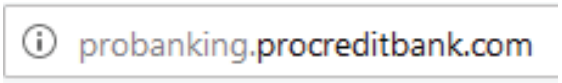
Part of the ProCredit Group

ProCredit Bank

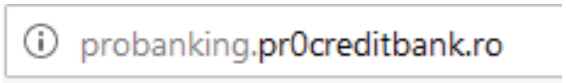
Cum pot identifica un site de phishing?

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 în bara de adresă. Adresa site-ului poate începe cu numele real al domeniului site-ului, însă a ceasta nu reprezintă o garanție că duce spre un site real. Alte trucuri includ utilizarea de adrese numerice, înregistrarea unei adrese similare. Multe dintre link-urile din aceste pagini pot duce chiar la site-ul real, însă nu vă lăsați păcăliți deoarece traficul este interceptat de către infractorii cibernetici.

➤ Pagină falsă cu terminația ".com" în loc de ".ro"

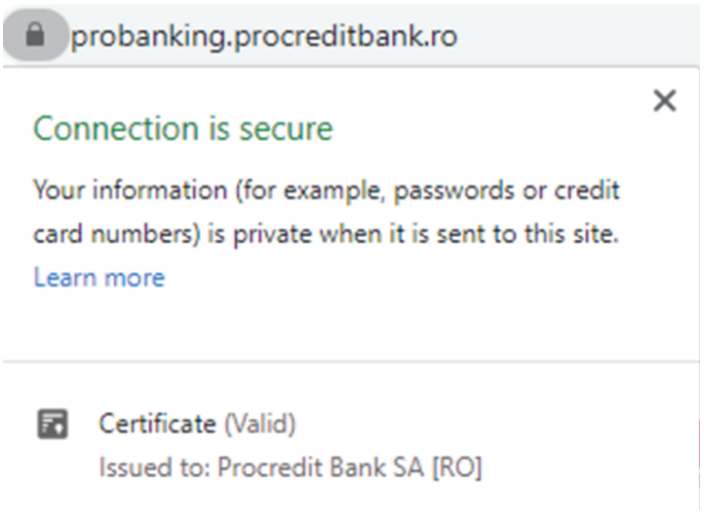


➤ Pagină falsă asemnătoare prin înlocuirea caracterului "o" cu "0" (zero)

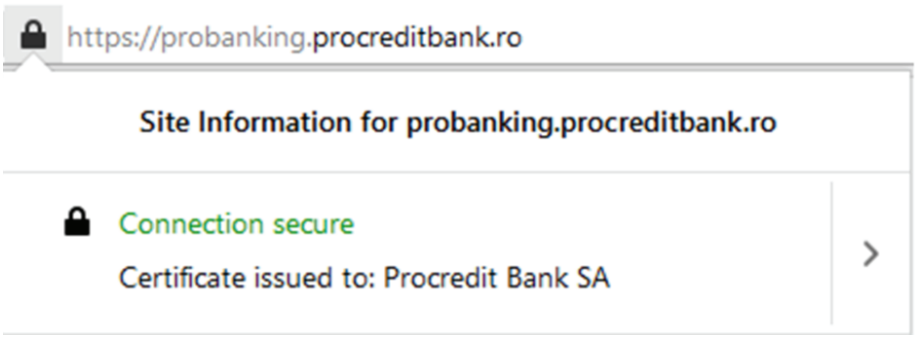


Puteți confirma că sunteți pe site-ul oficial securizat ProCredit Bank prin compararea simbolului pentru conexiunea securizată. După cum se poate observa în exemplele de mai sus, acesta lipsește pentru paginile web false.

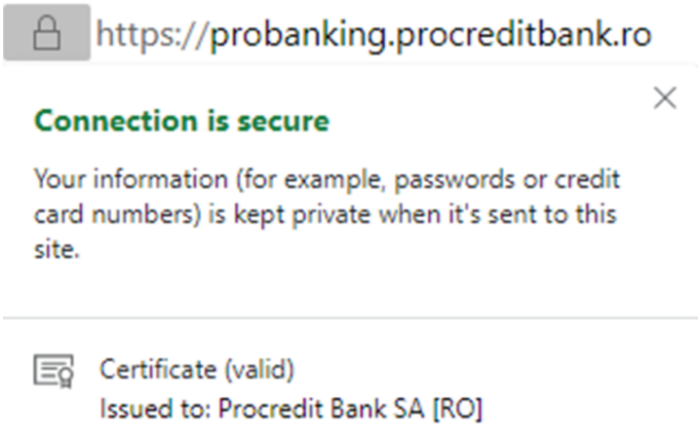
➤ Google Chrome



➤ Mozilla Firefox



➤ Microsoft Edge



Raportarea e-mail-urilor suspecte

În cazul în care primiți un e-mail suspect sau aveți dubii privind validitatea unui e-mail care pare să provină de la ProCredit Bank, vă rugăm să ne informați imediat, vizitând cea mai apropiată sucursală, contactând administratorul de cont, sau apelând la numărul de telefon 0372.100.200. De asemenea puteți transmite e-mail-ul mai departe la următoarea adresă headoffice@procreditbank.ro. Pentru a putea investiga e-mail-ul corespunzător, acesta nu trebuie redirecționat (“forwarding”) ci transmis ca și atașament.

Part of the ProCredit Group

ProCredit Bank

Reţineţi !

ProCredit Bank nu va trimite e-mail-uri prin care vă solicită să „confirmaţi" sau să „actualizaţi" parola, sau orice alte informaţii personale prin accesarea unui link şi vizitarea unui site web.

Trataţi orice e-mail-uri nesolicitate cu precauţie şi nu accesaţi link-urile din astfel de email-uri, respectiv nu vă introduceţi niciodată informaţiile personale.
Pentru a accesa Internet Banking, deschideţi browser-ul de internet şi tastaţi singuri adresa sau folosiţi un bookmark creat manual anterior.
Instalaţi un program anti-virus, menţineţi-l actualizat şi efectuaţi scanări de securitate regulate.

Păstraţi-vă parolele, token-urile şi PIN-urile în siguranţă.

Instalaţi cele mai recente actualizări de securitate.

Nu ezitaţi să ne contactaţi în cazul în care aveţi suspiciuni.