GHID DE SECURITATE SADD Telebank (ECBank)

Cuprins

1. Prevederi generale

Sistemul ECBank (în continuare Sistem, ECBank) – sistem automatizat de deservire bancară la distanță de tip Web Banking și Mobile Banking (denumirea veche – Telebank), prin intermediul căruia clientul, de la un telefon mobil tip smartfon sau tabletă conectat la rețeaua Internet, precum și accesând site-ul ecbank.md poate efectua tranzacții, plăți, vizualiza situația conturilor sale bancare etc.

2. Accesarea și înregistrarea în SADD ECBank (web)

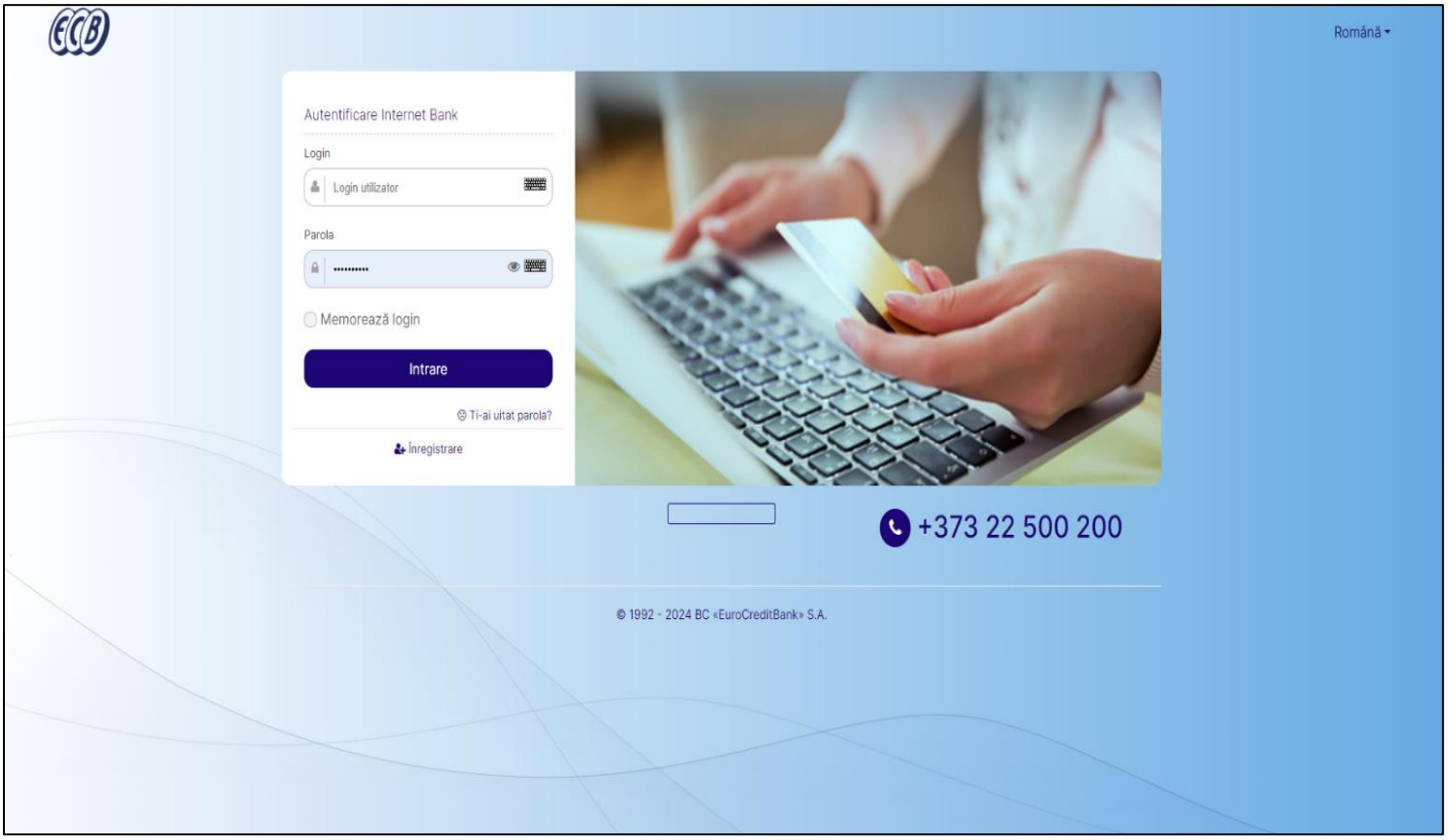
Procedura de înregistrare în aplicația ECBank (web) presupune parcurgerea a următorilor pași:

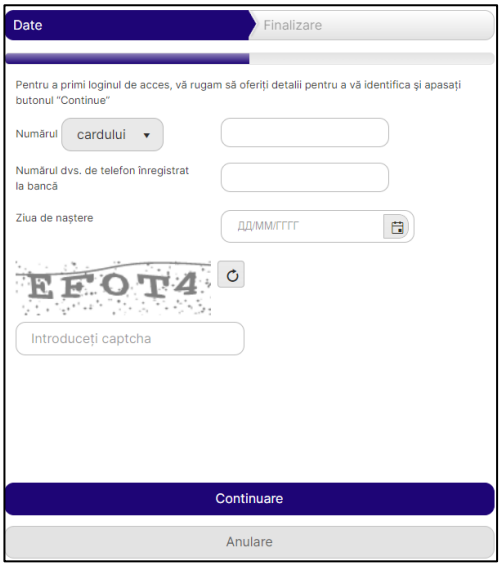
- Accesare site my.telebank.md;
- Accesare buton "Înregistrare"
- Introducerea în câmpurile indicate a datelor necesare pentru identificarea clientului: Nr.card sau IDNP, numărul de telefon al clientului înregistrat în sistemul informațional al băncii, informații privind data/luna/anul nașterii;

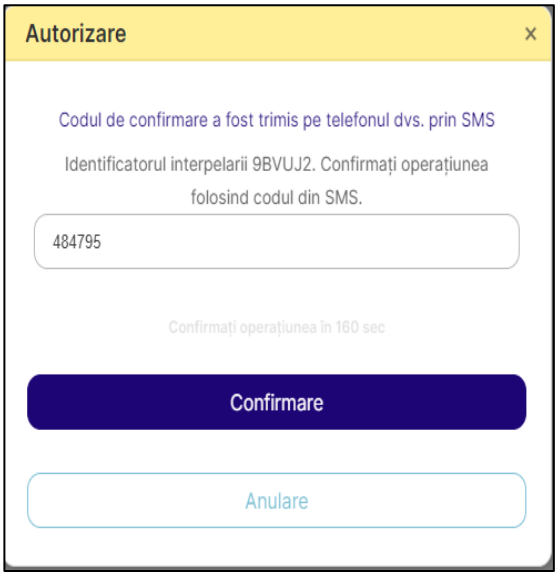
La numărul de telefon al clientului va fi expediată parola OTP.

După confirmarea cu parola OTP, clientul va fi redirecționat către pagina de setare a parolei,

După setarea parolei, clientul va fi redirecționat către pagina de log-are, unde va putea folosi loginul obținut și parola setată pentru acces în sistem.




Date
Finalizare
Pentru a primi loginul de acces, vă rugam să oferiți detalii pentru a vă identifica și apasați butonul "Continue"
Numărul cardului
Numărul dvs. de telefon înregistrat la bancă
Ziua de naștere
ДД/ММ/ГГГГ
EFOT4
Introduceți captcha
Continuare
Anulare


Autorizare
Codul de confirmare a fost trimis pe telefonul dvs. prin SMS
Identificatorul interpelarii 9BVUJ2. Confirmați operațiunea folosind codul din SMS.
484795
Confirmați operațiunea în 160 sec
Confirmare
Anulare

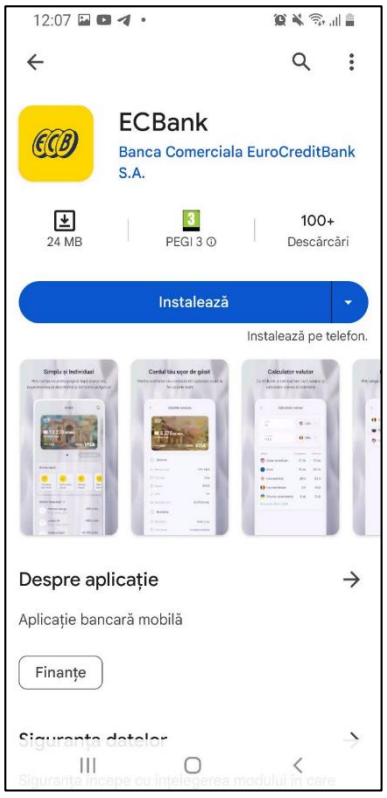

Modificarea parolei
Parola curentă a expirat! Este necesar să modificați parola.
Reguli de creare a parolei:
Parola trebuie să conțină cel puțin 8 caractere, inclusiv cel puțin o literă mică, o literă mare, un număr și un caracter special (~!@#$%^&*()_+=[]{}<>\/;:"',.?)
Parolă nouă
Schimbare

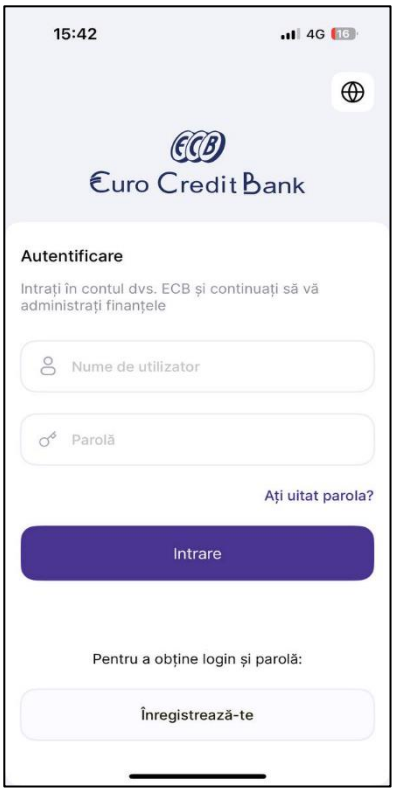

Informație
Felicitări, te-ai înregistrat cu succes!
Acum te poți loga în ECBank.
OK

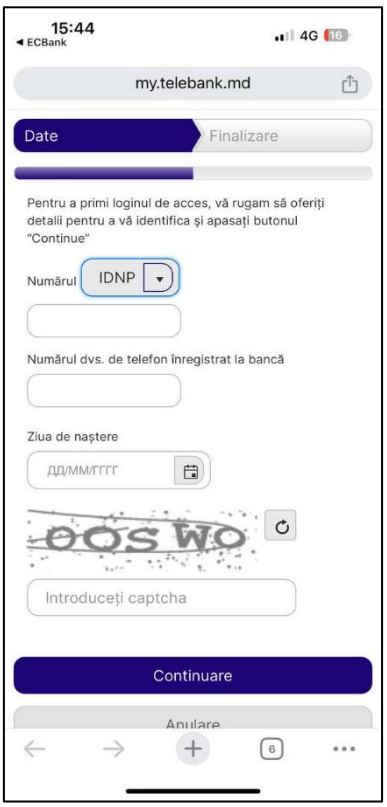
3. Accesarea SADD ECBank (mobile)

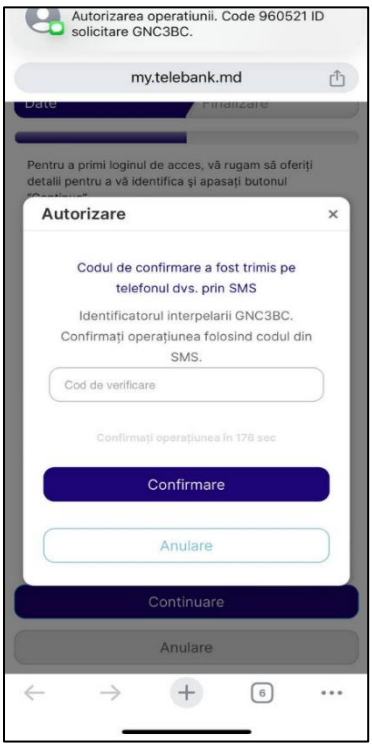
Procedura de înregistrare în aplicația ECBank (mobile) presupune parcurgerea a următorilor pași:

- Descărcarea aplicației mobile din Play Store sau App Store
- Accesare buton "Înregistrare"
- Introducerea în câmpurile indicate a datelor necesare pentru identificarea clientului: Nr.card sau IDNP, numărul de telefon al clientului înregistrat în sistemul informațional al băncii, informații privind data/luna/anul nașterii.
- La numărul de telefon al clientului va fi expediată parola OTP.
- După confirmarea cu parola OTP, clientul va obține login-ul, și ulterior va fi redirecționat către pagina de setare a parolei;
- După setarea parolei clientul va fi redirecționat automat către pagina de log-are în aplicația ECBank, unde va introduce login-ul și parola.
- Aplicația va solicita clientului crearea unei parole de acces compusă din 5 cifre.
- După log-are Utilizatorul primește acces la funcționalitățile disponibile în ECBank mobile. Parola de acces va fi folosită ulterior la accesarea aplicației. Pe parcursul folosirii aplicației utilizatorul va putea activa opțiunea de accesare a aplicației în cadrul unei sesiuni autorizate (după log-are cu succes) prin metoda de deblocare telefon cu biometrie (Touch ID, Face ID, daca dispozitivul o suportă tehnic).



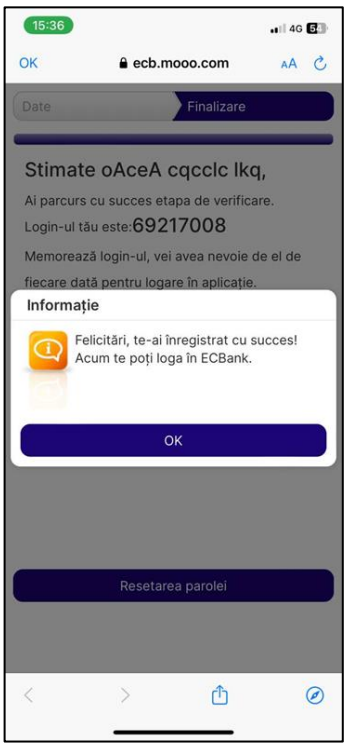


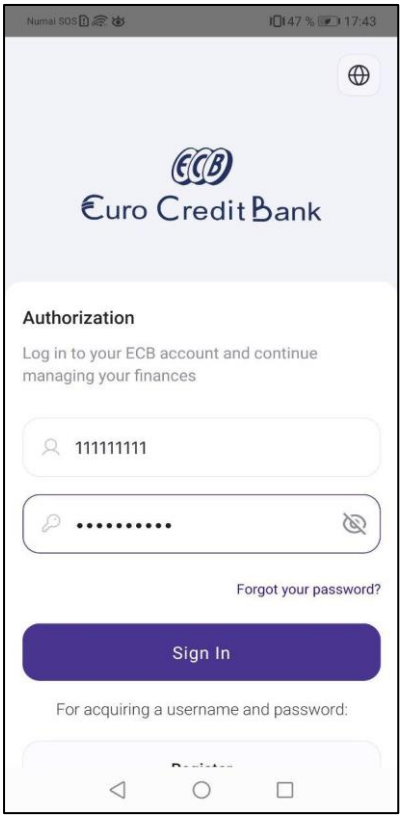



Autorizarea operațiunii. Code 960521 ID solicitare GNC3BC.
my.telebank.md
Pentru a primi loginul de acces, vă rugam să oferiți detalii pentru a vă identifica și apasați butonul
Autorizare
Codul de confirmare a fost trimis pe telefonul dvs. prin SMS
Identificatorul interpelarii GNC3BC.
Confirmați operațiunea folosind codul din SMS.
Cod de verificare
Confirmați operațiunea în 176 sec
Confirmare
Anulare
Continuare
Anulare

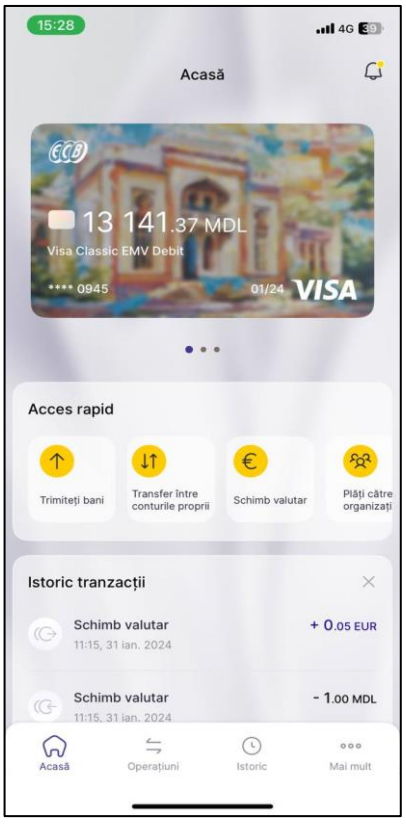

15:33
OK
ecb.mooo.com
AA
Date
Finalizare
Stimate oAceA cqcclc lkq,
Ai parcurs cu succes etapa de verificare.
Login-ul tău este:69217008
Memorează login-ul, vei avea nevoie de el de fiecare dată pentru logare în aplicație.
Resetarea parolei


15:34
OK
ecb.mooo.com
AA
Date
Finalizare
Modificarea parolei
Parola curentă a expirat! Este necesar să modificați parola.
Reguli de creare a parolei:
Parola trebuie să conțină cel puțin 8 caractere, inclusiv cel puțin o literă mică, o literă mare, un număr și un caracter special (~!@#$%^&*()_-+={}[]<>\/;:'",.?)
Parolă nouă
Introduceți o parolă nouă
Confirmați parola
Schimbare


15:36
OK
ecb.mooo.com
AA
Date
Finalizare
Stimate oAceA cqcclc lkq,
Ai parcurs cu succes etapa de verificare.
Login-ul tău este:69217008
Memorează login-ul, vei avea nevoie de el de fiecare dată pentru logare în aplicație.
Informație
Felicitări, te-ai înregistrat cu succes! Acum te poți loga în ECBank.
OK
Resetarea parolei


Euro Credit Bank
Authorization
Log in to your ECB account and continue managing your finances
111111111
Forgot your password?
Sign In
For acquiring a username and password:


Creați un cod de acces
1
2
3
4
5
6
7
8
9
0


15:28
Acasă
13 141.37 MDL
Visa Classic EMV Debit
**** 0945
01/24
VISA
Acces rapid
Trimiteți bani
Transfer între conturile proprii
Schimb valutar
Plăți către organizații
Istoric tranzacții
Schimb valutar
+ 0.05 EUR
11:15, 31 ian. 2024
Schimb valutar
- 1.00 MDL
11:15, 31 ian. 2024
Acasă
Operațiuni
Istoric
Mai mult

4. Modificarea parolei

În cazul în care ați uitat parola, atât în ECBank web cât și în ECBank mobile puteți schimba parola.

Este important de reținut că parola trebuie să corespundă următoarelor cerințe - să conțină cel puțin 8 caractere, dintre care: litere (majuscule și mici), cifre și simboluri speciale (cum ar fi, !%?*). Asigurați-vă că introduceți în câmpuri parola pe care o aveți (litere majuscule, mici, cifre și simboluri speciale), în caz contrar la introducerea incorectă a parolei de 3 ori aceasta va fi blocată. În cazul în care parola a fost blocată aceasta poate fi resetată apelând serviciul de suport al băncii. Pentru schimbarea parolei, introduceți următoarele date:

- Parola curentă;
- Parola nouă;
- Confirmă parola nouă – reintroduceți parola nouă;

După modificarea parolei se va afișa mesajul corespunzător și veți putea continua utilizarea aplicației.

De fiecare data când este accesat SADD ECBank, banca întreprinde toate masurile de asigurare de securitate a informației, care au drept scop protecția confidențialității și integrității datelor.

5. Criptarea informatiei

Criptarea informației reprezintă o metoda sigura de protecție a informației, care nu permite persoanelor neautorizate de a intercepta sau schimba datele transmite si procesate in SADD ECBank.

Pentru a asigura criptarea informațiilor in SADD ECBank se utilizează tehnologia SSL (Secure Socket Layer). Pentru a verifica faptul, ca conectarea la SADD ECBank se efectuează in regim securizat cu criptarea informației este nevoie de fiecare data sa verificați, daca in linia de adrese a paginii web, formatul protocolului este http**s**:// cu prezenta obligatorie a literei "**s**" la sfârșit (spre exemplu: **https://my.telebank.md/**) și să verificați afișarea iconiței sub forma de lacăt in partea dreapta a liniei de adrese web.

6. Protecția datelor de autentificare si autorizare

Pentru protecția datelor de autentificare si a preveni eventuale tentative de fraude/furt de identitate este strict necesar să respectați următoarele cerințe minime de gestionare si asigurare a securității parolei:

1. Cerințe minime de gestionare parole

Parolele trebuie sa îndeplinească următoarele cerințe:

- sa aibă o lungime minima de 8 caractere;
- sa fie complexă formata dintr-un şir de caractere compus din litere minuscule, majuscule, cifre și simboluri (%$#&^*);
- sa fie schimbate de utilizator periodic, cel puțin o dată la 30 de zile;
- sa fie schimbate imediat, daca exista suspiciuni ca o parolă a putut fi divulgată.

2. Cerințe minime de asigurare a securității parolei

Parolele trebuie sa respecte minimum următoarele cerințe de securitate:

- sa nu coincidă cu codul numeric personal;
- sa nu coincidă cu data nașterii;
- sa nu fie numărul dvs. de telefon;
- sa nu fie asemănătoare cu numele dvs. de utilizator (login - ul);
- sa nu fie asemănătoare cu numele dvs.;
- sa nu coincidă cu funcția, departamentul etc.;
- sa nu coincidă cu nume de străzi, nume proprii;
- sa nu coincidă cu mărci sau modele de mașini etc;
- sa nu fie termeni tehnici;
- sa nu coincidă cu numele sau sloganul unor organizații;
- sa nu fie cuvinte din dicționar:
- sa nu fie transmisa altor persoane, inclusiv colegilor de birou, prietenilor chiar dacă aceștia ofera suport in utilizarea ei.

Pentru a preveni tentativele frauduloase de autentificare si autorizare a tranzacțiilor, banca recomanda:

- sa păstrați semnătura electronica pe suporturi securizate (token, usb, cartela cu chip);
- sa utilizați semnătura electronica numai pe calculatoarele personale sau de serviciu;
- sa conectați la calculator suportul pe care este păstrata semnătura electronica **numai pentru perioade scurte de timp necesare autentificării in sistem sau autorizarii tranzactiilor**;
- sa nu transmiteți/divulgați semnătura electronica si parola altor persoane terțe.

IMPORTANT: BC „EuroCreditBank" SA NU poartă răspundere pentru utilizarea necorespunzătoare a datelor de autentificare si autorizare (login, parola etc.) în ECBank.

7. Măsuri de protecție în timpul utilizării SADD ECBank

Pentru asigurarea unei protecții sigure, in timpul utilizării SADD ECBank, a datelor si a calculatorul dvs, banca recomandă:

- Sa nu salvați parolele, login-urile si alte date ce țin de securitate informațiilor în locații nesigure, in special, pe masa de lucru a calculatorului;
- Sa folosiți un firewall personal, care este activ si configurat corespunzător;

- Sa descărcați si sa instalați periodic actualizari de la producator pentru aplicatii si pentru sistemul de operare;
- Sa folosiți un sistem anti-virus, care este actualizat periodic si asigura o protectie anti-virus sigura;
- Sa nu încercați sa accesați SADD ECBank de pe calculatoare nesigure, deoarece acestea pot fi infectate sau avea anumite vulnerabilități de securitate;
- Sa nu lăsați, niciodată, calculatorul conectat la SADD ECBank nesupravegheat;
- Sa închideți sesiunea de lucru in SADD ECBank la finalizarea activitatilor in mod regulamentar, conform instrucțiunii de utilizare a sistemului.

7. Masuri de protecție împotriva atacurilor Social engineering

Atac de tip Social engineering sau inginerie sociala reprezintă o formă de manipulare in care atacatorii imită o sursă de încredere pentru a convinge victima să îndeplinească anumite sarcini cum ar fi să acorde acces la un sistem bancar sau un cont, sau sa dezvăluie informații confidențiale, cum ar fi parole.

Exemple de situații de atac de tip Social engineering

Sunteți contactat telefonic de o persoana necunoscuta, care se prezinta drept reprezentant al băncii. In urma discuției, persoana (atacatorul) va comunica ca banca are o problema tehnica sau ca ați câștigat la un premiu de fidelitate oferit de banca si va cere sa comunicați prin telefon datele dvs. personale (date de acces la sistemele de transfer, datele cu caracter personal, detalii despre conturi/carduri, PIN, parole, etc).

IMPORTANT: BC „EuroCreditBank" SA NU solicita de la clienți sai prin telefon, email, SMS date confidențiale sau date cu caracter personal.

Banca nu transmite, in orice situații, mesaje e-mail/SMS clienților săi pentru a solicita informații privind:

- identitatea persoanei;
- numărul de cont/card;
- datele de autentificare/autorizare, inclusiv parole/PIN;
- alte date cu caracter personal sau confidențial.

In cazul in care recepționați astfel de mesaje e-mail/apeluri telefonice/SMS-uri prin care se solicită informații de tipul celor prezentate mai devreme, banca recomandă:

- sa nu răspundeți la aceste mesaje;
- sa nu accesați link-urile si deschideți atașamentele transmise in mesajele e-mail;
- sa nu divulgați nimănui, niciodată parola/PIN, indiferent de persoana sau situația in care se cere acest lucru;
- sa informați imediat banca prin canale sigure de comunicare despre situația apărută.

8. Masuri de protecție împotriva atacurilor de tip Phishing

Phishing-ul reprezintă o metodă de furt de identitate prin care se încearcă obținerea, de la clienții unei bănci a unor date cu caracter personal sau confidențial. Acestea pot fi folosite ulterior in mod ilegal de către răufăcători, pentru a efectua tranzacții in contul clientului respectiv. Pentru obținerea datelor, in atacurile de tip phishing răufăcătorii folosesc mijloace de comunicare electronica (e-mail, telefon, mobil) sau programe rău intenționate, care exploatează vulnerabilitățile sistemului pentru a fura date.

Identificarea atacurilor de tip Phishing

Pentru a lansa un atac **Phishing**, persoanele rău intenționate, aplică următoarele metode:

- Sună și se pot prezenta drept angajați ai băncii, care vă informează ca: ați câștigat un premiu, detin informații ca contul bancar a fost blocat si va pot ajuta sa deblocați contul sau cardul bancar, veți putea incasa bani in cardul bancar, vă pot ajuta sa modificați parola;
- Lansează site-uri false care aparent sunt asemănătoare cu site-urile originale ale băncii, pe care apoi le promovează prin intermediul mesajelor email/SMS, cu scopul de a sugera clienților sa viziteze aceste site-uri ca să își actualizeze datele cu caracter personal (date de acces la sistemele băncii, date despre conturi/carduri, parole, PIN, etc);
- Transmit mesaje e-mail/SMS ce pretind a fi trimise de către bancă.

Pentru a va influenta, si a va convinge sa introduceți datele sus enumerate pe site-urile false, acestea inventează situații ale unor evenimente care va captează atenția.

Exemple de situații de atac de tip phishing:

- Sunteți contactat de o persoana necunoscuta si felicitat cu ocazia câștigării unui premiu important, dar, in acelasi timp, se solicita sa efectuați un transfer de pe card pe un anumit cont;
- Sunteți contactat de o persoana necunoscuta, care declara precum ca este reprezentantul Serviciului de securitate al băncii. Aceasta persoana va anunta ca sistemul bancar s-a defectat, si ca datele de autentificare si autorizare s-au pierdut, iar pentru restabilirea lor este necesara obținerea si verificarea datelor dvs. de către banca.

Pentru a vă proteja de acest tip de atac, asigurați-vă că adresa paginii web prin care accesați SADD Telebank ECBank pentru persoane fizice, este cea specificată. De asemenea, verificați prezenta iconiței sub forma de lacăt in partea dreapta a adresei web si numele pentru care a fost eliberat certificatul paginii web, prin accesarea iconiței respective. In plus, luați următoarele masuri:

- Nu răspundeți la mesajele suspecte;
- Nu transferați bani in conturile solicitate;
- Nu oferiți informații personale sau date financiare;
- Nu deschideți atașamente sau dați click pe butoane sau pe link-uri.
- Nu accesați pagini web in care sa iti introducții datele personale.

În plus, măsurile de protecție a securității informației includ:

- educarea clienților în privința atacurilor de tip phishing și inginerie socială și a modului în care aceștia pot identifica si evita astfel de atacuri;

- verificarea de către clienți a adresei URL a site-ului web pentru confirmarea prezenței pe site-ul corect si evitarea site-urilor web cu adrese URL suspecte;

- verificarea de către clienți a sursei e-mail-ului si evitarea deschiderii sau descărcării fișierelor atașate sau a link-urilor din e-mail-uri suspecte;

- păstrarea de către clienți a software-ului de securitate actualizat și instalarea de actualizări de securitate pentru browser-ul web, sistemul de operare si alte aplicații software.