

Ghid de Securitate pentru aplicația bancară pentru persoanele fizice ECBank

Cuprins

1. Prevederi generale	3
2. Accesarea și înregistrarea în aplicația ECBank (web)	4
3. Accesarea aplicației ECBank (mobile)	6
5. Criptarea informației	8
6. Protecția datelor de autentificare și autorizare	9
7. Măsuri de protecție în timpul utilizării ECBank.....	10
8. Măsuri de protecție împotriva atacurilor Social engineering.....	11

1. Prevederi generale

1.1. Prezentul Ghid de securitate pentru aplicația bancară pentru persoanele fizice ECBank (în continuare Ghid de securitate) au drept scop oferirea utilizatorilor de recomandări și măsuri practice pentru utilizarea sigură a aplicației bancare destinate persoanelor fizice - ECBank, prevenirea fraudelor și protejarea datelor personale și financiare împotriva accesului neautorizat, tentativelor de phishing și altor riscuri cibernetice. Ghidul contribuie la creșterea nivelului de conștientizare privind securitatea digitală și la diminuarea riscurilor asociate utilizării serviciilor bancare online.

1.2. Prezentul Ghid de securitate constituie parte integrantă a relațiilor dintre BC EuroCreditBank S.A. (în continuare Banca), și Utilizator în procesul utilizării aplicației mobile ECBank.

1.3. Termeni:

- a. **Aplicația ECBank** (în continuare Sistem, aplicația ECBank) – instrument de plată cu acces la distanță de tip web și mobile prin intermediul căruia utilizatorul, de la un telefon mobil tip smartphone, tabletă, PC, conectat la rețeaua de internet, poate efectua operațiuni de plată, inclusiv plăți instant, constituirea depozitelor la termen, achitarea serviciilor comunale, vizualiza și monitoriza situația conturilor sale bancare, recepționa notificările privind operațiunile efectuate la distanță, etc.
- b. **Ghidul utilizatorului ECBank** prezintă în mod detaliat modul de utilizare a aplicației în cadrul IPAD- instrumentului de plată cu acces la distanță (în continuare IPAD) – ECBank. Ghidul descrie explicit lucrul cu aplicația mobilă ECBank, pentru explorarea eficientă și utilizarea la maximum a funcționalităților oferite. În cazul în care întâmpinați dificultăți în utilizarea aplicației ECBank, vă rugăm să contactați la numărul de telefon +373 22 500 200.
- c. **Parolă** - parolă statică setată de către utilizator la etapa înregistrării și folosită ulterior pentru logare în aplicația ECBank, **element care asigură securitatea utilizării ECBank.**
- d. **Parolă de acces (PIN5)** – combinație succesivă de cifre, utilizată în scopul autentificării clientului după conectarea în aplicația ECBank pe tot parcursul unei sesiuni active. Parola de acces poate fi modificată doar de către utilizator și doar după autentificarea acestuia în sistem ECBank.
- e. **Parolă de unică folosință / One Time Password** (în continuare OTP) – cod numeric, generat automat de sistem, transmis utilizatorului prin mesaj SMS, la numărul de telefon înregistrat și verificat în sistemul informational al Băncii și utilizat în cadrul aplicației ECBank ca element de autentificare la accesarea acestuia.
- f. **SCA (Autentificarea Strictă ale Clienților/Strong Customer Authentication)** – este o măsură obligatorie de securitate bancară care asigură verificarea identității utilizatorului prin folosirea cel puțin doi factori independenți de autentificare (cunoaștere, posesie, inerență) pentru accesarea aplicației ECBank și confirmarea operațiunilor efectuate de la distanță prin cardurile de plată și ECBank, garantând astfel securitatea tranzacțiilor și a fondurilor clienților plasate pe conturile bancare.
- g. **Utilizator (Client)** – orice persoană fizică care beneficiază de serviciile Băncii cu acces la distanță, instrumentele de plată cu acces la distanță.

2. Accesarea și înregistrarea în aplicația ECBank (web)

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

- Accesare site <https://ecbank.md> (fig.2.1);
- Accesare buton "Înregistrare"
- Introducerea în câmpurile indicate a datelor necesare pentru identificarea clientului (fig.2.2):
 - Numărul de card de plată sau IDNP;
 - Numărul de telefon al clientului înregistrat în sistemul informațional al băncii
 - Informații privind data/luna/anul nașterii;
 - codul captcha (fig.2.2).

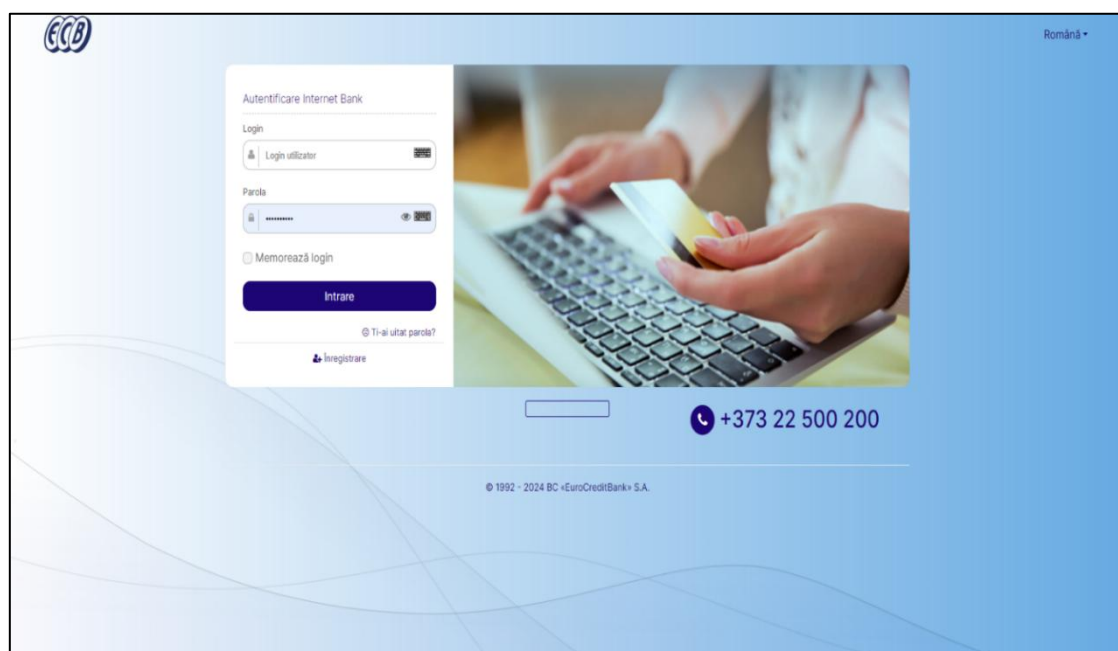
La numărul de telefon al clientului va fi expediată parola OTP (fig.2.3)

După confirmarea cu parola OTP, clientul va fi redirecționat către pagina de setare a parolei (fig.2.4).

După finalizarea procesului de înregistrare utilizatorul este informat despre finalizarea procesului (fig.2.5)

După setarea parolei, utilizatorul va fi redirecționat către pagina de logare, unde va putea folosi login-ul obținut și parola setată pentru acces în sistem.

Login-ul by default este nr. de telefon (fără zero "0" la început) înregistrat în sistemul informațional al băncii.



(fig.2.1)

Page: Date Finalizare

Pentru a primi loginul de acces, vă rugăm să oferiți detalii pentru a vă identifica și apăsați butonul "Continuare"

Numărul cardului

Numărul dvs. de telefon înregistrat la bancă

Ziua de naștere

EFOT4

Continuare

Anulare

(fig.2.2)

Autorizare

Codul de confirmare a fost trimis pe telefonul dvs. prin SMS

Identificatorul interpelării 9BVUJ2. Confirmați operațiunea folosind codul din SMS.

Confirmați operațiunea în 180 sec

Confirmare

Anulare

(fig.2.3)

Parolele OTP transmise prin SMS la numărul de telefon verificat de bancă au un timp limitat de valabilitate.

IMPORTANT!

Nu comunicați parolele OTP expediate prin SMS persoanelor terțe.

Angajații băncii nu vă vor solicita niciodată parolele.

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

(fig.2.4)

Informație

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

OK

(fig.2.5)

3. Accesarea aplicației ECBank (mobile)

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

- a. Descărcarea aplicației mobile din Play Store sau App Store (fig.3.1)
- b. Accesare buton "Înregistrează-te aici" (fig.3.2)
- c. Introducerea în câmpurile indicate a datelor necesare pentru identificarea clientului:
 - c1. Nr.card sau IDNP,
 - c2. numărul de telefon al clientului înregistrat în sistemul informațional al băncii,
 - c3. informații privind data/luna/anul nașterii,
 - c4. codul promo (dacă îl dețineți).
- d. La numărul de telefon al clientului va fi expediată parola OTP (fig.3.4).

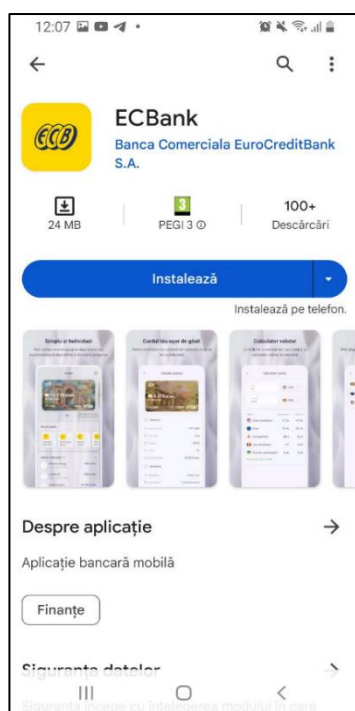
După confirmarea cu parola OTP, clientul va obține login-ul, și ulterior va fi redirecționat către pagina de setare a parolei (fig.3.5);

După setarea parolei clientul va fi redirecționat automat către pagina de log-are în aplicația ECBank, unde va introduce login-ul și parola.

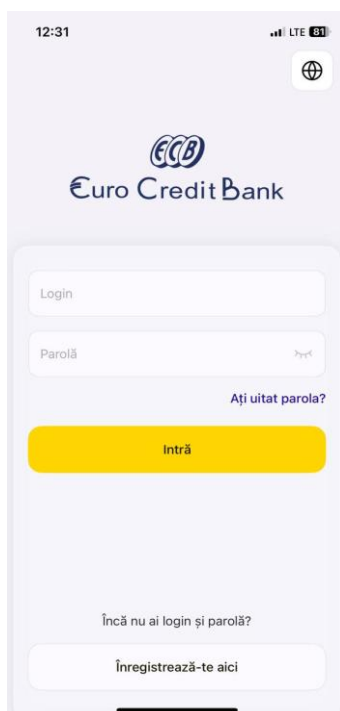
Aplicația va solicita clientului crearea unei parole de acces compusă din 5 cifre (fig.3.6).

După log-are Utilizatorul primește acces la funcționalitățile disponibile în ECBank mobile (fig.3.7).

Pe parcursul utilizării aplicației ECBank, utilizatorul poate activa autentificarea biometrică a telefonului, care oferă posibilitatea accesării aplicației în cadrul unei sesiuni autorizate (după autentificarea inițială cu succes), prin utilizarea metodelor biometrice ale dispozitivului mobil (Touch ID, Face ID, PIN5). Accesul se realizează în cadrul unei sesiuni securizate, cu generarea tokenului de autentificare și aplicarea mecanismelor criptografice de protecție a datelor.



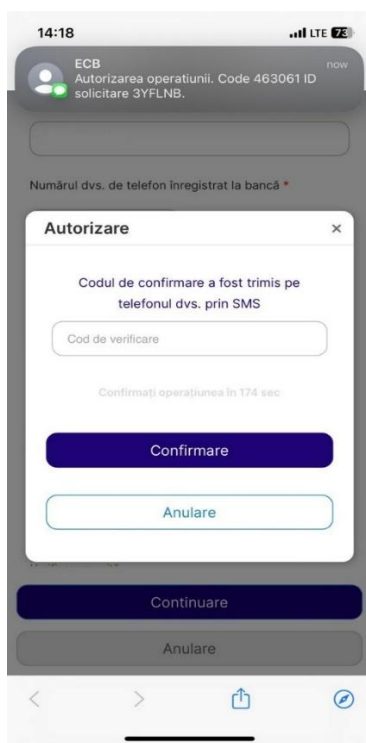
(fig.3.1)



(fig.3.2)



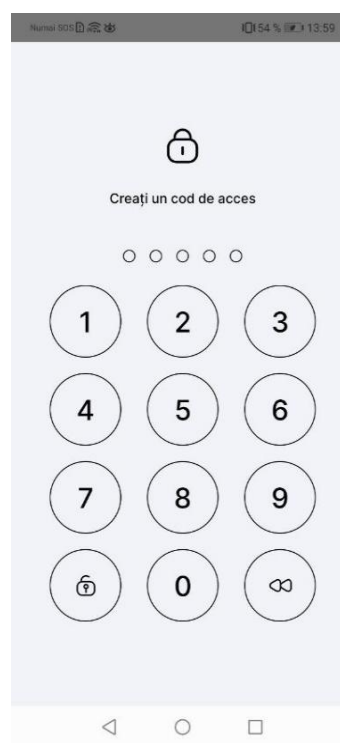
(fig.3.3)



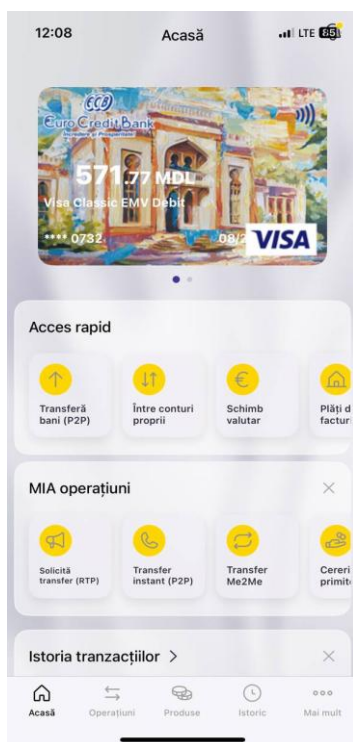
(Fig.3.4)



(fig.3.5)



(fig.3.6)



(fig.3.7)

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:

- a. Lungimea parolei minim 8 caractere;
- b. Litere mari, minim o literă (A-Z);
- c. Litere mici (a-z);
- d. Cifre (0-9);
- e. Simboluri (!@#%^ ș.a.).

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:

- a. Parola curentă;
- b. Parola nouă;
- c. 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 aplicația ECBank, banca întreprinde toate măsurile de asigurare de securitate a informației, care au drept scop protecția confidențialității și integrității datelor.

5. Criptarea informației

Criptarea informației reprezintă o metodă sigură de protecție a informației, care nu permite persoanelor neautorizate de a intercepta sau schimba datele transmise și procesate în ECBank.

Pentru a asigura criptarea informațiilor în ECBank se utilizează tehnologia SSL/TLS v1.2 (Secure Socket Layer). Pentru a verifica faptul, că conectarea la ECBank se efectuează în regim securizat cu criptarea informației este nevoie de fiecare dată să verificați, dacă în linia de adrese a paginii web, formatul protocolului este <https://> cu prezenta obligatorie a literei "s" la sfârșit (ex. <https://ecbank.md>) și să verificați afișarea iconiței sub forma de lacăt în partea dreaptă a liniei de adrese web.

Aplicația monitorizează continuu securitatea dispozitivului. Dacă este detectată o problemă de securitate, sesiunea este închisă automat. Pentru verificarea dispozitivului, aplicația folosește serviciile de securitate Google și Apple, iar validarea este confirmată de server. În cazul indisponibilității serviciilor Google/Apple, aplicația blochează accesul (aceeași reacție ca la eșecul verificării) și înregistrează evenimentul pentru monitorizare.

Pentru securizarea informației în timpul utilizării aplicației ECBank și anume procesarea operațiunilor, confirmarea are loc prin SCA (Autentificarea strictă a clienților / Strong Customer Authentication) care este compus din trei factori:

- a) factorul ce îl cunoaște utilizatorul (parolă, PIN);
- b) factorul ce îl deține utilizatorul (numarul de telefon);
- c) factorul de inerentă, cea ce îl reprezintă (amprenta digitală (TouchID), recunoaștere facială (FaceID)).

6. Protecția datelor de autentificare și autorizare

La fiecare logare reușită în aplicația mobile ECBank utilizatorul, va fi informat printr-un mesaj cu textul **"Atentie: S-a detectat o logare în profilul Dvs, pe dispozitivul "Marca si Modelul".** **Daca nu sunteti Dvs.,contactati banca la nr. de tel. 022500200"**, expediat prin SMS la numărul de telefon indicat de către client la inițierea relațiilor de afaceri cu bancă, în Chestionarul – cunoaște-ți clientului cât și la adresa de email a acestuia.

Scopul acestui mesaj este de a detecta încercările de acces neautorizat.

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

1. Cerințe minime de gestionare a parolei

Parolele trebuie să îndeplinească următoarele cerințe:

- Lungimea parolei minim 8 caractere;
- Litere mari, minim o literă (A-Z);
- Litere mici (a-z);
- Cifre (0-9);
- Simboluri (!@#%^ ș.a.);
- Să fie schimbate de utilizator periodic, cel puțin o dată la 30 de zile;
- Să fie schimbate imediat, dacă exista suspiciuni că o parolă a putut fi divulgată.

2. Cerințe minime de asigurare a securității parolei

Parolele trebuie să respecte minimum următoarele cerințe de securitate:

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

Pentru a preveni tentativele frauduloase de autentificare și autorizare a tranzacțiilor, banca recomandă:

- Să păstrați semnătura electronică pe suporturi securizate (token, usb, cartelă cu chip);
- Să utilizați semnătura electronică numai pe calculatoarele personale sau de serviciu;
- Să conectați la calculator suportul pe care este păstrată semnătura electronică numai pentru perioade scurte de timp necesare autentificării în sistem sau autorizării tranzacțiilor;
- Să nu transmiteți/divulgați semnătura electronică și parola altor persoane terțe;

- Toate notificările adresate Clientului / Utilizatorului / Deținătorului, vor fi efectuate, în una din următoarele modalități (dacă nu se prevede altfel în contractele specifice încheiate cu clienții):
 - prin intermediul paginii oficiale a Băncii: www.ecb.md;
 - la nr. telefon mobil, înregistrat în sistemul informațional al băncii;
 - la adresa email înregistrată în sistemul informațional al băncii;
 - prin intermediul extrasului de cont;
 - prin aplicația ECBank;
 - prin scrisoare înmănată personal sau trimisă prin poștă

În procesul de logare ECBank acceptă ca utilizatorul poate introduce incorect parola de 3 ori, după care utilizatorul va fi blocat pentru cca 2 ore.

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

7. Măsuri de protecție în timpul utilizării ECBank

Pentru asigurarea unei protecții sigure, în timpul utilizării ECBank, a datelor și a calculatorul dvs, banca recomandă:

- Să nu salvați parolele, codurile SMS, login-urile și alte date ce țin de securitatea informațiilor în locații nesigure, în special, pe masa de lucru a calculatorului;
- Mențineți activată funcția de protecție a dispozitivului împotriva accesului neautorizat din rețea (firewall);
- Să descărcați și să instalați periodic actualizări de la producător pentru aplicație și pentru sistemul de operare;
- Să folosiți un sistem anti-virus, care este actualizat periodic și asigură o protecție anti-virus sigură;
- Să nu încercați să accesați ECBank de pe calculatoare nesigure, deoarece acestea pot fi infectate sau avea anumite vulnerabilități de securitate;
- Să nu lăsați calculatorul conectat cu sesiune activă în ECBank nesupravegheat;
- Să închideți sesiunea de lucru în ECBank la finalizarea activităților în mod regulamentar, conform instrucțiunii de utilizare a sistemului.

În scopul protejării datelor fiecărui utilizator în timpul utilizării aplicației ECBank pe un dispozitiv cu sistem de operare Android sau iOS, banca a introdus următoarele măsuri de securitate, și anume:

- Blocarea temporară a cardurilor direct din ECBank mobile cât și deblocarea acestora doar dacă au fost blocate din aplicație;
- Setarea/modificarea PIN cod la cardurile noi și existente;
- Aplicația nu funcționează pe telefoane sau tablete Android la care a fost activat accesul root, adică a fost obținut acces complet la sistemul de operare prin eliminarea unor restricții de securitate;
- Aplicația nu funcționează pe iPhone sau iPad dacă sistemul de operare a fost modificat prin jailbreak, o procedură care elimină restricțiile de securitate impuse de Apple;
- În cazul când se încearcă suprapunerea ecranelor, va fi vizibil ecran alb;
- Nu va fi posibil de făcut capturi de ecran;
- În cazul derulării unei aplicații de acces de la distanță (ex. teamviewer, anydesk) pe ecranul vizualizat nu se va afișa informație;
- Aplicația nu va funcționa când se va depista că pe dispozitiv sunt activate careva opțiuni de accesibilitate, cum ar fi citirea ecranelor (chatGPT, Bixby, Gemini, etc.)
- Aplicația nu va funcționa când se va depista că pe dispozitiv sunt instalate și active programe care permit acces la distanță – AnyDesk, TeamViewer, etc.
- În cîmpurile critice (login, parolă, etc.) nu este posibil de utilizat acțiunile copy/paste;
- Tastatura random pentru introducerea la ecranele de autentificare și confirmare SCA;

- Timp de așteptare pentru aplicația ECBank după care aplicația se închide automat (devine inactivă), este 5 min.

8. Măsuri de protecție împotriva atacurilor Social engineering

Atac de tip Social engineering sau inginerie socială reprezintă o formă de manipulare în care atacatorii imită o sursă de încredere pentru a convinge victima să îndeplinească anumite sarcini cum ar fi să acorde acces la o aplicația bancară sau la un cont, sau să dezvăluie informații confidențiale, cum ar fi parole, coduri de unică folosință (OTP), elemente de securitate a cardurilor, aplicațiilor bancare, etc.

Exemple de situații de atac de tip Social engineering:

Sunteți contactat telefonic de o persoană necunoscută, care se prezintă drept reprezentant al băncii. În urma discuției, persoana (atacatorul), va comunica ca banca are o problemă tehnică sau ca ați câștigat un premiu de fidelitate oferit de bancă și va cere să comunicați prin telefon datele dvs. personale (ex.: date de acces la sistemele de transfer, datele cu caracter personal, detalii despre conturi/carduri, PIN, parole, etc).

IMPORTANT: BC „EuroCreditBank” SA niciodată NU solicita de la clienții sai nici-o informație: date confidențiale, Pin-codurile, codurile de unică folosință, date cu caracter personal (prin telefon, email, SMS, etc).

Banca nu transmite, in orice situație, 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.

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

- Să nu accesați link-urile și deschideți atașamentele transmise în mesajele SMS/E-mail;
- Să nu divulgați nimănui, niciodată parola/PIN, indiferent de persoană sau situația în care se cere acest lucru;
- Să informați imediat banca prin canale sigure de comunicare despre situația apărută, expedind un email la info@ecb.md sau apelând la numerele de tel: [022 500 200](tel:022500200), [022 853 220](tel:022853220), canalele de comunicare la fel sunt publicate pe site-ul oficial al [băncii](#).
- Să nu răspundeți la apelurile/mesajele suspecte;
- Să apelați înapoi la nr.dat dacă simțiți unele momente suspecte. (De obicei, apelurile nu sunt conformate)

9. Măsuri 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 în mod ilegal de către răufăcători, pentru a efectua tranzacții din contul clientului respectiv. Pentru obținerea datelor, în atacurile de tip phishing răufăcătorii folosesc mijloace de comunicare electronică (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, dețin informații ca contul bancar a fost blocat și vă pot ajuta să deblocați contul sau cardul bancar, veți putea încasa bani în cardul bancar, vă pot ajuta să 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 să viziteze aceste site-uri ca să își actualizeze datele cu caracter personal (date de acces la sistemele băncii, date despre conturi/carduri, parole, coduri, PIN-codul, etc);
- Transmit mesaje e-mail/SMS ce pretind a fi trimise de către bancă.

Pentru a vă influența, și a vă convinge să introduceți datele sus enumerate pe site-urile false, acestea inventează situații ale unor evenimente care vă captează atenția.

Exemple de situații de atac de tip phishing:

- Sunteți contactat de o persoană necunoscută și felicitat cu ocazia câștigării unui premiu important, dar, în același timp, se solicită să efectuați un transfer de pe card pe un anumit cont.
- Sunteți contactat de o persoană necunoscută, care declară precum că este reprezentantul Serviciului de securitate al băncii. Această persoană vă va anunța că sistemul bancar s-a defectat, și că datele de autentificare și autorizare s-au pierdut, iar pentru restabilirea lor este necesară obținerea și verificarea datelor dvs. de către banca.

Pentru a vă proteja de acest tip de atac, asigurați-vă că adresa paginii web prin care accesați ECBank pentru persoane fizice, este veridică. De asemenea, verificați prezența iconiței sub forma de lacăt în partea dreaptă a adresei web și numele pentru care a fost eliberat certificatul paginii web, prin accesarea iconiței respective.

În plus, luați următoarele măsuri:

- Nu răspundeți la mesajele suspecte;
- Nu transferați bani în conturile solicitate;
- Nu oferiți informații personale sau date financiare;
- Nu deschideți atașamente sau accesați butoane sau pe link-uri;
- Nu accesați pagini web suspicioase sau pe care este nevoie să introduceți datele personale.

IMPORTANT! În scopuri de securitate, pentru protecția datelor personale, în cazul compromiterii datelor personale ce pot facilita accesul la ECBank, fiecare client are posibilitatea de a solicita blocarea accesului, prin contactarea, serviciului Contact Centru al băncii la nr. **de tel. 022500200**.