GHID DE SECURITATE SADD TELEBANK BUSINESS

Cuprins

1. Prevederi generale

Sistemul automatizat de deservire la distanta (in continuare – SADD) Telebank Business este un sistem securizat, al carui mecanisme implementate asigura confidentialitatea, autenticitatea, integritatea si nonrepudierea tranzactiilor. SADD Telebank Business poate fi accesat de catre utilizator numai dupa introducerea corecta a loginului si parolei, iar orice transfer efectuat in SADD Telebank Business este aditional semnat de utilizator prin introducerea parolei corespunzatoare cheii criptografice individuale, generate in SADD Telebank Business si activat de catre Banca.

SADD Telebank Business oferă posibilitatea clienţilor Băncii să acceseze serviciile de gestiune a produselor bancare, fără a se prezenta personal, utilizând calculatorul personal şi reţeaua Internet.

2. Accesarea SADD Telebank Business

SADD Telebank Business este accesibil pentru clienții bancii, care au solicitat conectarea la acest sistem și posedă un contract activ de conectare. Pentru a folosi SADD Telebank Business este necesar să accesați pagina web https://business.telebank.md și să introduceți Login utilizator (login) și Parola utilizatorului (Parola). Acestea sunt oferite la încheierea contractului de deservire la distanta prin SADD Telebank Business.

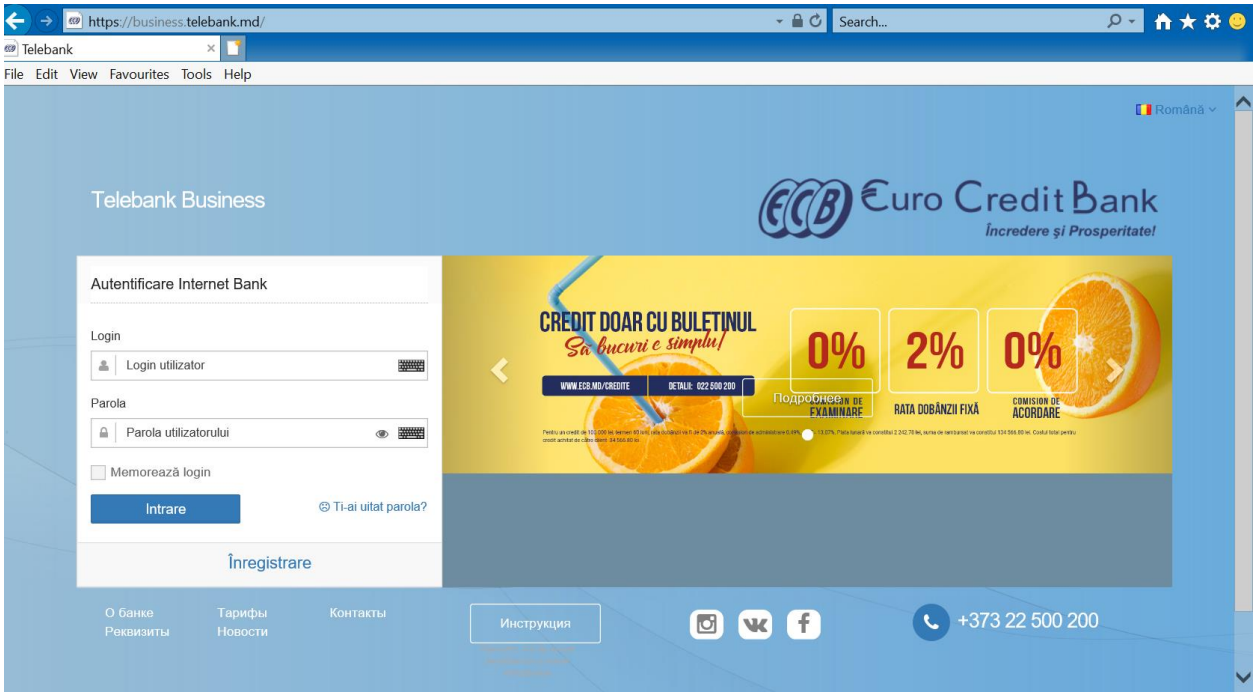

Figura 1. Accesarea sistemului de deservire bancara la distanta

Accesarea iconiței sub forma de lacăt permite verificarea autenticității paginii web a sistemului de deservire bancara la distanta (faptul ca sunteti pe pagina oficiala a sistemului si nu una falsa, clonata de un răufăcător). In fereastra care se deschide dupa apasarea acestei iconite trebuie sa fie obligatoriu specificat **business.telebank.md** (Figura 2).

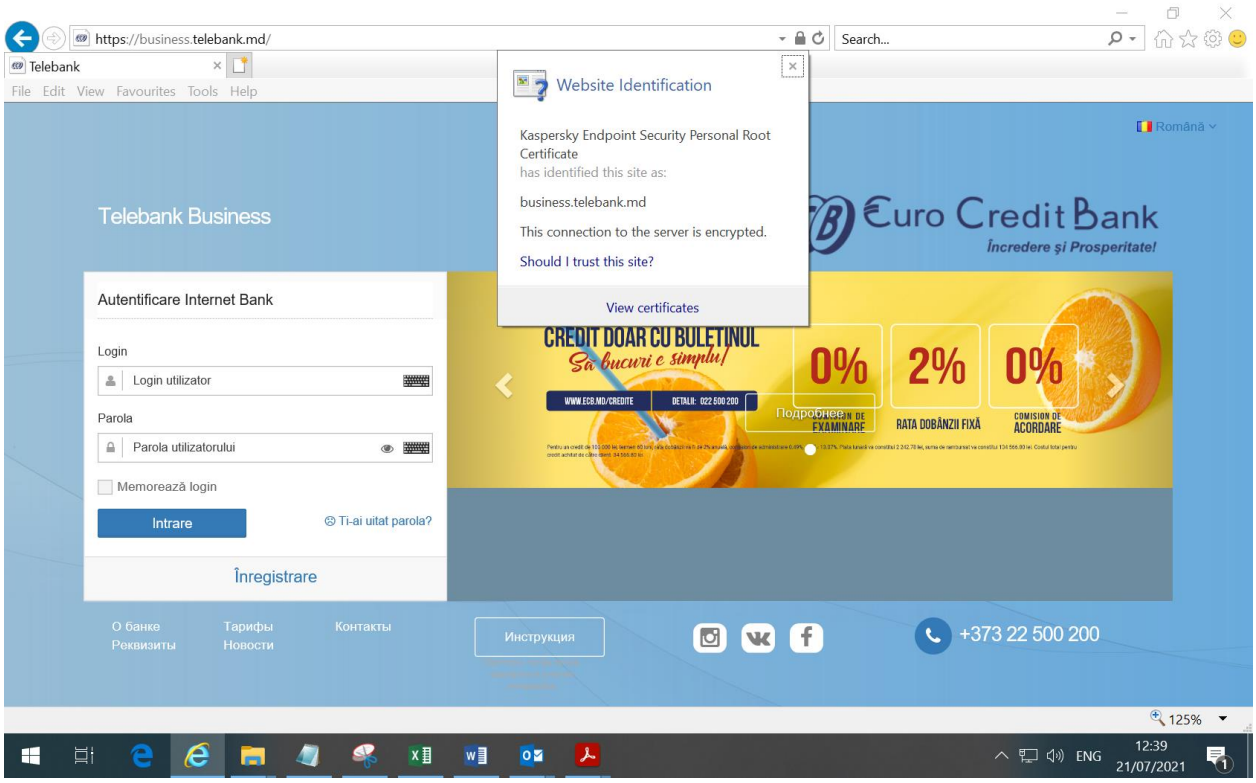

Figura 2. Identificarea paginii web

După introducerea corectă a datelor de autentificare a utilizatorului (login și parola de assces), tastați butonul **Intrare**.

3. Modificarea parolei

La prima accesare a aplicației, după ce ați completat câmpurile respective și ați tastat butonul **Intrare**, aplicația vă va cere să vă schimbați parola, în vederea asigurării securității maxime a utilizării serviciului în viitor.

Este important de reținut că parola trebuie să corespundă urmatoarelor cerințe - să conțină cel puțin 9 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 apelind serviciul de suport al băncii. Pentru schimbarea parolei, introduceți următoarele date:

- Parola curentă;
- Parola nouă;
- Confirmă parola nouă – reintroduceți parola nouă;
- Tastați butonul Schimbare.

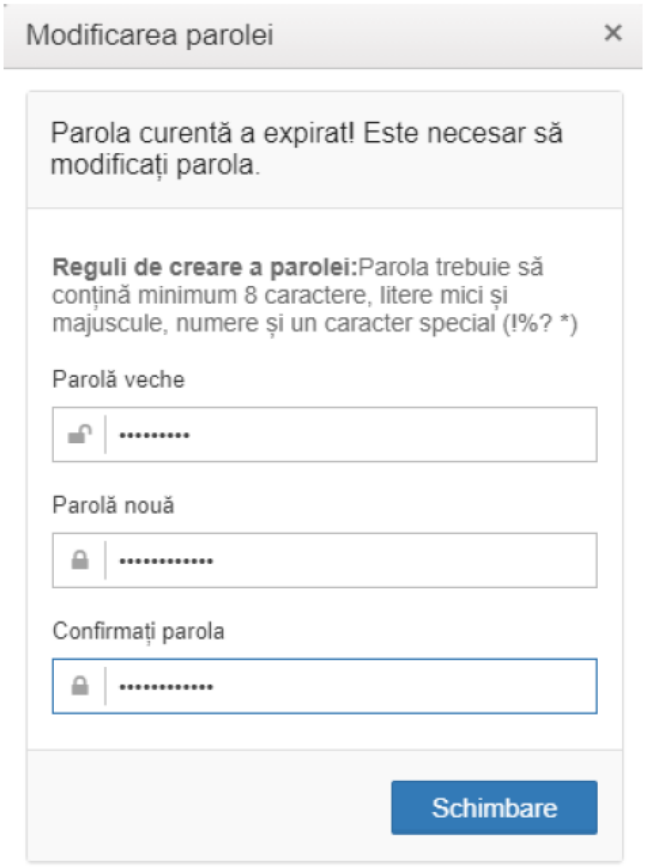

Figura 3. Modificare parola

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

IMPORTANT. În cazul schimbării parolei de intrare în SADD Telebank Business, parola cheii de semnare nu se schimbă automat, dar ramine aceeași. Dacă doriți să modificați parola cheii, atunci este necesar sa urmați pașii din pct.7 din ghidul Gestionare chei chriptografice.

De fiecare data cand este accesat SADD Telebank Business, banca intreprinde toate masurile de asigurare de securitate a informatiei, care au drept scop protectia confidentialitatii si integritatii datelor.

4. Criptarea informatiei

Criptarea informatiei reprezinta o metoda sigura de protectie a informatiei, care nu permite persoanelor neautorizate de a intercepta sau schimba datele transmite si procesate in SADD Telebank Business.

Pentru a asigura criptarea informatiilor in SADD Telabank Business se utilizeaza tehnologia SSL (Secure Socket Layer). Pentru a verifica faptul, ca conectarea la SADD Telebank Business se efectueaza in regim securizat cu criptarea informatiei este nevoie de fiecare data sa verificati, daca in linia de adrese a paginii web, formatul protocolului este http**s**:// cu prezenta obligatorie a literei "**s**" la sfirsit (spre exemplu: **https**://business.telebank.md) si sa verificati afisarea iconitei sub forma de lacat in partea dreapta a liniei de adrese web.

5. Protectia datelor de autentificare si autorizare

Pentru protectia datelor de autintificare si a preveni eventuale tentative de fraude/furt de identitate este strict necesar sa respectati urmatoarele cerinte minime de gestionare si asigurare a securitatii parolei:

1. Cerinte minime de gestionare parole

Parolele trebuie sa îndeplinească urmatoarele cerinte:

- sa aibă o lungime minima de 9 caractere;
- sa fie complexă formata dintr-un şir de caractere compus din litere minuscule, majuscule, cifre şi simboluri (%$#&^*);
- sa fie schimbate de utilizator periodic, cel putin o dată la 30 de zile;
- sa fie schimbate imediat, daca exista suspiciuni ca o parolă a putut fi divulgată.

2. Cerinte minime de asigurare a securitatii parolei

Parolele trebuie sa respecte minimum urmatoarele cerinte de securitate:

- sa nu coincidă cu codul numeric personal;
- sa nu coincidă cu data naşterii;
- 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 tranzactiilor, banca recomanda:

- sa pastrati semnatura electronica pe suporturi securizate (token, usb, cartela cu chip);
- sa utilizati semnatura electronica numai pe calculatoarele personale sau de serviciu;
- sa conectati la calculator suportul pe care este pastrata semnatura electronica **numai pentru perioade scurte de timp necesare autentificarii in sistem sau autorizarii tranzactiilor**;
- sa nu transmiteti/divulgati semnatura electronica si parola altor persoane terte.

IMPORTANT: BC „EuroCreditBank" SA NU poarta raspundere pentru utilizarea necorespunzatoare a datelor de autentificare si autorizare (login, parola etc.) si/sau a semnaturii electronice de catre utilizatorii SADD Telebank Business.

6. Masuri de protectie in timpul utilizarii SADD Telebank Business

Pentru asigurarea unei protectii sigure, in timpul utilizarii SADD Telebank Business, a datelor si a calculatorul dvs, banca recomanda:

- Sa nu salvati parolele, login-urile si alte date ce tin de securitate informatiilor in locatii nesigure, in special, pe masa de lucru a calculatorului;
- Sa folositi un firewall personal, care este activ si configurat corespunzator;
- Sa descarcati si sa instalati periodic actualizari de la producator pentru aplicatii si pentru sistemul de operare;

- Sa folositi un sistem anti-virus, care este actualizat periodic si asigura o protectie anti-virus sigura;
- Sa nu incercati sa accesati SADD Telebank Business de pe calculatoare nesigure, deoarece acestea pot fi infectate sau avea anumite vulnerabilitati de securitate;
- Sa nu lasati, niciodata, calculatorul conectat la SADD Telebank Business nesupravegheat;
- Sa inchideti sesiunea de lucru in SADD Telebank Business la finalizarea activitatilor in mod regulamentar , conform instructiunii de utilizare a sistemului.

7. Masuri de protectie impotriva atacurilor Social engineering

Atac de tip Social engineering sau inginerie sociala reprezinta o forma de manipulare in care atacatorii imita o sursa de incredere pentru a convinge victima sa indeplineasca anumite sarcini cum ar fi sa acorde acces la un sistem bancar sau un cont, sau sa dezvaluie informatii confidentiale, cum ar fi parole.

Exemple de situatii de atac de tip Social engineering

Sunteti contactat telefonic de o persoana necunoscuta, care se prezinta drept reprezentant al bancii. In urma discutiei, persoana (atacatorul) va comunica ca banca are o problema tehnica sau ca ati castigat la un premiu de fidelitate oferit de banca si va cere sa comunicati 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 clienti sai prin telefon, email, SMS date confidentiale sau date cu caracter personal.

Banca nu transmite, in orice situatii, mesaje e-mail/SMS clientilor sai pentru a solicita informatii privind:
- identintatea persoanei;
- numarul de cont/card;
- datele de autentifcare/autorizare, inclusiv parole/PIN;
- alte date cu caracter personal sau confidential.

In cazul in care receptionati astfel de mesaje e-mail/apeluri telefonice/SMS-uri prin care se solicita informatii de tipul celor prezentate mai devreme, banca recomanda:
- sa nu raspundeti la aceste mesaje;
- sa nu accesati link-urile si deschideti atasamentele transmise in mesajele e-mail;
- sa nu divulgati nimanui, niciodata parola/PIN, indiferent de persoana sau situatia in care se cere acest lucru;
- sa informati imediat banca prin canale sigure de comunicare despre situatia aparuta.

8. Masuri de protectie impotriva atacurilor de tip Phishing

Phishing-ul reprezinta o metoda de furt de identitate prin care se incearca obtinerea, de la clientii unei banci a unor date cu caracter personal sau confidential. Acestea pot fi folosite ulterior in mod ilegal de catre raufacatori, pentru a efectua tranzactii in contul clientului respectiv. Pentru obtinerea datelor, in atacurile de tip phishing raufacatorii folosesc mijloace de comunicare electronica (e-mail, telefon, mobil) sau programe rau intentionate, care expoateaza vulnerabilitatile sistemului pentru a fura date.

Identificarea atacurilor de tip Phishing

Pentru a lansa un atac **Phishing**, persoanele rau-intentionate, aplica urmatoarele metode:
- Suna si se pot prezenta drept angajati ai bancii, care va informeaza ca: ati castigat un premiu, detin informatii ca contul bancar a fost blocat si va pot ajuta sa deblocati contul sau cardul bancar, veti putea incasa bani in cardul bancar, va pot ajuta sa modificati parola;

- Lanseaza site-uri false care aparent sunt asemanatoare cu site-urile originale ale bancii, pe care apoi le promoveaza prin intermediul mesajelor email/SMS, cu scopul de a sugera clientilor sa viziteze aceste site-uri ca sa isi actualizeze datele cu caracter personal (date de acces la sistemele bancii, date despre conturi/carduri, parole, PIN, etc);
- Transmit mesaje e-mail/SMS ce pretind a fi trimise de catre banca.

Pentru a va influenta, si a va convinge sa introduceti datele sus enumerate pe site-urile false, acestea inventeaza situatii ale unor evenimente care va capteaza atentia.

Exemple de situatii de atac de tip phishing:

- Sunteti contactat de o persoana necunoscuta si felicitat cu ocazia castigarii unui premiu important, dar, in acelasi timp, se solicita sa efectuati un transfer de pe card pe un anumit cont;
- Sunteti contactat de o persoana necunoscuta, care declara precum ca este reprezentantul Serviciului de securitate al bancii. 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 obtinerea si verificarea datelor dvs. de catre banca.

Pentru a va proteja de acest tip de atac, asigurati-va ca adresa paginii web prin care accesati SADD Telebank Business pentru persoane juridice, este cea specificata in Figura.1. De asemenea, verificati prezenta iconitei sub forma de lacat in partea dreapta a adresei web si numele pentru care a fost eliberat certificatul paginii web, prin accesarea iconitei respective. In plus, luati urmatoarele masuri:

- Nu raspundeti la mesajele suspecte;
- Nu transferati bani in conturile solicitate;
- Nu oferiti informatii personale sau date financiare;
- Nu deschideti atasamente sau dati click pe butoane sau pe link-uri.
- Nu accesati pagini web in care sa iti introduciti datele personale.