GHID DE SECURITATE

Accesarea sistemului Internet Banking pentru persoane juridice, pentru perioada exploatarii sistemului in pilot, se realizeaza doar prin adresa
https://corporate.maib.md/bankflexCB/login.aspx?locale=ro-RO

Inainte de a introduce datele de autentificare (Id Companie, Id Utilizator, Parola, Semnatura Digitala) asigurati-va ca adresa web a site-lui este cea specificata mai sus. Totodata, verificati prezenta iconitei sub forma de lacat in partea dreapta a respectivei bare de adrese (a se vedea p.2 din fig.1):

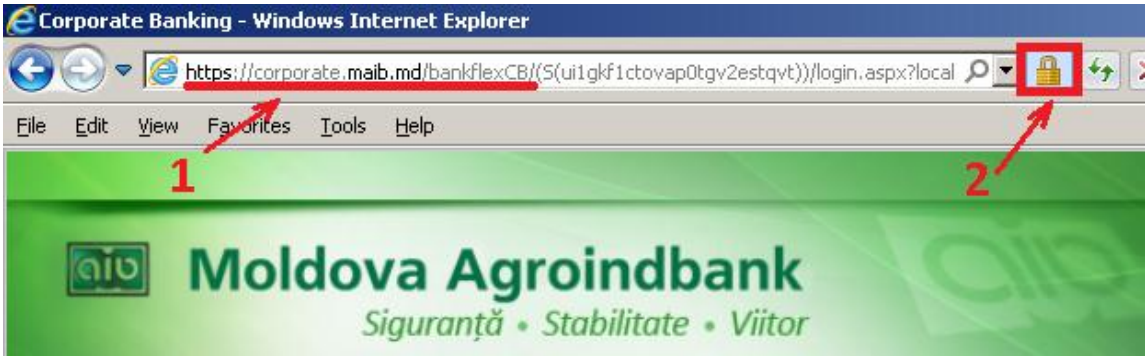

Fig. 1: Accesarea sistemului de deservire bancara la distanta

Accesarea iconitei sub forma de lacat permite verificarea autenticitatii paginii web a sistemului de deservire bancara la distanta (faptul ca sunteti pe pagina oficiala a sistemului si nu una clonata de un raufacator). In fereastra care se deschide dupa apasarea acestei iconite trebuie sa fie indicat **corporate.maib.md** si nicidecum altfel:

Fig. 2: Identificarea paginii web

De fiecare data cand este accesata aplicatia Internet Banking, banca intreprinde masuri de securitate care au drept scop protectia confidentialitatii si integritatii datelor D-stra, si anume:

- ✓ **Criptarea informatiei**

Criptarea informatiei impiedica utilizatorii neautorizati de a intercepta sau schimba datele Dumneavoastra.

BC „Moldova-Agroindbank" SA cripteaza informatiile folosind tehnologia SSL (Secure Socket Layer). Puteti identifica daca v-ati conectat la aplicatia Internet Banking in regim securizat, urmarind in adresa paginii web formatul https:// cu "**s**" la final (ex: **https**://corporate.maib.md/bankflexCB/...) (a se vedea p.1 din fig.1) sau verificand afisarea iconitei sub forma de lacat in partea dreapta a adresei web (a se vedea p.2 din fig.1).

✓ **Inchiderea automata a sesiunii**

Dupa fiecare conectare validata in aplicatia Internet Banking, la un timp de inactivitate de 10 minute, sesiunea de acces expira automat. Orice alta tranzactie si/sau accesare a aplicatiei Internet Banking necesita autentificarea repetata:

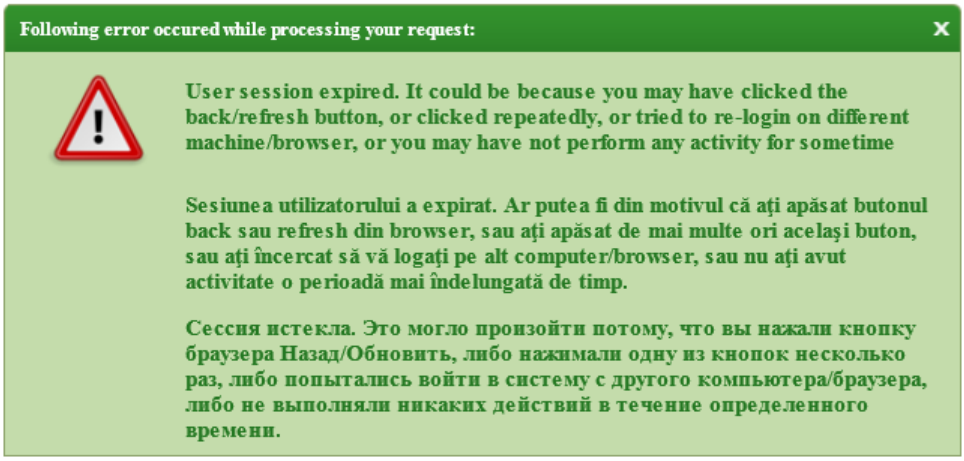

Fig. 3: Mesajul de eroare aparut in urma expirarii sesiunii

✓ **Protectia datelor de autentificare**

<u>Pentru a preveni eventuale tentative de fraude/furt de identitate nu dezvaluiti datele de acces nimanui!</u>
BC „Moldova-Agroindbank" SA recomanda:

- Utilizarea parolelor care sunt greu de ghicit (nu folositi data de nastere, numarul de telefon, numele etc). Pentru a va conforma politicii cu privire la parole, utilizati cel putin 8 caractere alfanumerice si simboluri speciale (ex: **Do3idY&s**);
- Utilizarea a doi factori de autentificare in sistem. Astfel utilizatorii care vor opta pentru o autentificare in doi factori, se vor loga utilizand parola de acces si semnatura digitala:

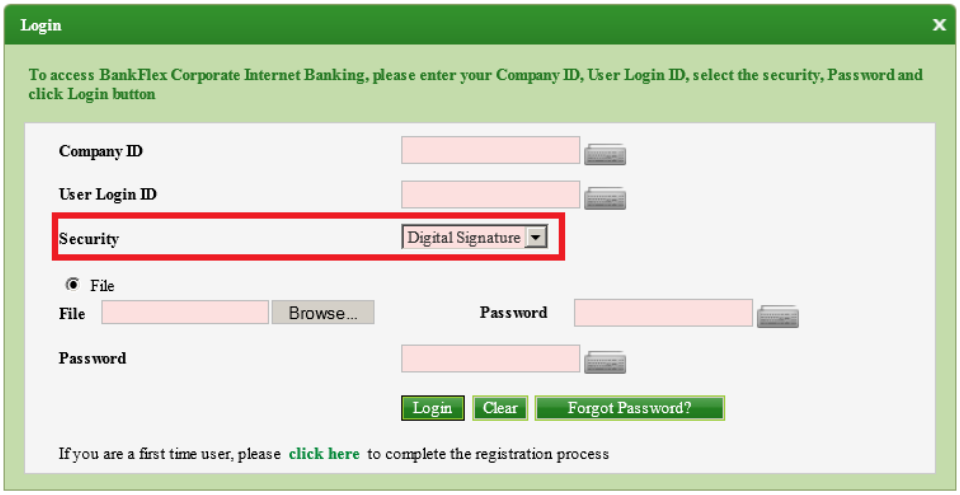

Fig. 4: Interfata de logare in cazul utilizarii semnaturii digitale

✓ **Protectia datelor de autorizare**

Pentru a preveni tentativele frauduloase de autorizare a tranzactiilor, va recomandam:

- sa utilizati semnatura digitala numai de la calculatoarele personale/de serviciu;
- sa pastrati semnatura digitala pe suporturi magnetice externe securizate (cartela cu chip, token, usb);
- sa conectati suportul magnetic pe care este stocata semnatura digitala la calculator **numai pe perioade scurte de timp necesare autentificarii in sistem sau la autorizarea tranzactiilor**;
- sa nu transmiteti/divulgati semnatura digitala si parola de acces, **NIMANUI** sub nici o forma.

ATENTIE: Banca NU poarta raspundere de utilizarea inadecvata a credentialelor de securitate (login, parola etc.) si/sau a semnaturii digitale de catre utilizatorii sistemului Internet Banking.

Cum sa va protejati datele si calculatorul in timpul utilizarii aplicatiei Internet-Banking?

- ✓ Sa nu salvati parolele, Id utilizator, Id companie si alte date legate de securitate in memoria calculatorului;
- ✓ Sa folositi un firewall personal;
- ✓ Sa descarcati si sa instalati periodic actualizari autorizate pentru sistemul de operare;
- ✓ Sa folositi un produs anti-virus, pe care sa-l actualizati periodic;
- ✓ Nu accesati aplicatia Internet Banking de la calculatoare din internet cafe-uri sau calculatoare nesigure, deoarece acestea pot prezenta un pericol de securitate;
- ✓ Nu lasati niciodata nesupravegheat calculatorul conectat la aplicatia Internet Banking;
- ✓ Intotdeauna asigurati-va ca v-ati deconectat corect de la aplicatie la finalizarea utilizarii acesteia.

Sfaturi pentru protectia impotriva atacurilor *Phishing*

Atac de tip phishing – proces prin care o persoana neautorizata incearca sa intre in posesia unor date confidentiale in mod fraudulos.

Cum puteti depista un atac de tipul „Phishing”?

Pentru a lansa un atac **Phishing**, persoanele rau-intentionate, aplica urmatoarele tactici:

1. Construiesc site-uri false care imita site-urile originale ale institutiilor financiare-bancare, 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 Internet Banking, date despre conturi/carduri, parole, PIN, etc).
2. 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/contexte ale unor evenimente care va capteaza atentia.

Exemple:

- Va felicita pentru castigarea unui premiu important dar in acelasi timp va cer sa platiti in avans;
- Serviciul de securitate al bancii va anunta ca sistemul bancar a cedat, si datele de autentificare s-au pierdut, iar pentru actualizarea bazei de date a bancii, este necesara verificarea datelor Dvs. de catre banca.

Pentru a va proteja de acest tip de atac, asigurati-va ca adresa paginii web prin care incercati sa accesati sistemul Internet Banking pentru persoane juridice, este cea specificata mai sus, verificati prezenta iconitei sub forma de lacat in partea dreapta a adresei web (a se vedea p.2 din fig.1) si numele pentru care a fost eliberat certificatul paginii web, prin accesarea iconitei respective. (a se vedea fig.2)

Sfaturi pentru protectia impotriva atacurilor *Social engineering*

Atac de tip Social engineering - manipulare a unei persoane astfel incat aceasta sa intreprinda o actiune dorita de atacator sau ca acesta sa isi divulge informatiile confidentiale.

Cum puteti depista un atac de tipul „Social engineering”?

Exemplu:

Dvs. 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 o tombola oferita de banca si va cere sa comunicati prin telefon datele dvs. personale (date de acces la Internet Banking, datele din buletinul Dvs. de identitate, detalii despre conturi/carduri, PIN, parole, etc).

BC „Moldova-Agroindbank” SA nu va solicita NICIODATA telefonic, prin email, SMS sau in alte forme datele confidentiale ale Dumneavoastre!

BC „Moldova-Agroindbank” SA nu va transmite, sub niciun pretext, mesaje e-mail/SMS clientilor pentru a cere informatii despre:

- identintatea acestora;
- 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 in care vi se cer informatii de tipul celor invocate mai sus, va recomandam:

- nu raspundeti la aceste mesaje;
- nu accesati link-urile trasmise in mesajele e-mail;
- nu divulgati nimanui, niciodata parola/PIN, indiferent de persoana sau contextul in care vi se cere acest lucru;
- informati imediat banca, mentionand toate detalii si circumstantele posibile.