GHID DE SECURITATE

B.C. „ENERGBANK" S.A. Vă oferă posibilitatea să gestionați banii Dumneavoastră atunci când aveți nevoie de aceasta prin intermediul Sistemului de deservire bancară la distanță **Business Online**. În același timp face tot posibilul să VĂ protejeze de diverse amenințări de securitate. Dar toate eforturile depuse de bancă sunt inutile dacă nu veți conștientiza că dumneavoastră sunteți parte a sistemului de securitate și în mare măsură securitatea banilor depinde de Dumneavoastră, în calitate de responsabil primar pentru asigurarea securității informației de autentificare și autorizare (login, parolă, telefon mobil, dispozitive criptografice, ș.a.).

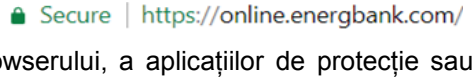
În acest context Vă recomandăm să urmați niște instrucțiuni simple pentru asigurarea securității tranzacțiilor Dumneavoastră:

1. Asigurați siguranța stațiilor de lucru și a dispozitivelor utilizate.

Pentru accesarea Sistemului **Business Online** optați pentru utilizarea dispozitivele proprii și rețelele în care aveți încredere asigurându-vă că pe dispozitivul de pe care accesați Sistemul **Business Online** este instalată aplicația antivirus și sunt instalate actualizările de rigoare. Nu utilizați rețelele publice pentru accesarea Sistemului **Business Online** sau asigurați-vă că ați luat măsuri adiționale de securitate. Niciodată nu utilizați dispozitivele publice pentru accesarea Sistemului **Business Online**, cum ar fi internet terminalele din aeroport sau alte dispozitive.

Nu lăsați fără control telefoanele mobile și dispozitivele criptografice utilizate pentru autentificare și autorizare în cadrul aplicației **Business Online** și nu păstrați în același loc datele de autentificare (login, parola, PIN) și dispozitivele utilizate pentru autentificare și autorizare bifactorială.

2. Accesați Sistemul doar din locații sigure cum ar fi pagina oficială a băncii sau adresa salvată anterior în browser.

Accesați sistemul urmând adresele de pe pagina oficială a băncii sau introducând direct adresa electronică în browser. La accesare sistemului verificați dacă se aplică metode criptografice de protecție a informație care pot fi identificate prin prefixul https:// în adresa electronică 

În cazul în care primiți avertizări de securitate ale browserului, a aplicațiilor de protecție sau aveți suspiciuni referitor la veridicitatea paginii web renunțați la accesarea sistemului și apelați serviciul suport clienți al băncii.

Colaboratorii B.C.„ENERGBANK" S.A. nu Vă vor transmite niciodată scrisori electronice, mesaje SMS sau alt tip de mesaje prin intermediul cărora să vă solicite să urmați anumite adrese URL pentru accesarea Sistemului **Business Online** și nu vor solicita informații referitor la elementele de securitate cum ar fi parole de acces, coduri de autorizare expediate prin SMS sau e-mail, sau alte informație confidențiale.

3. Utilizați parole impredictibile, complexe dar ușor memorabile și nu le comunicați nimănui, nici colaboratorilor Băncii.

Pentru accesarea sistemului utilizați parole complexe, care pe lângă faptul că satisfac cerințele minime de securitate impuse de bancă nu vor fi predictibile și vor fi ușor memorabile. Complexitatea parolei în mare parte depinde de lungimea acesteia. Nu utilizați în calitate de parole numele de utilizator, date de naștere, cuvinte de uz comun și evitați utilizarea în cadrul Sistemului **Business Online** a parolelor pe care le mai utilizați în alte sisteme informatice.

Nu comunicați nimănui, inclusiv colaboratorilor băncii, și nu vă notați în nici un mod parolele de acces. Chiar dacă ați uitat parola aceasta poate fi ușor restabilită.

4. Optați pentru utilizarea semnăturii electronice ca factor adițional de autentificare în Sistemul Business Online, aceasta va asigura un nivel sporit de securitate.

Sistemul **Business Online** vă oferă posibilitatea să alegeți dintre autentificarea prin intermediul unei parole de unică folosință expediată prin intermediul unui SMS, Semnătura electronică mobilă și Semnătura electronică eliberată de către Centrul de certificare a cheilor publice din cadrul Întreprinderii de Stat „Centrul de Telecomunicații Speciale" precum și din cadrul IP „Agenția Servicii Publice". Utilizarea SMS-urilor ca factor adițional de autentificare asigură un nivel mai redus de securitate comparativ cu celelalte metode. Chiar dacă ați ales această metodă de autentificare evitați utilizarea aceluiași dispozitiv mobil pentru accesarea sistemului și autentificare sau autorizare bifactorială.

5. Nu introduceți informația de autentificare în paginile web accesate direct din scrisorile electronice și nu o comunicați nimănui.

Banca nu vă va expedia scrisori electronice prin intermediul cărora să vă ceară să furnizați oricare din datele dvs. de autentificare.

Dacă primiți un e-mail care pare a fi de la Bancă, prin care se solicită astfel de informații, tratați-l cu suspiciune deoarece ar putea fi o încercare de a vă afla datele de autentificare.

De asemenea fiți conștienți de daunele care pot fi cauzate prin apelurile telefonice nesolicitate și nu comunicați informații confidențiale, cum ar fi date personale, login, parola, codul PIN sau alte informație. Reveniți cu un apel la Bancă la unul din numerele de telefon de care dispuneați anterior sau care sunt publicate pe pagina Băncii și verificați legitimitatea apelului.

6. Optați pentru utilizarea Serviciului Cont Alert pentru a primi notificări referitor la tranzacțiile efectuate și monitorizați starea conturilor.

Utilizând serviciul Cont Alert veți primi înștiințări referitor la tranzacțiile efectuate și veți avea posibilitatea să depistați în timp util tranzacțiile frauduloase. Verificați periodic starea conturilor și istoricul tranzacțiilor efectuate. Verificați istoricul accesărilor Sistemului **Business Online** și dacă accesarea anterioară a fost efectuată de Dvs

.