Securitatea serviciilor prin Internet
Recomandari Intesa Sanpaolo Bank

Serviciul Intesa Sanpaolo Bank de tip Internet Banking respecta standardele tehnice specifice pentru a oferi clientilor un nivel avansat de securitate a informatiior.

Pentru a preveni eventuale tentative de frauda, va recomandam sa aveti in vedere urmatoarele:

✘ **NU** accesati niciodata link-uri provenite din email-uri sau de pe alte site-uri care nu apartin Intesa Sanpaolo Bank. Banca nu trimite niciodata clientilor sai mesaje, de orice natura, prin care sa solicite divulgarea sau modificarea unor elemente de identificare, accesarea unor link-uri pentru a va conecta la serviciul de Internet Banking sau la orice alte site-uri.

✘ **NU** divulgati nimanui codul PIN al Token-ului sau cardului Dvs., pentru niciun motiv; Dispozitivul Token aflat in posesie trebuie tinut in deplina siguranta (sa nu fie tinut la vedere, sa nu aiba inscriptionat codul PIN, sa fie pastrat in dulapuri sau spatii incuiate atunci cand nu este utilizat).

✘ **NU** lasati calculatorul nesupravegheat, si conectat la pagina de Internet Banking, mai ales daca sunteti intr-un loc public; inchideti sesiunea de Internet Banking prin apasarea butonului “Logout” din aplicatie.

✔ Accesati serviciul de Internet Banking doar de pe website-ul oficial al Bancii, ***www.intesasanpaolobank.ro.***

✔ Verificati autenticitatea paginii de Internet Banking a Intesa Sanpaolo Bank, urmarind urmatoarele elemente de securitate:

- Sigla Secured by Thawte, alaturi de data curenta, trebuie sa apara in coltul dreapta jos al paginii de IB, la introducerea numelui de utilizator si a parolei, garantand autenticitatea paginii accesate;
- In bara de adresa, trebuie sa apara pictograma reprezentand un lacat in miniatura, alaturi de numele Bancii; in situatia activarii cu mouse-ul a pictogramei respective, se pot vizualiza informatii legate de autenticitatea paginii web respective - Identified by Thawte.
- Adresa URL a paginii de Internet Banking, care asigura conexiune criptata in zona de navigare a browser-lui, trebuie sa fie *https://internetbanking.intesasanpaolobank.ro*
- Langa adresa URL a serviciului de Internet Banking va aparea intotdeauna informatia referitoare la proprietarul site-ului (B.C. INTESA SANPAOLO ROMANIA S.A.).

✔ Daca elementele de securitate nu sunt prezente pe pagina de Internet Banking, sau daca datele difera celor prezentate anterior, va rugam sa abandonati logarea si sa contactati de urgenta Banca.

✔ Verificati informatiile afisate de aplicatia de Internet Banking cu privire la data si ora ultimei autentificari si anuntati de urgenta Banca in eventualitatea unei discrepante.

✔ Verificati in mod regulat conturile Dvs., precum si mesajele primite de la Banca prin intermediul aplicatiei Internet Banking, aflate in meniul Inbox -> Mesaje primite. Contactati imediat serviciul CALL CENTER in cazul in care observati tranzactii pe care nu le recunoasteti.

✔ Este recomandat sa anuntati Banca prin intermediul serviciului CALL CENTER in orice situatie in care aveti suspiciuni privind securitatea contului si a tranzactiilor Dvs., indicand cat mai multe informatii in acest sens (data utilizarii, browserul folosit, adresa IP de la care s-a facut conectarea, eventuale mesaje sau notificari din pagina).

✔ **Acordati atentie e-mail-urilor suspecte – email-uri de tip spam/scam**
Email-urile de tip spam/scam reprezinta email-uri trimise in masa catre destinatari, prin care se ofera joburi bine platite, premii, castiguri, toate avand ca scop ulterior solicitarea de bani de la acestia.
De asemenea, majoritatea virusilor actuali vin sub forma unor atasari la mesaje de e-mail. In consecinta, nu deschideti fisiere atasate email-urilor primite de la persoane pe care nu le cunoasteti sau email-urilor primite chiar si de la persoane cunoscute.
Recomandarea este sa stergeti direct email-urile suspecte, mai ales daca au in continut link-uri sau fisiere atasate. Verificati mereu expeditorul chiar daca pare cunoscut (informatiile privind expeditorul si destinatarul sunt deseori alterate in mesajele de spam, astfel incat sa sugereze ca sunt autentice).

✔ **Evitati fraudele on-line – fenomenul phishing**
Phishing-ul este un proces fraudulos prin care clientii unei companii sunt determinati sa dezvaluie date personale sau confidentiale care ulterior sunt folosite ilegal pentru a efectua tranzactii in contul clientului respectiv. Atacurile de phishing pot fi realizate prin:

- e-mail/ SMS: un mesaj electronic este trimis clientilor, pretinzand a fi din partea unei surse legitime (de exemplu Banca), prin care se solicita introducerea de date confidentiale intr-un link indicat in textul mesajului, si care directioneaza catre un site falsificat.

- telefon: o persoana pretinde ca suna din partea Bancii si, invocand probleme tehnice (de exemplu probleme in sistemul de plati), solicita informatii confidentiale precum codul PIN, numarul contului, parola, etc.

ATENTIE!

Intesa Sanpaolo Bank NU va trimite niciodata clientilor sai mesaje, de orice natura, prin care sa solicite divulgarea sau modificarea unor elemente de identificare, accesarea unor link-uri pentru a va conecta la serviciul de Internet Banking sau la orice alte site-uri.

Intesa Sanpaolo Bank NU va contacta niciodata clientii pentru a solicita coduri, parole de acces sau PIN-uri. Daca sunteti contactati de persoane care pretind ca reprezinta Banca si va solicita aceste informatii, va rugam sa incheiati discutia si contactati serviciul CALL CENTER.

Daca totusi va confruntati cu un asemenea caz va rugam sa contactati de indata serviciul CALL CENTER, numar telefon 0800 800 888, apelabil gratuit din orice retea de telefonie.

Recomandari pentru protectia calculatorului Dvs.

Iata cateva reguli de urmat pentru a avea un calculator protejat:

✔ UTILIZATI UN PROGRAM ANTIVIRUS

De fiecare data cand va conectati la Internet, va expuneti pericolelor virusilor. Ne referim la virusi informatici, care sunt produse software create cu diverse scopuri (furt de identitate, etc.). Ei ataca prin intermediul programelor dobandite prin intermediul unor surse neverificate, a site-urilor dubioase, atasamentelor de e-mail sau pur si simplu se raspandesc de la un calculator la altul prin mecanisme puse la dizpozitie chiar de utilizatori. Unii virusi pot cauza disfunctionalitati ale calculatorului, se pot multiplica sau pot permite accesul hackerilor.
Instalarea unui program anti-virus nu este suficienta. Un lucru esential in exploatarea unui astfel de program, este actualizarea automata a listei de semnaturi (lista de virusi cunoscuti).

✔ FOLOSITI PROGRAME ANTI-SPYWARE

Spyware este denumirea data unei categorii de programe folosite pentru captarea de date (prin analizarea site-urilor accesate de utilizator, de exemplu: moda,stiri, site-uri de socializare, etc) si de a transmite eventual acelui utilizator reclame conform datelor extrase de spyware.
Programele spy pot incetini calculatorul, conexiunea la Internet, dar pot si sa copieze informatii confidentiale precum numarul si PIN-ul cardului, codul sau parola utilizate in cadrul autentificarilor electronice.

✔ ATENTIE LA PROGRAMELE DESCARCATE DE PE INTERNET

Fiti atenti la documentele pe care le descarcati in computer, dintre cele primite prin email, sau diferite programe descarcate din surse necunoscute.
Nu descarcati programe de pe Internet daca sursa nu este de incredere si nu deschideti fisiere a caror provenienta nu o cunoasteti. Acestea pot contine virusi care odata instalati pe calculatorul Dvs., compromit protectia si cauzeaza daune semnificative.

✔ MENTINETI CALCULATORUL ACTUALIZAT LA ZI

Asigurati-va ca sistemul si browser-ul dumneavoastra sunt actualizate cu ultimele patch-uri de securitate care vor asigura o protectie sporita in timpul navigarii pe Internet.
Asigurati-va ca v-ati setat computerul sa primeasca regulat cele mai recente actualizari si corectii de securitate. Acestea nu vizeaza numai sistemul de operare, de exemplu Microsoft Windows sau Apple Mac OS X, ci si aplicatii precum Adobe Flash, Microsoft Internet Explorer sau Mozilla Firefox.