Slider 1

Internet Banking - Internet Banking, sau online banking, este un termen folosit pentru sistemele de plăți cu acces la distanță utilizate pentru efectuarea de tranzacții bancare prin intermediul Internetului. Acestea sunt sisteme bancare care permit accesul electronic de la distanță, la conturile bancare, în vederea operării de tranzacții și obținerii de situații referitoare la propriile conturi.

Slider 2

Tipuri:

1. **Internet Banking** – instrument de plată cu acces la distanță, care se bazează pe conexiunea la Internet și pe sistemele informatice ale emitentului, conectarea realizându-se folosind o aplicație de tip browser;
2. **Home Banking** – instrument de plată cu acces la distanţă, care se bazează pe o aplicație software a emitentului instalată la sediul deținătorului, pe o stație de lucru individuală sau în rețea.
3. **Mobile Banking** - – instrument de plată cu acces la distanţă, care presupune utilizarea unui echipament mobil (smartphone, 1ablet, PDA – Personal Digital Assistant etc) și a unor servicii oferite de către operatorii de telecomunicații

Slider 3

Utilizarea Internet Banking-ului a devenit o soluție tot mai răspândită și acceptată de publicul larg ca alternative la metoda clasică prin prezentarea într-o filială bancară pentru realizarea operațiunilor uzuale. Avantajele precum mobilitatea și disponibilitatea 24/7 au fost permanent suplimentate prin extinderea gamei de operațiuni care pot fi derulate în condiții de siguranță, oferind în ziua de astăzi posibilitatea executării ușoare de la distanță a mai multor tipuri de operații, spre exemplu:

1. Deschidere de conturi
2. Transferuri intre conturi
3. Plati in lei sau valuta
4. Constituire/lichidare depozite
5. Schimb valutar
6. Ordine de plata intrabancare si interbancare
7. Vizualizare extrase bancare
8. Actualizare rapida a datelor personale

Slider 4

Când este adusă în discuție securitatea serviciilor de Internet Banking, primele lucruri la care ne gândim de regulă sunt calculatoarele și conexiunea între client și bancă. De cele mai multe ori însă, securitatea acestor servicii nu se rezumă doar la calculatoare și conexiuni, deși acestea rămân extrem de importante și sensibile. Măsurile de securitate sunt gândite și aplicate ca un pachet integrat și complet cu rolul de a permite maximum de beneficiu utilizatorilor în condiții minime de risc.

1. **Autentificarea cu user și parolă** – Aceasta metodă clasică de recunoaștere a utilizatorilor autorizați, datorită nivelului limitat de securitate pe care îl oferă, este pusă la dispoziție în general pentru accesarea unor date cu cerințe reduse privind nivelul de confidențialitate sau pentru realizarea unui număr limitat de operațiuni cu un grad de risc redus asupra clientului..
2. **Autentificarea cu token fizic** - Dispozitivul de autentificare generează coduri aleatoare, valabile pentru o singură utilizare într-un interval de timp prestabilit, care vor fi utilizate de către utilizatori la momentul autentificării în aplicație și pentru semnarea tranzacțiilor efectuate prin intermediul acesteia. Dispozitivul este pus la dispoziție de către banca la achiziționarea serviciului de Internet Banking și în funcție de tipul acestuia poate fi securizat la rândul său prin intermediul unui cod PIN ales de beneficiar la prima utilizare. În plus, tokenul fizic poate să ofere și un cod de control care apare pe pagina de Internet Banking și care este generat în funcție de codul pentru identificare.
3. **Autentificarea cu token virtual** – Această metodă de autentificare constă în transmiterea automată prin SMS a unui cod de acces cu perioadă limitată de valabilitate.
4. **Autentificarea printr-un certificat instalat în browser** – Certificatele, împreună cu un parametru de autentificare, sunt folosite pentru verificarea identității persoanei care trimite mesaje și pentru a oferi posibilitatea destinatarului de a codifica/decodifica răspunsurile. O persoană care vrea să trimită un mesaj codat, trebuie să ceară mai întâi un certificat de la o autoritate de certificare și să îl instaleze în browser. Dacă se dorește utilizarea serviciului de Internet Banking de pe mai multe calculatoare, utilizatorii vor trebui să solicite și să instaleze câte un certificat pe fiecare dintre sisteme.
5. **Aplicații dedicate mobile banking** - Pentru dispozitivele de tip mobile au fost puse la dispoziția clienților aplicații specifice care oferă pe lângă o interfață ușor de utilizat și siguranță sporită datorită încorporării mecanismelor enumerate anterior (nume de utilizator, parolă/PIN și/sau token încorporat).
6. **Autentificarea în doi pași** – Clienții sunt obligați să se autentifice după două criterii de identificare: ceva pe care utilizatorul îl cunoaște (un nume de utilizator și o parolă) și ceva care este foarte probabil să dețină (un token fizic, un telefon mobil etc).
7. **Criptarea comunicațiilor** - Criptarea datelor înainte de a fi transmise prin Internet constă în transformarea acestora într-un șir de caractere indescifrabil cu rolul de asigurare a confidențialității pe timpul realizării comunicației între sistemul băncii si cel al clientului.
8. **Limitarea numărului de încercări eșuate de autentificare** – Odată cu depășirea numărului maxim de tentative, contul este blocat.
9. **Limitarea timpului de inactivitate într-o sesiune** – Odată cu atingerea limitei de timp, se realizează o deactivare automată a sesiunii de lucru.
10. **Limitarea orară privind efectuarea tranzacțiilor cu nivel de risc ridicat**
11. **Evidența conectărilor** – Furnizorii de Internet Banking pot pune la dispoziție, prin intermediul contului de Internet Banking, situații privind conectările realizate pe conturile respective cu rolul de a facilita beneficiarului posibilitatea de a identifica eventuale conectări neautorizate. Datele furnizate se vor referi în general doar la ID-ul de sesiune, data conectării, data deconectării și stația de la care v-ați conectat (adresa IP sau nume calculatorului).

12. **Informarea clară și completă a beneficiarilor** – Pe site-urile publice ale furnizorilor de servicii de Internet Banking pot fi găsite toate informațiile necesare utilizării în condiții optime a mecanismelor de autentificare puse la dispoziția propriilor clienți, precum și modul de acțiune al acestora în vederea remedierii situațiilor neprevăzute sau solicitării de suport.

Slider 5

1. **Niciun furnizor de servicii de Internet Banking nu solicita date confidențiale utilizatorilor** – Indiferent de metoda prin care sunt cerute aceste date nu trebuie dat curs solicitărilor. Băncile nu apelează la clienții săi pentru a-i fi transmise date precum: numărul cardului, data expirării, PIN-ul, parola, ID-ul de logare, codul token sau orice alte date personale.
2. **Nimeni nu are dreptul de a solicita unui client conectarea pe propriul cont de Internet Banking sau transmiterea datelor personale** – Acest tip de înșelătorie este cunoscut sub numele de „phishing". De obicei apare ca un presupus mesaj de la bancă în care clienților li se spune că trebuie să comunice sau să introducă într-un formular informații personale/confidențiale în vederea validării/actualizării și astfel ele sunt capturate în mod fraudulos de către necunoscuți sau rău-voitori (parolă de acces, număr card, etc.). Pentru a fi mai convingători, aceștia recurg la motivații false precum mesaje de alertare privind posibilitatea de a fi 3entat unei fraude, motiv pentru care s-ar impune verificarea de urgentă a propriilor conturi, oferind de asemenea un link pentru accesarea serviciului, dar care în realitate redirecționează spre un site clonat. Atacurile de tip phishing se folosesc de canale electronice de comunicație (e-mail, telefon) sau de programe rău intenționate, care exploatează vulnerabilitățile sistemului pentru a fura date. În situația în care se primesc mesaje de acest gen este cel mai indicat ca acestea sa fie șterse direct, fără a fi accesate, mai ales daca au inserate link-uri sau atașamente și provin de la adrese de e-mail necunoscute. Alternativ, dacă se încearcă astfel de înșelătorii prin telefon este recomandat să se 3entat comunicarea datelor solicitate și contactarea furnizorului de servicii în baza datelor de contact postate pe site-ul 3entativ, pentru a verifica veridicitatea solicitării. Un indiciu pentru a vă feri dumneavoastră de astfel de fraude, îl reprezintă faptul că de cele mai multe ori inițiatorii unui atac nu știu cu ce bancă lucrează destinatarul mesajului. De aceea, mesajele sunt transmise la întâmplare către liste de adrese în speranța că vor găsi 3entat cu cont la banca al cărei site a fost duplicat şi care nu realizează pericolul căruia se expun.
3. **Atunci când site-ul de Internet Banking funcționează cu erori sau apar solicitări suplimentare nejustificate de reautentificare** – În multe dintre situații, erorile potențiale ar putea avea ca sursă incompatibilitatea unor aplicații, dar uneori sunt generate de inserarea malițioasă în calculatorul clientului, de către 3entativ rău-intenționate, a unor aplicații sau troieni (ex. Zeus, SpyEye, Citadel etc) cu rolul de a fura datele de conectare sau de a-i redirecționa către site-uri clonate. Dacă apar mesaje nejustificate prin care este solicitata reautentificarea unui utilizator, deși sesiunea pe care este conectat este în continuare validă sau a fost închisă prin apăsarea butonului Logout, este cel mai probabil să fie o 3entative de furt de date. Dacă se observă erori evidente de funcționare a site-ului băncii sau al serviciului de Internet Banking (ex: unele link-uri din meniu nu conduc spre paginile care ar fi trebuit să fie disponibile) este foarte posibil ca utilizatorul vizat de atacator sa fi fost redirecționat către unul din acele site-uri falsificate.

Slider 6

Fiecare furnizor de servicii de Internet Banking aplică masuri de securitate pentru a asigura confidențialitatea datelor și tranzacțiilor clienților săi, dar având în vedere tentativele tot mai frecvente și mecanismele tot mai complexe de furt a identității informatice în societatea actuală este necesar ca inclusiv beneficiarii serviciilor să poată identifica o acțiune răuvoitoare și sa aplice masurile de protecție aferente. Prin urmare, acțiunile furnizorilor și ale clienților trebuie sa fie complementare, având același obiectiv comun respectiv protecția datelor, astfel:

1. **Accesarea serviciul doar de pe site-ul oficial al furnizorului** - Se recomandă evitarea conectării la Internet Banking prin intermediul unui link pus la dispoziție în corpul unui e-mail (inserat doar pentru a facilita accesul la acest serviciu).
2. **Păstrarea confidențialității numelui de utilizator și a parolei** - Deși, simpla divulgare a datelor de autentificare nu este suficientă pentru a produce efecte negative semnificative asupra unui utilizator, ele trebuie sa rămână confidențiale deoarece ar elimina poate chiar și jumătate din rolul măsurilor de securitate. Similar oricăror alte credențele, fiecare utilizator nu trebuie să le divulge sau să și le noteze pe diverse medii de stocare.
3. **Păstrarea în condiții de siguranță a token-ului** - Fiecare utilizator trebuie să se asigure că token-ul care i-a fost pus la dispoziție nu rămâne nesupravegheat, iar atunci când securitatea acestuia este sporită prin intermediul unui cod PIN nu-l va divulga niciunei persoane. Daca a fost constatată pierderea dispozitivului se impune anunțarea imediată a furnizorului în vederea blocării acestuia.
4. **Accesarea serviciului doar pe paginile HTTPS** - Întotdeauna, înaintea conectării la serviciul Internet Banking, se impune verificarea paginii de logare afișată în browser pentru a exista siguranța că adresa URL este de forma https și NU http. Verificarea trebuie sa includă de asemenea și certificatul digital al serverului la care se realizează conectarea (este suficient un dublu click pe lăcățelul din dreapta jos sau cel prezentat în bara de adrese a browser-ului). Din datele furnizate de certificat ar trebui să fie identificate fără nicio îndoială numele companiei și numele autorității de certificare care l-a emis.
5. **Solicitarea clarificărilor necesare prin intermediul serviciul suport al furnizorului** - Indiferent dacă este există suspiciuni privind eventuale tentative de fraudare sau există nelămuriri privind utilizarea uneia dintre opțiunile serviciului accesat, se recomandă utilizarea facilităților de suport puse la dispoziție de furnizorul de servicii de Internet Banking. Pentru contactarea furnizorului recomandăm a se utiliza doar datele de contact făcute publice pe site-ul oficial.
6. **Activarea alertelor pe telefon sau email** - Dacă furnizorul de servicii de Internet Banking poate pune la dispoziție, ca un control suplimentar, mecanisme de alertare prin telefon sau e-mail privind operațiunile derulate în conturile tale, recomandăm utilizarea acestora. Astfel de alerte vor semnala toate tranzacțiile efectuate pe contul beneficiarului și oferă posibilitatea descoperirii în timp util a operațiunilor ilicite.
7. **Verificarea în mod regulat a conturilor** - Verificarea conturilor cu regularitate poate fi considerată o alternativă la situația în care nu există un mecanism automat de alertare prin SMS

sau e-mail. O astfel de practică permite identificarea tranzacțiilor necunoscute, iar pentru obținerea clarificărilor necesare se recomandă contactarea imediată a serviciul suport pus la dispoziție de furnizor.

8. **Închiderea sesiunilor de lucru** - Recomandăm ca după utilizarea serviciului de Internet Banking sesiunile de lucru să fie închise imediat de către utilizator, mai ales dacă sistemul de pe care s-a realizat conexiunea va rămâne nesupravegheat. Pentru aceasta, este necesară utilizarea de fiecare dată a opțiunii Logoff sau Logout la finalizarea operațiunilor.
9. **Renunțarea la opțiunea de salvare a datelor de autentificare în browser** - Toate browserele de Internet oferă facilitați pentru salvarea username-ului și a parolei din aplicațiile accesate, oricare ar fi acestea. Pentru siguranța dumneavoastră, se recomandă verificare stării acestor facilități sau optarea pentru a nu salva aceste date atunci când sunt afișate aceste întrebări.
10. **Utilizarea serviciului doar de pe calculatoarele/dispozitivele cunoscute** - Se recomandă evitarea accesării acestui serviciu de pe sisteme necunoscute, precum cele din sălile de Internet. Similar, se recomandă utilizarea doar a conexiunilor wireless cunoscute pentru accesarea Internet Banking.
11. **Schimbarea credențialelor de acces** - Cu o anumită regularitate, sau mai ales atunci când există bănuieli privind cunoașterea credențialelor de acces de către o altă persoană, se recomandă schimbarea acestor date în măsură în care sistemul pus la dispoziție de furnizorul de Internet Banking o permite. Totodată, pentru definirea unei parole noi se recomandă evitarea cuvintelor uzuale și alegerea combinațiilor de litere mici, litere mari, cifre si/sau caractere speciale. De asemenea, nu se recomandă stabilirea parolelor de acces sau a codurilor PIN în funcție de datele personale: ziua de naștere, vârsta, etc.
12. **Utilizarea aplicațiilor mobile doar de pe site-urile oficiale** - Pentru a evita situațiile în care clienții ar putea fi păcăliți să utilizeze aplicații pentru mobilebanking cu cod malițios inserat, toți furnizorii acestui serviciu și-au definit clar lista de siteuri specializate prin care se poate intra în posesia aplicației oficiale. Ca atare, se recomandă verificarea site-ului furnizorului pentru a identifica aceste site-uri înainte de a inița descărcarea aplicației

Slider 7

Este extrem de ușor să se realizeze cumpărături de pe un site web. Este nevoie doar de un card de debit sau credit (este recomandat cel de debit, pentru a nu risca decât suma din cont). Deși majoritatea cardurilor emise în România, în lei, sunt în prezent acceptate și de magazine internaționale, cel mai bine este să se verifice acest lucru la banca respectivă. Însă, dacă este vorba despre un card Visa sau MasterCard, nu ar trebui să existe probleme. Înainte de a se face achiziția, trebuie să se creeze un cont pe site-ul respectiv (se va cere acest lucru o singură dată). De obicei, se cere numele (uneori așa cum apare pe cardul bancar), adresa completă, adresa de e-mail, telefon și numărul cardului (atât cele 16 de pe fața cardului, cat și ultimele trei de pe spate). După aceea, tot ce trebuie făcut este să se aleagă produsele și să se urmeze instrucțiunile pentru plată. Ca să nu existe probleme privind produsele achiziționate, trebuie citite cu atenție condițiile de vânzare, pentru a se ști sigur cât timp este la dispoziție pentru returnare, dacă produsul ajunge la destinație stricat sau nu se mai dorește achiziționarea acestuia.

Slider 8

1. Cumpărăturile se vor face din magazine online cunoscute şi de încredere. Trebuie ales ca punct de plecare un site cunoscut şi de încredere, în loc să se utilizeze un motor de căutare web. De asemenea, chiar dacă se accesează o adresă cu nume cunoscut gen amazon.com, este necesar să se acorde o atenție deosebită la modul în care este scrisă (litere omise sau incorecte) şi domeniul unde este găzduită (de genul .net în loc de .com). Adeseori, aceste mici erori ascund, de fapt, site-uri pirat concepute astfel încât să semene ca nume cu originalul, cu scopul de a vinde produse fictive sau, mai rău, pentru a transfera banii din conturi.
2. Niciodată nu se vor face cumpărături online, cu cardul bancar, de pe un site care nu este criptat cu protocolul SSL (Secure Sockets Layer). Ssite-ul utilizeaza acest protocol dacă adresa afișată în bara browser-ului începe cu HTTPS:// (în loc de HTTP://), iar în bara de adrese sau pe bara de la baza paginii, este afișată o mică imagine a unui lacăt închis.
3. Nu se vor furniza mai multe informații decât este necesar și normal. În general, magazinele online nu cer CNP-ul, sau data nașterii, pentru a perfecta o tranzacție. Pe de altă parte, dacă răufăcătorii obțin asemenea detalii, împreună cu numărul cardului de credit folosit la cumpărături, pot comite mult mai multe ilegalitati. Cu cât afla mai multe detalii, cu atât le este mai ușor să fure identități, fie pentru a goli conturile, fie pentru alte acte ilegale mult mai grave.
4. Trebuie verificate cat se poate de des operațiunile din contul bancar pentru a vedea daca există tranzacții suspecte sau către alte conturi față de cele știute;
5. Este foarte important sa se utilizeze numai computerul personal pentru cumpărături. Orice tranzacție online necesită securitate ridicată, iar dacă se efectuează de pe un dispozitiv care nu aparține cumpărătorului, de fapt, datele personale sunt puse la dispoziția posesorului acelui calculator. Evident, este total contraindicat să se folosească în acest scop un computer public (ex. Internet-cafe, sau terminale puse gratuit la dispoziția publicului în diverse instituții sau centre comerciale), dar nici chiar computerul sau telefonul unei cunoștințe nu reprezintă alternative recomandabile, pentru că nu se cunoaște nivelul de securitate şi cine mai are acces la acel terminal.
6. Sunt de evitat „ofertele de nerefuzat” deoarece de multe ori sunt înșelătoare. Dacă un produs este oferit mult sub prețul pieței, apare întrebarea „de ce?”. Ce câștigă comerciantul care dă aproape gratis ceva care, altfel, este foarte scump? Amazon, eBay, chiar și site-uri autohtone abundă de asemenea oferte.

Proiect realizat de Bozian Camelia și Bulbuc Răzvan.