Ce este internet banking? (– Nistor Niculae-Filip)

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. Astfel de sisteme sunt reprezentate de:

• **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;

• **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.

• **Mobile Banking** – instrument de plată cu acces la distanţă, care presupune utilizarea unui echipament mobil (smartphone, tableta, PDA - Personal Digital Assistant etc) și a unor servicii oferite de către operatorii de telecomunicații.

Furnizorul de servicii Internet Banking reprezintă acea instituție de credit sau instituție financiară nebancară care emite şi pune la dispoziția deținătorului un instrument de plată electronică, pe baza unui contract încheiat cu acesta, iar anual are obligația de a supune aceste sisteme unui proces strict de avizare/reavizare conform normelor legale.

(**Operatii ce faciliteaza utilizarea internet banking (-Ganenco Eugen)**

Utilizarea Internet Banking-ului a devenit o soluție tot mai răspândită și acceptată de publicul larg ca alternativă la metoda clasică prin prezentarea într-o sucursală 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 facile de la distanță a mai multor tipuri de operații, spre exemplu:

deschidere de conturi;

transferuri între conturi;

plăți în lei sau valută;

constituire/lichidare depozite;

schimb valutar;

ordine de plată intrabancare și interbancare;

vizualizare extrase bancare;

actualizare rapidă a datelor personale.

Pentru a beneficia de aceste servicii trebuie îndeplinite câteva cerințe minime în raport cu banca emitentă, precum:

persoana să dețină cel puțin un cont curent activ;

persoana să aibă încheiat un contract de furnizare de servicii electronice bancare.

Aceste condiții pot fi suplimentate de către orice instituție bancară din motive ce țin de propriul proces de lucru, iar ulterior beneficiarul primește numele de utilizator și codul personal de identificare/parola şi/sau orice altă dovadă similară (ex: token) a identității necesară autentificării.

Mecanisme de Securitate (Nistor Niculae Filip)

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. Pentru stabilirea numelui de utilizator au fost adoptate metode diferite, de la stabilirea unui set de cifre de pe un card al clientului, până la stabilirea acestuia de către utilizator în faza de contractare a serviciului.

Autentificarea cu token virtual – Această metodă de autentificare constă în transmiterea automată prin SMS a unui cod de acces cu perioadă limitată de valabilitate. Pentru a utiliza acest mecanism de autentificare se impune comunicarea către banca a unui număr de telefon pe care se dorește primirea mesajelor

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).

Mecanisme de Securitate (-Ganenco Eugen)

Autentificarea în doi pași - Această metodă asigură faptul ca persoana care accesează contul sa fie chiar utilizatorul legitim al acestuia. Astfel, atunci când este implementată această metodă de către furnizorul de

servicii de Internet Banking, 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).

Limitarea numărului de încercări eșuate de autentificare – Cu scopul de a limita numărul tentativelor ilicite de autentificare din partea unor persoane diferite de beneficiarii autorizați se poate stabili un număr maxim de încercări eșuate după care se va proceda la blocarea automată a contului de acces. Clienții legitimi pot apela la serviciile suport puse la dispoziție de furnizorii serviciilor și în urma unei proceduri de identificare bazată pe datele comunicate în faza de contractare și se poate debloca contul respectiv.

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).

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.

Depistarea tentativelor de frauda (-Ganenco Eugen)

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 victima 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 refuze comunicarea datelor solicitate și contactarea furnizorului de servicii în baza datelor de contact postate pe site-ul oficial, 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 clienți cu cont la banca al cărei site a fost duplicat şi care nu realizează pericolul căruia se expun.

Depistarea tentativelor de frauda (-Nistor Niculae-Filip)

Nivelul de securitate asigurat acestor servicii se bazează într-o măsură semnificativă și pe vigilenta utilizatorilor. Pentru a asigura un nivel corespunzător privind informarea și conștientizarea acestora, furnizorii de servicii de Internet Banking apelează în mod frecvent la diverse canale de comunicare cu scopul de a le aduce în atenție metode privind depistarea potențialelor tentative de fraudare. În acest ghid vor fi reluate unele dintre cele mai frecvente indicii, astfel:

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. Suplimentar, dacă sunt constatate astfel de încercări de furt de date ar trebui semnalat inclusiv furnizorul în numele căruia a fost formulată solicitarea.

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 persoane 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 tentativă 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.

Cum sa ne portejam de fraude? (-Ganenco Eugen)

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).

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 Pagină 11 din 20 credențele, fiecare utilizator nu trebuie să le divulge sau să și le noteze pe diverse medii de stocare.

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.

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.

Cum sa ne portejam de fraude? (-Nistor Niculae-Filip)

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.

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.

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.

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.

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.