GHID
privind securitatea serviciilor Internet Banking si Online Shopping

Ghid realizat de către:

în cadrul campaniei de conştientizare a riscurilor de securitate cibernetică derulată în România sub egida ECSM de către CERT-RO.

Pagină albă

CUPRINS

Pagină albă

1. Despre OTP Bank România

OTP Bank România este parte a OTP Group, unul dintre cele mai importante grupuri financiare din Europa Centrală şi de Est, cu operațiuni în țări precum Ungaria, Muntenegru, Croația, Bulgaria, Rusia, Ucraina, Slovacia, Serbia şi România.
Prezentă din 2004 pe piața bancară locală, OTP Bank România şi-a propus să devină o bancă universală puternică, care să ofere servicii complete pentru clienți persoane fizice şi companii.
În toate acțiunile pe care le-a întreprins de-a lungul celor aproape zece ani de când este prezentă pe piața locală, OTP Bank România şi-a construit, prin inovație şi competență, drumul către acest obiectiv, oferind servicii bancare atât persoanelor fizice, cât şi companiilor.

2. Scopul ghidului

Prezentul ghid oferă o înfățișare a întregului complex de măsuri pe care se bazează securitatea serviciilor Internet Banking și online shopping. Necesitatea acestui ghid a rezultat din nevoia de informare și conștientizare a publicului privind siguranța acestor servicii și ca atare, documentul surprinde cele mai răspândite practici și masuri de securitate specifice agenților economici din România și se adresează în special utilizatorilor acestor servicii pentru a le face mai bine înțelese. Totodată, prin abordarea aplicată se dorește conștientizarea acestora privind rolurile ce revin fiecărei părți implicate în realizarea unei tranzacții în condiții de securitate.

3. Internet Banking

3.1. Descrierea serviciului

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.

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.

3.2. Mecanisme de securitate

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.
Deși ponderea masurilor de natură tehnică este net superioară vom aduce în discuție toate categoriile de măsuri pentru a avea o imagine de ansamblu, astfel:

- **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 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.

- **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.

- **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.

- **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).

- **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).

- **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.

- **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.

- **Limitarea timpului de inactivitate într-o sesiune –** Pentru a elimina riscurile la care se expun utilizatorii când nu se asigură de închiderea unei sesiuni deschisă în Internet Banking, sunt prestabiliți timpi maximi de inactivitate după care se realizează o dezactivare automată a sesiunii de lucru.

- **Limitarea orară privind efectuarea tranzacțiilor cu nivel de risc ridicat** – Deși acest serviciu este disponibil în permanență (24/7), unele bănci pot prestabili o serie de ordine cu execuție imediată, iar pentru celelalte se realizează doar înregistrarea acestora urmând a fi operate în intervalul orar de lucru.

- **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.

3.3. Indicii pentru depistarea tentativelor de fraudă

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.

- **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.

- **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.

3.4. Ce trebuie să facem pentru a ne proteja

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:

- **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 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.

- **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.

- **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.

- **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.

- **Utilizarea aplicațiilor mobile doar de pe site-urile oficiale**

Pentru a evita situațiile în care clienții ar putea fi păcăliți să utilizeze aplicații pentru mobile-banking cu cod malițios inserat, toți furnizorii acestui serviciu și-au definit clar lista de site-uri 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 iniția descărcarea aplicației.

4. Cumpărăturile online

Deși nu reprezintă o practică foarte răspândita în România, cumpărăturile online încep să câștige din ce în ce mai mulți adepți.
Cumpărăturile online prezintă o serie de particularități şi avantaje față de cumpărăturile clasice, cel mai important fiind prețul mai redus al produselor, față de cel din magazinele clasice, având în vedere ca clientul nu trebuie sa suporte si costurile aferente unui magazin clasic concomitent cu reducerea cheltuielilor de deplasare la sediul magazinului.
Un alt avantaj este reprezentat de faptul că pe Internet există o varietate mult mai mare de produse, iar prețurile acestora pot fi comparate foarte ușor cu cele de pe alte site-uri, oferind posibilitatea de a alege cel mai bun preț.

4.1. Cum se efectuează o achiziție online

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.
Chiar și în condițiile în care se utilizează cel mai recent și mai sigur browser, un calculator echipat cu firewall, program antivirus și anti-spyware, este important sa se păstreze vigilența atunci când se realizează cumpărături on-line, iar pentru aceasta trebuie urmate câteva reguli elementare, astfel:

- **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.

- **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.

- **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.

- **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;

- **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.

- **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.

4.2. Înrolarea cardului de cumpărături online în sistemul 3D-Secure

3D Secure este un sistem antifraudă dezvoltat de Visa și MasterCard. Folosirea acestui sistem permite creșterea securității tranzacțiilor online, prin solicitarea unei parole la fiecare plată online. În caz de pierdere sau furt, cardul înrolat la 3D Secure, nu poate fi folosit de terțe persoane pentru cumpărături online, dacă acestea sunt realizate la comercianții înrolați în 3D Secure.
Deținătorul cardului se poate orienta pentru cumpărături numai către site-urile care afișează logo-urile Verified by Visa sau Mastercard SecureCode. În aceste magazine virtuale, utilizatorul este invitat să se autentifice la fiecare tranzacție păstrând astfel controlul asupra cumpărăturilor on-line.
Procesul de autentificare nu necesită instalarea vreunei aplicații speciale pe computerul clientului și nici nu îngreunează navigarea pe Internet și determină creșterea încrederii în aceasta modalitate de a cumpăra bunuri/servicii.
Marele dezavantaj al acestui sistem constă în faptul că nu oferă o protecție suplimentară clienților înrolați, în cazul în care cumpărăturile se realizează la comercianți ce nu sunt înrolați în acest sistem. 3D Secure ar fi cu adevărat un mijloc eficient de protecție împotriva utilizării neautorizate a cardurilor bancare daca toți comercianții din lume ar fi înrolați în acest sistem.
Funcționarea serviciului 3D Secure implică efortul comun al băncilor emitente de carduri, al băncilor cu care posesorii magazinelor virtuale au încheiat contracte de acceptare la plată a cardurilor, al comercianților respectivi și al organizațiilor internaționale de carduri. Pe măsură ce tot mai multe magazine virtuale împreună cu băncile lor și tot mai multe bănci emitente de carduri aderă la acest serviciu, crește încrederea tuturor părților implicate în tranzacțiile pe Internet și implicit volumul acestora, scăzând concomitent riscul de fraudă.

5. Ghid practic pentru clienții online

5.1. Protecția sistemelor clienților

În timp ce Internetul oferă avantaje și oportunități enorme, prezintă de asemenea diverse riscuri de securitate. În mod normal furnizorii de servicii de Internet Banking sau magazinele online nu au nicio influență asupra sistemelor utilizate de clienții lor, iar asigurarea securității la nivelul acestor echipamente le revine în întregime acestora din urmă.
Riscurile cele mai frecvente la care se expun clienții atunci când utilizează Internetul constau în accesarea, ștergerea sau modificarea datelor de către terți în timp ce sunt procesate și transmise sau obținerea de informații sub pretexte false. Aceste riscuri pot deveni efective cu ajutorul:

- Virușilor și viermilor de rețea: programe care se auto-multiplică și răspândesc sau sunt transmise prin e-mail și care pot deteriora sistemele informatice;
- Troieni: programe care, fără știința utilizatorului, pot compromite securitatea calculatoarelor (de exemplu, prin interceptarea parolelor);
- Phishing: tehnică ce constă în folosirea unui nume, site sau adresă falsă în scopuri frauduloase;
- Pharming: tehnică ce constă în redirecționarea utilizatorilor către un server fraudulos;
- Rootkit-uri: software malițios ce oferă acces neautorizat cu privilegii de administrator;
- Hacking: înglobează toate tehnicile utilizate în vederea accesării neautorizata a unui calculator prin intermediul Internetului.

Deși companiile au implementate măsuri tot mai complexe de securitate susținute prin bugete anuale semnificative în vederea asigurării protecției propriilor sisteme, pentru a avea un mediu virtual securizat prin care să se deruleze operațiunile oferite prin aceste servicii online se impune o implicare inclusiv a clienților prin protejarea propriilor sisteme. Suplimentar măsurilor și recomandărilor enunțate în capitolul anterior de data aceasta ne referim la cele tehnice, după cum urmează:

- **Utilizarea programelor anti-virus și anti-spyware**

Astfel de programe protejează calculatoarele să nu se infecteze cu aplicațiile malițioase prezentate anterior. Datorită sofisticării permanente a acestor atacuri este esențial să fie asigurată periodic actualizarea semnăturilor antivirus pentru a avea o protecție eficientă. Un astfel de program se poate cumpăra sau descarcă gratuit de pe Internet, sub restricția folosirii în scop personal.
Recomandăm a nu se folosi mai mulți antiviruși odată deoarece securitatea nu este dublată și în plus programele s-ar putea încurca unul pe altul. Trebuie avut in vedere utilizarea unui produs antivirus funcțional deoarece multe calculatoare sunt cumpărate cu un antivirus „trial" preinstalat, ce are o durată limitată de funcționare, iar după expirare necesită cumpărarea unei licențe pentru acel produs. În acest caz este indicată achiziționarea

licenței, dar dacă acest lucru nu este posibil recomandăm folosirea unei variante gratuite în locul uneia nefuncțională.

- **Utilizarea programelor de tip firewall**

Aceste aplicații au capacitatea de a depista, investiga și bloca încercările de transmitere a datelor furate din sistem sau a conectărilor neautorizate la propriul sistem. Totodată, oferă posibilitatea selectării programelor și aplicațiilor ce se pot conecta la Internet.

- **Instalarea patch-urilor sistemului de operare și ale browser-ului**

Se recomandă utilizarea unei versiuni cât mai recente a sistemului de operare ales și configurarea opțiunilor de actualizare astfel încât să fie instalate automat update-urile de securitate critice, în cel mai scurt timp posibil. Lipsa acestor patch-uri poate lăsa deschise unele breșe de securitate la nivelul sistemului clientului și/sau pot crea probleme de compatibilitate cu aplicațiile de Internet Banking sau online shopping.

- **Verificarea compatibilității browser-ului folosit**

Pentru navigarea pe Internet se recomandă folosirea unui browser cât mai modern și actualizat întrucât, din punct de vedere a securității pe care o oferă, cele mai recente înglobează îmbunătățiri semnificative.
Trebuie avut în vedere faptul că pot exista diferențe de compatibilitate între aplicațiile puse la dispoziție de furnizorul de servicii de Internet Banking și brawserul utilizat pe calculatorul sau mobilul clientului.
De regulă aceste aspecte sunt testate, identificate și publicate de către furnizor pe site-ul oficial. Pentru a evita astfel de neplăceri se recomandă să fie consultate aceste date și instalat un alt browser dacă este cazul. Totodată, este indicată configurarea browser-ului astfel încât să accepte notificările de securitate emise de acesta, deoarece aplicațiile de tip browser cele mai cunoscute emit avertizări în cazul în care este vizitat un site care a fost raportat ca fiind malițios.

- **Protejarea contului de acces la sistem sau mobil printr-o parolă complexă**

Pentru a evita accesarea neautorizată a propriului sistem de calcul sau dispozitiv mobil, atât fizic cât și de la distanță, se recomandă protejarea printr-o parolă de acces. Protecția oferită de aceasta este proporțională cu lungimea, complexitatea și frecvența de schimbare. Mai mult, nu se recomandă utilizarea aceleiași parole pentru accesarea mai multor resurse informatice diferite (ex: sistem de operare, e-mail, Internet Banking etc).
Simultan, este necesară dezactivarea tuturor conturilor neutilizate ale sistemului de operare, mai ales pe acelea care nu solicita parolă de acces (de exemplu, conturile „Guest”), și configurarea screensaver-ului astfel încât să solicite reautentificarea prin parolă la deblocarea ecranului. Acest lucru va preveni utilizarea calculatorului personal de către o persoană neautorizată atunci când nu este supravegheat, mai ales daca este utilizat un sistem informatic la care pot avea acces și alte persoane.

- **Activarea opțiunii „ștergere de la distanță” pentru dispozitivele mobile**

În cazul dispozitivelor mobile, care sunt mai frecvent supuse riscurilor de pierdere sau furt, se recomandă utilizarea opțiunii de ”ștergere de la distanță” a datelor de pe acestea daca o persoană neautorizată încearcă să obțină acces la datele stocate.

- **Utilizarea exclusivă a aplicațiilor software licențiate**

Din punct de vedere al securității datelor, aplicațiile software utilizate fără a licență pot prezenta o serie de vulnerabilități sau breșe de securitate semnificative. Din acest motiv, se recomandă utilizarea doar a aplicațiilor licențiate si procurate din surse sigure pentru a nu deveni victima unor persoane rău-intenționate.

- **Utilizarea doar a rețelelor wireless securizate**

Pentru limitarea accesului neautorizat la astfel de dispozitive se recomandă în primul rând setarea unei parole de acces pentru rețeaua wireless personală și daca este posibil, evitarea utilizării protocolului de securizare WEP, luând în considerare alternativele WPA sau WPA2 cu PSK. De asemenea este foarte important să se evite accesarea contului bancar sau realizarea de cumpărături on-line prin conexiuni la rețele wireless publice.

În dorința de a veni în sprijinul utilizatorilor propriilor servicii, unii furnizori de Internet Banking au mers mai departe și oferă, în mod gratuit pe baza unor parteneriate cu firme importante în domeniul securității informatice, aplicații/soluții de securitate destinate protejării sistemelor de calcul ale acestora.

5.2. Protejarea datelor personale

Datele personale reprezintă acele informații cu privire la o persoană fizică identificată sau identificabilă. Cele mai cunoscute astfel de informații sunt cele ce țin de nume, prenume, data nașterii, codul numeric personal, adresa, numărul de telefon, contul bancar etc., în general, orice informație care poate duce la identificarea unei persoane.
Când vine vorba despre tranzacționarea on-line, în condiții de siguranță, prevenirea este mult mai importantă și mai utilă decât combaterea. Cumpărătorii trebuie să rămână tot timpul vigilenți și precauți în divulgarea informațiilor personale atât pe site-urile de socializare cat și prin răspuns la mesajele e-mail nesolicitate.
Trebuie avut în vedere faptul ca hoții de identitate au nevoie doar de câteva informații cheie, care puse cap la cap le oferă accesul acestora la conturile dumneavoastră. Protejarea împotriva acestor amenințări nu este atât de dificilă precum pare. Sunt doar câteva aspecte ce trebuie avute în vedere de fiecare cumpărător înainte de a face tranzacții on-line:

- Este foarte important să se verifice politica de confidențialitate a comerciantului privind datele personale ale clienților, dobândite în timpul procesului de tranzacționare. Trebuie înțeles modul în care se realizează administrarea acestor

date, iar în cazul în care nu se consideră politica aplicată ca fiind acceptabilă, se poate avea în vedere opțiunea privind adresarea către un alt comerciant;

- Indiferent de situație, nu se recomandă divulgarea parolelor personale, iar pentru evitarea compromiterii acestora este indicată schimbarea periodica a acestora;
- Pentru selectarea unei parole complexe care poate oferi un grad mai ridicat de protecție, se recomandă folosirea unei combinații de litere mari, litere mici, cifre și caractere speciale, astfel încât aceasta să nu fie ușor de ghicit. Cu cât aceasta este mai lungă și mai complexă, cu atât este mai greu de spart sau ghicit;
- Daca există posibilitatea, se recomandă utilizarea unei metode de autentificare cat mai puternica - „strong authentication". O persoană rău-intenționată poate avea șanse să ghicească numele de utilizator și parola de acces dar ii este foarte greu sa intre în posesia dispozitivului (token, smartcard sau telefon mobil) care generează codul de securitate „One Time Password - OTP" necesar realizării unei autentificări puternice (cu doi factori);
- Este necesară verificarea cu atenție a setărilor de confidențialitate aferente conturilor de pe site-urile de socializare și se recomandă configurarea de la început a acestora pentru a oferi maximum de securitate, urmând a le diminua restricțiile în cazul în care sunt întâmpinate dificultăți în exploatare;
- Se recomandă vigilență în selectarea persoanelor de pe rețelele de socializare deoarece oricine poate crea un cont cu orice nume dorește și în unele situații nu reflectă realitatea;
- Înainte de a publica informații personale pe diverse site-uri care în general sunt utilizate de companii sau organizații pentru a verifica identitatea utilizatorilor (data și locul nașterii, numele mamei înainte de căsătorie etc) se recomandă ca decizia de publicare să fie bine justificată;
- Când se solicită completarea formularelor on-line pe anumite site-uri, trebuie avut în vedere faptul că nu toate câmpurile sunt obligatorii și recomandăm completarea doar a acelor informații fără de care nu se poate trece mai departe în aplicație;
- Când se solicită selectarea întrebărilor și precizarea răspunsurilor proprii ca metodă alternativă de autentificare în cazul uitării parolei, mai ales pe site-uri care nu sunt foarte importante pentru dumneavoastră, trebuie avut în vedere faptul că nu este necesar ca acestea să fie adevărate și în nici un caz nu este obligatorie selectarea aceluiași set de întrebări și răspunsuri folosite pe site-urile importante sau la serviciu;
- Ocazional, se recomandă utilizarea motoarelor de căutare pentru a identifica ce fel de informații personale sunt disponibile in Internet, iar în cazul în care sunt identificate și date pentru care nu se mai dorește publicarea, vă recomandăm să contactați proprietarii site-urilor respective pentru a le șterge;
- În funcție de posibilitățile proprii se recomandă criptarea tuturor mediilor de stocare (HDD, Memory Stick etc.) aflate în posesia dumneavoastră și în special cele pe care sunt stocate informații personale sensibile (fotografii, factui, documente scanate, etc.);
- Recomandăm distrugerea tuturor mediilor de stocare la care urmează a se renunța, mai ales dacă au conținut informații personale (HDD-uri, CD-uri, Memory Stick-uri, hârtii etc) deoarece acestea sunt adesea reutilizate iar informațiile pot fi recuperate cu ușurință.

Pe site-urile multor comercianți există opțiunea salvării datelor personale astfel încât să fie disponibile și mai târziu pentru cazurile în care se dorește realizarea altor tranzacții. Comercianții permit de obicei stocarea datelor referitoare la nume, adresă de livrare și facturare, preferințe de plată și detalii financiare cum ar fi numărul cardului de credit sau informații legate de contul bancar. Stocând astfel de informații pe site-urile comercianților apar riscuri suplimentare deoarece:

- Prin creșterea numărului locurilor în care sunt stocate informații personale crește proporțional numărul posibilităților ca acestea sa fie compromise.
- Prin stocarea datelor pe o perioada nedeterminată de către comercianți se extinde perioada în care poate apare posibilitatea compromiterii acestora. Chiar și prin implementarea unei politici de securitate destul de sofisticată, în timp aceștia pot deveni țintele unor atacuri, iar datele clienților vor fi supuse riscurilor.

6. BIBLIOGRAFIE

1. Regulament nr. 6 din 11.oct.2006, publicat în Monitorul Oficial Partea I 927 15.noi.2006, privind emiterea şi utilizarea instrumentelor de plată electronică şi relațiile dintre participanții la tranzacțiile cu aceste instrumente.
2. www.enisa.europa.eu
3. www.financiarul.ro