CEC Bank

Protectia individuala in accesarea serviciilor de tip Internet Banking

SUMAR

Prin respectarea anumitor reguli, chiar si un nespecialist se poate proteja pe parcursul utilizarii de servicii Internet Banking.

I. Securitatea online in general

Pentru a garanta confidentialitatea informatiilor introduse prin intermediul sesiunilor Internet, CEConline utilizeaza un sistem de criptare SSL avand dimensiunea cheii de criptare reprezentata pe 128 biti.

Internetul deschide noi oportunitati, dar ca sa iti protejezi calculatorul, trebuie sa te aperi de hackeri. Cu totii am auzit de fraudele online; nu trebuie sa folosesti cardul la bancomatele “fantoma”. La fel se procedeaza si pe internet: trebuie sa iei cateva masuri elementare desecuritate si noi iti spunem cum sa faci acest lucru.

Te asiguram ca CEConline respecta toate masurile de securitate, insa nu avem cum sa garantam pentru utilizarea calculatorului tau de acasa; acesta este in intregime responsabilitatea ta.

Foarte important cand te conectezi la CEConline:

- Sa accesezi serviciul CEConline direct din cadrul browser-ului Internet. Sa introduci de la tastatura adresa URL: https://www.home.ceconline.ro sau adresa WEB a bancii www.cec.ro.
- Verifica intotdeauna certificatul digital de pe serverul la care te conectezi (dublu click pe lacatelul din dreapta sus). In plus, verifica intotdeauna, ca esti pe o conexiune sigura respectiv https, si nu http.
- Cu un “ click” de mouse pe simbolul certificatului digital (logo), se poate verifica in timp real autenticitatea paginii afisate;
- Sa NU salvezi PIN-ul, numele de utilizator sau alte informatii legate de securitatea serviciului CEConline in memoria calculatorului;
- Sa NU divulgi nimanui PIN-ul si informatiile legate de securitatea conturilor tale; banca nu te va contacta niciodata sa-ti solicite aceste informatii; daca esti contactat prin e-mail sau telefon pentru a ti se cere aceste informatii este cu siguranta frauda!
- Sa schimbi IMEDIAT PIN-ul dispozitivului digipass daca banuiesti ca le cunoaste si alta persoana;
- Sa nu folosesti cuvinte uzuale pentru definirea numelui de utilizator (exemplu numele tau sau al unor persoane apropiate, date de nastere, numele unui animal de companie);
- Nu utiliza in mod frecvent calculatoarele din locuri publice precum Internet café deoarece nu iti ofera suficienta securitate;
- Nu lasa calculatorul nesupravegheat si conectat la pagina ce deserveste serviciul CEConline, mai ales daca utilizezi un calculator public;
- Verifica in mod regulat conturile tale, precum si mesajele primite de la banca prin intermediul aplicatiei I.B. aflate in meniul MESAJE->MESAJE PRIMITE
- In cazul in care observi tranzactii de care nu-ti amintesti, contacteaza imediat serviciul suport clienti CEC Bank S.A. Nu amana aceasta decizie, pentru ca exista termene limita pentru depunerea contestatiilor impuse de reglementari internationale. Dupa incheierea acestor intervale de timp, personalul CEC Bank S.A. cu toata bunavointa, nu mai poate face nimic pentru recuperarea prejudiciului.

II. Protejeaza-ti calculatorul!

Ce poti sa faci pentru a proteja calculatorul / laptopul personal?

- Foloseste un firewall;
- Foloseste un anti-virus;
- Blocheaza programele spy;
- Evita fraudele online.

Foloseste un firewall!

1. Ce este un firewall?

Este un dispozitiv sau un pachet program care blocheaza accesele nedorite initiate din Internet catre calculatorul tau.

2. Cum functioneaza?

In general, daca nu sunteti foarte familiarizat cu utilizarea lui, valorile implicite furnizate de producator sunt suficiente pentru o protectie eficienta. Configuratii avansate permit modificarea comportamentului implicit, permitand specificarea programelor si aplicatiilor ce se pot conecta la Internet sau care pot primi solicitari dinspre Internet. De exemplu poti sa permiti accesul programului autorizat Outlook Express, dar poti restrictiona foarte usor accesul unui program suspect. In general, sistemele de operare moderne au in cadrul pachetului de instalare inclusa si existenta unui program de tip firewall.

3. Am nevoie de un firewall?

Da! Toti ar trebui sa foloseasca un firewall. Acesta identifica si interzice eventualele atacuri dinspre Internet si blocheaza accesul programelor neautorizate.

4. Nu sunt expert in calculatoare, chiar pot invata sa-l utilizez?

Da. Odata instalat, acest program nu necesita prea multa atentie iar majoritatea firewall-urilor sunt livrate cu un set de instructiuni de urmat “pas cu pas” (poti utiliza ZoneAlarm Internet Security Suite sau Norton Internet Security). In lipsa unor programe specializate este necesara utilizarea firewall-ului livrat odata cu sistemul Dvs. de operare.

Foloseste un program anti-virus!

1. Am nevoie de un asemenea program?

Da! De fiecare data cand te conectezi la internet, te expui pericolului virusilor. Ne referim la virusi informatici care in fapt sunt produse software (adeseori doar cateva rutine program), create de utilizatori din Internet cu diverse scopuri (furt de identitate, propaganda, comercial etc.). Ei te 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 dispozitie chiar de catre utilizatori.

2. Am program anti-virus instalat; Acum sunt protejat?

Instalarea unui astfel de program nu este suficienta. Un lucru esential in exploatarea programelor anti-virus, este existenta unei licente de actualizare automata a listei de semnaturi (lista de virusi cunoscuti). In conditiile in care in fiecare luna apar mii de virusi noi, furnizorii de programe anti-virus, cerceteaza si actualizeaza in permanenta programul pe baza noilor tipuri de amenintari aparute.

3. Ce fac virusii?

Unii sunt doar enervanti, dar majoritatea virusilor sunt distrugatori. De exemplu, unii virusi pot cauza disfunctionalitati ale calculatorului, se pot multiplica si raspandi la alte calculatoare sau pot permite accesul hackerilor (persoane rau-intentionate plasate in Internet) la fisierele si informatiile personale de pe PC-ul tau.

4.Este greu sa invat cum se utilizeaza?

Nu. Majoritatea programelor anti-virus se livreaza impreuna cu un manual, poti apela la paginaInternet de suport sau la ajutorul unui expert pus la dispozitie de furnizor.

5.Trebuie sa platesc pentru un produs program anti-virus?

Poti cumpara un program antivirus sau poti sa-l descarci gratuit de pe Internet daca il folosesti in scop personal. Este importanta totusi alegerea programului anti-virus, de performantele acestuia depinzand siguranta si stabilitatea sistemului tau de calcul. Este recomandabil ca inainte de a cumpara sau instala un program anti-virus sa apelezi la un specialist sau chiar la o campanie de informare personala prin intermediul motoarelor de cautare (Google, Live Search, Yahoo, Lycos, Ask, About, etc), unde se regasesc forumuri de discutii pe Internet cu clasamente si argumente pertinente in favoarea unuia sau altuia dintre acest gen de programe.

Nu folosi mai multi antivirusi odata; securitatea nu este dublata si in plus exista posibilitatea ca programele sa nu fie compatibile intre ele afectandu-si reciproc performantele.

Utilizeaza programe anti-spyware, anti-adware si anti-malware!

1. Ce este un program spy?

Spyware este denumirea data unei categorii de programe de calculator, de obicei atasat unor programe gratuite (jocuri gratuite, programe de schimbat fisiere, programe de „chat” pornografic, etc.) care este folosit pentru a capta date de marketing (prin a analiza ce situri cauta utilizatorul, de exemplu: moda, pantofi, cluburi de tenis, s.a.m.d.) si de a transmite eventual acelui utilizator reclame conform datelor de marketing extrase de spyware.

Adware este varianta de spyware care nu extrage date de marketing, ci doar transmite reclame.

Malware este considerat orice program (avand sensul oricarui set de instructiuni) care are ca efect modificarea parametrilor de functionare al unui calculator fara permisiunea utilizatorului.

Este un termen generic care include dar nu se limiteaza la: virusi informatici, viermi informatici, cai troieni, spyware, bombe logice etc.

Exista programe de spyware care modifica modul de comportare a unor motoare de cautare (Google, Yahoo, MSN, etc.) pentru a trimite utilizatorul la situri (scumpe) care platesc comisioane producatorului de spyware.

Unele programe spyware utilizeaza resursele calculatorului dumneavoastra ca parte integranta a unui sistem de calcul distribuit (de exemplu, operatiuni contabile pentru firme din India). SETI@home face acelasi lucru dar nu este considerat spyware, deoarece face acest lucru numai cu consimtamantul activ si constient al utilizatorului. In aceste situatii, calculatorul dumneavoastra poate deveni lent in exploatare, lucrand preponderent pentru altcineva; Exista situatii in care chiar si conexiunea la internet se blocheaza datorita traficului foarte ridicat (ca efect neintentionat).

In general, la stergerea programului gratuit care a instalat spyware, spywareul ramane active in continuare. Exista o sumedenie de programe anti-spyware, unele dintre ele fiind false anti-spyware care ele insele contin spyware.

Aceste programe sunt in general ascunse in calculatorul tau, pot invada toate fisierele tale personale, colecta informatii despre tine raspandindu-le in Internet, fara acceptul tau. Uneori poate sa modifice comportamentul web-browser-ului si sa afiseze reclame pop-up nedorite.

2. Esta daunator?

Da. In cel mai fericit caz poate sa-ti incetineasca calculatorul si conexiunea Internet, dar in cel mai rau caz poate sa copieze informatii confidentiale precum numarul si PIN-ul cardului tau, codul sau parola utilizate in cadrul autentificarilor electronice si sa le puna la dispozitia hacker-ilor.

3. Este o incalcare a intimitatii?

Da. Uneori este instalat in paralel cu un alt program (utilizat de obicei pentru a descarca muzica de pe Internet) sau se poate instala fara permisiune. Este greu de inlaturat fara un program anti-spy.

4. Cum imi dau seama daca PC-ul meu este afectat de programele spy?

Simptomele tipice sunt incetinirea vitezei calculatorului si a conexiunii Internet, schimbari neasteptate ale web-browser-ului si nedoritele reclame pop-up. Unele programe spy pot ramane nedetectate cat timp iti copiaza informatiile, asa incat pentru a fi foarte sigur trebuie sa iti instalezi un program anti-spy si sa scanezi calculatorul cu regularitate (poti utiliza programul AdAware).

Evita fraudele online!

1. Ce inseamna “phishing”?

“Phishing”, termen derivat din engleza, se refera la notiunea de fraudare a informatiilor originale puse la dispozitia utilizatorilor Internet de catre firme sau societati cu de altfel buna reputatie. Fraudarea se realizeaza prin copierea (“clonarea”) pana la nivel de detaliu a elementelor vizuale si auditive din cadrul paginilor de WEB originale, pe server-e aflate in Internet, dar sub controlul unor persoane rau intentionate (hackers).

Atacurile de tip “phishing” NU sunt indreptate asupra firmelor sau societatilor al caror format de pagina Internet si servicii sunt copiate. Pierderile directe la nivelul acestor societati pot fi doar de natura reputationala. Atacul este indreptat asupra CLIENTILOR acestor societati, cu scopul de a-i determina pe acestia sa furnizeze informatii legate de autentificarea proprie. Pe baza acestor informatii, hack-erii, vor incerca ulterior accesarea adevaratelor servicii puse la dispozitie de societatile in cauza cu scopul obtinerii de avantaje materiale.

Prima etapa din scenariul atacurilor de tip “phishing” o constituie de obicei campanii de transmitere masiva a unor mesaje E-mail sau SMS (mass mail) ca un presupus mesaj de la societatea cu care clientul se presupune ca are o relatie contractuala sau de parteneriat. In cele mai multe din cazuri, cei care initiaza acest atac, NU STIU care sunt clientii care lucreaza cu o anumita societate, dar bazandu-se pe numarul imens de mesaje transmise va exista si un segment tinta.

In general, in cadrul acestor mesaje (care par sosite din partea societatii cu care clientul colaboreaza), se solicita (in scop de verificare, etc.) furnizarea de informatii legate de autentificarea individuala (nume utilizator parole, etc.).

ACEST GEN DE SOLICITARI NU VOR FI NICIODATA EMISE DE CATRE ADEVARATELE FIRME, COMPANII, SOCIETATI SAU INSTITUTII CARE PRESTEAZA ASTFEL DE SERVICII ON-LINE.

2. De unde au adresa mea de e-mail?
Liste cu adrese de e-mail circula pe Internet si sunt schimbate in mod frecvent intre hackeri.

3. De unde stiu ei cu ce banca lucrez?
Nu stiu, dar daca trimit multe mesaje, cu siguranta gasesc cateva persoane care au un sistem precar de securitate sau nu realizeaza pericolul caruia se expun.

4. Ce fac daca primesc un e-mail “suspect”?
Cel mai bine este sa-l stergi direct, mai ales daca are link-uri sau fisiere atasate. Nu descarca programe de pe Internet daca sursa nu este de incredere.

5. Calculatorul meu functioneaza; de ce am nevoie sa-l protejez?
Hackerii cauta noi modalitati de a ataca calculatoarele. Cand este descoperita o noua vulnerabilitate, companiile de software introduc pe piata versiuni noi care sa inlature amenintarea (“patch”).

6. Este riscant daca nu imi protejez calculatorul?
Unele programe vizeaza aspecte esentiale; daca nu le ai, calculatorul tau este expus hackerilor, iar acesta este un risc pe care nu ti-l poti asuma.

7. De ce sa ma protejez daca antivirusul meu este actualizat?
Poate ca asa este, insa daca te protejezi poti obtine performante mai bune ale calculatorului si o imbunatatire a securitatii informatiilor. De asemenea, iti protejezi calculatorul impotriva virusilor care nu sunt detectati cu programele anti-virus pe care le ai instalate.

8. Cat de des trebuie sa verific aceasta protectie?

Este recomandata utilizarea unor programe care verifica la intervale regulate (zeci de minute) existenta unor eventuale actualizari pe site-ul furnizorului. Este importanta verificarea functionarii actualizarii automate, existand rare ocazii in care tocmai firewall-ul instalat sa blocheze accesul catre site-ul furnizorului in scopul aducerii celor mai noi versiuni de program.

III. Protejeaza-ti telefonul / tableta

Multi dintre noi folosim, in prezent, dispozitive mobile inteligente: telefoane de tip smartphone si tablete, inclusiv pentru accesul la serviciile de tip internet banking.

De aceea, devine important ca aceste dispozitive sa fie protejate, la randul lor, impotriva accesului neautorizat.

Foloseste un PIN / o alta metoda de blocare

Blocarea telefonului / tabletei este extrem de importanta pentru impiedicarea accesului neautorizat, in situatii in care telefonul este pierdut, furat sau pur si simplu lasat undeva, nesupravegheat.

Protejarea datelor senzitive

In prezent, telefoanele / tabletele sunt adevarate mini-computere. Este recomandat sa eviti stocarea de fisiere importante in memoria telefonului, sau informatii importante precum parole, detalii de conectare in diverse aplicatii (inclusiv internet banking), numere de cont sau orice alte informatii de acest tip.

Pentru protectie, se pot folosi aplicatii de criptare, care se pot downloada din App Store / Google Play. In plus, specialistii recomanda stocarea fisierelor la distanta, pe servere online securizate, unde credentialele de acces pot fi schimbate, in eventualitatea pierderii / furtului telefonului.

Atentie la retelele wireless

Retelele wireless si hotspoturile din spatii publice sunt unul din riscurile mari prin care dispozitivele mobile pot fi atacate (atacul de tip “evil twin”). Intr-o astfel de situatie, de exemplu, este posibil sa apara cerinte de furnizare de date – orice cerinte de acest tip trebuie, categoric, ignorate. O metoda foarte buna de protectie, atunci cand folosim telefonul / tablet in afara casei (unde presupunem ca accesul wifi se face printr-un echipament de tip router, cu acces securizat) este sa dezactivam modulul wifi si sa folosim, in masura in care este posibil, doar datele mobile.

Bluetooth

Conexiunile de tip Bluetooth sunt, la randul lor, un punct de vulnerabilitate utilizat de atacatori. Pentru a diminua riscul de atac si pentru a creste protectia, este recomandat ca interfata Bluetooth sa fie dezactivata, daca nu este folosita. De asemenea, la activare, este important sa setam ca

implicit modul “non-discoverable” – ceea ce inseamna ca alti utilizatori din proximitate nu vor detecta telefonul / tableta.

Atentie mare la aplicatiile folosite

Se recomanda atentie sporita atunci cand instalam aplicatii pe telefon / tableta. Este important sa ne asiguram ca, cerintele de instalare sunt normale si ca nu se solicita accesul la diferitele functionalitati ale telefonului, atat timp cat acestea nu au legatura directa cu aplicatia respectiva. De asemenea, este recomandata instalarea de aplicatii doar prin canalele oficiale (App Store / Google Play), orice alte surse reprezentand un risc de securitate.

In plus, permisiunile pe care aplicatiile instalate le au, trebuie revizuite in mod periodic si pastrate doar acele elemente fara de care aplicatia nu poate fi utilizata. De exemplu, daca nu este o aplicatie prin care se pot executa apeluri audio, este lipsit de sens si chiar riscant sa fie permis accesul la microfon.

Software de protectie

Si in cazul dispozitivelor mobile exista aplicatii software de securitate (de tip antivirus, dar nu numai), care ajuta si protejeaza impotriva potentialelor pericole din mediul online. Aceste aplicatii protejeaza, de regula, impotriva unui vulnerabilitati cunoscute si adreseaza in mod particular situatii comune, care se pot intampla oricui.

Spre exemplu:

- Controlul telefonului de la distanta si localizare GPS, in cazul pierderii / furtului
- Blocarea de la distanta a telefonului (solicitare parola / cod de acces, in cazul in care se doreste accesarea acestuia)
- In cazuri extreme, stergerea datelor senzitive, de la distanta.

Actualizarea sistemelor de operare

Multe update-uri ale sistemelor de operare (IOS si Android) contin exact solutii pentru anumite elemente de vulnerabilitate si modalitati sporite de protectie, astfel incat actualizarile reprezinta o modalitate esentiala prin care protejam dispozitivele mobile.

ATENTIE!

CEC Bank S.A. nu-ti va solicita niciodata divulgarea PIN-ului si a codului furnizat de dispozitivul digipass.

CEC Bank S.A. nu-ti va trimite niciodata mesaje de orice natura prin care-ti solicita divulgarea sau modificarea unor elemente de identificare, sa accesezi adrese URL sau link-uri pentru a te conecta la CEConline.

Daca totusi te confrunti cu un asemenea caz te rugam sa contactezi de indata serviciul suport clienti CEC Bank S.A.:

Adresa	Calea Victoriei nr. 11-13, Sector 3, Bucuresti
Telefon	+40212025050
Telverde (apel gratuit in reteaua Telekom)	0800800848
Email:	suport@ceconline.ro