GHID PRIVIND SECURITATEA PLĂŢILOR PE INTERNET

ALPHA BANK ROMANIA S.A.

Alpha Bank Romania SA

Cuprins

I. Ameninţările informatice

CE ESTE MALWARE?
Malware (prescurtarea de la "malicious software" în limba engleză) este un termen generic şi se referă la orice software rău-intenţionat (maliţios) care a fost creat cu scopul de a rula în mod neautorizat şi ascuns faţă de utilizatorul computerului.

CE ESTE UN TROIAN?
Un troian este un program maliţios (malware) care este adesea prezentat utilizatorului ca un program legitim.
Utilizatorul fiind păcălit, adesea prin inginerie socială, să descarce şi execute aplicaţia maliţioasă pe computerul său. Odată activat troianul permite atacatorului să controleze şi să monitorizeze calculatorul victimei sau să acceseze informaţii sensibile (parole, poze, etc) stocate pe acesta.

CE ESTE UN "KEYLOGGER"?
Înregistratoarele de taste, keyloggers în limba engleză, sunt programe destinate înregistrării tastelor apăsate de către utilizator şi folosite, de pildă în troieni, pentru a obţine informaţii sensibile ca parole, coduri PIN, numere de carduri, etc. Aceste programe rulează în background şi sunt invizibile pentru un utilizator obişnuit. Ele pot fi instalate pe un calculator în urma unui atac de tip "drive-by-download" sau pot fi instalate împreună cu programele piratate.

CE ESTE UN ADWARE?
Adware, cunoscut si sub numele de software de publicitate, generează venituri pentru dezvoltatorii săi prin generarea automată de anunțuri pe ecran, de obicei, într-un browser web. Adware este de obicei creat pentru computere, dar poate fi găsit, de asemenea, pe dispozitive mobile. Unele forme de adware sunt extrem de manipulatoare și deschide o ușă pentru programe rău intenționate.

CE ESTE UN ATAC DE TIP "DRIVE-BY DOWNLOAD"?
Un atac de tip "drive-by-download" se referă la **descărcarea neintentionata** (fără ştiinţa utilizatorului) şi fără ca acesta să observe, pe un computer sau terminalul mobil, a unor programe maliţioase. De obicei un astfel de atac reuşeşte datorită lipsei actualizărilor de securitate (ex. actualizări ale browserului sau ale sistemului de operare).

CE ESTE UN ATAC DE TIP "MAN-IN-THE-MIDDLE"?
Un atac de tip "man-in-the-middle" (omul de la mijloc), este un atac sofisticat în care atacatorul se interpune ca "stație de tranzit" în comunicația dintre două sisteme, utilizatorul legitim având impresia că cele două sisteme discuta direct, când de fapt, în realitate, atacatorul controlează toată conversația, fiind capabil să intercepteze şi modifice mesajele schimbate de cele două părţi. Folosind un astfel de atac atacatorul ar putea modifica date ale unor tranzacţii financiare.

CE ESTE UN ATAC DE TIP "MAN-IN-THE-BROWSER"?
Un atac de tip “man-in-the-browser” este un tip de atac “man-in-the-middle” prin care un troian de tip proxy infectează un browser web folosindu-se de vulnerabilitățile de securitate ale browser-ului. Troianul modifică pagini web, elemente ale unei tranzacții sau chiar întreaga tranzacție, toate aceste acţiuni având loc “în background”, fără ca utilizatorul să observe. Un astfel de atac ar putea fi contracarat prin utilizarea unei metode de verificare a tranzacției care să folosească un canal de comunicare diferit (ex. SMS) de cel care a fost utilizat pentru iniţierea tranzacţiei. (ex. web).

II. Ameninţări de tip inginerie socială

Ingineria socială, **social engineering** în limba engleză, este arta de a manipula, minţi sau influenţa pe ceilalţi ca să realizeze/nu realizeze anumite acţiuni ori să divulge informaţii confidenţiale.
Este oarecum similar cu un truc de câştigarea încrederii sau cu o simplă fraudă. Acest termen se aplică de obicei celor care utilizează şiretlicuri pentru a culege informaţii sau pentru a accesa sistemele informatice, în unele cazuri atacatorul nu vine niciodată faţă-în-faţă cu victima.

În continuare prezentăm cele mai cunoscute tipuri de inginerie socială.

CE ÎNSEAMNĂ "PHISHING"/ “SMSishing?
Phishing-ul se referă la mesaje false care induc în eroare destinatarii, pentru a-și divulga date personale, financiare ori de securitate. Aceste email-uri: pot arăta identic cu acelea pe care le primiți de la bancă, imită logo-ul și designul mesajelor reale, solicită descărcarea unui atașament sau deschiderea unui link, utilizează un limbaj care sugerează urgența.

Smishing (combinație de cuvinte dintre SMS și Phishing) este încercarea de inducere în eroare prin mesaje text, pentru obținerea de date personale, bancare ori de securitate. Prin mesajul text (SMS), autorii, de obicei, solicită apelarea unui număr de telefon sau accesarea unui link prin care”îți verifici, actualizezi, reactivezi” contul. Dar, în realitate sunteți direcționat către un website fals sau un operator-complice, pretins reprezentant al băncii.

Un exemplu de phishing: primiţi un email în care aţi fost informat că aţi câşitgat o excursie în străinătate iar tot ce trebuie să faceţi pentru a primi voucherul de călătorie este să introduceţi (pe un site asemenator cu cel al băncii) următoarele informaţii pentru a confirma identitatea: numele, adresa şi datele cardului dvs.

Un exemplu de smsihing: primiţi un mesaj SMS de la un număr necunoscut care pretinde a fi banca dvs. şi care va invită să descărcaţi o nouă versiune a aplicaţiei de mobile banking.
ATENŢIE! Cel mai probabil în acest caz veţi descărca şi rula un malware care va da atacatorului posibilitatea să controleze şi să monitorizeze telefonul dvs. mobil, inclusiv să poată captura credenţialele de acces pentru aplicaţia legitimă de online banking.

DE UNDE AU ADRESA MEA DE E-MAIL SAU NUMĂRUL MEU DE TELEFON?
De cele mai multe ori aceste informaţii sunt culese din surse publice (ex. site-uri de anunţuri) dar şi din bazele de date făcute publice în urma unor breşe de securitate ale diferitelor servicii online unde aţi furnizat datele respective de contact. Aceste informaţii sunt schimbate sau vandute în mod frecvent de atacatori pentru a fi folosite în atacuri de tip “phishing”.

DE UNDE ȘTIU EI CU CE BANCĂ LUCREZ?
Atactorii nu știu acest lucru, dar dacă trimit multe mesaje cu siguranță nimeresc şi persoane care lucrează cu banca prezentată în mesajul de phishing. Dacă personele nu sunt atente acestea furnizează atacatorilor informaţiile pe care aceştia le caută.

CE FAC DACĂ PRIMESC UN E-MAIL SAU UN SMS "SUSPICIOS"?
Cel mai bine este să ștergeți direct mesajul respectiv, mai ales dacă conţine link-uri sau atașamente. De asemenea, ori de câte ori aveţi suspiciuni cu privire la originea unui mesaj (email sau sms) este bine să contactaţi banca pe unul din canale de suport oficiale (ex. telefonul sau email-ul menţionat pe websiteul public).

CE ESTE VISHING?
Vishing (combinație de cuvinte între”Phishing” și ”voce”) este o fraudă în care autorii, apelând telefonic victima și folosind diverse pretexte, o conving să divulge date personale și/sau financiare ori să le transfere bani.

Un exemplu de vishing: primiţi un telefon de la o persoană care pretinde a fi un angajat al băncii care doreşte să verifice numărul cardului, codul PIN sau codul de securitate al cardului deoarece a fost iniţiată o alertă de securitate.

CE ESTE “CEO FRAUD”?
Un alt tip atac încadrat în categoria Inginerie Socială este “CEO Fraud” sau “Business Email Compromise (BEC)”. Atacatorul reuşeşte să compromită serverul de email al unei companii sau să creeze o căsuţă de email asemănătoare cu cea oficială a companiei vizate. Eventual schimbând o literă, cifra zero (0) în loc litera O.

Atacatorul foloseşte aceasta identitate falsă pentru a informa prin email partenerii de afaceri ai companiei cu privire la schimbarea conturilor de plată a facturilor. De obicei persoana care este impersonată este directorul companiei sau directorul financiar. În email-ul trimis directorul financiar precizează că începând de acum înainte
plăţile către companie să fie efectuate într-un cont nou, cont care se află la dispoziţia atacatorului. Partenerul de afaceri fără să suspecteze frauda şi fără să facă verificări suplimentare efectuează plata în contul indicat, astfel banii ajung în posesia atacatorului.

Pentru a preveni astfel de situații, vă recomandăm să:

- evitați, pe cât posibil, să folosiți corespondența electronică neprotejată pentru transmiterea informațiilor cu caracter comercial sensibil sau cu caracter confidențial (coduri IBAN, parole, detalii de plată, etc);
- folosiți întotdeauna softuri antivirus pentru protecția calculatoarelor dvs;
- NU efectuați plăți către conturi noi pe care nu le-ați mai utilizat, pe baza unor instrucțiuni primite prin e-mail şi fără să verificați mai întâi validitatea acestor conturi cu partenerii dvs, prin intermediul altor canale de comunicație care nu au

legătură cu poșta electronică. Pe lipsa acestei verificări mizează infractorii, deci dacă o veți face, veți contracara cu succes tentativa de fraudă. Verificarea nu o faceți în niciun caz prin e-mail sau prin mijloace de contact sugerate prin intermediul poștei electronice – vă sfătuim să luați legătura în mod direct cu partenerii dvs, prin mijloace sigure și cunoscute (numere de telefon/fax pe care le-ați mai folosit în trecut);

- în situația în care ați efectuat o plată către un cont eronat, contactați urgent banca dvs. pentru a putea afla dacă mai sunt posibile demersuri de blocare/returnare a sumelor implicate.

De asemenea, vă încurajăm ca în situația în care considerați că ați fost victima unei astfel de tentative de fraudă să înștiințați cât mai rapid organele de poliție locale.

FRAUDE LA VÂNZAREA ONLINE A BUNURILOR

Pot exista situații în care persoanele care doresc să vândă anumite bunuri sau produse apelează la diferite platforme on-line aparținând unor companii care se ocupă cu intermedierea schimburilor pe internet (pagini de vânzări/cumpărări online, market-uri online, etc). În urma unei tranzacții încheiate pe o astfel de platformă, vânzătorul primeşte un mesaj e-mail de la cumpărător. În acest mesaj cumpărătorul îi cere vânzătorului să expedieze obiectul vândut prin poștă/serviciu de curierat.

Pentru a determina vânzătorul să expedieze produsul înaintea primirii prețului de achiziționare potențialul cumpărător include în mesajul e-mail o confirmare de plată (falsă). Din aceasta reiese, în mod eronat, faptul că s-a efectuat plata prin transfer bancar și că vânzătorul poate să intre în posesia banilor doar după ce va face dovada faptului că a expediat produsul către adresa indicată de falsul cumpărător. În realitate vânzătorul a fost înşelat şi nici o sumă de bani nu a fost transferată de cumpărător. Astfel de mesaje frauduloase de confirmare a tranzacțiilor pot include logo-ul sau denumirea unor bănci cunoscute sau chiar numele unor angajați ai băncilor respective.

O altă variantă a aceastui tip de înșelăciune este aceea în care potențialul cumpărător încearcă să convingă vânzătorul să trimită împreună cu produsul vândut și o sumă de bani, reprezentând contravaloarea unei taxe fictive pe care ar fi trebuit s-o plătească pentru tranzacție, urmând să-și recupereze banii la finalizarea tranzacţiei ce ar avea loc după dovedirea expedierii coletului și a sumei de bani cerute. În realitate vânzătorul este înşelat şi nici o sumă de bani nu mai ajunge la acesta.

Pentru a preveni astfel de situații, vă recomandăm să:

- nu efectuaţi tranzacţii decât pe platformele cunoscute de intermedieri online
- verificaţi cu atenţie reputaţia cumpărătorului şi ce tranzacţii a efectuat în trecut (atunci când este posibil)
- comunicaţi cu partenerul de afaceri şi pe alte canale nu doar pe email (ex. telefon, video-call)
- verificaţi cu atenţie termenii şi condiţiile platformei care intermediază vânzarea
- vă informaţi cu privire la riscurile care pot apărea în urma unei astfel de tranzacţii.

De asemenea, vă încurajăm ca în situația în care considerați că ați fost victima unei astfel de tentative de înșelătorie să înștiințați cât mai rapid organele de poliție locale.

III. Ameninţări asupra terminalelor de comunicaţii

Terminalele (calculatoare, laptopuri, tablete, telefoane mobile, etc) folosite de dvs. pentru efectuarea tranzacţiilor electronice reprezintă elemente importante ce trebuie securizate corespunzător. Adesea atactorii ţintesc aceste terminale în speranţa că ele nu sunt suficient protejate, iar prin compromiterea lor aceştia reuşesc să desfăşoare tranzacţii frauduloase şi să obţină câştiguri materiale (în defavoarea/dauna dumneavoastră).

Prin urmare vă recomandăm în continuare o serie de măsuri pe care să le aveţi în vedere în securizarea diferitelor terminale:

A. Calculator/Laptop

Instalaţi pe calculatorul/laptop-ul dumneavoastră numai aplicaţii cu licenţă validă (comercială sau gratuită) şi care provin din surse sigure (de ex: site-ul web al producătorului). De cele mai multe ori un software piratat descărcat dintr-o sursă care nu este de încredere ascunde şi un malware!

Încercaţi pe cât posibil să utilizaţi calculatoare/laptop-uri şi sisteme de operare moderne (ultimele versiuni de Windows, Linux, etc). Sistemele de operare moderne au controale de securitate îmbunătăţite său complet noi, iar acestea sunt activate implicit (nu trebuie activate de utilizator, după instalare). Multe dintre aceste controale de securitate pot preveni sau limita impactul pentru multe dintre atacurile informatice.

Furnizorii de sisteme de operare sau aplicaţii **publică periodic actualizări** pentru acestea în vederea remedierii unor probleme de securitate sau pentru îmbunătăţirea unor controale de securitate. De aceea este indicat:

- Să vă asiguraţi că mecanismul de actualizare automată a sistemului de operare este activat. În general aceasta este opţiunea implicită în cadrul procesului de instalare.
- Să vă asiguraţi că mecanismul de actualizare automată pentru aplicaţiile care au această funcţionalitate este activat (de ex. pachetele de aplicaţii de tip “office” – Microsoft Office, navigatoarele web – Edge, Safari, Google Chrome, soluţii de securitate - antivirus, antimalware, etc).

Instalaţi o **soluţie de securitate** ce oferă cel puţin protecţie anti-virus, anti-malware şi anti-phising. Soluţiile de securitate complexe asigură şi funcţionalităţi de tip firewall şi IPS (Intrusion Prevention System) de prevenire a atacurilor informatice precum şi de navigare web securizată. Este important ca soluţia de securitate să fie actualizată periodic cu ultimele semnături anti-virus. De asemenea verificaţi că sunt efectuate automat scanări periodice ale calculatorului (ex. în fiecare săptămână).

Evitaţi să utilizaţi conturi cu privilegii de administrator la nivelul sistemului de operare. Creaţi un cont cu privilegii reduse pentru activităţile obişnuite (navigare web, editare documente, citire email, etc). Conturile cu privilegii administrative ar trebui utilizate doar pentru activităţi ca instalarea/dezinstalarea aplicaţiilor sau configurarea parametrilor de securitate. Utilizarea conturilor cu privilegii de administrator în activităţi obişnuite (de ex. navigare web), dă posibilitatea atacatorilor să preia controlul total asupra calculatorului în

cazul unui atac informatic reuşit. Acest lucru se poate întâmpla fără ca utilizatorul să observe.
Nu conectaţi dispozitive necunoscute la calculatorul dumneavoastră (de ex. stick-uri USB găsite în locuri publice). Aceste dispozitive pot fi lăsate sau "uitate" la îndemâna/la vedere intenţionat de atacatori. Acestea pot conţine viruşi (sau alte tipuri de cod maliţios), iar când sunt conectate la calculatorul dumneavoastră pot infecta în mod automat aceste dispozitive, urmând ca atacatorul să preia controlul complet asupra staţiei.

Obişnuiţi să blocaţi staţia de lucru când plecaţi din faţa ei apăsând simultan tastele: WIN şi L (Windows + Lock).

Folosiţi opţiunile sistemului de operare de blocare automată a ecranului de lucru atunci când calculatorul sau laptop-ul nu este utilizat o perioadă de timp. Puteţi activa opţiunea de "Screen Saver" la 10 minute de inactivitate, iar la reactivare să solicite utilizatorului introducerea parolei.

Dezactivaţi conexiunile de reţea pe care nu le utilizaţi, de exemplu dacă aveţi o conexiune cu fir, dezactivaţi opţiunile wireless – WiFi, Bluetooth. În felul acesta eliminaţi posibilele canale de intruziune pe care un potenţial atacator le-ar putea utiliza pentru a obţine acces la calculatorul dumneavoastră.

Efectuaţi actualizări periodice ale aplicaţiilor folosite pe calculator, în special Flash Player, Java şi aplicaţiile utilizate pentru vizualizarea fişierelor PDF. Toate aceste elemente reprezintă potenţiali vectori de atac care pot fi utilizaţi pentru compromiterea calculatorului.

Nu uitaţi să efectuaţi copii de siguranţă pentru datele dvs. pe un suport extern (backups în limba engleză) în mod periodic (o dată pe săptămână sau o dată pe lună). Această practică vă poate ajuta să vă recuperaţi fişierele (poze sau documente) în urma unei probleme hardware a hard-disk-ului sau în cazul în care aţi fost victima unui atac "ransomware" (atac care vă restricţionează accesul la fişiere prin criptarea acestora).
De asemenea, este important că suportul extern folosit pentru salvarea datelor (ex. un stick USB sau un hard-disk portabil) să nu fie în permanenţă conectact la calculator ci doar atunci când efectuaţi copiile de siguranţă. Altfel acesta ar putea fi infectat cu malware iar datele salvate pe el să fie modificate sau criptate, în felul acesta pierzându-şi posibilitatea de a ajuta la resturarea fişierelor compromise.

Statistic persoanele încep să efectueze copii de siguranţă pentru date abia după ce pierd o dată fişiere importante. Nu aşteptaţi până este prea târziu şi efectuati o copie de siguranţă cât mai repede cu putinţă.

Nu folosiţi computere care nu vă aparţin (la Internet Café, hotel, aeroport sau la "prieteni") atunci când faceţi tranzacţii bancare, deoarece acestea pot conţine deja programe maliţioase (instalate în mod intenţionat sau neintenţionat) care vă pot captura datele de autentificare sau/şi datele bancare.

B. Smartphone/Tableta

Protejaţi accesul la smartphone-ul sau tableta dumneavoastră folosind una din opţiunile de securitate disponibile (PIN, parola, amprenta, recunoaştere facială). În cazul în care echipamentul este pierdut sau furat informaţiile aflate pe el sunt protejate împotriva accesului neautorizat.

Atunci când este posibil actualizaţi sistemul de operare de pe smartphone-ul sau tableta dumneavoastră (Android, iOS). În general producătorii de echipamente care utilizează sistemul de operare Android oferă versiuni personalizate ale acestuia (Samsung, LG, etc). În cazul în care Google (producătorul Android) publică o actualizare de securitate care remediază o problemă de securitate, actualizarea nu se va instala automat pe echipamentele ce utilizează versiuni personalizate ale sistemului de operare. De aceea este important să urmăriţi când apar noi update-uri şi să le instalaţi manual. Aceste vulnerabilităţi pot fi remediate doar când producătorul echipamentului publică o nouă versiune personalizată a sistemului de operare Android.

Instalaţi aplicaţii (Apps) doar din magazinele de aplicaţii oficiale (Google Play, Apple App Store). Aplicaţiile care provin din “magazine” necunoscute pot conţine şi cod maliţios (malware) care vă poate infecta şi compromite securitatea echipamentului. De exemplu, împreună cu aplicaţia descărcată instalaţi şi un malware de tip trojan care poate fura credenţialele aplicaţiei de mobile banking, precum şi codurile OTP (One Time Passcode) primite prin SMS necesare pentru autorizarea plăţilor 3D Secure.

Pentru a evita pe cât posibil infectarea cu malware se recomandă să vă protejaţi telefonul sau tableta cu o aplicaţie antivirus. Este recomandat de asemenea să verificaţi şi “permisiunile” pe care aplicaţiile le solicită la instalare. Aplicaţiile maliţioase vă pot cere permisiuni suplimentare care poate afecta securitatea dispozitivului dvs.

Dezactivaţi opţiunile de conectivitate (Wi-Fi, Bluetooth, NFC, etc) pe care nu le utilizaţi în mod curent. Eliminaţi astfel posibilele canale de intruziune pe care un potenţial atacator le-ar putea utiliza, în plus, economisiţi resursele bateriei şi prelungiţi durata de funcţionare a echipamentului.

Evitaţi operaţiuniile de “jailbreak” (iOS) sau “root” (Android). Este posibil ca în urma acestui proces sistemul de operare să nu mai funcţioneze în parametrii normali (se poate bloca mai des), bateria să se consume mai rapid, aplicaţiile malware să fie mai uşor instalate iar actualizările de securitate şi suportul producătorului să nu mai fie disponibile pentru acest terminal.

Evitaţi să lăsaţi echipamentele portabile (telefoane, tabelete, laptopuri) nesupravegheate în spaţii publice (cafenele, restaurante, aeroporturi) sau la vedere în maşină (suport de bord sau pe scaune).

Ori de câte ori este posibil securizaţi datele păstrate pe echipamentele mobile prin aplicarea unui mecansim de criptare. Păstraţi cu grijă cheile de criptare deoarece fără ele puteţi risca să nu mai recuperaţi informaţiile păstrate în aceste echipamente.

IV. Ameninţări privind utilizarea serviciilor de plată pe internet

Nu este recomandat să accesaţi site-ul de Online Banking al băncii dintr-un link primit pe email sau SMS. Întotdeauna navigaţi (scriind adresa www.alphabank.ro în browser) pe siteul oficial şi folosiţi linkurile de acces indicate pe home page. Linkurile primite pe email sau din motoarele de căutare vă pot redirecţiona către un website fals controlat de atacator. Acesta vă poate păcăli să introduceţi credenţialele de acces pe acest site fals controlat de atacatori.

Activaţi opţiunea de blocare a ferestrelor pop-up. Nu daţi click pe “Agree” sau “OK” pentru a închide o fereastră. În schimb, faceţi click pe “X” în colţul ferestrei sau apăsaţi Alt+F4 pe tastatură.

Verificaţi cu atenţie dacă atunci când desfăşuraţi operaţiuni financiare (transferuri sau plăti cu cardul) conexiunea utilizată este una securizată (https://). Băncile folosesc certificate de securitate cu validare extinsă şi adresa siteului vizitat apare cu verde şi poate fi văzută imaginea unui lăcăţel închis în bară de adresa URL (🔒).
Dacă browserul vă avertizează că există o problemă cu certificatul siteului este recomandabil să nu continuaţi şi să contactaţi banca.

Dezactivaţi salvarea parolelor (în special salvarea automată a acestora) în browser. Această metodă nu reprezintă o opţiune pentru păstrarea în siguranţă a acestora.

Credenţialele de acces (utilizator, parola, cod acces, etc) sunt **informaţii personale** şi nu trebuie comunicate altor persoane. **NU** notaţi pe foi hârtie sau în fişiere text nesecurizate aceste informaţii sensibile.

Încercaţi pe cât posibil să folosiţi **parole complexe de minim 8 carcatere**, aceste parole trebuie să **conţină cel puţin 4 caractere** de formă:
1. O literă mare (A... Z)
2. O literă mică (a... z)
3. O cifră (0... 9)
4. Un semn special (!, @, #, $, %, ?, ^, etc)

O parolă complexă este de formă: **IfMmlflo8!**

Folosiţi ca parola **o frază pe care o puteţi ţine minte uşor**. De exemplu fraza “*În fiecare Miercuri merg la film la ora 8!*” ar putea fi transformată într-o parolă uşor de ţinut minte de formă: *IfMmlflo8! (utilizând prima literă a fiecărui cuvânt).*

Pentru că există posibilitatea că parola dvs. să fie aflată odată cu trecerea timpului este recomandat că **parola să fie schimbată periodic**. De asemenea este foarte important să **nu folosiţi aceeaşi parolă** pentru mai multe servicii (ex. cont email, cont internet banking, cont reţea socializare, etc).
Dacă aveţi cel mai mic dubiu că o parolă a fost aflată (compromisă) **schimbaţi-o imediat**!

Aveţi grijă ca nimeni **să nu vă privească atunci când introduceţi o parolă sau un cod PIN**. Evitaţi să introduceţi parole pe **terminale** (computere din internet cafe-uri, tablete, telefoane, etc) **pe care nu le deţineţi sau cunoaşteţi**, aceste terminale pot avea instalate programe de tip keylogger care vă pot capta credentiale de acces. Întotdeauna alegeţi

opţiunea de deconectare (Log Off sau Sign Out) atunci când nu mai folosiţi un anumit serviciu.

Pentru orice nelămuriri sau probleme legate de serviciile de plată pe internet se recomanda **utilizarea canalelor de suport** puse la dispoziţie de către bancă (ex. email, telefon, etc). În astfel de situaţii nu folosiţi decât datele de contact publicate pe site-ul oficial al băncii.

Banciile NU apelează (telefonic, email sau SMS) la clienţii săi pentru a cere informaţii precum: CNP, număr card, PIN, ID logare, parola, cod token sau orice alte informaţii personale. O astfel de cerere reprezintă o posibilă tentativă de fraudă şi pentru siguranţa dvs. este recomandat să informaţi banca folosind canalele oficiale.

V. Ameninţări privind plăţile cu cardul

Păstraţi cardul bancar cu aceeaşi grijă cu care păstraţi şi actul de identitate. Memoraţi Numărul Personal de Identificare (PIN), nu îl scrieţi și nu îl păstrați scris alături de card, scris în telefon sau altundeva unde poate fi citit de o altă persoană. Nu comunicaţi acest număr nimănui, nici celor din familie.

În cazul în care alegeţi să vă creaţi un nou PIN sau să îl schimbaţi pe cel ce v-a fost dat, evitaţi alegerile evidente cum ar fi data naşterii personală sau a membrilor familiei.

Se recomandă să utilizaţi un PIN diferit pentru fiecare card pe care îl deţineţi.

Se recomandă să păstraţi securizat o listă cu numerele cardurilor pe care le deţineţi, împreună cu numerele de contact unde trebuie să anunţaţi în cazul în care acestea au fost pierdute sau furate. Un număr de card poate fi stocat securizat sub următoarea forma 4256 03XX XXXX 1234.

La efectuarea unei tranzacţii pe internet sunt necesare următoarele date:

- Tipul cardului: Visa, MasterCard, etc.
- Nume (aşa cum apare pe card)
- Numărul cardului (cele 4 grupuri a câte 4 cifre aflate pe card)
- Data expirării cardului (se găseşte sub numărul cardului şi este de forma ll/aa)
- **CVV2** (Card Verification Value – nume utilizat de Visa) sau **CVC2** (Card Verification Code – nume utilizat de MasterCard), acesta este un cod de siguranţă format din 3 cifre şi este tipărit pe verso-ul cardului. Mai poate fi întâlnit pe Internet şi sub denumiri cum ar fi Card Security Code/Verification Code etc.
- Autorizarea tranzactiei fie prin intermediul aplicației Alpha Pay Online fie prin utilizarea parolei si a codului unic (OTP) primit prin SMS, pentru tranzacţii prin sistemul “3D Secure” (Verified by Visa, sau Mastercard Securecode), în cazul în care tranzactia este efectuata pe site-uri inrolate 3D Secure.

Toate aceste informaţii, mai puţin parola, se află înscrise pe card, de aceea trebuie să păstraţi cardul în siguranţă şi să nu daţi ocazia să fie obţinute aceste informaţii de către alte persoane.

Autorizarea tranzacției prin Alpha Pay Online folosind datele biometrice, codul PIN setat la instalarea aplicației sau prin utilizarea parolei și a codului unic generat (OTP) permite creşterea securităţii tranzacţiilor online, persoana care efectuează tranzacția fiind singura care are acces la aceste elemente.
Activarea serviciului 3D Secure se face automat pentru cardurile de credit și de debit Alpha Bank active ai căror deținători au un număr de telefon mobil valid în sistemul Băncii. Pentru efectuarea unei tranzacții pe un site înrolat 3D Secure, clienții vor parcurge initial pasii de înrolare în aplicația Alpha Pay Online astfel: vor descărca aplicația din App Store/Google Play, vor introduce numărul de telefon mobil utilizat în relatie cu banca și ultimele 6 cifre ale cardului, după care vor primi un mesaj SMS cu codul prin care vor confirma înrolarea în aplicație. Utilizatorii de telefoane cu sistem de operare iOS vor trebui să seteze un cod PIN din 6 cifre, ce va fi folosit atunci când autorizarea tranzacției prin datele biometrice nu va fi disponibilă. Ulterior, clientii vor primi pentru autentificarea tranzacțiilor, o notificare de tip “push”. Accesând notificarea vor fi transferați automat în pagina cu detaliile tranzactiei, unde vor putea aproba tranzacția. Pentru siguranța tranzacțiilor, aplicația Alpha Pay Online nu poate fi utilizată de pe un telefon care nu are nicio cheie de securitate disponibilă.

Nu răspundeţi e-mailurilor care par a fi trimise de banca emitentă, în care vă sunt solicitate datele sensibile ale cardului (număr card, data expirării, codul CVV2/CVC2, parola 3D Secure sau codul PIN) sub pretextul unor verificări, modificări, premii, culegerii de informaţii pentru respectarea unor modificări legislative etc.

Atunci când efectuaţi cumpărături online încercaţi să achiziţionaţi de la comercianţi cunoscuţi, care se bucura de o bună reputaţie.

Se recomanda folosirea pentru plăţile pe Internet a unui card dedicat, acest card se poate ataşa unui cont în care să aveţi doar sumele pe care doriţi să le utilizaţi în acest scop. Evitaţi folosirea cardurilor ataşate conturilor de salarii sau cele cu descoperire de cont (overdraft).

VI. Ameninţări privind utilizarea reţelelor wireless (WiFi)

Evitaţi conectarea laptopului sau a smartphone-ului la o reţea wireless nesecurizată. Reţele Wi-Fi gratuite (restaurant, cafenele, aeroporturi) sunt cele mai vulnerabile dacă nu sunt securizate corespunzător. Atunci când vă conectaţi la o reţea nesecurizată orice persoană aflată în raza de acţiune a reţelei ar putea intercepta traficul dvs. şi “vedea” anumite informaţii ce au fost transmise nesecurizat. Dacă totuşi sunteţi nevoit să vă conectaţi la o astfel de reţea evitaţi să introduceţi parole de acces sau să folosiţi servicii financiare online..

Nu lăsaţi router-ul de acasă nesecurizat şi nu folosiţi protocolul de securizare WEP. Acest protocol nu este sigur şi un atacator poate obţine acesul la reţeaua wireless şi intercepta traficul din această reţea.

Se recomandă să folosiţi protocolul WPA2, să configuraţi o parolă cât mai lungă şi să schimbaţi numele implicit (SSID-ul) al reţelei wireless.

Schimbaţi parola preconfigurată din fabrică pentru interfaţa de administrare şi configurare a router-ului, folosind o altă parolă puternică, deoarece parolele iniţiale se pot găsi uşor pe internet şi pot fi folosite de persoane rău voitoare care au acces în reţeaua dumneavoastră pentru a modifica în mod maliţios anumite setări precum DNS-ul (putând fi astfel ameninţaţi de un atac de tip "**DNS Pharming**" – unde chiar dacă introduceţi manual şi corect adresa web a băncii sau a instituţiei financiare direct în browser, sau o accesaţi prin cele mai recente bookmark-uri folosite anterior, veţi deschide de fapt un site maliţios de tip clona fără să vă puteţi da seama că nu
sunteţi pe site-ul real al băncii).

VII. Ameninţări privind utilizarea social media

Evitaţi publicarea online a informaţiilor sensibile (informaţii personale, informaţii financiare (serie card, data expirare card, CVV, credentiale de acces la soluţiile internet banking), informaţii de localizare etc), pe siteurile social media (Facebook, Twiter, Instagram, etc).

Folosiţi opţiunile de protejare a intimităţii (aceste opţiuni sunt specifice fiecărui site) şi limitaţi expunerea informaţiilor personale în mediul online. În general fiţi atenţi la orice informaţie publicaţi pe site-urile de socializare. Aceste informaţii pot fi utilizate de atacatori, de exemplu sunt cazuri cunoscute de locuinţe sparte de infractori, pentru că proprietarii publicaseră pe site-urile de socializare poze, comentarii, localizări din concedii, practic informând că nu sunt acasă pentru o perioadă de timp.

Fiţi atenţi la persoanele pe care le contactaţi în mediul online. Oricine îşi poate crea un cont pe site-urile de socializare (Facebook, Twiter, Instagram, etc), asumându-şi o altă identitate.

Fiţi suspicios atunci când sunteţi contactat de prieteni sau cunoscuţi în mediul online (email-uri, mesaje pe aplicaţiile de mesagerie instant), atunci când comportamentul acestora este neobişnuit. De exemplu: primiţi mesaje care conţin doar un link sau fişiere ataşate, dar fără nici o altă explicaţie sau într-un limbaj neobişnuit pentru prietenul/cunoscutul dvs. Gândiţi-vă că este posibil ca respectiva persoană
să aibă contul compromis, iar atacatorul încearcă să intre în contact cu dvs (de exemplu pentru a vă infecta calculatorul).

Evitaţi pe cât posibil să urmaţi link-urile scurte (hxxp: //goo.gl/dBICml). Fără o verificare prealabilă, nu puteţi sa ştiţi pe ce site vă redirectionează acel link. Puteţi fi redirecţionat spre un site compromis care găzduieşte aplicaţii malware.