Exim
Banca Românească

România crește cu noi!

# GHID PRIVIND SECURITATEA PLĂŢILOR PE INTERNET

# CUPRINS

# I. Ameninţări 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 conceput pentru a perturba sau fura date de pe un computer, retea sau server..

## 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 să execute aplicaţia maliţioasă pe dispozitivul său. Odată activat, troianul permite atacatorului să controleze şi să monitorizeze dispozitivul 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 dispozitiv de comunicatie în urma unui atac de tip "*drive-by-download*" sau pot fi instalate împreună cu programele piratate.

## CE ESTE UN ADWARE?

*Adware-ul* este o formă de malware care descarcă sau afişează anunţuri nedorite când utilizatorul navighează online, de asemenea, acesta colectează date de marketing sau alte informaţii fără ştirea utilizatorului şi redirecţionează căutările utilizatorului către diferite website-uri ce afişează anunţuri publicitare. Aplicaţiile adware se instalează automat cu unele programe gratuite pe care dvs. le instalaţi de pe Internet sau cel mai adesea "vin la pachet" cu programele piratate.

# I. Ameninţări informatice

## CE ESTE UN ATAC DE TIP "DRIVE-BY DOWNLOAD"?

Un atac de tip "*drive-by-download*" se referă la **descărcarea ne-intenționată** (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 browser-ului 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*) are loc atunci cand atacatorii intercepteaza date sau compromit reteaua pentru a intra in posesia informatiilor schimbate intre utilizator si aplicatii/servicii (credentiale, mesaje, informatii financiare, date cu caracter personal). Aceste atacuri sunt frecvente atunci cand se utilizeaza retele Wi-Fi publice, care pot fi compromise cu usurinta.

## 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" (un alt mediu de transmisie, ex.: SMS) diferit de cel care a fost utilizat pentru iniţierea tranzacţiei (ex.: web).

## II. Ameninţări de tip *inginerie socială*

*Ingineria socială*, **social engineering** în limba engleză**,** se refera la toate tehnicile menite sa convinga o tinta (utilizatorul) sa dezvaluie informatii confidentiale. Atacatorii se bazeaza pe “people skills” pentru a castiga increderea utilizatorilor in vederea obtinerii drepturilor de conectare la sisteme. In multe cazuri, aceasta metoda este cea mai usoara forma de obtinere de acces la un sistem informational. În continuare prezentăm cele mai cunoscute tipuri de inginerie socială.

**CE ÎNSEAMNĂ "PHISHING"/ “SMSishing?**

În domeniul informatic, **phishing** reprezintă o formă de activitate criminală care constă în obţinerea datelor confidenţiale, cum ar fi credenţialele de acces (nume utilizator, parola, PIN, OTP) pentru aplicaţii financiare sau informaţii referitoare la cardul de credit, folosind tehnici de manipulare a identităţii unei persoane sau a unei instituţii.

Un atac de tip phishing constă, în mod normal, în trimiterea de către atacator a unui mesaj electronic, folosind programe de mesagerie instantă *(e-mail)* – **PHISHING,** *sau telefon (SMS)* **- SMSishing**, în care utilizatorul este sfătuit să introducă credenţialele de acces (nume utilizator, parola), numere de card, coduri PIN, etc.

***Un exemplu de phishing****:* primiţi un email în care aţi fost informat că aţi câștigat o excursie în străinătate iar tot ce trebuie să faceţi pentru a primi voucherul de călătorie este să introduceţi (pe un site asemănător 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 re-vândute în mod frecvent de atacatori pentru a fi folosite în atacuri de tip “phishing”.

**DE UNDE ȘTIU EI CU CE BANCĂ LUCREZ?**

Atacatorii nu știu acest lucru, dar dacă trimit multe mesaje cu siguranță nimeresc şi persoane care lucrează cu banca prezentată în mesajul de phishing, iar dacă persoanele 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 website-ul public).

**CE ESTE VISHING?**

*Vishing* este un termen care provine din termenii **v**oice și ph**ishing** și reprezintă o formă de înșelătorie prin care utilizatorul este păcălit să furnizeze informaţii sensibile, credenţialele de acces, numere de card, sau coduri de acces, cu scopul de a impersona utilizatorul de drept sau a fi folosite de atacator în alte atacuri de inginerie socială.
***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 de atac încadrat în categoria *Inginerie Socială* este “CEO Fraud” sau “Business Email Compromise (BEC)”. În ce constă aceasta înşelătorie, atacatorul reuşeşte să compromită serverul de email al unei companii sau să creeze o căsuţă de email asemănătoare cu cea oficială a companiei vizate.
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.

## FRAUDE LEGATE DE SOLUTII DE INVESTITII

O data cu dezvoltarea a noi platforme de tranzactionare a criptomonedelor, bazata pe interesul tot mai crescut al utilizatorilor, numarul de fraude din domeniu a inregistrat o crestere semnificativa in ultima perioada.
Cel mai des scenariu de frauda care vizeaza criptomonedele, este cel in care atacatorii contacteaza utilizatorii de servicii de plata propundu-le acestora o afacere de nerefuzat prin care se poate obtine un profit garantat intr-un timp foarte scurt.
In cazul in care utilizatorul este de acord cu propunerea facuta, atacatorul il va convinge că, pentru obținerea profitului, este nevoie să își instaleze o aplicație care permite controlul dispozitivului personal de la distanță. Acest tip de aplicație va oferi atacatorului acces la telefonul utilizatorului, acesta putand să urmărească exact datele pe care le introduce fie în platforma crypto, fie în aplicațiile bancare. Astfel, utilizatorul ajunge să ofere, fără să vrea, date cu caracter personal, date de pe actul de identitate, IBAN, datele cardului sau datele de logare și codurile de autentificare (OTP) pentru conturile bancare, informatii ce sunt folosite de persoanele rau intentionate in efectuarea de operatiuni frauduloase.
Banca nu solicita date privind tranzactionarea criptomonedelor si nici nu transmite informatii pentru a determina clientii să faca investiții în criptomonede.


**Pentru a preveni astfel de situații, vă recomandăm să**:

- ✓ evitați, pe cât posibil, să folosiți corespondența electronică neprotejată pentru vehicularea informațiilor cu caracter comercial sensibil sau cu caracter confidențial (coduri IBAN, parole, detalii de plată, etc);
- ✓ folosiți întotdeauna softuri antivirus pentru protecția dispozitivelor dvs. de comunicatie;
- ✓ **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, de obicei către destinații din zona continentului african (dar nu numai).

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 acestui 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.

Un alt exemplu de fraudă externă atunci când se fac plăți on-line cu cardul: clientul cumpărător sesizează instituția de credit cu privire la faptul că nu poate finaliza o serie de plăți pe site-urile unor comercianți sau platforme de plăți, motivând că sumele aferente acestor tranzacții au fost blocate pe contul său, dar că tranzacția nu s-a finalizat cu succes. Pentru a justifica aceste sesizări clienții transmit instituțiilor de credite mesaje ce par a fi primite de la respectivele platforme, iar instituția de credit deblochează sumele reclamate de client, însă, ulterior, sumele respective vin spre decontare, astfel încât clientul intră în debit neautorizat cu sumele respective.

**Pentru a preveni astfel de situaţii, 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

Dispozitivele (calculatoare, laptopuri, tablete, telefoane mobile, etc) folosite de dvs. pentru efectuarea tranzacţiilor electronice reprezintă elemente importante ce trebuie securizate corespunzător. Adesea atacatorii ţintesc aceste dispozitive 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 dispozitive:

**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, CD/DVD-uri achiziţionate împreună cu calculatorul/laptop-ul). 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 sau 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 sau al aplicatiilor folosite este activat. În general aceasta este opţiunea implicită în cadrul procesului de instalare.

- 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/laptopului (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 precum 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 dispozitivului.

- 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 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 dispozitivului folosit.

- Nu uitaţi să efectuaţi copii de siguranţă pentru datele dvs. pe un suport extern (*back-up* 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 ca 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 restaurarea 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 efectuaţi o copie de siguranţă cât mai repede cu putinţă!

- Nu folosiţi alte 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.

***Smartphone/Tableta***

- ✓ Protejaţi accesul la smartphone-ul sau tableta dumneavoastră folosind una din opţiunile de securitate disponibile (PIN, parola, sau "semn grafic"). 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, Windows). În general producătorii de echipamente care utilizează sistemul de operare Android oferă versiuni personalizate ale acestuia (Samsung, LG, HTC, 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 (Samsung, LG, HTC, etc) publică o nouă versiune personalizată a sistemului de operare Android.

- ✓ Instalaţi aplicaţii (Apps) doar din magazinele de aplicaţii oficiale (Google Play, Apple App Store, Microsoft 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 troian care poate fura credenţialele aplicaţiei de mobile banking, precum şi codurile OTP (One Time Password) 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 pot 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.

- ✓ Nu efectuați operațiunea de "jailbreak" (iOS) sau "root" (Android). Prin acest proces se elimina limitările de securitate impuse de vânzătorul sistemului de operare. 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 mecanism de criptare. Păstraţi cu grijă cheile de criptare deoarece fără ele riscati 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 Internet Banking al băncii dintr-un link primit pe email sau SMS. Întotdeauna navigaţi (scriind adresa în browser) pe site-ul oficial şi folosiţi link-ul de acolo. Link-urile primite pe e-mail vă pot redirecţiona către un site fals, controlat de atacator.

- 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 site-ului vizitat apare cu verde şi poate fi văzută imaginea unui lăcăţel închis în bară de adresa URL ( ). Dacă browser-ul vă avertizează că există o problemă cu certificatul site-ului 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. Dacă doriţi să păstraţi securizat aceste date folosiţi întotdeauna un manager de parole.

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

- Folosiţi **parole complexe de <u>minim 8 caractere</u>**, care să **conţină <u>cel puţin</u> 3 tipuri de caractere** din categoriile urmatoare:
    - literă mare (A... Z)
    - literă mică (a... z)
    - cifră (0... 9)
    - semn special (!, @, #, $, %, ?, ^, etc.)

- Pentru că există posibilitatea ca 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 captura credenţialele de acces**. Întotdeauna alegeţi **opţiunea de deconectare** (Log Off sau Sign Ouţ) 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.

**Băncile NU apelează** (**telefonic, email sau SMS**) 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), nefiind recomandata pastrarea acestuia 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.

- Dacă alegeţi să păstraţi documentul de la bancă, prin care vi s-a comunicat PIN-ul, în nicio situaţie să nu păstrați acest document în acelaşi loc unde este cardul (**nu se recomandă păstrarea documentului**).

- 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 de asemenea să semnaţi imediat pe banda de semnătura de pe spatele cardului, după ce îl primiţi de la bancă.

- 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.
  - parola sau codul OTP pentru tranzacţii prin sistemul “3D Secure” (Verified by Visa, sau Mastercard Securecode), în cazul în care cardul este înrolat într-un astfel de sistem.


Toate aceste informaţii, mai puţin parola 3D Secure, 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.

**Parola 3D-Secure** sau codul unic OTP sunt elemente de siguranţă, de antifrauda, dezvoltate de VISA şi MasterCard. Folosirea acestui sistem permite creşterea securităţii tranzacţiilor on-line, deoarece parola sau codul unic OTP (ori ambele) sunt solicitate la fiecare comandă online prin sistemul 3D Secure.

Dacă aveţi unul sau mai multe carduri emise sub sigla Visa sau MasterCard aveţi opţiunea de a le înrola în acest sistem. Primul pas este să contactaţi banca emitentă a cardului dumneavoastră şi să solicitaţi înrolarea în acest sistem, apoi să urmaţi paşii indicaţi de către bancă.

Avantajele 3D Secure sunt:

- Reducerea riscului de frauda datorită faptului că doar persoana care cunoaşte parola 3D Secure, sau care cunoaşte codul OTP creat unic pentru acea tranzacţie 3D Secure (şi primit prin SMS, token sau alte canale), poate tranzacţiona online pe site-uri care folosesc acest sistem antifrauda;

- Dacă datele cardului dumneavoastră **înrolat în 3D Secure** sunt folosite **fraudulos de către o terţă parte** pentru a comanda pe site-ul unui comerciant care nu foloseşte acest sistem de protecţie, veţi avea câştig de cauză la disputarea sumei aferente tranzacţiei.

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 on-line 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).

Majoritatea cardurilor nu sunt activate implicit pentru plăţile pe Internet. Activaţi această opţiune doar dacă intenţionaţi să faceţi plati pe Internet cu acel card. Activarea se poate face cu ajutorul băncii sau direct în aplicaţia băncii, depinde de fiecare bancă în parte. Nu păstraţi această opţiune activă în situaţia în care consideraţi că nu veţi mai folosi acel card la plăţi pe Internet.


## VI. Ameninţări privind utilizarea reţelelor wireless (WiFi)

- Evitaţi conectarea laptopului sau a smartphone-ului la o reţea wireless nesecurizată. Reţelele 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 accesul 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 introduci manual şi corect adresa web a băncii tale sau a instituţiei financiare direct în browser, sau o accesezi prin cele mai recente bookmark-uri folosite anterior, vei deschide de fapt un site maliţios de tip clona fără să vă puteţi da seama că nu sunteţi pe site-ul real al băncii – acest tip de atac fiind mult mai periculos chiar decât atacul de tip Phishing pentru că nu exista modalităţi de identificare a site-ului maliţios).

## VII. Ameninţări privind utilizarea social media

- Evitaţi publicarea on-line a informaţiilor sensibile (informaţii personale, informaţii financiare (serie card, data expirare card, CVV, credenţiale de acces la soluţiile internet banking), informaţii de localizare etc), pe site-urile 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 on-line. 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 on-line. 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 on-line (email-uri, mesaje pe aplicaţiile de mesagerie instant), atunci când comportamentul acestora este neobişnuit. De exemplu: primiţi mesaje care conţin doar un link URL, sau e-mail cu link URL 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 să ştiţi pe ce site vă redirectează acel link, putand fi astfel redirectat spre un site compromis care găzduieşte aplicaţii malware.

- Evitaţi accesul conturilor de plăţi, prin instalarea aplicaţiilor de tip „acces la distanţă” (de exemplu Any Desk), în paralel cu aplicaţii de tranzacţionare cu criptoactive (de tipul Binance) sau cu alte tipuri de aplicaţii, în vederea prevenirii unor scenarii de fraudă :
  - Ulterior instalării celor 2 tipuri de aplicaţii menționate, atacatorii reușesc să convingă clienţii să își deschidă cont și să inițieze operaţiuni de cumpărare a criptoactivelor cu scopul de a se face legatura în cadrul aplicaţiei cu instrumentul de plată al victimei și de a se permite inițierea de plăţi ulterioare, fără a fi necesară o autorizare suplimentară;
  - Sub pretextul retragerii profitului înregistrat, cu promisiunea falsă de obținere a unor câștiguri, ca urmare a activităţii de tranzacţionare pe platforma de criptoactive, clienţii sunt manipulaţi să ofere date sensibile (date bancare) privind plăţile;

Persoanele vizate de astfel de fraude sunt contactate prin diverse canale de comunicare de către terţe persoane care pretind că sunt reprezentanţi ai unor companii sau platforme de investiţii care facilitează achiziţionarea de criptomonede.

**Pentru a preveni astfel de situații, vă recomandăm să:**

- ✓ Vă asiguraţi că verificaţi din mai multe surse orice propunere de investiție cu câștig substanțial și rapid;
- ✓ Acordați o atenție sporită asupra mesajelor nesolicitate pe e-mail și/sau social media, prin care se oferă sume mari;
- ✓ Nu accesați link-urile de pe platformele de socializare care promit obținerea unor câștiguri;
- ✓ Indiferent de insistența și presiunile pe care le exercita reprezentanții falși ai platfomelor financiare, nu comunicați date confidențiale;
- ✓ Instalați doar aplicații din surse oficiale, atât pe telefon, cât și pe calculator;
- ✓ Nu furnizați niciodata alor persoane datele personale sau bancare;
- ✓ Nu răspundeți și nu accesați link-ul din cadrul mesajelor de e-mail necunoscute și/sau suspecte;
- ✓ Anuntați imediat banca în cazul în care considerați că ați fost înșelați sau ați furnizat datele bancare altor persoane.