Recomandari de Securitate pentru platile online

Pentru protectia dvs. va aducem la cunostinta faptul ca ocazional, emailuri false ori programe malitioase pot fi utilizate de fraudatori cu scopul de a extrage datele bancare ale clientilor. Urmati recomandarile noastre de mai jos pentru a preveni si a detecta incercarile de frauda online.

Atentie la incercarile de FRAUDA online (pe care va rugam sa le raportati catre Banca imediat):
In cazul in care primiti un email ce pare a fi trimis de catre Vista Bank, va rugam sa tineti cont de urmatoarele:

- Banca NU va solicita niciodata prin email date precum: parole de acces, coduri PIN, conturi bancare, sau datele cardului de credit sau debit, ori coduri de Token!
- Mailul oficial din partea Bancii se va adresa catre dumneavoastra folosind corect numele si prenumele dumneavoastra, sau numele companiei, dupa caz!
- Mesajul din partea Bancii nu va contine atasamente pe care nu le-ati solicitat si nu va cere sa dati click pe vreun link care sa va re-directioneze catre un alt server/website din Internet

Asigurati-va intotdeauna ca aveti acces la serviciul nostru de **Internet Banking** in urma accesarii site-ului oficial al Vista Bank Romania: https://www.vistabank.ro. Asigurati-va ca in timpul autentificarii, va aflati pe site-ul oficial de Internet Banking al Vista Bank Romania (fostul Marfin Bank Romania):

- https://ebanking.marfinbank.ro/tellerb2c/index.htm (vechiul Internet Banking disponibil pana pe 31.Oct.2019)
- Sau https://ibkvbr.vistabank.ro/eb/ (noul Internet Banking disponibil din 12.Sept.2019)

Pentru **Mobile Banking** oficial al Vista Bank Romania, **asigurati-va ca instalati** aplicatia doar din urmatoarele locatii de incredere / magazine de aplicatii oficiale:

- (pentru **Android** din Google Play) : https://play.google.com/store/apps/details?id=ro.vista.mobile&gl=RO
- (pentru **iOS** din Apple Store): https://apps.apple.com/bm/app/vista-mobile-banking/id1477309312

Pentru aplicatia de **eToken** oficial al Vista Bank Romania, **asigurati-va ca instalati** aplicatia doar din urmatoarele locatii de incredere / magazine de aplicatii oficiale:

- (pentru **Android** din Google Play) : https://play.google.com/store/apps/details?id=com.vistaetoken&gl=RO
- (pentru **iOS** din Apple Store): https://apps.apple.com/bm/app/vista-etoken/id1477189905

Actualizati aplicatiile Mobile Banking si eToken atunci cand sunt disponibile versiuni noi in Google Play (pentru Android) sau in Apple Store (pentru iOS), deoarece noile versiuni aduc imbunatatiri si pot remedia erori sau vulnerabilitati.

Atentie la mailurile false (de phishing) pe care ati putea sa le primiti, precum:

- Un mail in care vi se solicita urgent sa actualizati/validati datele personale, in majoritatea cazurilor este o incercare de Frauda!
- Mailuri in care identificati greseli gramaticale sau de scriere (traduceri gresite din alte limbi), intotdeauna sunt incercari de frauda!

Anuntati Vista Bank Romania:
In cazul in care ati primit un mail suspect ce pare a veni din partea Vista Bank, va rugam sa **contactati imediat cel mai apropiat sediu al Bancii sau sa sunati la Call Center-ul Vista Bank (Telefon: +4021.222.33.10**) pentru a verifica autenticitatea mailului respectiv. De asemenea, trimiteti/forward-ati (ca atasament) mailul suspect si catre adresa de mail : abuse@vistabank.ro . In niciun caz nu sunati la alte numere de telefon mentionate in mailurile suspecte.

Sfaturi pentru Securitatea Computerului Dvs:

- Scaneaza periodic calculatorul pentru a va proteja impotriva virusilor informatici si a altor programe de tip malware utilizand software Antivirus actualizat zilnic.
- Folositi un cont al sistemului de operare care nu are drepturi de administrator (pentru ca virusii sa nu se poata instala usor);
- Evitati instalarile implicite (default) ale aplicatiilor, alegeti instalarile personalizate (custom) si nu instalati Toolbar-uri sau Extensii periculoase in Browser-ul folosit pentru navigarea pe Internet;
- Actualizati periodic sistemul de operare si asigurati-va ca folositi un browser recent, stabil, iar aplicatia Java, player-ul Flash si reader-ul PDF sunt actualizate la cele mai recente versiuni ;
- Blocati computerul cand plecati din fata lui.
- Nu folositi alte computere care nu va apartin (la Internet Café, hotel, aeroport sau la “prieteni”) atunci cand faceti tranzactii bancare, deoarece acelea pot contine deja programe malitioase (instalate in mod intentionat sau neintentionat) care va pot fura datele de autentificare sau/si datele bancare.

Navigarea sigura pe Internet:

- Evitati accesarea link-urilor aflate in mailuri ce va re-directioneaza catre alte website-uri care pot imita eventual site-ul bancii (deoarece exista riscul sa introduceti user-ul, parola, Token-ul sau PIN-ul pe un site fals/clona care va fura datele de autentificare pentru a le refolosi in mod malitios).
- Introduceti/Scrieti dvs direct in browser adresa site-ului bancii.
- Invatati sa recunoasteti semnele conectarii la un site sigur: conexiune prin “**https://**” si certificat valid al site-ului. Daca browser-ul avertizeaza ca certificatul site-ului nu se potriveste cu al serverului, este recomandabil sa nu continuati !
- Dezactivati salvarea parolelor in browsere (in special salvarea automata a acestora).
- Activati optiunea de blocare a ferestrelor pop-up.
- NU descarcati fisiere de pe site-uri de torente sau site-uri cu aplicatii piratate. Aceste fisiere pot ascunde software malitios care se instaleaza in calculator fara informarea utilizatorului
- Nu faceti click pe “Agree” sau “OK” pentru a inchide o fereastra. In schimb, faceti click pe “X” in coltul ferestrei sau apasati Alt+F4 pe tastatura.

Utilizarea sigura a Retelelor Wireless (WiFi)

- Evitati conectarea laptopului sau a smartphone-ului la o retea nesecurizata. Retele Wi-Fi gratuite sunt cele mai vulnerabile daca nu sunt securizate.
- Atunci cand va conectati la o retea nesecurizata, orice persoana aflata in raza de actiune a punctului de acces poate sa “vada” informatiile transmise.
- Nu lasati router-ul de acasa nesecurizat si nu folositi tehnologia WEP. Se poate obtine accesul in cateva secunde, datorita vulnerabilitatiilor pe care le prezinta protocolul.
- Folositi numai WPA2, configurati o cheie cat mai lunga, schimbati SSID-ul retelei wireless. Altfel sunteti susceptibil atacurilor de tip rainbow-table.

Utilizarea sigura a Smartphone-urilor si a Tabletelor

- Restrictionati accesul la telefon/tableta utilizand PIN, sau parola, ori fingerprint (amprenta digitala);
- Instalati doar aplicatii cu reputatie buna, cu numar mare de descarcari si recenzii ;
- Instalati un Antivirus pentru a scana aplicatiile instalate ;
- Faceti update la telefon, atat pentru sistemul de operare cat si pentru aplicatii ;
- Nu faceti “Jailbreak”/”Rooting” la telefon/tableta.

Siguranta parolelor:

- Folositi numai parole puternice (de minim 8 caractere continand litere mari, mici, cifre si caractere speciale) si evitati cuvintele din dictionar, secvente consecutive din litere sau cifre, ori nume de persoane sau date de nastere (ori alte informatii care se regasesc publice pe retelele de socializare)
- Nu folositi aceleasi parole cu cele folosite pe alte site-uri (precum Retelele sociale, Mailuri personale, etc)
- Nu comunicati parola altor persoane
- Schimbati periodic parolele

Siguranta Token-ului / eToken-ului (care genereaza "Parola unica"):

- Tineti intotdeauna Token-ul sau dispozitivul pe care este instalata aplicatia eToken la dumneavoastra si nu permiteti sa fie accesibil altor persoane;
- Nu divulgati nimanui "Parola unica" (One-Time Passcode) generata de Token.
- Daca ati pierdut / sau a fost furat Token-ul sau dispozitivul pe care este instalat eToken-ul, anuntati imediat Banca pentru a se dezactiva acel token!

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 INSEAMNA "PHISHING"/ "SMSishing?
În domeniul informatic, **phishing** (eng) reprezintă o formă de activitate criminală care constă în obţinerea datelor confidenţiale, cum ar fi credenţialele de acces (username, 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 access (nume utilizator, parola), numere de card, coduri PIN, etc.

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 identitata: 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 Internet 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-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 canalele de suport oficiale (ex. telefonul sau email-ul menţionat pe websiteul public si la inceputul acestui document).

CE ESTE VISHING?
Vishing este un termen care provine din termenii **v**oice și ph**ishing** și reprezintă o formă de înșălatorie 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 atac încadrat în categoria Inginerie Socială este “CEO Fraud” sau “Business Email Compromise (BEC)”. În ce constă acesta 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. Eventual schimbând o literă, cifra zero (0) în loc litera O.

Atacatorul foloseşte această 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 preciează 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 vehicularea 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 email 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.