Recomandari de securitate in mediul online

Pentru protectia dvs., va reamintim ca, ocazional, email-uri false sau programe malitioase pot fi utilizate de fraudatori cu scopul de a extrage datele bancare ale clientilor. Va rugam sa urmati recomandarile noastre de mai jos pentru a preveni si a detecta potentialele incercari de frauda online.

A. Amenintari de tip *inginerie sociala*

Ingineria sociala, **social engineering** in limba engleza**,** este arta de a manipula, minti, sau influenta pe ceilalti ca sa realizeze/nu realizeze anumite actiuni ori sa divulge informatii confidentiale.
Este oarecum similar cu un truc de castigarea increderii sau cu o simpla frauda. Acest termen se aplica de obicei celor care utilizeaza siretlicuri pentru a culege informatii sau pentru a accesa sistemele informatice. In unele cazuri atacatorul nu vine niciodata fata-in-fata cu victima.
Aflati in cele ce urmeaza cele mai cunoscute tipuri de inginerie sociala.

Ce inseamna "PHISHING"/ “SMSishing”?

In domeniul informatic, **Phishing** (eng) reprezinta o forma de activitate criminala care consta in obtinerea datelor confidentiale, cum ar fi credentialele de acces (username, parola, PIN, OTP) pentru aplicatii financiare sau informatii referitoare la cardul de credit, folosind tehnici de manipulare a identitatii unei persoane sau a unei institutii.
Un atac de tip phishing consta, in mod normal, in trimiterea de catre atacator a unui mesaj electronic, folosind programe de mesagerie instanta *(e-mail)* – **PHISHING,** *sau telefon (SMS)* **- SMSishing**, in care utilizatorul este sfatuit sa dea click pe un link sau sa introduca credentialele de acces (nume utilizator, parola), numere de card, coduri PIN etc.

Atentie la incercarile de FRAUDA online prin email-uri sau SMS-uri false (Phishing/SMSishing) precum:

- Un email sau SMS prin care vi se solicita sa va actualizati/validati urgent datele personale si/sau de securitate, in majoritatea cazurilor este o incercare de frauda. NU furnizati astfel de informatii.
- Email-uri sau SMS-uri in care identificati greseli gramaticale sau de scriere (traduceri gresite din alte limbi), intotdeauna sunt incercari de frauda.

Un exemplu de phishing: Primiti un email in care ati fost informat ca ati castigat o excursie in strainatate si tot ce trebuie sa faceti pentru a primi voucherul de calatorie este sa introduceti (pe un site asemenator cu cel al bancii) urmatoarele informatii pentru a confirma identitatea: numele, adresa si datele cardului dvs.

Un exemplu de SMSihing: Primiti un mesaj SMS de la un numar necunoscut care pretinde a fi banca dvs. si care va invita sa descarcati o noua versiune a aplicatiei de Mobile Banking.
ATENTIE! Cel mai probabil in acest caz veti descarca si rula un malware care ar putea da atacatorului posibilitatea sa controleze si sa monitorizeze telefonul dvs. mobil, inclusiv sa poata captura credentialele de acces pentru aplicatia legitima de Internet Banking.

In cazul in care primiti un email/SMS ce pare a fi trimis de Vista Bank, va rugam sa tineti cont de urmatoarele:

- Banca NU va solicita niciodata prin email, SMS sau accesarea unui link date precum: parole de acces, coduri PIN, conturi bancare, datele cardului de credit sau debit, coduri de Token;
- Mesajul din partea Bancii NU va contine fisiere atasate pe care nu le-ati solicitat si NU va va cere sa dati click pe vreun link care sa va redirectioneze catre un server/website Internet diferit de cele oficiale ale Bancii;
- Banca NU va va cere sa descarcati aplicatiile oficiale de Mobile Banking sau eToken prin intermediul unui link trimis prin e-mail sau SMS. Singurele surse oficiale pentru aplicatiile noastre sunt App Store si Google Play.

Anuntati imediat Vista Bank Romania:
In cazul in care ati primit un e-mail/SMS suspect de Phishing/SMSishing 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 /SMS-ului respectiv. De asemenea, trimiteti/forward-ati (ca attachment) mailul suspect catre urmatoarea adresa: abuse@vistabank.ro . **In niciun caz nu sunati la alte numere de telefon mentionate in email-urile suspecte.**

De unde au adresa mea de e-mail sau numarul meu de telefon?
De cele mai multe ori aceste informatii sunt culese din surse publice (ex. site-uri de anunturi) dar si din bazele de date facute publice in urma unor brese de securitate ale diferitelor servicii online unde ati furnizat datele respective de contact. Aceste informatii sunt schimbate sau revandute in mod frecvent de atacatori pentru a fi folosite in atacuri de tip “phishing”.

De unde stiu ei cu ce banca lucrez?
Atactorii nu stiu acest lucru, dar daca trimit multe mesaje cu siguranta acestea vor ajunge si la persoane care lucreaza cu banca prezentata in mesajul de phishing, iar daca persoanele nu sunt atente ele vor furniza atacatorilor informatiile pe care acestia le cauta.

Ce fac daca primesc un e-mail sau un SMS suspect?
Cel mai bine este sa stergeti mesajul respectiv, mai ales daca el contine link-uri sau fisiere atasate. De asemenea, ori de cate ori aveti suspiciuni cu privire la originea unui mesaj (email sau sms) este bine sa contactati banca pe unul dintre canalele de suport oficiale (ex. telefonul sau email-ul mentionat pe websiteul public si la inceputul acestui document).

Ce este Vishing?
Vishing este un termen care provine din termenii **V**oice si ph**ishing** si reprezinta o forma de inselatorie telefonica prin care utilizatorul este pacalit telefonic sa furnizeze informatii sensibile, credentialele de acces, numere de card, sau coduri de acces, cu scopul de a impersona utilizatorul de drept sau a fi folosite de atacator in alte atacuri de inginerie sociala.

Un exemplu de vishing: primiti un telefon de la o persoana care pretinde a fi un angajat al bancii care doreste sa verifice numarul cardului, codul PIN sau codul de securitate al cardului deoarece a fost initiata o alerta de securitate.

Ce poti face?
- NU transmite datele tale confidentiale catre alte persoane.
- Atacatorul poate afla informatii despre tine pe internet sau retelele de socializare, pentru a parea cat mai credibil. Solicita mai multe detalii persoanei respective si anunt-o ca doresti sa verifici numarul de telefon direct cu Banca (prin website sau Call Center), dupa care vei reveni tu cu un apel. Nu ceda la insistentele acesteia in privinta urgentei de a furniza datele pe loc.

Ce este “CEO FRAUD” sau “BEC FRAUD”?
Un alt tip atac incadrat in categoria Inginerie Sociala este “CEO Fraud” sau “Business Email Compromise (BEC)”. Prin aceasta inselatorie atacatorul reuseste sa compromita serverul de email al unei companii sau sa creeze o casuta de email asemanatoare cu cea oficiala a companiei vizate. Eventual schimband o litera, cifra zero (0) in loc de litera O.

Atacatorul foloseste aceasta identitate falsa pentru a informa prin email partenerii de afaceri ai companiei cu privire la schimbarea conturilor de plata a facturilor. De obicei, persoana care este impersonata este directorul companiei sau directorul financiar. In email-ul trimis, directorul financiar precieaza ca incepand de acum inainte platile catre companie vor fi efectuate intr-un cont nou, cont care se afla de fapt la dispozitia atacatorului.

Partenerul de afaceri, fara sa suspecteze frauda si fara sa faca verificari suplimentare, efectueaza plata in contul indicat, banii ajungand astfel in posesia atacatorului.

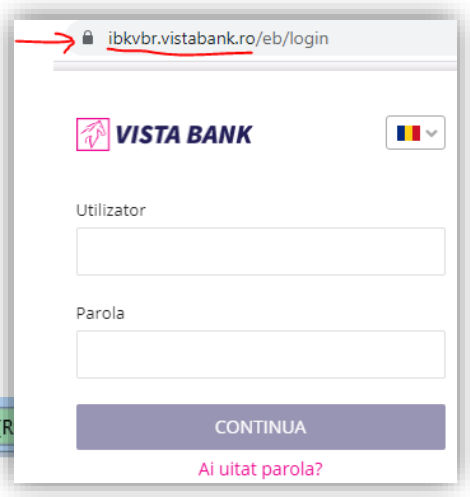
Pentru a preveni astfel de situatii, va recomandam sa:

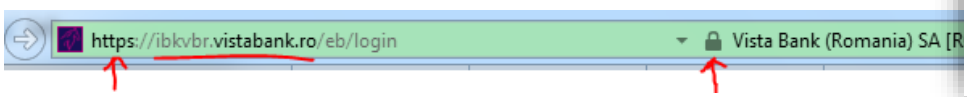
- evitati, pe cat posibil, sa folositi corespondenta electronica neprotejata pentru vehicularea informatiilor cu caracter comercial sensibil sau cu caracter confidential (coduri IBAN, parole, detalii de plata etc);
- folositi intotdeauna softuri Antivirus pentru protectia calculatoarelor dvs.;
- NU efectuati plati catre conturi noi pe care nu le-ati mai utilizat pe baza unor instructiuni primite prin email si fara sa verificati mai intai validitatea acestor conturi cu partenerii dvs. prin intermediul altor canale de comunicatie care nu au legatura cu posta electronica. Pe lipsa acestei verificari mizeaza infractorii, deci daca o veti face, veti contracara cu succes tentativa de frauda. Verificarea nu o faceti in niciun caz prin e-mail sau prin mijloace de contact sugerate prin intermediul postei electronice – va sfatuim sa luati legatura in mod direct cu partenerii dvs, prin mijloace sigure si cunoscute (numere de telefon/fax pe care le-ati mai folosit in trecut);
- in situatia in care ati efectuat o plata catre un cont eronat, contactati urgent banca dvs. pentru a putea afla daca mai sunt posibile demersuri de blocare/returnare a sumelor implicate.

De asemenea, va incurajam ca in situatia in care considerati ca ati fost victima unei astfel de tentative de frauda online sa instiintati cat mai rapid si organele de Politie locale, precum si CERT-RO (prin apel la numarul 1911, sau prin email catre : alerts@cert.ro).

B. Recomandari de securitate in utilizarea serviciilor de online banking

Accesati intotdeauna serviciul nostru de **Internet Banking** prin intermediul 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: https://ibkvbr.vistabank.ro/eb/
Verificati ca adresa site-ului sa fie cea corecta, sa fie precedata de **https://**, iar simbolul unui **lacat inchis** sa fie afisat in dreapta sau in stanga adresei web a site-ului, in functie de browserul utilizat, ca in exemplele de mai jos:





Asigurati-va ca instalati aplicatia oficiala de Mobile Banking a Vista Bank Romania 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

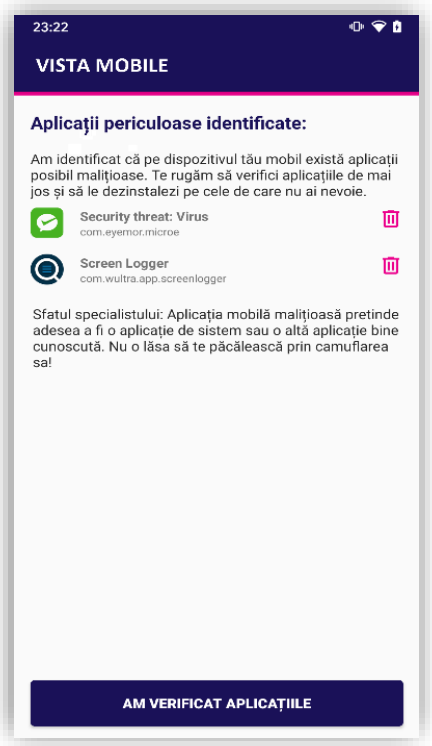
Asigurati-va ca instalati aplicatia oficiala de eToken a Vista Bank Romania doar din urmatoarele locatii de incredere / magazine de aplicatii oficiale:

- (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.

AppShielding si Antivirusul Malwarelytics – functii de Securitate aditionale implementate de Vista Bank pentru a va proteja aplicatiile mobile banking:

Aplicatiile mobile **Vista Mobile Banking** si **Vista eToken** integreaza functionalitatea de securitate **Appshielding**. Aceasta permite celor doua aplicatii sa se auto-protejeze mai bine impotriva unei game largi de atacuri cibernetice sofisticate, precum atacuri malware, vulnerabilitati legate de rooting / jailbreak al device-ului mobil, conexiuni de depanare (debugger), injectarea de Cod Sursa extern sau de Framework,reambalarea aplicatiilor (repackaging) si afectarea integritatii aplicatiei, cititoare de ecran (screen loggers) rau intentionate sau keyboard-uri externe malitioase, atacuri de tip "overlay" (ce se suprapun peste aplicatie), scenarii de atac de tip Man-in-the-App si Man-in-the-Middle, protectia cheii sensibile incorporate (white-box crypto). Ori de cate ori apare o activitate suspecta, App Shielding raspunde luand contramasurile necesare de protectie, impiedicand atacatorii sa modifice aplicatia mobila atat in timpul rularii, cat si in repaus.



Vista Mobile Banking, versiunea Android, integreaza **Antivirusul Malwarelytics** – o functionalitate de securitate ce protejeaza atat aplicatiile mobile Vista Bank, cat si intregul dvs. dispozitiv mobil.
La deschiderea aplicatiei Vista Mobile Banking, versiunea Android, in cazul in care sunt detectate eventuale aplicatii malitioase active pe telefonul sau tableta dvs. (mobile malware), veti fi semnalat de existenta acestora. Din ecranul respectiv aveti si posibilitatea de a le dezinstala imediat, apasand iconita cu cosul de gunoi.

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.

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.

C. Recomandari generale de securitate in mediul online

Sfaturi pentru Securitatea Computerului Dvs:

- Scanati periodic calculatorul pentru a va proteja impotriva virusilor informatici si a altor programe de tip malware utilizand un 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 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 si/sau datele bancare.

Utilizarea sigura a Smartphone-urilor si a Tabletelor:

- Restrictionati accesul la telefon/tableta utilizand un cod PIN, parola sau fingerprint (amprenta digitala);
- Instalati doar aplicatii cu reputatie buna, cu numar mare de descarcari si recenzii pozitive;
- Instalati un software 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.

Navigarea sigura pe Internet:

- Evitati accesarea link-urilor aflate in email-uri ce va redirectioneaza catre alte website-uri care pot imita eventual site-ul bancii. Exista riscul sa introduceti user-ul, parola, token-ul sau codul PIN 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 va 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 laptop-ului sau a smartphone-ului la o retea nesecurizata. Retele WiFi gratuite sunt extrem de 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.