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:
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!
- 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

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;
- 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/tablet.

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 (care genereaza “Parola unica”):

- Tineti intotdeauna Token-ul la dumneavoastra si nu permiteti sa fie accesibil altor persoane;
- Nu divulgati nimanui “Parola unica” generata de Token.