VISTA BANK

Recomandari de securitate pentru utilizarea cardului

Reguli generale de securitate privind cardul si codul PIN

- Verificati integritatea plicurilor continand cardul si/sau codul PIN. Va rugam sa informati imediat banca daca aveti suspiciuni privind integritatea acestora.
- **Nu pastrati niciodata impreuna cardul si codul PIN.** Nu scrieti codul PIN pe card si nici pe alt suport durabil (hartie) pastrat impreuna cu cardul.
- Schimbati de la ATM codul PIN primit initial de la banca sau memorati codul PIN si distrugeti suportul de hartie imediat dupa aceea.
- Nu expuneti cardul surselor electromagnetice, inclusiv celor emise de dispozitivul dvs. mobil (telefon/tableta), intrucat pot afecta negativ functionalitatea microprocesorului de pe card.
- Nu inmanati niciodata cardul si PIN-ul pentru a fi utilizate de catre alte persoane.
- Nu furnizati nimanui numarul cardului, codurile CVV / CVV2, data expirarii, chiar daca solicitarea **pare a proveni** din surse de incredere cum ar fi banca, politie sau entitati de impunere a legii. **Nici banca si nicio alta institutie nu va vor solicita, niciodata, aceste informatii.**
- Verificati regulat extrasul de cont/raportul de activitate card, cel putin lunar, si semnalati imediat bancii orice discrepante identificate.
- Contactati imediat Call Center-ul bancii (numarul de telefon este afisat pe site-ul bancii) si blocati cardul daca l-ati pierdut, nu il mai gasiti sau aveti suspiciuni ca ar fi fost duplicat / clonat in vreun fel.
- **Nu furnizati NICIODATA informatii privind cardul sau datele dvs. bancare atunci cand va sunt solicitate prin e-mail, telefon, SMS sau alte mijloace electronice de comunicare.**

  Fiti foarte atent(a) cand primiti mesaje e-mail prin care vi se solicita sa dezvaluiti date privind cardul dvs, deoarece este foarte posibil sa fie tentative de Phishing (tentative frauduloase de a obtine date personale).

  Mesajele de tip Phishing pot solicita actualizarea, confirmarea sau introducerea datelor privind cardul, cum ar fi numarul de card, data expirarii, codurile CVV/CVV2, parola de autorizare plata, codurile OTP (One-Time Passcode) de autorizare plata trimise prin SMS sau alte informatii personale, prin accesarea unui link care va va redirectiona catre un site fictiv. Atat adresa de pe care este trimis e-mailul, cat si cea a site-ului destinatie pot semana cu cele ale unei institutii/companii de incredere, insa la o privire mai atenta a URL-ului/adresei website-ului de phishing puteti descoperi ca cel putin o litera este diferita (exemplu: goo.gle.com in loc de google.com). Uneori aceste mesaje contin greseli gramaticale, fiind traduse automat din alte limbi si trimise catre un numar mare de detinatori de card.

  In astfel de cazuri, nu dati click pe link-urile incluse si stergeti mesajul respectiv. Anuntati Banca, precum si CERT-RO referitor la orice mesaj de tip phishing sau site de phishing pe care il descoperiti.

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

  De asemenea, astfel de solicitari pot fi transmise si prin SMS (SMSishing) sau telefonic (vishing = voice + phishing).

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

Vista Bank nu va va solicita niciodata sa transmiteti, confirmati sau actualizati date privind cardul prin accesarea unui link transmis prin e-mail sau SMS, respectiv prin conversatii telefonice.

VISTA BANK

Reguli de securitate privind utilizarea cardului la ATM-uri

- Verificati vizual daca vi se pare ceva neobisnuit la ATM. Daca pare sa aiba dispozitive atasate asupra fantei de introducere a cardului sau a tastaturii nu folositi echipamentul. Anulati tranzactia daca ati initiat-o deja si parasiti locatia. Nu incercati niciodata sa indepartati dispozitivele care v-au atras atentia. In acest caz, anuntati imediat banca pentru a putea intreprinde verificarile necesare.
- Protejati vizibilitatea codului PIN in timpul introducerii, blocand campul vizual al altora, stand aproape de ATM si protejand tastatura cu cealalta mana.
- Pe cat posibil, utilizati ATM-uri din zone bine luminate si cu vizibilitate buna.
- Asigurati-va ca celelate persoane de la rand se afla la o distanta rezonabila fata de dvs.
- Nu acceptati ajutorul persoanelor straine care se ofera “sa va ajute” atunci cand ATM-ul prezinta anumite erori.
- Evitati sa deschideti poseta, geanta sau portofelul in timp ce asteptati la rand. Securizati numerarul imediat ce l-ati primit.
- Nu lasati sa va fie distrasa atentia in timp ce operati ATM-ul.
- Asigurati-va ca ati recuperat cardul din ATM si, dupa caz, numerarul solicitat.

Reguli de securitate privind utilizarea cardului la comercianti fizici (plata la POS)

- Protejati vizibilitatea codului PIN in timpul introducerii la tastatura POS (acoperiti cu cealalta mana sau cu un obiect tastatura POS-ului in momentul cand tastati PIN-ul).
- Pastrati cardul tot timpul in posesia dvs. si nu inmanati nimanui cardul chiar daca vi s-ar solicita acest lucru de catre reprezentantul comercial (casier, ospatar etc).
- Cand aveti cardul in mana, asigurati-va ca nu vede nimeni cifrele codului CVV din spatele cardului.
- Pentru fiecare tranzactie, aprobata sau refuzata, trebuie sa primiti chitanta (pe care sa o pastrati la dvs.).
- Asigurati-va ca detineti cardul inainte de a parasi locatia comerciala.
- Pastrati cardul de tip contactless intr-o folie de aluminiu (sau in huse speciale de pastrat cardurile contactless in siguranta) cand nu aveti nevoie sa faceti plata la POS. Astfel, va protejati cardul de posibile tentative ale persoanelor rau-voitoare care se pot apropia de locul in care tineti cardul contactless cu POS-uri frauduloase si va pot extrage sume de bani (pana in 100 Lei) pentru care nu este necesara autorizarea platii prin introducere de PIN. Asigurati-va ca aveti activata Alerta SMS pentru a primi notificari prin SMS cu sumele si comerciantii unde au fost autorizate platile cu cardul dvs., iar in cazul in care nu recunoasteti o tranzactie ca fiind autorizata de dvs., va rugam sa anuntati Banca imediat. (NOTA: Serviciul Alerta SMS se activeaza la solicitarea dvs. in orice sucursala a Bancii).

Reguli de securitate privind utilizarea cardului la comercianti virtuali (e-commerce/tranzactii pe internet)

- Inainte de a efectua o tranzactie, asigurati-va ca respectivul comerciant este certificat sa opereze tranzactii Visa Secure (respectiv site-ul afiseaza logo-ul Visa Secure).
- Incercati sa obtineti in avans, din diferite surse, informatii privind seriozitatea/reputatia comerciantului virtual.
- Invatati sa recunoasteti semnele de conectare la un site sigur: conexiune prin https:// (din adresa URL a website-ului) si certificat valid al website-ului.
- Cititi cu atentie, INAINTE sa efectuati/finalizati o tranzactie, politica comerciantului privind procesarea unei tranzactii, anularea unei tranzactii, livrarea produselor/serviciilor etc, dupa caz, pentru a evita pe cat posibil litigii post tranzactionare.
- Inrolati-va cardul si utilizati aplicatia mobila e-commerce de autorizare a tranzactiilor online cu cardul (Vista 3D Secure) oferita de banca (pentru device-uri mobile cu Android si iOS).
- Atunci cand utilizati aplicatia mobila e-commerce de autorizare a tranzactiilor online cu cardul (**Vista 3D Secure**) oferita de banca, cititi INTOTDEAUNA cu atentie, INAINTE de a aproba tranzactia prin mijloace securizate specifice dispozitivului dvs. mobil (identificare biometrica, alte metode aplicabile), elementele

definitorii ale tranzactiei, cum sunt **denumirea comerciantului, valoarea tranzactiei, moneda tranzactiei** etc, dupa caz.

- **Nu introduceti niciodata codul PIN al cardului pe site-uri din Internet** (doar la ATM sau la POS este necesar PIN-ul, iar Banca nu va solicita niciodata sa comunicati PIN-ul cardului pe site-uri din Internet).
- Protejati-va calculatorul personal si dispozitivele mobile: utilizati programe antivirus si actualizati-le periodic. Nu deschideti atasamentele e-mailurilor primite de la persoane necunoscute si nu dati click pe link-uri. Nu instalati programe si aplicatii necertificate.
- Nu folositi un computer care nu va apartine (ex: la Internet Café, la hotel, la “prieteni” etc) atunci cand initiati tranzactii online cu cardul, deoarece computerul respectiv poate avea deja instalate programe malitioase care va pot fura datele cardului si codurile de autorizare a platilor.