Fraude prin platforme de tranzactionare cu criptoactive

In ultima perioada, in sistemul bancar, s-a inregistrat un numar in crestere de sesizari primite din partea utilizatorilor de servicii de plata, care au devenit victime ale unor faudatori / atacatori ce utilizeaza un anumit scenariu de frauda prin inginerii sociale.

Astfel, dorim sa va atragem atentia asupra riscurilor survenite in urma utilizarii diverselor platforme de tranzactionare cu criptoactive, din mediul online. Mai jos va prezentam modul de operare al fraudatorilor.

Fraudatorii contacteaza presupusa victima, pretinzand ca sunt reprezentanti ai unor platforme de criptoactive si reusesc sa o determine sa ofere informatii sensibile referitoare la datele bancare personale (datele cardului, parole de acces la aplicatiile de plata, coduri OTP primite prin SMS, etc.) si / sau sa instaleze pe telefonul personal aplicatii care le permit fraudatorilor sa acceseze de la distanta dispozitivul acestuia,

Fraudatorii apeleaza victima fie pentru a-i propune sa devină “client”, utilizator al platformei de tranzactionare, sau, daca victima este client existent, pentru a-i comunica profitul înregistrat ca urmare a activitatii de tranzactionare pe platforma respectiva. Au fost identificate doua situatii:

- ✓ sub pretextul consilierii victimei in vederea obtinerii unor castiguri mari cu investitii mici, atacatorii reusesc sa convinga victima sa investeasca in criptoactive si incearca sa o convinga, in cadrul apelului telefonic:
  - (1) sa instaleze pe dispozitivul propriu o aplicatie de tranzactionare cu criptoactive, impreuna cu o aplicatie de tip "control la distanta";
  - (2) sa isi deschida cont pe acea platforma si sa initieze operatiuni de cumparare a criptoactivelor cu scopul de a face legatura in cadrul aplicatiei cu instrumentul de plata al victimei si de a permite initierea de plati ulterioare in cadrul platformei cu respectivul instrument de plata, fara a fi necesara o autorizare suplimentara;
  - (3) sa transmita informatii cu privire la codurile OTP sau alte elemente de autentificare.
- ✓ sub pretextul retragerii profitului inregistrat ca urmare a activitatii de tranzactionare pe platforma dc criptoactive, victima este manipulata sa ofere informatii sensibile privind datele bancare personale (datele cardului, parole de acces la aplicatiile de plata, coduri OTP primite prin SMS, etc.), fie in cadrul apelului telefonic cu atacatorul, fie prin intermediul unui link transmis clientului prin mesaj.

Astfel, fraudatorii / atacatorii obtin acces la conturile de plati ale victimei si ulterior actioneaza in numele acesteia, respectiv efectueaza operatiuni de plata din conturile acesteia.

Pentru a preveni sa fiti victimele atacurilor de tip „Fraude prin platforme de tranzactionare cu criptoactive”, va recomandam să aplicati urmatoarele masuri de securitate:

- ✓ Sa nu divulgati / transmiteti nicio informatie privind datele personale sau cele bancare (datele cardului, parole de acces la aplicatiile de plata, coduri OTP primite prin SMS, etc.).
- ✓ Sa nu dati curs / crezare unor persoane suspecte care va apeleaza promitand oportunitati financiare sau se recomanda ca fiind reprezentati ale unor platforme de tranzactionare cu criptoactive.
- ✓ Sa nu instalati aplicatii la cererea unor persoane suspecte care va apeleaza pentru a va oferi diverse oportunitati financiare sau se recomanda ca fiind reprezentati ale unor platforme de tranzactionare cu criptoactive.

- ✓ Sa nu deschideti / accesati link-uri sau fisiere primite din surse necunoscute / suspecte.
- ✓

Daca aţi devenit victimele atacurilor de tip „Fraude prin platforme de tranzactionare cu criptoactive”, va recomandam sa aplicati imediat urmatoarele masuri:

- ✓ Sa sesizati imediat aceasta situatie Bancii si sa solicitati blocarea si reemiterea cardului, atfel inca sa se evite tranzactiile frauduloase pe contul dvs.
- ✓ Sa sesizati imediat aceasta situatie Bancii si sa solicitati blocarea contului de Internet Banking sau Mobile Banking, atfel inca sa se evite tranzactiile frauduloase pe contul dvs
- ✓ Daca ati suferit deja pagube materiale, sa depuneti plangere la Politie si sa completati formularul de refuz la plata la Banca.
- ✓ Sa aveti in vedere recomandarile Bancii privind securitatea serviciilor pe Internet, postate pe website-ul Bancii: https://www.intesasanpaolobank.ro/document/documents/ISPROMANIA/utile/ghid-securitatea-platilor-pe-internet.pdf