ROMÂNIA
MINISTERUL AFACERILOR INTERNE
INSPECTORATUL GENERAL AL POLIȚIEI ROMÂNE

INSPECTORATUL DE POLIȚIE JUDEȚEAN BRAȘOV
BIROUL ANALIZA ȘI PREVENIREA CRIMINALITĂȚII

ATENȚIE la fraudele cu CRIPTOMONEDE!

Noi metode de înșelăciune, prin tranzacționarea de criptomonede!

Victimele sunt abordate prin mesaje email/pop-up sau pe rețelele de socializare de către "reprezentanți" ai unor persoane publice/societăți binecunoscute, fiindu-le prezentate oferte de nerefuzat cu câștiguri rapide importante, printr-o minimă investiție, în tranzacționarea de criptomonede.

Sunt folosite site-uri scam de tranzacționare a criptomonedelor, controlate de societăți comerciale din paradisuri fiscale.

Conving persoanele vulnerabile să descare pe telefon/calculator, laptop, etc, diferite **aplicații de control la distanță (ex. Anydesk, TeamViewer)**, sub pretextul unei comunicări mai eficiente și ajutor în domeniul tehnic.

Ulterior, victimele cumpără criptomonede prin procesarea unor plăți sau direct de pe crypto exchange-uri și le transmit în portofele electronice controlate de infractori.

Astfel, sunt induse în eroare asupra unor câștiguri importante și pentru a retrage "câștigul" li se solicită ca și taxe cu titlu de comision/tranzacționări bancare, până victima rămâne fără fonduri disponibile.

Fraudele pot merge mai departe, deoarece unii infractori anticipează mișcările victimelor, reușind să creeze site-uri care pretind că pot recupera prejudiciul în schimbul unui comision procentual din suma pierdută inițial.

Pentru a nu deveni victimă a infracțiunilor cibernetice, Poliția Brașov vă recomandă să:

- ignorați e-mailurile, mesajele private sau campaniile promovate pe rețelele de socializare prin care vă sunt garantate câștiguri ușoare;
- închideți fără ezitare apelurile care vă informează despre "oferte de creditare de nerefuzat", "investiții cu profituri garantate";
- nu transmiteți datele personale sau copii ale documentelor de identitate prin intermediul rețelelor de socializare, e-mail, etc.;
- nu completați datele cardului și nici credențialele aplicației de internet banking pe paginile (link-urile) primite de la așa zișii brokeri de investiții;

- nu instalați aplicații care oferă acces la distanță, la cererea persoanelor care vă abordează, pe dispozițivele utilizate. Nu oferiți acces la dispozitivele dvs (remote/screensharing)!
- nu accesați link-urile primite prin e-mailuri care solicită actualizarea informațiilor personale, entitățile legitime nu vă vor solicita niciodată furnizarea sau verificarea unor informații sensibile printr-un mijloc nesigur (precum e-mailul).

Dacă ați fost victima unei infracțiuni, sesizați cea mai apropiată unitate de poliție și puneți la dispoziția polițiștilor cât mai multe informații și dovezi!