ROMÂNIA
MINISTERUL AFACERILOR INTERNE
INSPECTORATUL GENERAL AL POLIȚIEI ROMÂNE

INSPECTORATUL DE POLIȚIE JUDEȚEAN BRAȘOV
BIROUL ANALIZA ȘI PREVENIREA CRIMINALITĂȚII

CAMPANIA DE PREVENIRE A FRAUDELOR INFORMATICE CARE AU CA MOD DE OPERARE INVESTIȚIILE ONLINE ÎN ACȚIUNI/CRIPTOMONEDE !

Fraudele și manipulările online au cunoscut o creștere semnificativă în ultima perioadă, concretizate în cazuri de extorcare și phishing, dar și site-uri clonate care fură date financiare sau platforme false de investiții care vizează atât persoanele vulnerabile, cât și familiile și apropiații acestora.

Pentru prevenirea victimizării ca urmare a fraudelor informatice care au ca mod de operare investițiile online în acțiuni/criptomonede, Poliția Română continuă campania de informare la nivel național.

Diversificarea modurilor de operare și utilizarea tot mai frecventă a tehnologiei de tip Inteligența Artificială pentru crearea și promovarea de platforme false de investiții online în acțiuni/criptomonede, care folosesc nelegitim imaginea unor personalități/companii cunoscute, impun continuarea și dezvoltarea activității de prevenire a împșelăciunilor și transmiterea de mesaje de conștientizare și informare în masă.

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.

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.

Reclamele de tip **phishing** cu oferte de neratat funcționează astfel:

- ***Oferte tentante*** : Atacatorii creează reclame care promit produse sau servicii la prețuri extrem de reduse, atrăgând utilizatorii.
- ***Site-uri false***: Reclamele duc la site-uri web care imită site-uri legitime, unde utilizatorii sunt încurajați să introducă date personale sau financiare.
- ***Capturarea informațiilor:***Datele colectate sunt trimise către atacatori, care le folosesc pentru fraude financiare sau furt de identitate.
- ***Evitarea detectării***: Site-urile false sunt adesea active pentru scurt timp sau folosesc redirecționări și tehnici de mascare.
- Printr-o simplă verificare a link-ului cu o soluție de securitate disponibilă online gratis (**virustotal.co, scamadviser.com**) puteți observa ce se afă de fapt în spatele mesajului/reclamei!

Pentru a nu deveni victimă a fraudelor informatice care au ca mod de operare investițiile online în acțiuni/criptomonede, Poliția Brașov vă recomandă să:

- 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.;
- Ignorați e-mailurile, mesajele private sau campaniile promovate pe rețelele de socializare prin care vă sunt garantate câștiguri ușoare;
- 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!