București, 22 decembrie 2023

#SigurantaOnline: Nu accesați și nu promovați anunțurile care promit câștiguri fabuloase

Poliția Română, Directoratul Național de Securitate Cibernetică (DNSC) și Asociația Română a Băncilor (ARB) atrag atenția asupra fraudelor legate de investiții financiare, în cadrul Proiectului Național de prevenire a criminalității informatice și educație digitală #SigurantaOnline (sigurantaonline.ro).

În ultimele luni, atacatorii folosesc intens rețelele de socializare ca metodă de propagare a unor tentative de fraudă cu propuneri false de investiții. În cadrul acestei inițiative frauduloase, se folosesc de conturi sau pagini de social media compromise, ori unele nou create, de pe care lansează reclame sponsorizate, în care includ clipuri alterate cu tehnologia *deepfake* și construite într-o manieră în care personajele din clip par că promovează un „program național de îmbogățire".

Pentru a fi convingători și a avea o rată cât mai mare de succes în rândul potențialelor victime, atacatorii folosesc deopotrivă imaginea unor companii și persoane cunoscute din România (televiziuni, oameni de afaceri, demnitari, vedete TV sau jurnaliști). În reclamele promovate pe social media, se folosește, totodată, imaginea unor companii cunoscute, pentru câștigarea încrederii cu privire la legitimitatea ofertei - câștiguri imediate foarte mari prin „cumpărarea de acțiuni" care vor „genera dividende" de zeci de mii de lei. Companiile a căror imagine este folosită, fără drept, sunt în cele mai multe cazuri din domeniul energetic. În astfel de cazuri, atacatorii folosesc link-uri de *phishing*, cu ajutorul cărora încearcă să obțină datele personale și financiare. Aceste atacuri se înscriu în așa-numitele *Fraude cu investiții - investment frauds*, care reprezintă scheme frauduloase prin care investitorilor potențiali li se promit oportunități de investiții extrem de profitabile, dar care, în realitate, nu există.

Atunci când întâlniți astfel de anunțuri, vă recomandăm să nu accesați link-urile, să nu furnizați date personale, bancare și să verificați temeinic toate ofertele de investiții prin accesarea site-urilor oficiale ale companiilor a căror imagine este folosită pentru promovarea lor. De asemenea, vă recomandăm să verificați cu atenție link-urile și platformele prin intermediul cărora se cer date personale și financiare pentru investiții, prin compararea cu adresele oficiale de internet ale companiei a cărei imagine este utilizată în anunțul de pe rețelele de socializare, dar și verificarea ofertanților pe site-ul Autorității de Supraveghere Financiară - ASF.

O altă capcană des întâlnită în ultimele luni folosește ca metodă de propagare aplicații de mesagerie. Concret, utilizatori din România primesc mesaje nesolicitate pe aceste platforme, prin care li se oferă șansa de a câștiga bani rapid și ușor. După ce execută câteva sarcini simple, care de obicei presupun aprecierea (*like*), în faza inițială, a unui număr de clipuri video, utilizatorii primesc în conturile personale sume modice de bani.

Încurajați de faptul că pot face bani pe termen scurt prin acțiuni simple, utilizatorii sunt redirecționați către grupuri de conversație, unde vor discuta 1 la 1 cu atacatori deghizați în specialiști în investiții. În acest mod, utilizatorii sunt convinși să achiziționeze „pachete promoționale" care le-ar facilita un câștig mult mai consistent pentru fiecare *like*. În continuare, folosindu-se de tehnici de inginerie socială, atacatorii vor încerca extragerea de la potențialele victime a unor date sensibile (personale, de autentificare, dar și financiare), precum și sume

importante de bani. Ei încearcă să atingă acest obiectiv prin folosirea aceluiași pretext – „investiții" generatoare de profit pe termen scurt - pentru a motiva necesitatea ca potențiala victimă să furnizeze date sensibile, să se aboneze la anumite servicii, să deschidă noi conturi sau chiar, în unele cazuri, să instaleze aplicații malițioase. Datele respective ajung de fiecare dată în posesia atacatorilor.

Metode de a te proteja de fraudele legate de investiții:

- Asigură-te că verifici din mai multe surse (nu doar cele furnizate de atacatori) orice propunere de investiție cu un câștig mare de la persoane necunoscute. Câștigurile mari pot ascunde o fraudă;
- Raportează tentativele de fraudă prin anunțuri sponsorizate către rețeaua de socializare unde este promovat conținutul fraudulos;
- Mare grijă la mesajele nesolicitate pe e-mail sau în social media prin care se oferă câștiguri rapide sau mari. Nu accesa link-urile de pe platformele de socializare care promit câștiguri masive de bani, într-un termen scurt de timp;
- Nu comunica și nu întreține o relație cu reprezentanți ai platformelor financiare, când se arată foarte insistenți și exercită presiuni pentru a te determina să investești;
- Instalează aplicații pe telefon/calculator doar din surse oficiale;
- Asigură-te că ești singura persoană care are acces la aplicațiile/site-urile de investiții, nu și persoana care ți-a vorbit de investiții;
- Nu furniza niciodată altor persoane datele personale sau bancare (cont, user, parola Mobile/Internet banking, numărul cardului, codul de securitate de pe spatele cardului etc.);
- Atunci când primești un e-mail sau un mesaj din surse necunoscute, nu îi răspunde și nu accesa link-uri din conținutul acestuia;
- Dacă crezi că ai fost înșelat sau ai furnizat datele bancare altor persoane, anunță imediat banca la care ai conturile, Poliția și DNSC.

Proiectul de prevenire a criminalității informatice și educație digitală *#SiguranțaOnline* este menit să ofere cele mai bune practici de securitate cibernetică, prin accesarea platformei *sigurantaonline.ro*, pentru a evita ca utilizatorii de internet să devină victime ale fraudelor informatice, ale pornografiei infantile sau ale atacurilor de tip malware. #SigurantaOnline este o inițiativă a Poliției Române, Directoratului Național de Securitate Cibernetică și Asociației Române a Băncilor.