INSPECTORATUL DE POLIȚIE JUDEȚEAN
B R A Ş O V
BIROUL ANALIZA ŞI PREVENIREA CRIMINALITĂŢII

Atenție la fraudele informatice!
-Shema votului online -

În contextul actual al amenințărilor cibernetice, Poliția Română a identificat o tendință de înșelăciune care se răspândește rapid prin intermediul aplicațiilor de mesagerie.

În special, una dintre aplicațiile de mesagerie a devenit un teren fertil pentru autorii care caută să exploateze încrederea și naivitatea utilizatorilor.

Cum funcționează schema de înșelăciune? Sub pretextul simplu al ***„exprimării unui vot online în cadrul unui concurs”,*** autorii încearcă să atragă utilizatorii într-o schemă de înșelăciune în mediul online.

Astfel, infractorii îndeamnă victimele să acceseze un link pentru a acorda ajutor (în sensul de a-i acorda un vot în cadrul unui sondaj) unei persoane pe nume “X”, care participa la un concurs de dans al cărui premiu era o bursă de studii la o școală de prestigiu din străinătate. Mesajul ar arăta astfel: „*Bună! Te rog să o votezi pe “X” în acest sondaj. Este fiica prietenei mele, iar premiul este o bursă pentru studii în străinătate. Mulțumesc mult!*” urmat de un link malițios. În etapa următoare, după ce accesează respectivul link, potențialele victime sunt redirecționate către pagina web a aplicației de mesagerie, care permite configurarea și conectarea contului aferent aplicației și pe alte dispozitive electronice, precum alte telefoane mobile, unități pc sau laptop-uri.

Autorii efectuează demersurile necesare în vederea configurării contului aferent aplicației de mesagerie al victimei, prin intermediul platformei web, pe alte dispozitive electronice controlate de aceștia, folosind una dintre opțiunile existente, respectiv **„Conectează-te folosind numărul de telefon”**. Astfel, utilizând acea opțiune, autorii introduc o solicitare de asociere pe alte dispozitive a contului aferent aplicației de mesagerie al potențialei victime, prin introducerea numărului de telefon al acesteia.

Pentru a finaliza conectarea contului la dispozitivele electronice utilizate de autori, este necesar ca potențiala victimă (titularul contului aplicației de mesagerie) să introducă pe telefonul său mobil (pe care se afla deja configurat contul) un cod pin din 8 caractere (alcătuit de regulă din litere și cifre), cod unic generat de serviciul aplicației de mesagerie la momentul fiecărei solicitări de conectare pe alte dispozitive, solicitare introdusă în acest caz de autori și nu de titularul contului aplicației de mesagerie.

Tot în cadrul aplicației de mesagerie, autorul transmite mesaje în mod aleatoriu către diverse persoane din agenda victimei, prin care le solicită acestora, cu ***titlu de împrumut, diverse sume de bani***.

În măsura în care acestea din urmă dau curs solicitării, autorii le comunică mai departe un cod IBAN și numele titularului contului bancar unde trebuie virați banii, titularul contului fiind altul decât persoana de la care se presupune că provine solicitarea sumei de bani cu titlu de împrumut, respectiv titularul contului aplicației de socializare.

De asemenea, în cazurile în care persoanele cărora li se solicită sume de bani observă acest aspect, respectiv că numele titularului contului este diferit de numele celui care se

presupune că solicită sumele de bani, autorii motivează prin faptul că le-a fost blocat contul personal și trebuie să facă o plată exact către acel cont bancar comunicat.

Acest mod de operare se bazează pe mai mulți factori, printre care putem aminti:

1. Încrederea utilizatorilor: Autorii profită de naivitatea și dorința de a ajuta a oamenilor, folosind pretexte credibile.

2. Lipsa de informare: Mulți utilizatori nu sunt conștienți de riscurile asociate cu phishing-ul și nu recunosc semnele unei fraude.

3. Urgența și presiunea socială: Mesajele trimise de infractori pot crea un sentiment de urgență, făcând presiuni asupra victimelor să acționeze rapid fără a verifica autenticitatea solicitării.

4. Prin intermediul acestor activități infracționale, în unele cazuri, autorii, având acces la toate conversațiile purtate de victime prin aplicația de mesagerie, reușesc să obțină și alte date personale ale victimelor, existente în cadrul conversațiilor purtate de regulă cu persoane de încredere sau rude, prin aplicație, cum ar fi **date de identificare, financiare ori de autentificare la alte aplicații folosite**, expunându-le, totodată, și la alte riscuri, mai exact utilizarea datelor în vederea săvârșirii altor infracțiuni sau crearea altor pagube în sarcina acestora sau cunoscuților.

Pentru a evita victimizarea, Poliția Brașov recomandă:

1. **Evitați accesarea link-urilor suspecte** sau cele din mesajele nesolicitate sau din surse necunoscute, deoarece acestea ar putea conduce către site-uri malware sau ar putea fi utilizate pentru phishing.
2. **Nu introduceți informații sensibile**: Niciodată nu introduceți coduri sau informații personale pe site-uri care nu sunt oficiale sau pe care nu le recunoașteți. De asemenea verificați dacă site-urile pe care sunteți redirecționați sunt oficiale și nu introduceți coduri sau alte date personale pe aceste site-uri dacă dumneavoastră nu ați efectuat nicio solicitare în acest sens, precum este descrisă pe site-ul accesat.
3. **Nu introduceți coduri nesolicitate aferente conectării/asocierii contului dumneavoastră de pe aplicația de mesagerie sau al altor canale de comunicare online pe alte dispozitive electronice dacă nu le-ați solicitat dumneavoastră.**
4. **Folosiți metode alternative de comunicare**: Dacă primiți un mesaj suspect de la un prieten, contactați-l printr-un alt canal (de exemplu, telefonic) pentru a verifica autenticitatea solicitării.
5. **Sesizați infracțiunile**: Dacă ați fost victima unei astfel de fraude sau ați observat activități suspecte, contactați imediat autoritățile competente și sesizați incidentul.
6. **Informați-vă** despre tehnicile de fraudă și tacticile utilizate de autorii infracțiunilor informatice și **fiți mereu vigilenți în mediul online**. De asemenea, discutați cu familia și prietenii despre aceste tipuri de fraude pentru a-i ajuta să se protejeze.
7. **Folosiți autentificarea în doi pași,** aceasta adăugând un nivel suplimentar de securitate la conturile dumneavoastră online, solicitând o parolă suplimentară sau un cod de verificare înainte de a vă conecta;