O NOUĂ METODĂ DE ÎNȘELĂCIUNE A APĂRUT ÎN SPAȚIUL 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.

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.

Activitatea infracțională începe cu primirea de către utilizatori a unor mesaje nesolicitate, formulate în limba română, care îi îndeamnă să acceseze un link pentru a acorda ajutor (în sensul de a-i acorda un vot în cadrul unui sondaj) unei persoane pe nume Adeline, care participa la un concurs de dans al cărui premiu era o bursă de studii la o școală de prestigiu din străinătate.

Mesajul arăta astfel: „Bună! Te rog să o votezi pe Adeline în acest sondaj. Este fiica prietenei mele, iar premiul este o bursă pentru studii în Franța. 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.

În prealabil, anterior trimiterii link-ului menționat către potențialele victime, 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, folosind 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.

După acest demers, pentru a determina potențialele victime să introducă acel cod pin, autorii le creează iluzia (prin link-ul expediat, precizat mai sus) că vor exprima un vot într-un sondaj, iar pentru aceasta este necesară o presupusă asociere a contului aplicației de mesagerie deși, în fapt, acestea erau redirecționate către pagina web accesată anterior de autor pe dispozitivul său electronic pe care dorea să-și configureze contul aplicației de mesagerie al potențialei victime.

În fapt, asocierea contului victimei se efectua cu dispozitivul electronic controlat de autor și nu pentru presupusa participare în cadrul unui sondaj.

Pe această pagină web, aferentă serviciului de mesagerie, potențialei victime îi erau prezentați pașii pe care trebuia să-i urmeze pentru asocierea contului, după cum rezultă și în imaginea de mai jos.

Astfel, aceasta este îndrumată să deschidă aplicația pe telefonul său mobil și, în final, să introducă acel cod pin unic, generat de serviciul de mesagerie al aplicației, fără ca victima să conștientizeze că, în fapt, prin introducerea acelui cod pin va asocia contul său pe alte dispozitive electronice necunoscute, controlate de autori.

Ulterior, după ce victima introduce codul PIN generat, autorul finalizează astfel configurarea și conectarea contului victimei pe dispozitivul său electronic, după care restricționează accesul victimei la contul său.

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.

Prin acest mod de operare, autorii reușesc astfel inducerea în eroare, în primă fază, a titularului contului aplicației de socializare asupra căruia preiau controlul și îi restricționează accesul la contul său, prin crearea iluziei că participă la un sondaj.

Astfel, acesta introduce codul pin generat de serviciul de mesagerie ca urmare a solicitării efectuate în prealabil de autori de asociere a contului de pe aplicația de socializare cu alte dispozitive și le permite astfel acestora să-i configureze și conecteze contul personal pe alte dispozitive electronice controlate de aceștia.

Mai departe, în a doua fază, autorii induc în eroare persoane din agenda telefonică a victimei inițiale solicitându-le sume de bani, cu titlu de împrumut, în numele acesteia, creând aparența faptului că solicitările ar proveni din partea victimei, prin urmare o persoană cunoscută, determinându-le astfel să remită sume de bani în conturi bancare controlate de autori.

Facem precizarea că 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 proteja cetățenii împotriva acestor tipuri de infracțiuni, este necesar să fie conștienți de modurile de operare ale autorilor și educați în mod constant cu privire la tacticile de manipulare ale acestora, noile moduri de operare precum și la tehnicile de protecție în mediul online.

Îndemnăm cetățenii să fie extrem de precauți și să evite orice interacțiune cu mesaje sau link-uri suspecte pe aplicațiile de comunicare online sau platformele de socializare.

La nivelul țării noastre, au fost înregistrate o serie de fapte cu acest mod de operare, iar pentru o mai bună prevenție, cetățenii trebuie să se protejeze în mediul online și astfel, recomandăm să aibă în vedere mai multe măsuri de contracarare, după cum urmează:

1. Nu accesați link-uri din mesaje nesolicitate, chiar dacă acestea par a proveni de la prieteni sau cunoștințe.

2. 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.

3. 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.

4. 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.

5. 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.

6. Sesizați infracțiunile: Dacă ați fost victima unei astfel de fraude sau ați observat activități suspecte, contactați imediat autoritățile competente și sesizați incidentul.

7. Educați-vă și educați-i pe alții: 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.

8. 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;

9. Fiți la curent cu cele mai recente amenințări cibernetice și cu modalitățile de protejare împotriva acestora, participând la cursuri de pregătire sau consultând resurse online de încredere;

Securitatea dumneavoastră online este esențială. Vă rugăm să rămâneți vigilenți și să acționați cu prudență pentru a evita să deveniți victime ale acestor infracțiuni.

Comunitatea educată este mai rezistentă la amenințările cibernetice!