ROMÂNIA

MINISTERUL AFACERILOR INTERNE
INSTITUŢIA PREFECTULUI – JUDEŢUL BACĂU
Comitetul Consultativ de Dialog Civic pentru
Problemele Persoanelor Vârstnice
Nr. SD 9555 din 13.06.2025

ORDINEA DE ZI

a şedinţei Comitetul Consultativ de Dialog Civic pentru Problemele Persoanelor Vârstnice

Locul de desfăşurare: Noua locaţie a sediului Instituţiei Prefectului – judeţul Bacău, Centrul de Afaceri şi Expoziţii Bacău (PAVILIONUL 2, etajul 1).

Data : 25 iunie 2025, ora: 13.00

1. **Vigilența face diferența! Noi forme de fraudă online îndreptate împotriva persoanelor vârstnice.**
   Prezinta : Inspectoratul de Poliţie Judeţean Bacău
2. Diverse

Cu deosebită considerație,

P R E F E C T,
Claudiu-Augustin ILIŞANU

Ilisanu Claudiu-Augustin
Digitally signed by Ilisanu Claudiu-Augustin
Date: 2025.06.17 10:51:07 +03'00'

SUBPREFECT,
EMILIA GAL

SERVICIUL MONITORIZAREA SERVICIILOR PUBLICE DECONCENTRATE, SITUAŢII DE URGENŢĂ ŞI AFACERI EUROPENE,
ŞEF SERVICIU,
Sorina NASTASĂ

Întocmit,
Donici Ştefan

Vigilența face diferența!
Noi forme de fraudă online îndreptate împotriva persoanelor vârstnice

Criminalitatea în mediul digital reprezintă un fenomen în continuă expansiune, alimentat de avansul rapid al tehnologiei și de creșterea dependenței societății de internet. De la furtul de date personale și financiare, până la escrocherii complexe derulate prin rețele sociale, e-mailuri sau aplicații de mesagerie, infracțiunile cibernetice afectează persoane, companii și instituții deopotrivă. Într-un context în care mulți utilizatori nu dețin cunoștințele necesare pentru a se proteja eficient, în special persoanele vârstnice, criminalii informatici exploatează vulnerabilitățile tehnice și emoționale, provocând pierderi financiare semnificative și traume psihologice.

- **Spoofing** – este o tehnică de înșelăciune prin care un atacator își modifică numărul de telefon, astfel încât să apară ca și cum apelul provine de la un alt număr de telefon. Această metodă este utilizată pentru a induce în eroare victima, determinând-o să creadă că interlocutorul reprezintă o entitate legitimă, cum ar fi o bancă sau o altă instituție, fiind folosită pentru a obține informații personale sau bancare sensibile.

Atacatorii sună și pretind că reprezintă diverse bănci, informând potențiala victimă că are bani de primit de la Fondul Proprietatea. Tactica este foarte subtilă, victimele fiind asigurate că nu le se solicită date bancare, ci doar să precizeze banca la care dețin cont. După câteva minute, sunt contactate din nou, aparent de sucursala băncii respective, pentru verificări de identitate. În realitate, bancile sau alte instituții financiare serioase nu cer date personale, mai ales prin telefon, fără un motiv clar și fără ca dumneavoastră să inițiați contactul.

Este important de reținut că instituțiile bancare sau societățile comerciale nu vor solicita niciodată informații personale sau coduri de securitate prin telefon sau mesaje SMS! Dacă aveți îndoieli cu privire la legitimitatea unui apel sau mesaj, contactați direct instituția bancară sau societatea comercială în cauză, folosind numerele de contact oficiale.

- **Deepfake - când realitatea devine iluzie digital**

Tehnologia deepfake utilizează inteligența artificială pentru a crea conținut audio, video sau imagini aparent autentice, dar complet fabricate. Aceste materiale pot fi folosite pentru dezinformare, șantaj sau manipulare a opiniei publice.

Semne că un material ar putea fi deepfake:

- Mișcări ale buzelor nesincronizate cu sunetul
- Imperfecțiuni faciale (de exemplu, clipire neregulată, trăsături distorsionate)
- Anomalii în iluminare sau umbre
- Lipsa detaliilor naturale (cum ar fi dinții sau limba)

- **Metoda votului online**

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.

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. 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.

- **Metoda investițiilor**

Prin această metodă, infractorii folosesc elementele de brand ale unor entități (companii mari precum Romgaz, Hidroelectrica, Enel, Petrom ș.a.), pentru a-i atrage pe oameni aparent să investească în aceste direcții, prin intermediul unor reclame pe rețelele de socializare; în fapt, urmăresc să le obțină datele personale și identitatea pentru a le sustrage bani din conturile bancare.

Modul de operare al acestei fraude poate varia, dar, de obicei, începe cu contactarea telefonică a cetățenilor, transmiterea de mesaje pe rețelele de socializare sau postarea de anunțuri online și promovarea unei investiții care este legată de compania, firma sau banca pe care aceștia pretind că o reprezintă, pentru a-i face pe oameni să creadă că investiția este sigură și profitabilă.

Pentru a-i convinge pe oameni să investească, bănuiții folosesc diverse tactici, cum ar fi prezentarea de declarații false, asigurări despre profituri rapide și mari, manipularea emoțională sau presiunea de a lua o decizie rapidă și neîntârziată, precum și site-uri realizate foarte bine vizual și tehnic, care fie sunt noi, fie imită site-uri adevărate, pentru a convinge potențialii clienți de veridicitatea investițiilor.

Astfel, cetățenii sunt determinați să alimenteze/ să investească, prin efectuarea de transferuri financiare către conturile indicate, controlate de către bănuiți, atât bancare, cât și nonbancare (criptomonede), de pe diverse platforme (Wise, Revolut, Binance, MoonPay ș.a.), uneori fiindu-le chiar afișate pe profilul personal de pe site-ul fals/fraudulos valori pe profit (neadevărate).

În unele cazuri, aceste asigurări despre profituri rapide și mari sunt utilizate mai apoi de autori pentru a-i convinge să accepte să primească sume de bani în conturile personale de la bănci, sau în conturi pe care le creează autorii în numele „clienților", de la alți „investitori" care ar fi atins deja diferite plafoane și nu mai pot efectua operațiuni, ultimii fiind de fapt tot victime ale acestei modalități de înșelăciune.

Având în vedere și nepriceperea clienților de a înțelege și executa diferite comenzi pe telefon, tot suportul este acordat de către „experții financiari" telefonic-audio de la diferite numere, fie prin aplicații de chat, fie a altora care afișează numere neadevărate (apărând numere de fix din țară sau din străinătate), cât și prin intermediul unor aplicații de control de la distanță precum AnyDesk, AirDroid sau TeamViewer, dispozitivele mobile fiind controlate tendențios de autori pe parcursul sesiunilor, pentru accesarea sau crearea conturilor pe aplicații sau la bănci, la unele dintre acestea fiind ulterior și blocat accesul pentru a preîntâmpina clienților retragerea banilor transferați fraudulos.

- **Metoda „Generalul american"**

Această metodă presupune contactarea victimelor pe rețelele de socializare, escrocii pretinzând că au funcții importante în armata americană. Odată câștigată încrederea, celor contactați li se promite o relație amoroasă. Apoi încep și cererile de împrumuturi.

Victimele sunt, de obicei, persoane cu puțină experiență în lumea virtuală.

- **Metoda „Moștenirea"**

Escrocii din mediul online profită de orice ocazie pentru a face bani pe seama persoanelor credule. O altă metodă pe care aceștia o folosesc este metoda „moștenirii". Persoanele primesc diferite mail-uri în care sunt informați că o bancă din străinătate (ex. Istanbul) este în căutarea moștenitorului unui milionar în dolari, care ar fi murit după ce s-a îmbolnăvit de virusul COVID-19. Hackerii solicită

oamenilor doar să trimită datele personale la o adresă indicată de aceștia. Mesajele sunt generate automat, dar sunt personalizate în funcție de numele fiecărei victime.

Mesajele încep, de obicei, prin a spune că moștenitorul a fost găsit cu ajutorul profilului de Facebook, iar instituția bancară îl contactează pe mail pentru a stabili detaliile legate de bani. Escrocii mai folosesc și fraze precum „A fost dorința lui Dumnezeu să te găsesc", persoanele foarte credincioase putând cădea în plasă mai ușor.

Recomandări

- ✓ Verificați întotdeauna identitatea apelantului;
- ✓ NU oferiți date personale, bancare sau parole prin telefon;
- ✓ NU răspundeți la apeluri din afara țării, mai ales dacă nu cunoști persoanele din țările respective.
- ✓ Raportați orice apel suspect autorităților competente;
- ✓ Actualizați constant software-ul și aplicațiile instalate pe dispoztivele dvs;
- ✓ Mergeți direct la bancă dacă primiți apeluri suspecte;
- ✓ Verificați online numerele de telefon necunoscute, înainte de a intra în discuții;
- ✓ NU transmiteți date personale sau copii ale actelor de identitate prin intermediul rețelelor sociale sau prin link-uri primite pe e-mail sau prin aplicații de mesagerie;
- ✓ NU răspundeți la mesaje nesolicitate sau neașteptate care vă propun câștiguri;
- ✓ NU acceptați oferte de muncă de la societăți ce nu pot fi verificate sau de la persoane ce comunică doar prin intermediul aplicațiilor de mesagerie online. Propuneți întotdeauna o întâlnire față în față;
- ✓ NU transferați persoanelor necunoscute sume de bani la îndemnul unor persoane necunoscute sub promisiunea unor câștiguri imediate fără a presta o activitate lucrativă;
- ✓ NU acceptați sume de bani provenite de la persoane necunoscute. Informați de îndată unitatea bancară la care ați deschis cont despre încasări nejustificate.
- ✓ Sesizați de îndată unitatea bancară despre sume de bani ce au fost transferate fără acordul dvs.;
- ✓ NU oferiți accesul peroanelor necunoscute la telefonul mobil sau la computerul personal prin aplicații de tip AnyDesk sau TeamViewer.
- ✓ NU vă logați în aplicația de Internet/Mobile Banking printr-un link primit prin SMS sau e-mail. Intrați în aplicațiile sau platformele oficiale și securizate ale băncii;