



Poliția Română, DNSC, ARB și Mastercard lansează campania națională „Uniți împotriva escrocheriilor”

Inițiativa încurajează consumatorii să recunoască și să evite mai ușor diferitele tipuri de înșelătorii, prin exemple reale, educație și instrumente de prevenire

București, 24 martie 2026 – Poliția Română, Directoratul Național de Securitate Cibernetică (DNSC), Asociația Română a Băncilor (ARB) și Mastercard lansează „Uniți împotriva escrocheriilor”, o campanie Siguranța Online, ca răspuns la evoluția tot mai rapidă a înșelătoriilor comise prin telefon, SMS sau online. Inițiativa își propune să facă vizibile scenariile folosite de infractori pentru ca aceste tentative de fraudă să fie mai ușor de prevenit, în special pentru publicul 60+, ajutând oamenii să recunoască și să evite mai rapid capcanele. Campania creează un ecosistem sigur și colaborativ, în care autoritățile publice, instituțiile financiare și consumatorii împărtășesc informații despre tiparele de înșelătorii, pentru a le putea preveni mai eficient. Toate aceste resurse sunt disponibile pe www.sigurantaonline.ro/uniti-impotriva-escrocheriilor

„Creșterea siguranței în mediul online este o responsabilitate comună și o prioritate instituțională. În cadrul acestei campanii, acordăm o atenție deosebită persoanelor vârstnice, o categorie poate vulnerabilă în fața provocărilor online, dar care merită să se bucure de beneficiile lumii digitale fără teamă. Ne dorim să le oferim sprijinul necesar pentru a recunoaște pericolele și a se proteja de noile forme de înșelăciune online. Experiența lor de viață este o resursă valoroasă, iar misiunea noastră este să o completăm cu siguranță, încredere și protecție. Împreună, putem construi un spațiu digital mai sigur pentru fiecare”, a declarat Raluca-Claudia Seucan, director al Institutului de Cercetare și Prevenire a Criminalității din cadrul IGPR.

Campania „Uniți împotriva escrocheriilor” vine într-un context în care tot mai mulți români au fost expuși la mesaje suspecte, promisiuni de câștiguri rapide sau apeluri alarmante din partea unor presupuse rude aflate în dificultate sau preținși reprezentanți ai autorităților. Conform datelor DNSC, față de anul anterior, numărul fraudelor aproape s-a dublat în 2025. Phishingul a rămas cea mai utilizată metodă și este deopotrivă în creștere cu peste 70% față de 2024.

“Scopul nostru este să ajungem cu acest pachet de informații esențiale pentru protecția împotriva fraudelor la cât mai mulți utilizatori. Uneori există o barieră de limbaj pentru anumite categorii de vârstă, care transformă tehnologia și utilizarea dispozitivelor într-un demers mai complicat decât este de fapt. Dacă vorbim mai des și sincer despre capcanele pe care le întâlnim în mediul digital, fără o terminologie complicată, vom fi mai pregătiți să recunoaștem scenariile pe care atacatorii ni le servesc, astfel încât să nu devenim victime. Putem construi o rutină de securitate care să funcționeze ca un antivirus uman, bazată pe anumite reflexe de securitate pe care le putem dobândi din astfel de testimoniale ale unor oameni care au pățit-o.”, a declarat Mihai Rotariu, Manager Direcția Comunicare DNSC.

Dincolo de statistici, campania propune o schimbare de perspectivă: umanitatea în fața tehnologiei

Tehnologia joacă astăzi un rol dublu, contribuind la prevenirea și combaterea înșelătoriilor, dar este folosită tot mai des de infractori, care pot imita voci sau chipuri familiare cu ajutorul inteligenței artificiale. În acest context, campania pune accentul pe educație și pe însușirea unor mecanisme simple care îi ajută pe oameni să recunoască din timp potențialele fraude. De aceea, campania reunește într-un singur loc tipare, tactici și exemple concrete, astfel încât consumatorii să poată identifica și evita aceste înșelătorii fără a trece prin experiențe neplăcute.

Prima platformă din România actualizată constant cu exemple reale de fraudă: www.sigurantaonline.ro/uniti-impotriva-escrocheriilor



Pilonul central al campaniei este o platformă digitală care explică pe înțelesul tuturor cum funcționează cele mai răspândite metode de fraudă și cum pot fi oprite la timp. Dincolo de termeni tehnici, platforma aduce în fața publicului povești reale ale unor oameni care au trecut prin astfel de situații, pentru că astfel de fraude exploatează, de cele mai multe ori, emoții puternice.

*"Rata de fraudă pentru transferurile bancare către alte conturi era de 0,003% în România, după numărul tranzacțiilor, la finele anului 2024. În schimb, rata de fraudă după numărul tranzacțiilor cu cardul în totalul plăților cu cardul era de 0,005% în România, de trei ori mai redusă ca media Uniunii Europene. Obiectivul Sigurantaonline este creșterea nivelului de educație digitală ca utilizatorii români să evite furnizarea datelor bancare sensibile și să fie conștienți de riscul legat de manipularea privind transferul banilor sau instalarea de aplicații la cererea fraudatorilor", a subliniat **Gabriela Folcuț**, Director Executiv Asociația Română a Băncilor.*

Printre cele mai frecvente tipuri de fraudă documentate pe platformă se regăsesc:

Metoda WhatsApp „Telefonul stricat” presupune trimiterea unui mesaj de pe un număr necunoscut de către cineva care pretinde că este un membru al familiei și că și-a stricat telefonul. Victima este rugată să salveze noul număr și, sub presiunea urgenței, să trimită bani pe contul unui „prieteni”, deoarece ruda respectivă nu mai are acces nici la propriul cont bancar. Totul se desfășoară prin mesaje scrise, fără apel vocal, tocmai pentru a evita recunoașterea vocii.

Metoda Vishing - oportunitate de investiții Hidroelectrică începe, de cele mai multe ori, după ce o persoană își introduce datele într-un formular online care promite câștiguri rapide. Ulterior, aceasta este contactată telefonic de așa-zii „consultanți” care o conving să transfere bani pentru investiții fictive, iar sumele ajung direct în conturile atacatorilor.

Metoda BNR începe cu un apel telefonic al cărui număr pare să provină chiar de la banca victimei, în care aceasta este anunțată că un credit a fost solicitat fraudulos în numele ei. Victima este transferată succesiv către un „ofițer bancar”, un „polițist” și un „reprezentant BNR”, fiecare confirmat de un număr de telefon falsificat prin spoofing. Sub presiunea urgenței, persoana vizată este convinsă să își mute economiile într-un cont pretins „sigur”, însă sumele ajung direct la escroci.

Metoda Creditul - schema complexă cu autorități este o variantă extinsă a spoofingului, în care victima este contactată simultan de reprezentanți falși ai băncii, poliției și BNR, care o conving că identitatea sa este folosită într-o fraudă activă. Escrocii trimit documente false de legitimație și acorduri de confidențialitate prin WhatsApp pentru a părea credibili, apoi îi cer victimei să contracteze ea însăși un credit și să depună suma la un bancomat de criptomonede, folosind coduri QR furnizate de ei. Conversația este ștearsă imediat după transferul banilor.

Metoda „Accidentul” - vocea clonată cu AI presupune un apel telefonic în care escrocii folosesc inteligența artificială pentru a imita vocea unui membru al familiei, anunțând că a fost implicat într-un accident grav sau că se află în pericol legal iminent. Victima aude vocea familiară a copilului sau nepotului și, sub presiunea emoțională intensă, nu mai verifică identitatea apelantului.

Metoda Nepotul la ananghie - vocea clonată cu AI funcționează identic cu metoda accidentul, dar vizează în special persoanele în vârstă, mizând pe relația buni-nepoți. Escrocul, folosind o voce generată de AI, pretinde că a fost jefuit și că are nevoie urgentă de bani pentru a ajunge acasă. La fel ca și în cazul metodei clasice Accidentul, cel vizat nu mai verifică identitatea reală a celui care sună.

Exemplele evidențiază cât de ușor pot fi activate frica sau încrederea și subliniază necesitatea unei soluții simple și clare pentru a opri fraudă la timp. Campania promovează conceptul de **parole de familie** - nu parole formate din cifre, ci parole construite din amintiri și detalii cunoscute doar de cei apropiați. Aceste parole pot face diferența între o voce autentică și un apel fals generat cu ajutorul inteligenței artificiale.

„Numărul și diversitatea înșelătoriilor cresc de la o lună la alta, iar dincolo de cifre vorbim despre victime care își pierd liniștea și economiile. Tocmai de aceea, oamenii au nevoie de repere clare care să îi ajute să recunoască mai ușor tentativele de fraudă. Împreună cu partenerii noștri, punem la dispoziție instrumente de informare și promovăm soluții simple de prevenție, precum parola de familie. Pentru Mastercard, într-un ecosistem bazat pe plăți digitale, încrederea



și siguranța trebuie să meargă împreună”, a declarat **Cosmin Vladimirescu, General Manager Mastercard pentru România și Croația.**

Demersul va aduce în prim-plan și o serie de materiale și clipuri realizate împreună cu mai mulți creatori de conținut, astfel încât sfaturile de prevenire să ajungă la public într-un limbaj simplu și ușor de înțeles. Inițiativa își propune să arate, într-un mod accesibil și relevant, că vocea de la telefon poate fi o minciună, dar vigilența și comunicarea din familie rămân cele mai sigure forme de protecție.

Despre Proiectul #SigurantaOnline

Proiectul național de educație digitală și prevenire a criminalității informatice **#SigurantaOnline** este menit să ofere cele mai bune practici de securitate cibernetică, prin accesarea platformei sigurantaonline.ro, pentru a evita ca tinerii și adulții să devină victime ale fraudelor informatice. Proiectul este o inițiativă a Poliției Române, Directoratului Național de Securitate Cibernetică și Asociației Române a Băncilor, la care s-a alăturat Mastercard.