#SigurantaOnline: Cinci greșeli online care te pot costa. Le faci fără să-ți dai seama

București, 10 februarie 2026

De **Ziua Internațională a Siguranței pe Internet**, marcată anul acesta pe **10 februarie**, proiectul național de educație digitală **#SigurantaOnline** avertizează asupra unor greșeli frecvente pe care utilizatorii le fac în mediul online și care pot duce la pierderi financiare, furt de date sau compromiterea conturilor personale. Proiectul este susținut de **Asociația Română a Băncilor, Poliția Română și Directoratul Național de Securitate Cibernetică** și are ca obiectiv creșterea nivelului de conștientizare privind riscurile reale din mediul digital.

Tema internațională din acest an „*Tehnologie inteligentă, alegeri sigure – Explorarea utilizării sigure și responsabile a inteligenței artificiale”* subliniază cât de important este să înțelegem instrumentele digitale pe care le folosim zilnic și să luăm decizii informate, mai ales într-un context în care tehnologiile bazate pe Inteligența artificială (AI) sunt din ce în ce mai prezente inclusiv în fraudele online. În spatele multor fraude online nu se află tehnici complicate, ci gesturi simple, efectuate din grabă - un click pe un link, o descărcare de document sau instalarea unei aplicații nepotrivite - gesturi care pot avea consecințe financiare serioase.

Cinci greșeli online care te pot costa bani – și cum le poți evita

1. **Oferirea datelor cardului sau a codurilor de securitate**

Sub pretextul unor probleme urgente, infractorii cer datele cardului, codul de securitate format din 3 cifre de pe spatele cardului (CVV) sau parolele, ceea ce poate duce la pierderi financiare imediate. Tehnologia permite acum crearea de mesaje și pagini web aproape identice cu cele ale unor bănci sau instituții. Soft-uri inteligente și AI pot replica elemente vizuale și lingvistice, făcând frauda greu de detectat.

Sfatul #SigurantaOnline: Nu transmite niciodată datele cardului sau codurile de securitate la cerere! Verifică întotdeauna prin aplicația oficială a băncii sau contactează instituția direct. Datele cardului trebuie folosite exclusiv de posesorul cardului pentru plățile online efectuate pe site-uri securizate.

2. **Plata pe site-uri nesigure sau necunoscute**

Ofertele „prea bune ca să fie reale” și magazinele online false sunt folosite pentru a colecta datele cardului și a fura bani. Instrumentele bazate pe Inteligența artificială pot genera elemente vizuale, texte și logo-uri care imită perfect site-urile legitime, crescând șansele ca o persoană să introducă detalii personale sau bancare.

Sfatul #SigurantaOnline: Verifică cu atenție denumirea (adresa) site-ului, folosește și un antivirus pentru siguranță, ai grijă să aibă conexiunea securizată (https) - lacătul închis și caută informații despre comerciant, înainte de a plăti. Poți face o verificare preliminară a securității site-ului și cu soluții disponibile gratis online, precum ScamAdviser.com.

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

3. **Neactivarea alertelor și a autentificării suplimentare**

Fără notificări și autentificare în doi pași, fraudele pot trece neobservate până când banii sunt deja pierduți.

Sfatul #SigurantaOnline: Activează alertele pentru fiecare tranzacție și autentificarea în doi pași în aplicațiile bancare.

4. **Reacția impulsivă la mesaje care creează panică**

Mesajele care anunță conturi blocate, plăți suspecte sau urgențe sunt folosite pentru a forța decizii impulsive. Tot mai des apar apeluri sau mesaje vocale generate cu AI care pot imita vocea copilului sau a unei persoane apropiate, cerând bani „urgent”.

Sfatul #SigurantaOnline: Închide apelul și sună persoana respectivă pe numărul pe care îl cunoști, dar nu din WhatsApp. Verificarea directă este esențială înainte de a trimite bani. Îți poți stabili o parolă, un cuvânt cheie de siguranță pentru a evita astfel de amenințări.

5. **Obișnuința de a da click pe linkuri primite prin aplicațiile de mesagerie, SMS sau rețele sociale, fără o minimă verificare**

AI poate crea texte și documente care par extrem de convingătoare (inclusiv contracte sau oferte). Chiar dacă par venite de la cineva cunoscut, acestea pot fi capcane.

Sfatul #SigurantaOnline: Nu accesa linkuri direct din mesaje. Sună persoana care ți-a trimis mesajul sau accesează site-ul tastând manual adresa cunoscută.

Sprijin pentru copii, părinți și profesori

Educația digitală trebuie să înceapă de la vârste mici. Platforma sigurantaonline.ro oferă **resurse dedicate copiilor și cadrelor didactice**, materiale explicative, ghiduri și instrumente practice pentru folosirea responsabilă a tehnologiei și pentru înțelegerea riscurilor din mediul online, inclusiv a celor asociate utilizării inteligenței artificiale.

Profesorii sunt invitați să integreze aceste materiale în activitățile de la clasă, iar părinții pot găsi recomandări utile pentru discuții despre siguranță, încredere și comportament digital responsabil. Peste 10.000 de români și-au testat deja cunoștințele și abilitățile de siguranță online prin quiz-urile disponibile pe platforma sigurantaonline.ro. Cei interesați sunt invitați să afle dacă fac aceste greșeli accesând secțiunea de testare a cunoștințelor.

Mai multe informații, exemple reale de fraude și resurse educaționale sunt disponibile pe **www.sigurantaonline.ro**.

Conform *Global Cybersecurity Outlook 2026 al World Economic Forum*, 87% dintre liderii lumii au observat creșterea vulnerabilităților legate de AI, iar 94% se așteaptă ca inteligența artificială să fie una dintre cele mai importante forțe care conturează peisajul securității digitale în 2026, inclusiv în evoluția tacticilor de fraudă online. Pe de altă parte, statisticile recente arată că phishing-ul și fraudele asistate de tehnologie rămân printre cele mai frecvente cauze ale pierderilor financiare în mediul digital, subliniind importanța educației și a unui comportament responsabil în utilizarea tehnologiei.

Cu o singură greșeală online, poți pierde bani și date importante. Informarea te ajută să o eviți.

# # #

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 copiii să devină victime ale fraudelor informatice, ale pornografiei infantile sau ale atacurilor de tip malware. Proiectul este o inițiativă a Asociației Române a Băncilor, Poliției Române și Directoratului Național de Securitate Cibernetică, alături de care s-au alăturat pe parcurs și alți parteneri.

www.dreptullabanking.ro

www.sigurantaonline.ro

Facebook @DreptulLaBanking

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ