

București, 07 martie 2025

## **Cu ocazia Zilei Internaționale a Femeii, partenerii proiectului #*SiguranțaOnline* împart flori și recomandări pentru protecția digitală a doamnelor și domnișoarelor**

Cu ocazia Zilei Internaționale a Femeii, reprezentanții proiectului de educație digitală și prevenire a criminalității informatice #*SiguranțaOnline* au ieșit în stradă și au oferit doamnelor și domnișoarelor un trandafir roșu, alături de un sfat esențial de protecție online. De data aceasta, trandafirul roșu nu a fost simbolul dragostei, ci al unui „*steag roșu*” de atenționare, pentru a sublinia importanța protejării împotriva riscurilor cibernetice din viața digitală de zi cu zi.

Românii sunt utilizatori fervenți ai rețelelor de socializare, precum și ai aplicațiilor de dating, prin care țin legătura cu prieteni vechi și dezvoltă noi relații online. Totuși, unii dintre aceștia ajung victime ale fraudelor online, dintre care cele pe teme romantice reprezintă o amenințare importantă. Multe victime sunt femei, iar unul dintre modurile de operare folosite frecvent de infractori este *romance scam*.

**Înșelătoriile romantice - *romance scam*** sunt fraude în care infractorii încearcă să câștige încrederea victimei prin stabilirea unei relații emoționale false, pentru a obține bani sau alte beneficii. Aceste fraude pot fi foarte dureroase din punct de vedere emoțional, dar și financiar.

Fie că se folosesc de imaginea unor vedete sau a unor falși medici sau militari, răufăcătorii utilizează tehnici manipulative de limbaj și promisiuni romantice false, având drept scop final obținerea datelor personale, a informațiilor financiare și, în final, a banilor victimei.

Odată cu evoluția tehnologică, se schimbă și metodele prin care autorii fură bani de la victimele lor. Criptomonede și transferurile bancare sunt cele mai utilizate metode. Alte metode comune de plată includ cardurile cadou și aplicațiile de plăți online. Autorii preferă aceste metode deoarece oferă un anumit nivel de anonimitate, iar odată ce fondurile sunt trimise de victimă, tranzacția nu mai poate fi anulată.

Cu ocazia Zilei de 8 martie, partenerii proiectului #*SiguranțaOnline* ([sigurantaonline.ro](https://sigurantaonline.ro)), Asociația Română a Băncilor (ARB), Directoratul Național de Securitate Cibernetică (DNSC) și Poliția Română, atrag atenția asupra fraudelor online romantice, pentru a proteja și a oferi recomandări de prevenire femeilor, care sunt cele mai vizate de acest tip de fraudă.

Astfel, puteți fi ținta unui „*fraudator romantic*” dacă persoana cu care comunicați online prezintă unele dintre aceste semne/particularități:

- Pretinde că are o situație materială foarte bună, dar a fost ocupată cu munca și nu și-a găsit fericirea.
- Pretinde că locuiește, lucrează sau călătorește mult în străinătate, în locații exotice unde ți-ai dori și tu să ajungi.
- Îți mărturisește rapid problemele personale ca să provoace compasiune.



**POLIȚIA ROMÂNĂ**



DIRECTORATUL NAȚIONAL  
DE SECURITATE CIBERNETICĂ



asociația română a băncilor

- Trimite fotografii generale (de cele mai multe ori false/generate de AI) în care apare călătorind, făcând cumpărături sau luând masa în locuri luxoase.
- Menționează ideea de a se întâlni și de a fi împreună în curând.
- Îți mărturisește rapid dragostea.
- Oferă periodic scuze pentru imposibilitatea de a efectua un apel video. Dacă are loc un apel video, nu-i poți vedea clar fața.
- Solicită ca mesajele/conversațiile să fie mutate într-o aplicație separată (de exemplu, WhatsApp, Telegram).
- Solicită bani, câteodată prin metode netradiționale, cum ar fi criptomonede sau carduri cadou.
- Încearcă să te manipuleze și să îți distragă atenția atunci când îi pui la îndoială intențiile.

### **Sfaturi pentru a evita să pierdeți bani din cauza unei fraude romantice:**

- Fiți suspicioase/suspicioși la apelurile telefonice și mesajele text nesolicitate. Nu răspundeți la apeluri sau mesaje text de la numere necunoscute. Nu furnizați niciodată informații personale la telefon sau prin SMS. În plus, le puteți bloca sau raporta drept *spam*.
- Evitați să împărtășiți informații personale sensibile sau limitați ceea ce împărtășiți online. Infracorii se pot folosi de detaliile împărtășite postate/dezvăluite pe rețelele de socializare și pe site-urile de întâlniri, pentru a vă cunoaște mai bine și a vă transforma într-o posibilă victimă, creând o legătură și profitând de ceea ce se întâmplă în viața dumneavoastră.
- Transmiterea de fotografii nepotrivite sau de informații financiare ar putea fi folosită ulterior pentru șantaj.
- Ascultați-vă instinctul. Dacă persoana sau povestea pare prea bună pentru a fi adevărată, sau chiar dramatică, discutați cu cineva de încredere despre aceasta și lăsați rațiunea să ia decizii.
- Nu trimiteți bani unei persoane pe care abia ați cunoscut-o online, chiar dacă pare să fie o relație specială. Autorii încearcă adesea să construiască o legătură emoțională rapid pentru a face cereri financiare.
- Fiți atente/atenți la cererile de ajutor financiar, urgente, sau la presiunile emoționale. O persoană rău intenționată va inventa o urgență (de exemplu, spitalizare, accident, probleme financiare) și va cere bani pentru a „ajuta” într-o situație dificilă, făcându-vă să simțiți că sunteți singura persoană care îi poate ajuta.
- Căutați semne de autenticitate. Infracorii cibernetici adesea își ascund identitatea reală sau folosesc fotografii false. Dacă cineva pare perfect sau dacă imaginile lor sunt prea profesionale sau lipsite de personalitate, ar putea fi un semn de fraudă.
- Dacă cineva insistă să comunice doar prin mesaje text sau apeluri telefonice, dar nu vrea să vă întâlnească personal sau să își facă publice detaliile personale, ar putea fi un semn de alarmă.
- Fiți atenți la inconsecvențe în poveștile sau comportamentele lor. De exemplu, dacă persoana promite să vină să vă întâlnească, dar amână continuu, acest lucru ar putea fi un semn că ceva nu este în regulă.

## Despre Proiectul #SigurantaOnline

Proiectul național de educație digitală și prevenire a criminalității informatice **#SigurantaOnline** este o inițiativă a Asociației Române a Băncilor (ARB), Directoratului Național de Securitate Cibernetică (DNSC) și Poliției Române. Proiectul are ca obiectiv creșterea gradului de conștientizare cu privire la criminalitatea informatică, dezvoltarea abilităților de prevenire și educația digitală a populației. Una dintre cele mai importante resurse ale proiectului este platforma [sigurantaonline.ro](http://sigurantaonline.ro), prin accesarea căreia utilizatorii se pot informa și antrena să recunoască principalele forme de manifestare și modalități de prevenire a pericolelor din mediul digital.



[www.sigurantaonline.ro](http://www.sigurantaonline.ro)