

București, 28 octombrie 2026

De Black Friday #SigurantaOnline recomandă verificarea ofertelor, a solicitărilor de plată și a mesajelor despre livrări sau rambursări

- Tastați adresa magazinului online în browser; evitați linkurile din reclame sau mesaje.
- Nu divulgați PIN-ul cardului, parola de online banking sau codurile de autorizare a tranzacțiilor.
- Verificați înainte de a introduce datele cardului pentru cumpărături online.
- Verificați livrarea în aplicația oficială a curierului, nu prin linkuri din SMS.
- Ați divulgat datele cardului? Sunați imediat banca pentru blocarea lui.

București - O ofertă promovată pe rețelele sociale, un mesaj despre un colet care nu poate fi livrat sau o presupusă rambursare pot fi puncte de plecare pentru o tentativă de fraudă. În perioada Black Friday, Poliția Română, Directoratul Național de Securitate Cibernetică (DNSC) și Asociația Română a Băncilor (ARB) recomandă, prin Proiectul național de educație digitală și prevenire a criminalității informatice #SigurantaOnline, verificarea solicitărilor primite pe tot parcursul cumpărăturilor, mai ales înainte de efectuarea plății, dar și după.

Atacatorii pot imita identitatea unor magazine, firme de curierat sau instituții bancare pentru a obține date personale, informații sensibile aflate pe card ori acces la conturi. Atunci când utilizatorii așteaptă mai multe comenzi, un mesaj despre o problemă de livrare poate părea credibil. Faptul că o persoană a făcut recent cumpărături nu confirmă însă autenticitatea mesajului primit.

Oferta: verificați cine se află în spatele magazinului

O reclamă care folosește numele și identitatea vizuală ale unui brand cunoscut poate conduce către un site fals. Înainte de a introduce date personale sau bancare, verificați adresa completă a site-ului, identitatea comerciantului și informațiile despre contact, livrare și retur.

Accesați magazinul prin introducerea adresei cunoscute în browser sau prin aplicația oficială. Comparați prețurile și acordați timp verificărilor, mai ales când oferta este însoțită de presiunea de a plăti imediat.

Prezența „https” indică o conexiune criptată, dar nu garantează că magazinul este legitim.

Plata: verificați ce operațiune autorizați

Înainte de a confirma o plată în aplicația bancară, citiți informațiile afișate și verificați suma și beneficiarul. Nu aprobați operațiuni pe care nu le-ați inițiat și nu comunicați altor persoane parolele de acces, codul PIN sau codurile de autorizare primite prin SMS ori în aplicație.

Datele cardului trebuie introduse numai după verificarea comerciantului și a paginii de plată. O solicitare urgentă primită prin telefon, e-mail sau mesagerie nu este suficientă pentru a justifica efectuarea unei operațiuni bancare.

Livrarea și rambursarea: confirmați solicitarea printr-un canal oficial

Mesajele despre colete blocate, adrese incomplete sau taxe suplimentare trebuie verificate direct în aplicația ori pe site-ul oficial al comerciantului sau al firmei de curierat, accesate independent de linkul primit.

Aceeași precauție este necesară în cazul mesajelor care promit restituirea unei sume. Nu comunicați coduri de autorizare și nu aprobați o plată pentru a primi o presupusă rambursare. Contactați comerciantul folosind datele din comanda inițială sau de pe site-ul său oficial, inclusiv dacă vi se solicită o plată suplimentară.

Un mesaj bine scris poate fi tot o tentativă de fraudă

Instrumentele de inteligență artificială pot fi folosite pentru a genera texte și materiale vizuale convingătoare. Absența greșelilor gramaticale, un logo familiar sau aspectul profesionist al unei pagini nu confirmă autenticitatea acesteia. Verificarea sursei și a solicitării rămâne esențială.

Dacă ați oferit date sau observați tranzacții suspecte, contactați imediat banca

Dacă ați introdus informații bancare pe un site suspect, ați comunicat coduri de securitate sau observați operațiuni pe care nu le recunoașteți, contactați imediat banca, prin canalele oficiale, pentru luarea măsurilor necesare.

Păstrați mesajele, adresele site-urilor, capturile de ecran și dovezile tranzacțiilor. Dacă ați fost victima unei fraude, sesizați Poliția și notificați DNSC la numărul 1911 sau prin platforma pnrisc.dnsc.ro.

Pentru recomandări și resurse de educație digitală, accesați www.sigurantaonline.ro.