

București, 30 octombrie 2025

SFATURI ESENȚIALE PENTRU PREVENIREA FRAUDELOR ONLINE DE BLACK FRIDAY

Asociația Română a Băncilor (ARB), Poliția Română și Directoratul Național de Securitate Cibernetică (DNSC) avertizează, prin intermediul proiectului național de educație digitală și prevenire a criminalității informatice #SigurantaOnline (www.sigurantaonline.ro), că perioada campaniilor de Black Friday este una dintre cele mai vulnerabile din an din perspectiva fraudelor online.

Infractorii cibernetici profită de interesul crescut pentru reduceri și de volumul mare de tranzacții online și recurg la site-uri false, site-uri clonă, oferte prea bune pentru a fi adevărate și diverse metode de inginerie socială, cu scopul de a induce în eroare cumpărătorii să își ofere date sensibile, dar mai ales datele de card.

Modurile de operare utilizate frecvent în perioada campaniilor de Black Friday:

- Crearea de site-uri false sau clonate, care imită în detaliu paginile unor magazine legitime;
- Trimiterea de mesaje și e-mail-uri de tip phishing, care par a fi expediate de companii cunoscute, bănci sau instituții publice;
- Publicarea și promovarea de anunțuri frauduloase pe rețelele sociale, care promit reduceri spectaculoase;
- Comercializarea de produse contrafăcute, prezentate drept articole de brand;
- Solicitarea plății prin metode nesigure, care pot duce la compromiterea datelor de card.

Recomandări pentru prevenirea fraudelor online de Black Friday:

1. Verificarea sursei mesajelor primite.

În perioada campaniilor de reduceri, utilizatorii pot primi mesaje care par a fi transmise în numele unor instituții sau companii cunoscute – servicii poștale, firme de curierat, instituții bancare sau operatori de telecomunicații. Astfel de comunicări pot include informații false privind colete blocate, solicitarea actualizării datelor de client sau oferte exclusive.

Nu accesați linkurile primite!

Aceste mesaje trebuie tratate cu maximum de prudență, în special dacă conțin fișiere atașate, link-uri scurtate ori domenii suspecte. Instituțiile și companiile autentice nu solicită prin e-mail sau SMS date confidențiale. Situațiile reale pot fi verificate exclusiv pe site-urile oficiale, accesate manual, nu prin link-urile primite.

2. Verificarea autenticității magazinului online.

Se recomandă efectuarea cumpărăturilor doar de pe platforme care oferă:

- adresă web securizată (<https://>);

- date de identificare clare ale companiei;
- informații complete despre livrare, retur și contact.

Magazinele virtuale nou apărute sau cu informații incomplete (care nu prezintă elementele de mai sus) trebuie verificate suplimentar, cu atenție sporită.

3. Atenție la ofertele nerealiste de avantajoase („prea bune ca să fie adevărate”).

Infractorii cibernetici exploatează graba cumpărătorilor și construiesc site-uri care imită perfect magazinele autentice, inclusiv elementele vizuale și politicile comerciale.

Reduceri de 80–90% la produse de brand sau la dispozitive scumpe reprezintă, în majoritatea cazurilor, semnale clare de fraudă.

Se recomandă compararea prețurilor pe mai multe platforme și verificarea atentă a domeniului site-ului, mai ales dacă acesta folosește extensii neobișnuite (.shop, .store etc.).

4. Utilizarea exclusivă a metodelor de plată sigure.

Plata trebuie efectuată doar prin canale securizate, care oferă autentificare suplimentară și confirmări în timp real.

Se recomandă evitarea transferurilor directe către conturi personale sau plata prin link-uri primite pe rețele de socializare sau aplicații de mesagerie.

Se recomandă vigilență sporită la salvarea datelor cardului! Acestea nu trebuie salvate automat pe platforme necunoscute. Efectuați tranzacții când sunteți conectați la rețele de internet sigure.

5. Păstrarea dovezilor tranzacțiilor efectuate.

Salvează confirmările de plată, facturile, e-mail-urile și capturile de ecran. Acestea pot fi esențiale în cazul unei reclamații.

În situația identificării unei tranzacții neautorizate, este necesară informarea imediată a instituției bancare, sesizarea Poliției, precum și raportarea fraudei către Directoratul Național de Securitate Cibernetică, apelând 1911 sau accesând pnrisc.dnsc.ro

6. Monitorizarea periodică a conturilor bancare.

Verifică periodic conturile tale bancare. Monitorizează tranzacțiile și activează alertele automate din aplicațiile bancare. Astfel, poți detecta rapid orice activitate suspectă și poți bloca accesul neautorizat.

Pentru mai multă #SigurantaOnline

Pentru sfaturi detaliate privind siguranța digitală, accesează platforma www.sigurantaonline.ro și urmărește campania #SigurantaOnline, derulată de Poliția Română, DNSC și Asociația Română a Băncilor.