Nr. 1.765 din 7 noiembrie 2024

COMUNICAT DE PRESĂ

Sfaturi și soluții pentru prevenirea fraudelor online de Black Friday

Poliția Română, Directoratul Național de Securitate Cibernetică (DNSC) și Asociația Română a Băncilor (ARB) avertizează, prin intermediul proiectului național de prevenire a criminalității informatice și educație digitală **#SigurantaOnline** (sigurantaonline.ro), că infractorii cibernetici pot profita de perioada **Black Friday** pentru a obține venituri ilicite sau un volum mare de date sensibile (date personale și financiare). Atacatorii se folosesc mereu de context pentru a-și perfecționa metodele de atac, iar perioada cu cel mai mare volum de cumpărături online constituie o oportunitate perfectă de a se deghiza în furnizori de diverse servicii sau companii, pentru a atrage în capcană cumpărătorii interesați de promoții și de reduceri de prețuri.

În perioada *Black Friday*, a reducerilor consistente și una dintre cele mai aglomerate din punct de vedere al tranzacțiilor online, infractorii cibernetici 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.

Metode comune de fraudă și sfaturi pentru a le preveni:

- **Site-uri false de comerț online**
  - **Descriere**: Infractorii creează site-uri de cumpărături false, care imită/clonează paginile web ale magazinelor legitime, oferind prețuri incredibil de mici.
  - **Prevenire**: Efectuați cumpărături doar pe site-uri sigure, cu adrese securizate (*https*) și informații de contact verificate. Un magazin virtual trebuie să conțină date legate de compania care îl operează, adresă fizică, date de contact etc.
- ***Phishing* prin mesaje sau emailuri false**
  - **Descriere**: Cetățenii pot primi emailuri sau mesaje tematice de *Black Friday* prin care se solicită să acceseze link-uri malițioase sub pretextul unor oferte exclusive sau premii. Aceste link-uri pot duce la pagini de *phishing* care colectează informații financiare.
  - **Prevenire**: Evitați să dați click pe link-uri care provin din surse necunoscute și verificați adresa expeditorului. Magazinele nu cer informații sensibile prin email sau SMS. Accesați site-ul dorit prin scrierea adresei în browser. Fiți atenți la emailurile care pretind a fi de la magazine mari, în special cele care cer informații personale sau financiare.

- **Produse contrafăcute**
  - **Descriere**: Unele magazine oferă produse contrafăcute la prețuri mari, pretinzând că sunt originale.

- **Prevenire**: Cumpărați doar de la vânzători de încredere și evitați prețurile mult prea mici pentru produse de lux.

➢ **Fraude promovate prin anunțuri pe rețelele sociale**

- **Descriere**: Reclamele de pe rețelele de socializare cu anunțuri frauduloase care promit reduceri incredibile sunt tot mai frecvente și pot redirecționa/conduce către site-uri false/nesigure care colectează informații personale și de plată.
- **Prevenire**: Dacă o ofertă pare prea bună și prea ieftină, atunci riscul de fraudă este foarte mare. Verifică legitimitatea magazinului și a ofertei prin compararea prețurilor și recenziilor, dar nu vă lăsați influențați doar de recenziile de pe social media, în mod special de acolo unde ai găsit și „oferta" promovată.

➢ **Metode de plată nesigure**

- **Descriere**: Unele site-uri cer detalii de plată fără a avea măsuri de securitate adecvate.
- **Prevenire**: Folosiți metode de plată sigure, cum ar fi carduri cu protecție anti-fraudă și confirmare suplimentară a plăților. Activați alertele pentru conturile bancare și aplicațiile de plată pentru a detecta rapid activități suspecte.
- **Păstrați confidențiale datele cardului și parolele de acces la conturile bancare!** Să nu furnizați datele de pe cardul bancar în nicio situație: numărul, data de expirare și codul de securitate de pe spatele cardului format din trei cifre. Aceste date se folosesc doar de către utilizator pentru plata online pe site-uri securizate și nu atunci când sunteți conectat la o rețea Wi-Fi publică, ci trebuie să fie securizată

În plus, pentru a evita fraudele, înainte de a face vreo plată se pot verifica prin intermediul unor soluții gratis, cum sunt http://scamadviser.com/ sau http://virustotal.com/, site-urile de unde se face achiziția, sursele mesajelor de promovare sau alte informații primite.

Pentru informații suplimentare, recomandări complete despre siguranța în mediul digital sau chiar pentru posibilitatea de a vă antrena să evitați principalele amenințări din mediul online, accesați site-ul *www.sigurantaonline.ro*, parte a proiectului de prevenire a criminalității informatice *#Siguranțaonline*.

# # #

Despre Proiectul #SigurantaOnline

Proiectul național de prevenire a criminalității informatice și educație digitală ***#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 Poliției Române, Directoratului Național de Securitate Cibernetică și Asociației*

Române a Băncilor, alături de care s-au parteneriat pe parcurs o mai mulți parteneri, respectiv instituții publice, organizații non-guvernamentale, companii, cu interes în domeniu.

www.dreptullabanking.ro
www.sigurantaonline.ro

Facebook @DreptulLaBanking