București, 05 decembrie 2024

#SigurantaOnline: Atenție la reduceri false și investiții miraculoase!

Cum să evitați capcanele digitale în sezonul cadourilor

Sezonul sărbătorilor este o perioadă în care tentativele de fraudă online ating cote maxime. **Asociația Română a Băncilor (ARB), Directoratul Național de Securitate Cibernetică (DNSC) și Poliția Română,** inițiatorii proiectului național de conștientizare #SigurantaOnline (sigurantaonline.ro), oferă sfaturi esențiale pentru o vacanță liniștită, fără incidente financiare sau de securitate.

Campania #SigurantaOnline le oferă utilizatorilor informații clare și utile despre cele mai comune tipuri de fraudă și cum pot fi prevenite.

Ghid de prevenire a fraudelor: recunoaște tipologiile periculoase

1.Frauda „Reduceri false"

- *Exemplu*: Reducerile exagerate sau ofertele care par „prea bune pentru a fi adevărate" sunt adesea capcane. Accesarea linkurilor sau efectuarea plăților prin aceste platforme poate duce la furtul datelor personale și financiare.
- *Recomandare*: Acordați o atenție sporită site-urilor de cumpărături și evitați mirajul ofertelor prea bune ca să fie adevărate!

2. Frauda de tip „Investiții miraculoase"

- *Exemplu*: Dacă cineva îți oferă o oportunitate „unică" de investiție cu „zero riscuri" și „venituri garantate" într-un timp scurt, fii sigur că este o fraudă.
- *Recomandare*: Nu există surse de îmbogățire rapidă! Nu instalați aplicații legate de investiții la cererea unor consultanți financiari și, înainte de a investi, verificați dacă oferta este reală.

3. Frauda de tip Spoofing (preluarea identității altei instituții/persoane)

- *Exemplu*: Indiferent de numărul/denumirea instituției afișat/ă pe ecranul telefonului, rețineți că niciun angajat al Băncii, Poliției sau al altei autorități nu va cere să faceți un transfer, să accesați un credit sau să oferiți datele cardului bancar.
- *Recomandare*: Nu vă lăsați manipulați! Evitați să faceți orice plată sub presiune! Infractorii pot să folosească orice pretexte, datoria dumneavoastră este să faceți toate verificările înainte de a acționa. Spre exemplu, sunați la bancă apelând numărul de telefon de pe site-ul băncii, dacă primiți un telefon suspect legat de conturile bancare.

4. Frauda „Phishing" (e-mailuri sau mesaje suspecte)

- *Exemplu*: Mesajele care solicită actualizarea urgentă a datelor contului sau confirmarea plății prin linkuri suspecte pot redirecționa utilizatorii către pagini false care colectează informații sensibile.
- Recomandare: Actualizați datele personale prin canalele oficiale puse la dispoziție de banca la care aveți cont. Nu furnizați niciodată datele de conectare la Internet/Mobile Banking și nici datele de pe fața și spatele cardului. Datele de card se folosesc doar de utilizatorul acestuia când efectuează plăți pe site-uri securizate și nu atunci când este conectat la o rețea WI-FI publică, ci trebuie să fie securizată.

5. **Frauda „Social Media Giveaway"**

- *Exemplu*: Concursurile false de pe rețele sociale care solicită date personale sau plăți „pentru revendicarea premiului" pot fi capcane pentru furtul identității sau accesarea conturilor financiare.

- Rămâneți vigilenți la tentativele de fraudă online.

Alte recomandări pentru sărbători liniștite:

- Folosiți metode sigure de plată prin platforme recunoscute.
- Protejați-vă dispozitivele cu software actualizat și cu soluții antivirus.
- Nu partajați niciodată datele sensibile, cum ar fi PIN-ul cardului sau parolele, prin e-mail sau telefon.
- Fiți vigilenți la orice ofertă „prea bună pentru a fi adevărată”.

Întâmpinați sărbătorile în siguranță

Campania #SigurantaOnline are ca scop educarea și protejarea utilizatorilor în fața fraudelor cibernetice. Cu sprijinul ARB, DNSC și al Poliției Române, comunitatea poate adopta măsuri proactive pentru a evita capcanele digitale. Pentru mai multe informații și resurse, vizitați sigurantaonline.ro și testați-vă cunoștințele prin quiz-ul interactiv disponibil pe site.

###

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 Poliției Române, Directoratului Național de Securitate Cibernetică și al Asociației Române a Băncilor, alături de care s-au parteneriat pe parcurs* ***Ambasada Elveţiei în România, Swiss WebAcademy și*** *ATTACK Simulator.*

www.dreptullabanking.ro

www.sigurantaonline.ro

Facebook @DreptulLaBanking