București, 18 iunie 2024

#SigurantaOnline **oferă recomandări de vacanță în siguranță:**
cum să eviți capcanele și tentativele de fraudă din mediul online

Poliția Română, Directoratul Național de Securitate Cibernetică (DNSC) și Asociația Română a Băncilor (ARB), prin intermediul proiectului național de conștientizare #SigurantaOnline, vin cu o serie de recomandări esențiale dedicate utilizatorilor din România, pentru a-și proteja datele personale și financiare în sezonul estival. Oricine își dorește o vacanță de vară lipsită de griji și fără incidente neplăcute, dar pentru asta trebuie să ne formăm niște reflexe de securitate cu privire la datele noastre.

De la evitarea ofertelor prea frumoase pentru a fi adevărate până la utilizarea unor parole complexe și autentificarea în doi pași, aceste recomandări ajută utilizatorii să navigheze online în siguranță în timpul pregătirilor pentru vacanță:

1. Verificați site-urile web înainte de a face rezervări.
Înainte de a introduce date sensibile pe un site web, verificați dacă site-ul este legitim. Căutați simbolul în forma de lacăt în bara de adrese şi asigurați-vă că adresa URL începe cu "*https*". De asemenea, puteți verifica recenziile site-ului web pe internet pentru a vedea dacă alți utilizatori au avut experiențe pozitive sau negative.

2. Alegeți o agenție de turism de încredere.
Când vă planificați vacanța, este important să alegeți o agenție de turism de încredere şi cu o reputație bună. Puteți cere recomandări de la prieteni sau familie sau puteți căuta pe internet agenții cu recenzii pozitive. Asigurați-vă că agenția este licențiată şi că are o prezență online solidă. Informați-vă din mai multe surse, de preferat altele decât cele de pe site-urile proprii ale agențiilor.

3. Fiți atenți la ofertele speciale.

Dacă vedeți o **ofertă de vacanță care pare prea bună ca să fie adevărată**, probabil este o înșelătorie. Infractorii cibernetici se folosesc adesea de oferte irezistibile pentru a atrage victimele şi a le fura banii sau informațiile personale. Fiți sceptici față de ofertele care promit cazare de lux la prețuri foarte mici sau excursii gratuite.

Evitați să accesați link-uri, primite din surse necunoscute pe mail sau prin SMS, prin intermediul comunicărilor de pe social media, ori prin intermediul platformelor de tip chat (WhatsApp, Signal, Telegram etc.) și nu completați datele personale sau bancare la cerere pe acestea.

4. Folosiți autentificarea în doi pași

Când faceți rezervări online, utilizați o metodă de plată sigură. Asigurați-vă că aveți activată autentificarea în doi pași prin utilizarea a două elemente din următoarele categorii: ceva ce cunoști (codul PIN, parola), ceva ce deții (telefonul mobil, verificat prin parola transmisă prin SMS) și ceva ce îți aparține (amprenta, recunoașterea facială).

5. Protejați-vă dispozitivele.

Asigurați-vă că dispozitivele dvs. sunt protejate cu un software antivirus şi anti-malware actualizat. De asemenea, utilizați o parolă puternică pentru a vă conecta la contul dvs. de e-mail şi la alte conturi online.

6. Evitați utilizarea rețelelor publice de WI-FI.

Rețelele WI-FI publice pot fi nesigure, așa că evitați să le utilizați pentru a accesa informații sensibile, cum ar fi contul bancar sau cardul de credit. Dacă trebuie să utilizați o rețea Wi-Fi publică, utilizați o conexiune VPN (rețea privată virtuală) sau vă puteți configura propriul *hot-spot wireless*.

7. Manifestați o atenție suplimentară la plățile efectuate cu cardul și la folosirea ATM-ului.

Alocați-vă timp pentru a examina activitatea bancară și verificați tranzacțiile suspecte. Dacă depistați ceva ciudat la ATM, nu mai folosiți acel aparat, nu permiteți fotocopierea cardului și acoperiți ecranul ATM-ului când introduceți PIN-ul.

8. Fiți atenți la ceea ce postați pe rețelele de socializare.

Nu postați informații despre vacanța dvs. pe rețelele de socializare și evitați partajarea locației public. Revizuiți setările de confidențialitate pe conturile de social media. Infractorii cibernetici pot folosi aceste informații pentru a vă fura identitatea sau pentru a comite alte infracțiuni.

9. Raportați frauda.

Dacă sunteți victima unei fraude online, raportați-o imediat autorităților depunând o plângere oficială la Poliție. De asemenea, informați Directoratul Național de Securitate Cibernetică fie telefonic la numărul 1911, fie prin e-mail la alerts@dnsc.ro, pentru a contribui la prevenirea unor astfel de incidente în viitor.

Proiectul național de educație digitală **#SigurantaOnline** este menit să ofere cele mai bune practici de securitate cibernetică, prin accesarea platformei sigurantaonline.ro, pentru a evita ca utilizatori din România să devină victime ale fraudelor informatice. **#SigurantaOnline** este o inițiativă a Poliției Române, Directoratului Național de Securitate Cibernetică și Asociației Române a Băncilor, la care s-au raliat și alte entități public-private.