

13 februarie 2024

#SiguranțaOnline: Recomandări pentru copii și tineri în cadrul Clubului de Siguranță Online

Peste 300 de tineri au participat la workshop-urile interactive pe teme de siguranță online desfășurate la centrul comercial ParkLake, în perioada 6 – 10 februarie 2024, în „Clubul de Siguranță Online” **inițiat de** Poliția Română, Directoratul Național de Securitate Cibernetică (DNSC) și Asociația Română a Băncilor (ARB) în cadrul proiectului național de educație digitală **#SiguranțaOnline. Clubul de Siguranță Online** a fost lansat cu prilejul Zilei Internaționale a Siguranței pe Internet din acest an și a antrenat tinerii să se protejeze eficient de amenințările ce îi vizează în mediul online.

Într-o lume digitală în continuă expansiune, siguranța online a copiilor și adulților devine o prioritate tot mai mare. Navigarea pe internet vine cu o multitudine de beneficii educaționale și de divertisment, dar și cu riscuri. Educația digitală cu privire la amenințările cibernetice îi poate ghida pe utilizatori, încă de la vârste fragede, către decizii mai înțelepte.

Pentru a-i ajuta pe cei mici să navigheze în siguranță, inițiatorii **proiectului național #SiguranțaOnline** vin cu sfaturi pentru tineri, de care toți trebuie să ținem cont pentru siguranța noastră atunci când navigăm pe Internet:

1. 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 și nu completați datele personale sau bancare pe acestea.
2. Nu dezvăluiți datele de pe cardul bancar: nume, număr, data de expirare, CVV2/CVC (numărul de trei cifre de pe spatele cardului). Nu introduceți codul PIN pe site-uri de internet și nu îl divulgați niciodată. Site-ul pe care urmează să fie introduse datele cardului pentru efectuarea unei plăți online trebuie să fie securizat, adică linkul începe cu **https**. Plățile se efectuează doar când sunteți conectați la rețele sigure, nu la rețele publice.
3. Nu furnizați niciodată altor persoane datele de autentificare la conturi (username, parola, cod suplimentar de autentificare sau cod de back-up).
4. Nu dați click atunci când sunteți etichetați într-o postare din social media care promite câștiguri mari și fiți atenți la mesajele care par să vină din partea băncilor. Mesajele false conțin, de multe ori, formule de adresare impersonale, greșeli gramaticale sau de exprimare.
5. Nu trebuie efectuate transferuri și procesate operațiuni doar în baza unui e-mail sau a unei solicitări telefonice urgente, fără a face o verificare a autenticității mesajului. Băncile nu solicită niciodată date confidențiale cum ar fi datele cardurilor, parole de acces, coduri PIN, nici telefonic, nici prin SMS, nici prin e-mail și nici prin completarea acestora pe website.
6. Citiți cu atenție, înainte de a deschide, orice mesaj sau un fișier care pare a fi transmis de la bancă sau de alte persoane/instituții și, dacă aveți suspiciuni, contactați expeditorul, pentru validarea conținutului mesajului primit, pe un canal de comunicare diferit.

7. Dacă trebuie să primiți bani, IBAN-ul (numărul de cont format din 24 de caractere, litere și cifre) este cel ce trebuie comunicat și nu datele de pe card. Solicitarea datelor cardului de către alte persoane este de fapt o capcană, deoarece cardul este un instrument de plată și nu un instrument de încasare bani.
8. Atenție la propunerile de investiții! Câștigurile mari și neașteptate pot ascunde tentative de fraude. Verificați informațiile legate de investiții și atenție sporită la fenomenul în care imaginea și vocea persoanelor publice sunt folosite pentru a te convinge să investești sau să instalezi aplicații care au acces ulterior la contul tău bancar.

Organizatorii proiectului național **#SiguranțaOnline** sfătuiesc pe toți utilizatorii de Internet să instaleze cele mai recente actualizări ale sistemului de operare și un antivirus și să se asigure că toate dispozitivele pe care le folosesc pentru a naviga pe internet funcționează în baza versiunilor actualizate ale sistemelor de operare și sunt protejate cu o soluție antivirus eficientă.

www.sigurantaonline.ro