

Articol Campanie „Nu-ți da CVC-ul”

Nu-mi da CVC-ul tău!

Sau cum ne protejăm portofelul digital în perioade de shopping online intens cum este perioada din preajma sărbătorilor și a reducerilor de început de an

A venit decembrie, luna cea mai încărcată de cumpărături pentru cadouri, mese festive, mici atenții pentru noi, care să ne aducă un plus de bucurie în perioada sărbătorilor. Acum este momentul în care atenția noastră este distribuită în mai multe direcții.

Pentru a nu ne expune unor cazuri de fraudă, este esențial să acordăm atenție unor semne care ne arată că anumite website-uri sau mesaje primite pot proveni din partea unor infractori cibernetici.

Pașii pe care trebuie să-i parcurgem pentru siguranța noastră sunt:

- Nu dezvăluim datele de pe cardul personal: nume, număr, data de expirare, PIN, CVV2/CVC adică numărul de trei cifre de pe spatele cardului;
- Nu furniza niciodată datele personale de utilizare a contului tău (parola de acces la contul bancar) altor persoane;
- Site-ul pe care urmează să introduci datele cardului pentru efectuarea unei plăți online trebuie să fie securizat, adică linkul începe cu **https**;
- Nu furniza datele online, telefonic sau prin alte canale de comunicare (WhatsApp, SMS, pagini web etc.);
- Cardul este un instrument de plată și nu un instrument de încasare bani, astfel că cererea datelor cardului de către alte persoane este o capcană;
- Dacă trebuie să primești bani atunci trebuie să dai IBAN-ul, nu datele de pe card;
- Nu introduce codul PIN pe site-uri de internet și nu-l divulga telefonic;
- Nu scrie niciodată codul PIN pe spatele cardului.

Știm că de Crăciun primim multe link-uri cu felicitări funny de la rudele noastre sau în perioada reducerilor, cumpărături unice oferite de diferite branduri, însă **nu accesa linkuri suspecte, primite pe mail sau prin SMS, și nu completa datele tale pe acestea.**

Articol Campanie „Nu-ți da CVC-ul”

Dacă vrei să nu fi victima unei infracțiuni cibernetice, ține cont și de următoarele recomandări:

- Nu accesa linkuri suspecte, primite pe mail sau prin SMS și nu completa datele tale pe acestea;
- Băncile niciodată nu solicită 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;
- Verifică cu atenție înainte de a deschide un mesaj sau un fișier de la banca ta sau alte persoane / instituții;
- Atenție la mesajele care conțin formule de adresare impersonale, greșeli gramaticale, de exprimare;
- Verifică dacă e-mail-ul provine dintr-o sursă legitimă;
- Nu efectuați transferuri și nu procesați operațiuni doar în baza unui e-mail sau a unei solicitări telefonice urgente;
- Instalați cele mai recente actualizări ale sistemului de operare și un antivirus.

Chiar dacă urmează o perioadă intensă, în care vrem să cumpărăm repede tot ce ne dorim pentru cei dragi, trebuie să avem grijă să nu cădem în capcana infractorilor cibernetici.

Ce fac în caz de fraudă?

<https://sigurantaonline.ro/ce-fac-in-caz-de-frauda/>