GHID PRACTIC DE PROTECȚIE DIGITALĂ PENTRU UTILIZATORI

E momentul perfect pentru curățenie în viața digitală. Urmează sfaturile următoare și vei fi în siguranță tot anul.

SIGURANȚA ONLINE.RO

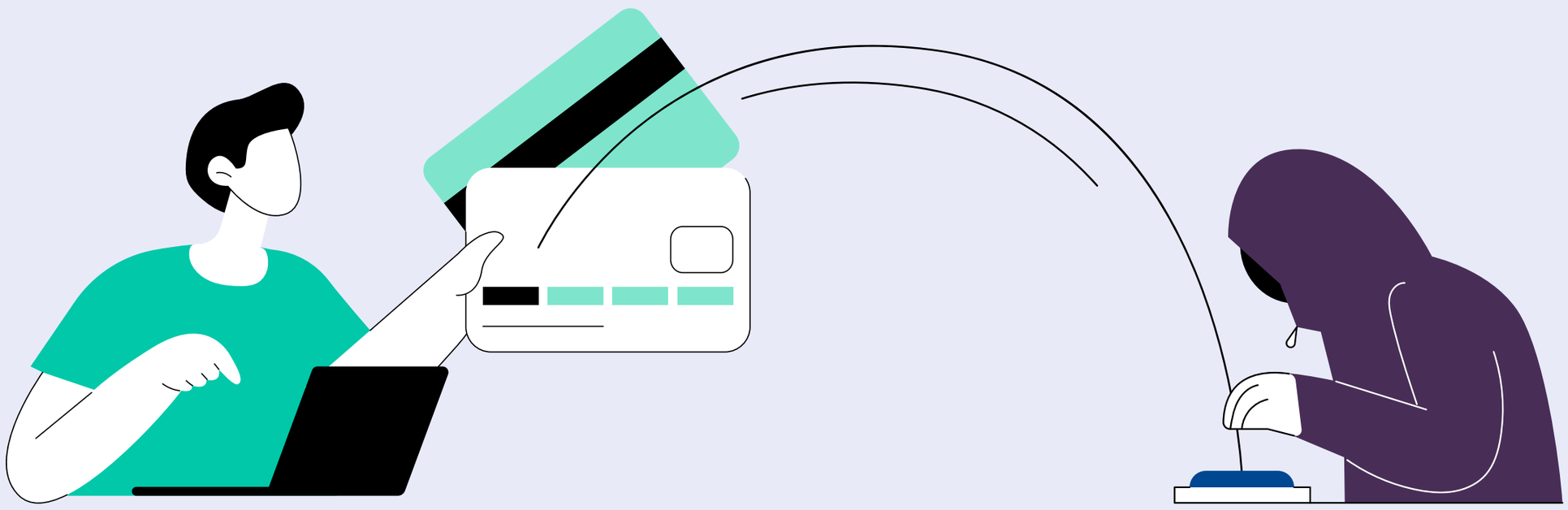
POLIȚIA ROMÂNĂ

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

O inițiativă

asociația română a băncilor

SIGURANȚA ONLINE.RO



Frauda se întâmplă pentru că:

Furnizezi datele bancare cum sunt cele de pe card, parole sau coduri de securitate;

Oferi acces la aplicațiile de Internet sau Mobile Banking, fie prin furnizarea username și a parolei sau instalezi aplicații de control la distanță la solicitarea unor persoane necunoscute;

Accesezi linkuri primite din surse suspecte și introduci date pe acestea;

Te încrezi în cei care te sună să te fraudeze fără să faci verificări;

„Investești” în folosul fraudatorilor.

SIGURANȚA ONLINE.RO

1. Atenție la link-uri suspecte!

Un link primit pe e-mail, SMS sau pe rețele sociale poate fi o capcană bine deghizată.

Hackerii sunt activi în permanență și se pricep să facă mesajele periculoase să pară nevinovate. Înainte să dai click, oprește-te și întreabă-te: așteptam acest mesaj? Îl cunosc pe cel care l-a trimis? Dacă ai orice îndoială, nu da click! Un singur click greșit poate compromite tot ce ai construit.

Dacă îți solicită astfel datele cardului sau datele de logare la Internet / Mobile Banking (username și parolă), este FRAUDĂ! Vigilența e cel mai bun scut al tău!

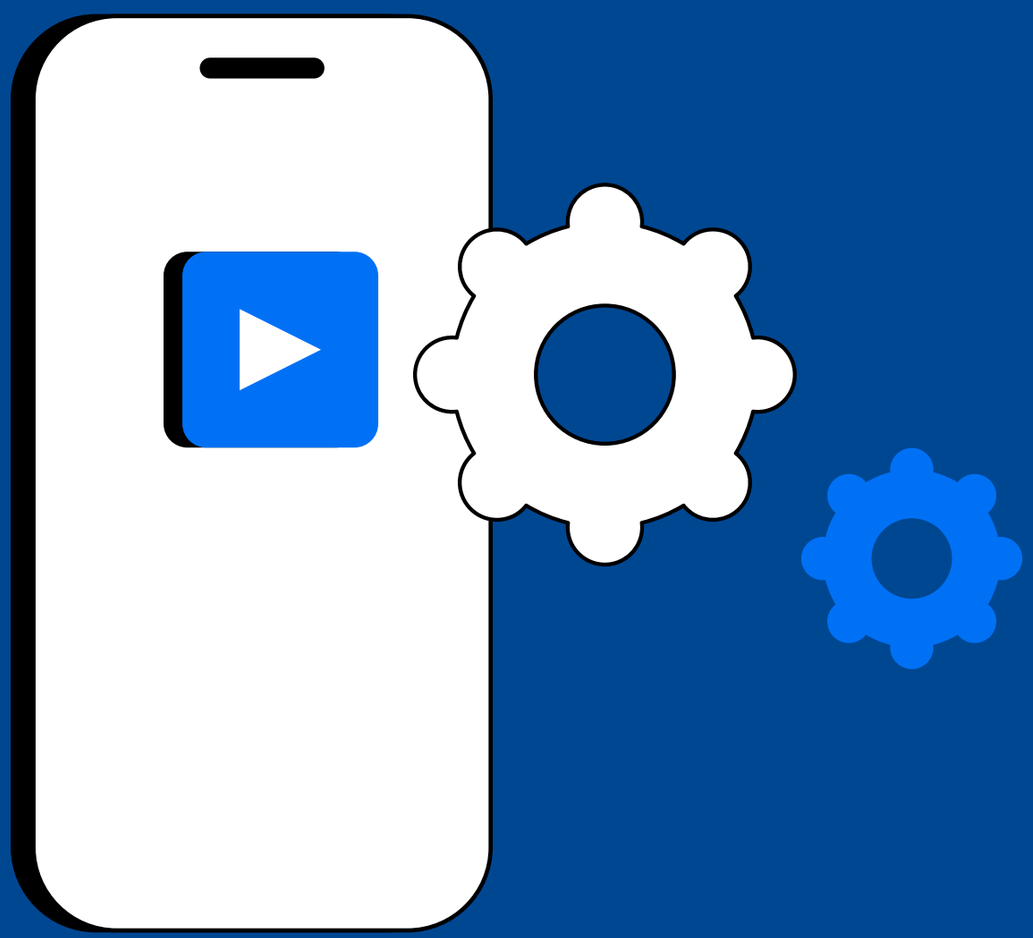
SIGURANȚA ONLINE.RO

2. Datele cardului tău sunt doar ale tale!

Cardul bancar este un instrument prin care TU plătești, nu prin care primești bani. Dacă trebuie să primești bani, trebuie să furnizezi IBAN-ul, nu datele de pe card.

Dacă cineva îți solicită numărul cardului, data expirării sau codul de securitate format din 3 cifre pretinzând că îți va face un transfer, te minte! Datele cardului trebuie folosite exclusiv de către posesorul cardului când face plăți online pe site-uri securizate (cu https și lacătul închis) și verificate și nu atunci când este conectat la rețele WI-FI publice.

SIGURANȚA ONLINE.RO



3. Verifică și actualizează aplicațiile de pe telefon!

Verifică ce aplicații ai instalate, șterge-le pe cele neutilizate și actualizează-le pe toate celelalte.

Actualizările conțin corecții esențiale de securitate pe care hackerii știu să le exploateze dacă le ignori. Setează deblocarea cu amprentă sau PIN robust și instalează un antivirus de calitate.

Un telefon actualizat și protejat nu te trădează niciodată. NU instala aplicații de control la distanță la solicitarea unor persoane necunoscute!

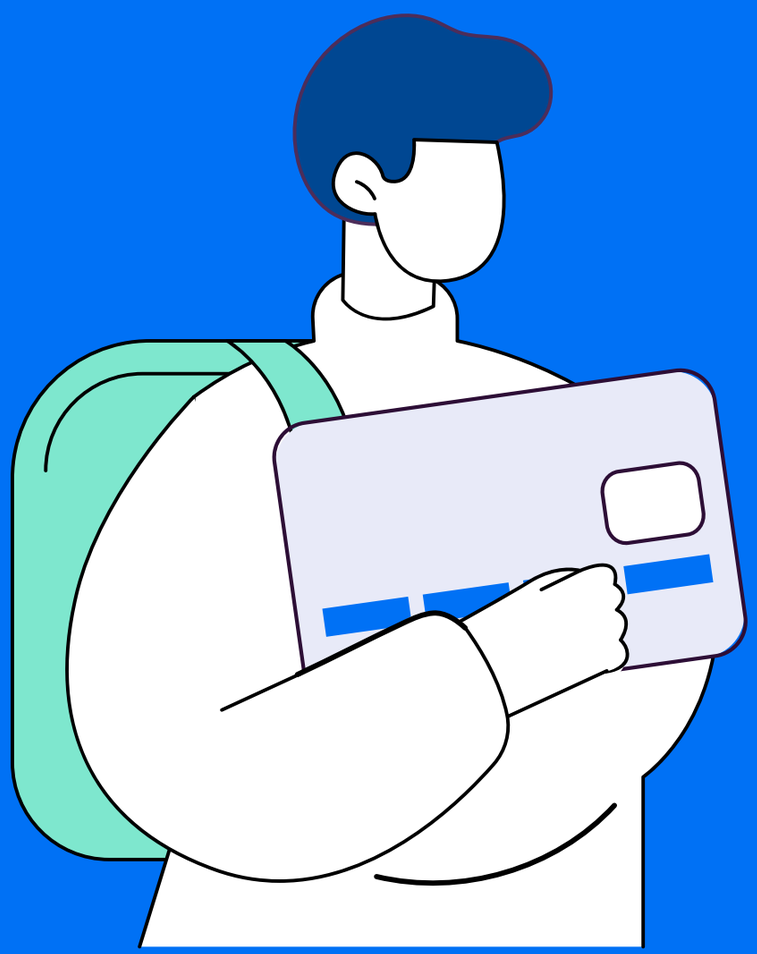
SIGURANȚA ONLINE.RO

4. „Zero riscuri și câștiguri garantate”? E o fraudă!

Dacă cineva îți promite „oportunitate unică de investiție”, „profit garantat rapid” sau „risc zero“, să știi că e o fraudă. Nicio investiție legitimă nu vine cu astfel de garanții. Dacă sună prea bine ca să fie adevărat, înseamnă că nu e. Închide apelul sau pagina, nu o distribui și raportează-o !

Dacă vrei să investești verifică pe site-ul www.asfromania.ro ca acea instituție să fie autorizată.

SIGURANȚA ONLINE.RO



5. Revizuiește regulile digitale pentru cei mici!

Nicio informație personală nu se dezvăluie în jocuri sau pe rețele sociale, iar datele cardului părinților sunt strict interzise fără acordul explicit al unui adult. Copiii sunt ținte preferate ale escrocilor tocmai pentru că sunt mai încrezători. Petrece timp cu cei mici și verifică împreună ce aplicații folosesc și cu cine vorbesc online.

SIGURANȚA ONLINE.RO

6. Verifică setările de confidențialitate pe rețelele sociale!

De când n-ai mai verificat cine îți poate vedea profilul pe rețelele sociale? Intră în setările de confidențialitate ale fiecărui cont și limitează accesul la informațiile tale personale – fotografii, postări, listă de prieteni – doar la persoanele în care ai cu adevărat încredere. Hackerii colectează date din profilurile publice pentru a construi atacuri personalizate.

SIGURANȚA ONLINE.RO

7. Ignoră apelurile suspecte de la „bănci” sau alte instituții!

Nu te lăsa manipulat, indiferent de cine te sună! Nicio bancă sau instituție nu îți va cere vreodată parole, coduri sau date personale prin telefon, SMS sau e-mail. Aceasta e o metodă clasică de fraudă. Dacă primești un astfel de apel, închide și sună direct la numărul oficial al băncii tale sau la instituția invocată în discuție. Banca nu te va suna să-ți spună că s-a aprobat creditul dacă tu nu ai solicitat unul, e un fraudator la telefon.

Chiar dacă cineva îți spune numele tău, denumirea băncii la care ai cont și IBAN-ul, nu te încrede! Sună tu direct la banca ta!

Pe ecranul telefonului tău poate să apară denumirea unei instituții, dar recomandarea este să nu crezi că e adevărat pentru că multe fraude așa se produc.

SIGURANȚA ONLINE.RO

8. Actualizează-ți parolele regulat!

O parolă veche e o parolă vulnerabilă.

Generează parole noi, complexe, unice pentru fiecare cont și stochează-le într-un manager de parole dedicat.

Nu folosi aceeași parolă în mai multe locuri - dacă un cont e compromis, celelalte trebuie să rămână protejate.

Dacă le știi pe toate pe de rost, e semn clar că trebuie schimbate.

SIGURANȚA ONLINE.RO

9. Activează autentificarea în doi pași (2FA)!

Chiar dacă cineva îți află parola, nu va putea accesa contul fără un al doilea cod de verificare. Activează 2FA la toate conturile importante: e-mail, banking, rețele sociale, magazine online. E cel mai simplu și mai eficient upgrade de securitate pe care îl poți face!

SIGURANȚA ONLINE.RO

10. Nu folosi rețele Wi-Fi publice pentru plăți online!

Niciodată nu introduce datele cardului sau nu te autentifica în conturi sensibile când ești conectat la o rețea Wi-Fi publică sau nesecurizată. Rețelele deschise nesecurizate pot fi monitorizate de atacatori care îți interceptează datele în timp real. Cumpărăturile online se fac exclusiv de pe rețeaua protejată de acasă sau prin date mobile.

SIGURANȚA ONLINE.RO

Dacă ai fost victima unei fraude online, urmează următorii pași:

1. Contactează imediat banca pentru a lua măsurile care se impun.
2. Contactează Poliția pentru a depune o plângere necesară deschiderii unei investigații.
3. Raporteaza incidentul pe platforma dedicată **pnrisc.dnsc.ro** sau la numărul de urgență **1911**, contribuind astfel la prevenirea altor incidente și la limitarea impactului acestor tipuri de atacuri.