Finanțat de
Uniunea Europeană

CRJM
Drepturi și justiție pentru toți

ECOCONTACT
Centrul de informare și consultanță de mediu Aarhus

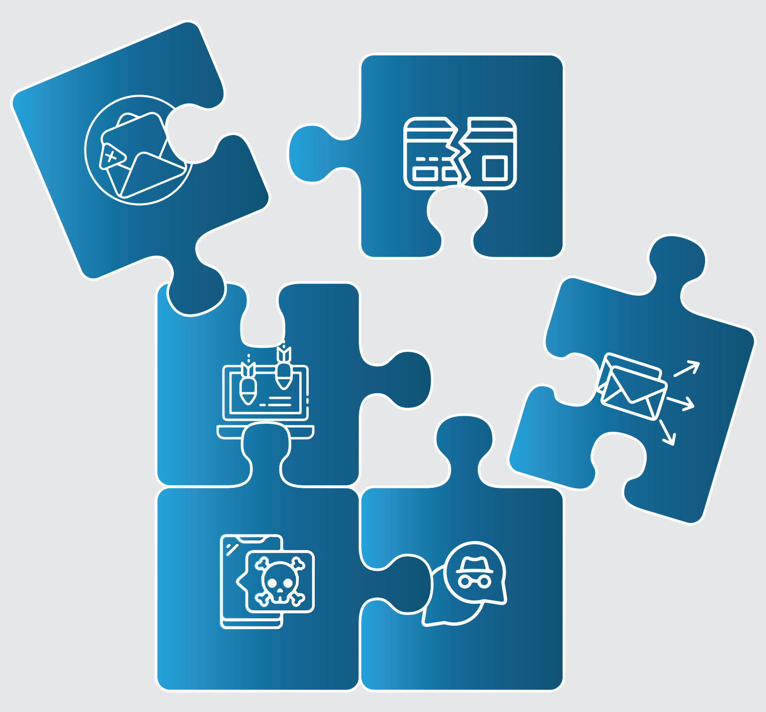
INSTRUMENTE PRACTICE

7 PAȘI PENTRU SECURITATEA CIBERNETICĂ A APĂRĂTORILOR DREPTURILOR OMULUI

(...ȘI NU NUMAI)

*Orice titulatură din acest infografic, utilizată la masculin sau feminin, se referă și se aplică în mod egal tuturor, indiferent de gen.

RISCURI POTENȚIALE



Spargerea adresei electronice și a conturilor sociale

Atacuri de tip DDoS asupra site-urilor gestionate de activiști

Atacuri și amenințări pe rețelele de socializare

Tentative de preluare a aplicațiilor bancare

Interceptarea comunicărilor electronice

Instalarea virușilor de spionare sau de compromitere tehnică

Pentru a verifica dacă datele Dumneavoastră au fost compromise pe anumite platforme pe care le-ați utilizat, accesați

Haveibeenpwned.com

Pentru a verifica dacă pe dispozitivele Dumneavoastră sunt instalați viruși, rulați

Un program antivirus licențiat

1 Creați parole puternice

Evitați crearea parolelor cu numele Dumneavoastră sau data nașterii. Folosiți parole lungi de minim 12 caractere și simboluri, unice pentru fiecare platformă sau aplicație folosită. Puteți încerca crearea parolelor după anumite sisteme, cum ar fi utilizarea primelor litere dintr-un vers cunoscut.

Exemplu: **L**imba **n**oastră-i **o** **c**omoară, **Î**n **a**dâncuri **î**nfundată → **Lnoc,Îaî**@LimbaNoastră

Pentru o mai bună gestionare a parolelor se recomandă utilizarea aplicațiilor precum:

- 1Password
- Dashline Premium
- Bitwarden

2 Activați autentificarea cu mai mulți factori

Poștele electronice, mesageriile, spațiile de stocare online și platformele pe care stocați cardurile bancare trebuie accesate neapărat prin autentificarea cu mai mulți factori.

Se recomandă utilizarea aplicațiilor de autentificare precum:

- Microsoft Authenticator
- Authy
- Google Authentificator

3 Mențineți dispozitivele actualizate

Actualizați sistemele de operare ale telefonului și computerului. În asemenea mod se asigură o mai bună funcționalitate a dispozitivelor și sunt eliminate potențiale breșe de securitate identificate de atacatori.

- Windows
- Mac OS
- Android
- iOS

4 Fiți precauți la „ofertele” gratuite

Tratați cu suspiciune e-mailurile, notificările pop-up sau alte tipuri de mesaje care vă anunță despre softuri, acțiuni sau oferte pe care nu le-ați solicitat.

5 Utilizați o Rețea Privată Virtuală (VPN) când vă conectați la Wi-Fi

Instalați un serviciu VPN și activați-l de fiecare dată când vă conectați la orice rețea Wi-Fi, întrucât acestea sunt detectabile și pot fi interceptate de către atacatori. Rețeaua Privată Virtuală creează un tunel criptat impenetrabil prin care este accesat internetul.

- NordVPN
- ExpressVPN
- ProtonVPN

6 Închideți conexiunile Wi-Fi și Bluetooth atunci când nu le utilizați

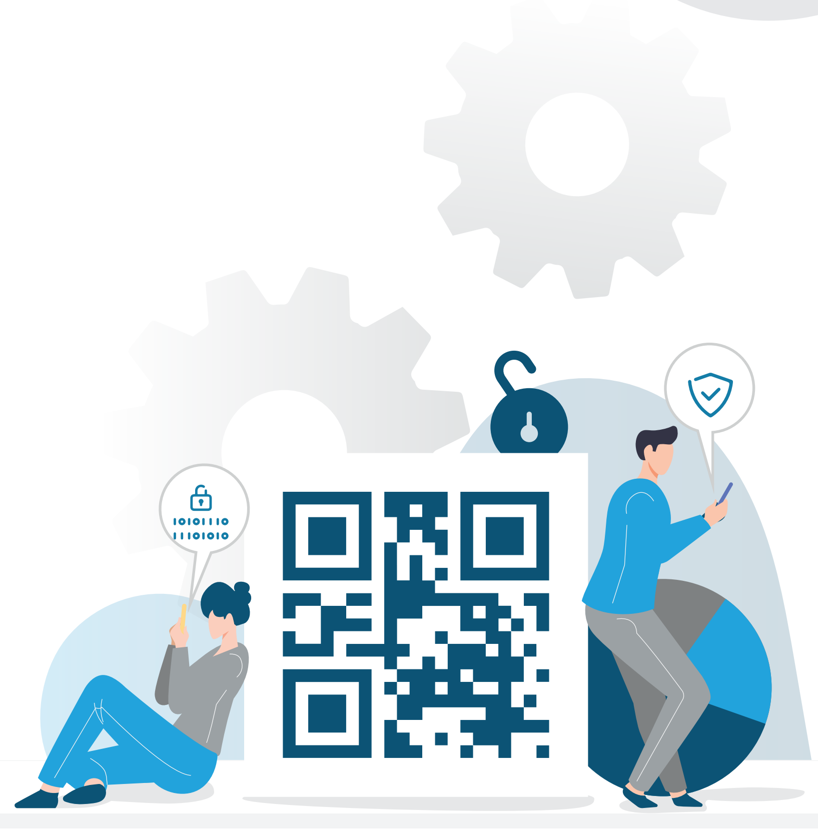
Această acțiune limitează punctele de acces prin care atacatorii v-ar putea intercepta. Pe lângă asta, contribuie la economia stocului de energie din bateria dispozitivului. De asemenea, eliminați rețelele Wi-Fi la care v-ați conectat anterior, mai ales dacă au fost înregistrate ca loc de muncă sau domiciliu.

- Windows
- MacOS

7 Scanați adresa web

Uneori, site-ul organizației sau blogul personal pot fi o pradă atractivă pentru atacatorii care au scopul de a vă intimida sau perturba activitatea. Există câteva instrumente gratuite care vă pot ajuta să identificați vulnerabilitățile.

- MX Toolbox
- Wormly
- Securi



Acest infografic a fost produs cu sprijinul financiar al Uniunii Europene în cadrul proiectului „Scut pentru apărătorii drepturilor omului - Sprijin apărătorilor drepturilor omului în Republica Moldova”, implementat de Centrul de Resurse Juridice din Moldova (CRJM). Conținutul prezentat este responsabilitatea exclusivă a CRJM și nu reflectă neapărat viziunea Uniunii Europene.