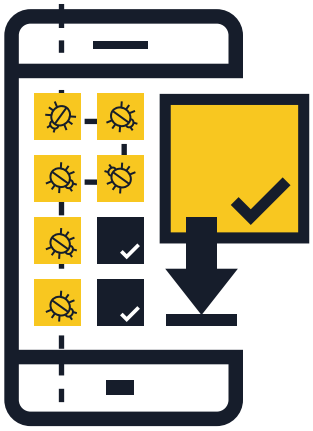
MALWARE PE DISPOZITIVELE MOBILE

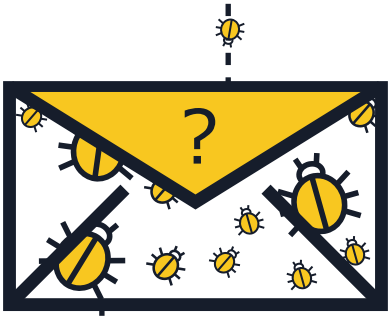
IDEI ŞI SFATURI UTILE PENTRU A VĂ PROTEJA

1 Instalaţi numai aplicaţii care provin din surse de încredere



- **Cumpăraţi aplicaţii din magazine oficiale** — Înainte de a descărca o aplicaţie, verificaţi atât aplicaţia, cât şi persoanele care au publicat-o. Aveţi grijă la linkurile pe care le primiţi în e-mail şi mesajele text care vă pot păcăli să instalaţi aplicaţii de la un terţ sau din surse necunoscute.
- **Verificaţi recenziile şi calificativele acordate de alţi utilizatori,** dacă sunt disponibile.
- **Citiţi permisiunile aplicaţiei** — Verificaţi ce tipuri de date poate accesa aplicaţia şi dacă vă poate partaja informaţiile cu alte părţi. Dacă aveţi suspiciuni sau nu vă simţiţi confortabil cu specificaţiile termenilor, nu descărcaţi aplicaţia.

2 Nu faceţi clic pe linkurile sau anexele din e-mailurile nesolicitate sau mesajele text



- **Nu aveţi încredere în linkurile din e-mailurile nesolicitate sau mesajele text necunoscute** (SMS şi MMS) — Ştergeţi-le de îndată ce le primiţi.
- **Verificaţi de două ori adresele URL şi codurile QR abreviate** — Acestea pot conduce la pagini web nocive sau pot descărca direct malware pe dispozitivul dvs. Înainte de a face clic, utilizaţi o pagină web de previzualizare URL pentru a confirma faptul că adresa web este legitimă. Înainte de a scana un cod QR, alegeţi un cititor QR care previzualizează adresa web încorporată şi utilizaţi un software de securitate mobilă care vă avertizează cu privire la linkurile periculoase.

3 După efectuarea unei plăţi, deconectaţi-vă de pe paginile web

- **Nu salvaţi niciodată numele de utilizator şi parolele în browser-ul mobil sau aplicaţiile mobile** — Dacă pierdeţi sau vi se fură telefonul sau tableta, oricine se poate conecta la conturile dvs. După finalizarea tranzacţiei, deconectaţi-vă de la pagina web în loc să închideţi pur şi simplu browser-ul.
- **Nu efectuaţi operaţiuni bancare sau cumpărături online folosind conexiunile publice Wi-Fi** — Efectuaţi operaţiuni bancare şi tranzacţii online numai din reţelele pe care le cunoaşteţi şi în care aveţi încredere.
- **Verificaţi de două ori adresa URL a paginii web** — Asiguraţi-vă că adresa web este legitimă,înainte de a vă conecta sau a trimite informaţii sensibile. Luaţi în considerare descărcarea aplicaţiei oficiale a băncii pentru a vă asigura că vă conectaţi întotdeauna la o pagină web reală.

4 Actualizaţi-vă sistemul de operare şi aplicaţiile

- **Descărcaţi actualizări software pentru sistemul de operare al dispozitivului mobil de îndată ce vi se solicită acest lucru** — Având instalate cele mai recente actualizări, nu numai că dispozitivul dvs. va fi mai sigur, dar va funcţiona mai bine.

5 Opriţi Wi-Fi-ul, serviciile de localizare şi Bluetooth-ul atunci când nu le utilizaţi

- **Opriţi conexiunea Wi-Fi dacă nu o utilizaţi** — Infractorii cibernetici vă pot accesa informaţiile în cazul în care conexiunea nu este sigură. Dacă este posibil, utilizaţi conexiuni de date 3G sau 4G în locul punctelor de acces la internet wireless. De asemenea, puteţi opta pentru un serviciu de reţea virtuală privată (VPN) pentru a vă păstra datele criptate în tranzit.
- **Nu permiteţi aplicaţiilor să utilizeze serviciile de localizare decât dacă acest lucru este necesar** — Aceste informaţii pot fi partajate sau divulgate şi utilizate pentru a promova anunţuri cu privire la locurile în care vă aflaţi.
- **Opriţi Bluetooth-ul atunci când nu aveţi nevoie de el** — Asiguraţi-vă că este complet oprit şi că nu se află doar în modul invizibil. Setările implicite sunt deseori configurate în prealabil pentru a permite altor persoane să se conecteze la dispozitivul dvs. fără ca dvs. să ştiţi. Utilizatorii rău intenţionaţi vă pot copia fişierele, accesa alte dispozitive ataşate sau chiar obţine acces la distanţă la telefonul dvs. pentru a efectua apeluri şi trimite mesaje text, având drept rezultat facturi mari.

6 Evitaţi să vă faceţi cunoscute informaţiile personale

- **Nu răspundeţi niciodată oferind informaţii personale** la mesajele text sau e-mailurile care pretind că sunt de la banca dvs. sau o altă companie legitimă. În schimb, contactaţi direct compania pentru a confirma solicitarea acestora.
- **Analizaţi periodic situaţiile de plată aferente dispozitivului dvs. mobil pentru a identifica orice cheltuieli suspicioase** — Dacă identificaţi cheltuieli pe care nu le-aţi efectuat, contactaţi imediat furnizorul de servicii.

7 Nu efectuaţi o operaţiune de jailbreak pe dispozitivul dvs.

- Jailbreaking este procesul prin care se elimină limitările de securitate impuse de vânzătorul sistemului de operare, oferind acces complet la sistemul de operare şi funcţii — **Efectuând o operaţiune de jailbreak pe dispozitivul dvs., securitatea acestuia poate fi redusă semnificativ**, oferind breşe de securitate care nu erau aparente imediat.

8 Efectuaţi o copie de siguranţă a datelor dvs.

- **Numeroase dispozitive smartphone şi tablete au capacitatea de a efectua wireless o copie de siguranţă a datelor** — Consultaţi opţiunile în funcţie de sistemul de operare a dispozitivului dvs. Creând o copie de siguranţă pentru dispozitivul dvs. smartphone sau tabletă, vă puteţi restaura cu uşurinţă datele personale dacă dispozitivul a fost pierdut, furat sau deteriorat.

9 Instalaţi o aplicaţie de securitate mobilă

- Toate sistemele de operare sunt supuse riscului de infecţie. Dacă este disponibilă, utilizaţi o **soluţie de securitate mobilă** care detectează şi previne malware, spyware şi aplicaţiile rău intenţionate, precum şi alte funcţii care vă protejează confidenţialitatea şi funcţii anti-furt.

EUROPOL EC3 European Cybercrime Centre | POLIŢIA ROMÂNĂ | DIICOT | CERT.RO | #MobileMalware