

MALWARE PE DISPOZITIVELE MOBILE



IDEI ȘI SFATURI UTILE PENTRU A VĂ PROTEJA

1 Instalați numai aplicații care provin din surse de încredere

- **Cumpărați aplicații din magazine oficiale** — Înainte de a descărca o aplicație, verificați atât aplicația, cât și persoanele care au publicat-o. Aveți grijă la linkurile pe care le primiți în e-mail și mesajele text care vă pot păcăli să instalați aplicații de la un terț sau din surse necunoscute.
- **Verificați recenziile și calificativele acordate de alți utilizatori**, dacă sunt disponibile.
- **Citiți permisiunile aplicației** — Verificați ce tipuri de date poate accesa aplicația și dacă vă poate partaja informațiile cu alte părți. Dacă aveți suspiciuni sau nu vă simțiți confortabil cu specificațiile termenilor, nu descărcați aplicația.



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

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



3 După efectuarea unei plăți, deconectați-vă de pe paginile web

- **Nu salvați niciodată numele de utilizator și parolele în browser-ul mobil sau aplicațiile mobile** — Dacă pierdeți sau vi se fură telefonul sau tableta, oricine se poate conecta la conturile dvs. După finalizarea tranzacției, deconectați-vă de la pagina web în loc să închideți pur și simplu browser-ul.
- **Nu efectuați operațiuni bancare sau cumpărături online folosind conexiunile publice Wi-Fi** — Efectuați operațiuni bancare și tranzacții online numai din rețelele pe care le cunoașteți și în care aveți încredere.
- **Verificați de două ori adresa URL a paginii web** — Asigurați-vă că adresa web este legitimă, înainte de a vă conecta sau a trimite informații sensibile. Luați în considerare descărcarea aplicației oficiale a băncii pentru a vă asigura că vă conectați întotdeauna la o pagină web reală.



4 Actualizați-vă sistemul de operare și aplicațiile

- **Descărcați 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 funcționa mai bine.



MALWARE PE DISPOZITIVELILE MOBILE



IDEI ȘI SFATURI UTILE PENTRU A VĂ PROTEJA

5 Opriți Wi-Fi-ul, serviciile de localizare și Bluetooth-ul atunci când nu le utilizați

- **Opriți conexiunea Wi-Fi dacă nu o utilizați** — Infractorii cibernetici vă pot accesa informațiile în cazul în care conexiunea nu este sigură. Dacă este posibil, utilizați conexiuni de date 3G sau 4G în locul punctelor de acces la internet wireless. De asemenea, puteți opta pentru un serviciu de rețea virtuală privată (VPN) pentru a vă păstra datele criptate în tranzit.
- **Nu permiteți aplicațiilor să utilizeze serviciile de localizare decât dacă acest lucru este necesar** — Aceste informații pot fi partajate sau divulgate și utilizate pentru a promova anunțuri cu privire la locurile în care vă aflați.
- **Opriți Bluetooth-ul atunci când nu aveți nevoie de el** — Asigurați-vă că este complet oprit și 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 știți. Utilizatorii rău intenționați vă pot copia fișierele, accesa alte dispozitive atașate sau chiar obține acces la distanță la telefonul dvs. pentru a efectua apeluri și trimite mesaje text, având drept rezultat facturi mari.



6 Evitați să vă faceți cunoscute informațiile personale

- **Nu răspundeți niciodată oferind informații personale** la mesajele text sau e-mailurile care pretind că sunt de la banca dvs. sau o altă companie legitimă. În schimb, contactați direct compania pentru a confirma solicitarea acestora.
- **Analizați periodic situațiile de plată aferente dispozitivului dvs. mobil pentru a identifica orice cheltuieli suspicioase** — Dacă identificați cheltuieli pe care nu le-ați efectuat, contactați imediat furnizorul de servicii.

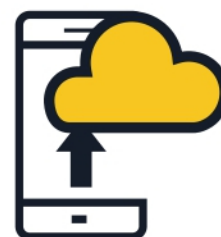


7 Nu efectuați o operațiune de jailbreak pe dispozitivul dvs.

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

8 Efectuați o copie de siguranță a datelor dvs.

- **Numeroase dispozitive smartphone și tablete au capacitatea de a efectua wireless o copie de siguranță a datelor** — Consultați opțiunile în funcție de sistemul de operare a dispozitivului dvs. Creând o copie de siguranță pentru dispozitivul dvs. smartphone sau tabletă, vă puteți restaura cu ușurință datele personale dacă dispozitivul a fost pierdut, furat sau deteriorat.



9 Instalați o aplicație de securitate mobilă

- Toate sistemele de operare sunt supuse riscului de infecție. Dacă este disponibilă, utilizați o **soluție de securitate mobilă** care detectează și previne malware, spyware și aplicațiile rău intenționate, precum și alte funcții care vă protejează confidențialitatea și funcții anti-furt.