DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Recomandări pentru securitatea dispozitivelor mobile

AUGUST 2025

TLP:CLEAR

Cuprins

Sumar executiv

Acest document oferă utilizatorilor de dispozitive mobile recomandări pentru protejarea datelor și a dispozitivelor împotriva amenințărilor cibernetice. Acesta explică diferențele de securitate dintre sistemele de operarea Android și iOS, prezintă principalele tipuri de atacuri cibernetice, de la phishing și malware, la exploatarea vulnerabilităților, și propune măsuri simple de protecție precum actualizarea software-ului, gestionarea atentă a aplicațiilor, utilizarea conexiunilor securizate, criptarea datelor și realizarea de backup-uri regulate. Scopul este de a ajuta publicul larg să adopte obiceiuri digitale mai sigure și să își reducă expunerea la riscuri.

Introducere

În prezent, smartphone-ul a devenit un instrument indispensabil al vieții cotidiene. Este utilizat zilnic pentru comunicare, muncă, acces la informații, divertisment sau plăți. Astfel, securitatea cibernetică pe dispozitivele mobile nu mai reprezintă o opțiune, ci o necesitate reală. Fiecare utilizator de telefon inteligent trebuie să fie conștient de riscurile la care este expus și să adopte măsuri simple și eficiente de protecție a datelor și dispozitivelor.

Importanța acestui subiect este susținută și de datele privind modul în care este accesat Internetul. La nivel global, peste 60% din traficul web este generat de pe dispozitive mobile, în timp ce traficul de pe calculatorul personal reprezintă mai puțin de 40%[1].

În România, tendința este similară (Figura 1): aproximativ 53% din traficul online provine de pe telefoane mobile, comparativ cu 47% de pe computere[2]. Mai mult, România avea, la începutul anului 2025, peste 25 de milioane de conexiuni mobile active, depășind chiar numărul de locuitori, și o rată de accesare a Internetului de către 94% din populație[3]. Aceste cifre demonstrează că telefonul mobil a devenit principalul punct de acces la viața digitală și, implicit, una dintre cele mai importante suprafețe de atac din punct de vedere cibernetic.

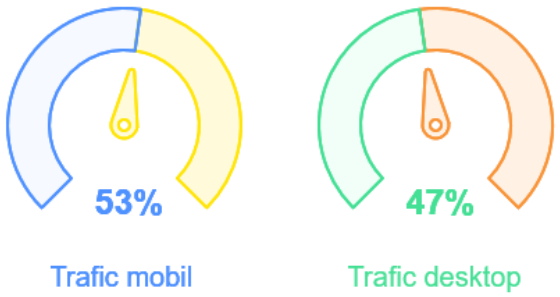


Figura 1 - Utilizarea Internetului în Romania - 2025

Sistemele de operare ale dispozitivelor mobile

Dispozitivele mobile funcționează pe o varietate de platforme software (sisteme de operare), în ultimii ani piața fiind dominată de Android (dezvoltat de Google) și iOS (dezvoltat de Apple). La nivel global, aceste două sisteme de operare dețin împreună peste 99% din piața smartphone-urilor, cu Android la aproximativ 72% și iOS 27%, în timp ce alte platforme (KaiOS, Windows Mobile etc.) însumează sub 1%[4].

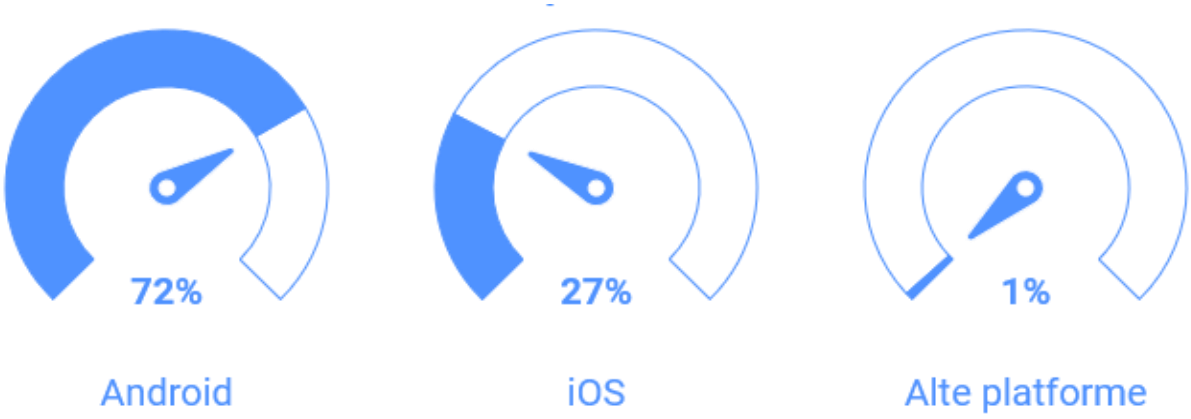


Figura 2 - Cota de piață a sistemelor de operare

[1] https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet
[2] https://gs.statcounter.com/platform-market-share/desktop-mobile/romania
[3] https://datareportal.com/reports/digital-2025-romania
[4] https://gs.statcounter.com/os-market-share/mobile/worldwide

Android este un sistem de operare open-source bazat pe nucleul Linux, utilizat de numeroși producători de telefoane și tablete (Samsung, Motorola, Huawei, Xiaomi, ș.a.), ceea ce contribuie la popularitatea sa. iOS este un sistem de operare proprietar, disponibil exclusiv pe dispozitivele Apple (iPhone, iPad), care se diferențiază printr-un ecosistem închis și un control strict al actualizărilor, furnizate direct de Apple.

Alte sisteme de operare mobile au o prezență redusă. Windows Mobile (dezvoltat de Microsoft) a fost o platformă populară în anii 2000, însă suportul a fost întrerupt în 2017, după ce cota sa de piață scăzuse sub 1%. KaiOS, un sistem de operare derivat din proiectul Firefox OS, este destinat așa-numitelor smart feature phones (telefoane cu funcții de bază dar cu acces la Internet). KaiOS a înregistrat peste 130 de milioane de dispozitive la nivel mondial, devenind al treilea sistem de operare mobil ca răspândire globală, deși cu o cotă procentuală mică raportat la Android și iOS[5]. Există și alte platforme de nișă (de exemplu, BlackBerry OS, Symbian, Sailfish OS, Tizen), însă influența lor actuală este neglijabilă.

Securitatea platformelor

Securitatea unui dispozitiv mobil este strâns legată de platforma pe care o utilizează. Principalele platforme Android și iOS adoptă abordări diferite în ceea ce privește controlul asupra aplicațiilor și accesul la sistem. Android prioritizează libertatea utilizatorului și permite instalarea de aplicații din surse externe, în timp ce iOS are un control strict asupra aplicațiilor și actualizărilor, pentru a reduce vectorii de atac.

Pe Android[6], fiecare aplicație rulează separat într-un spațiu izolat, iar accesul la funcții precum camera sau locația este permis doar cu acordul expres al utilizatorului. Aplicațiile trebuie semnate digital, iar stocarea este criptată pentru a proteja datele. Android include și un serviciu numit Google Play Protect, care scanează aplicațiile pentru a detecta comportamente periculoase. Pentru utilizatorii expuși unor riscuri mai ridicate, Android oferă un mod opțional de protecție avansată, ce include restricții asupra rețelelor Wi-Fi, porturilor USB și detectarea automată a tentativelor de fraudă.

În schimb, iOS[7] oferă un sistem mai controlat: aplicațiile pot fi instalate doar din App Store și trebuie semnate digital. Fiecare aplicație este izolată strict de celelalte, iar datele stocate sunt criptate automat la nivel hardware. Sistemul folosește un cip special (Secure Enclave) pentru gestionarea datelor biometrice și a cheilor criptografice. iOS include și funcții avansate de confidențialitate, cum ar fi ascunderea adresei IP, opțiunea „Hide My Email" pentru crearea de alias-uri care maschează adresa reală de e-mail și un mod de securitate extremă numit Lockdown Mode. Apple oferă actualizări rapide pentru remedierea vulnerabilităților, fără a necesita un update complet al sistemului de operare.

În acest material accentul va fi pus pe Android și iOS, platformele dominante, însă principiile generale de securitate se aplică, în linii mari, oricărui dispozitiv mobil conectat la Internet.

Amenințările cibernetice asupra dispozitivelor mobile

Dispozitivele mobile și utilizatorii acestora sunt ținte frecvente ale atacurilor cibernetice, mai ales datorită utilizării lor intensive în viața de zi cu zi. În cele ce urmează, vor fi prezentate cele mai întâlnite categorii de amenințări care vizează atât tehnologia, cât și comportamentul utilizatorilor.

Aceste amenințări includ atacuri de tip Man-in-the-Middle, exploatarea vulnerabilităților, malware, inginerie socială sau atacuri de tip DDoS, fiecare având potențialul de a compromite datele, funcționalitatea și securitatea dispozitivelor mobile (Figura 3). Ele pot exploata atât punctele tehnice slabe, cât și factorul uman, ducând la pierderi de informații, întreruperea serviciilor sau compromiterea confidențialității.

Phishing

În atacurile de tip **phishing**, utilizatorul este păcălit să dezvăluie informații sensibile (parole, date bancare, etc.) prin mesaje (SMS, WhatsApp, Messenger, etc.), aplicații sau site-uri ce par legitime. Atacatorul pretinde că este o entitate de încredere (o bancă, un serviciu cunoscut sau un contact real) și trimite e-mailuri, SMS-uri sau mesaje instantanee cu scopul de a determina utilizatorul să introducă datele sale într-o pagină sau aplicație falsă sau să descarce un fișier malițios.

---

[5] https://developer.kaiostech.com/docs/introduction/history/
[6] https://source.android.com/docs/security/features
[7] https://support.apple.com/guide/security sau https://support.apple.com/ro-ro/guide/personal-safety

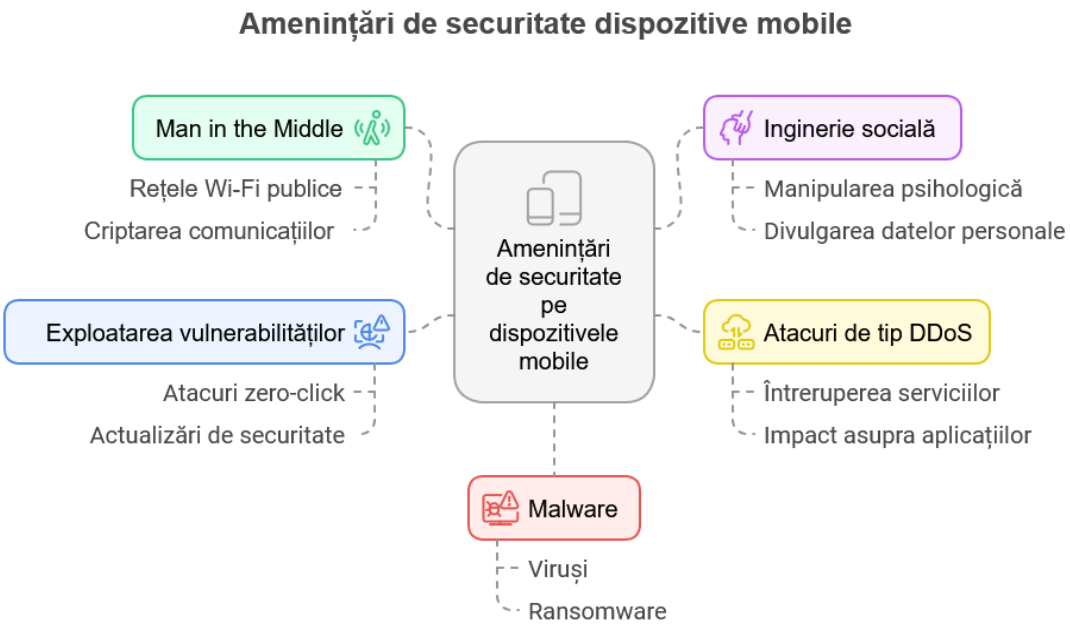


Figura 3 - Amenințări de securitate pe dispozitivele mobile

Pe dispozitivele mobile, phishing-ul ia adesea forme specifice: smishing (phishing prin SMS), vishing (phishing prin apel telefonic vocal) sau mesaje în aplicații populare de mesagerie sau rețele de socializare. Scopul final este furtul de date de autentificare, informații personale sau financiare, uneori ca prim pas în compromiterea unui cont sau dispozitiv.

Malware

Malware-ul este orice tip de program sau cod dăunător creat cu intenții malițioase. Acesta poate lua diverse forme precum viruși, viermi informatici, troieni (Trojan horses), ransomware, spyware ș.a.

Aceste programe pot infecta dispozitivele mobile compromițând funcționarea lor sau confidențialitatea datelor stocate. Pe mobil, malware-ul se răspândește adesea prin aplicații aparent legitime (de exemplu, aplicații descărcate din surse neoficiale ori clone ale unor aplicații populare) sau prin atașamente și link-uri malițioase. Consecințele pot fi grave, de la furtul datelor personale (mesaje, contacte, parole), monitorizarea activității, până la blocarea completă a accesului la dispozitiv (în cazul ransomware-ului).

Un exemplu actual îl reprezintă troianul de acces la distanță (Remote Access Trojan, RAT) Rafel[8], care oferă atacatorilor control de la distanță asupra telefonului infectat. Datele arată că 87,5% dintre dispozitivele Android compromise de acest malware rulau versiuni vechi de Android, fără actualizări de securitate, subliniind pericolul utilizării sistemelor de operare neactualizate.

O subcategorie specializată de malware o reprezintă **spyware,** conceput pentru a se ascunde pe dispozitiv și pentru a spiona utilizatorul, colectând pe ascuns date despre acesta. Programele de tip spyware pot înregistra apăsările de taste (keyloggers), pot accesa mesaje, conversații, lista de contacte și de apeluri, locația GPS și chiar camera sau microfonul dispozitivului, transmițând aceste informații către atacator.

Adesea, spyware-ul este atașat în aplicații aparent inofensive (inclusiv aplicații gratuite populare) și operează fără știrea utilizatorului. În funcție de scop, unele spyware sunt orientate pe furt de date personale (parole, date financiare), altele pe supraveghere pe termen lung (de exemplu, Pegasus[9] - un spyware avansat folosit în atacuri țintite, capabil să preia controlul complet al telefonului victimei). Indiferent de tip, spyware-ul reprezintă o gravă încălcare a confidențialității și poate fi dificil de detectat.

[8] https://www.dnsc.ro/citeste/alerta-rafel-remote-access-tool-rat-o-amenintare-cibernetica-ce-vizeaza-utilizatorii-de-android
[9] https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf

Man-in-the-Middle

În atacurile de tip **Man-in-the-Middle** (MitM) („Omul din mijloc”) atacatorul se interpune în mod invizibil între două dispozitive care comunică, interceptând și (posibil) modificând datele transmise între ele. În cazul dispozitivelor mobile, scenariul clasic implică rețele Wi-Fi publice nesecurizate, de exemplu, victima se conectează la o rețea Wi-Fi într-un loc public (o rețea creată de atacator, cu un nume tentant sau identic cu al unei entități legitime), iar atacatorul interceptează traficul necriptat. Astfel, datele transmise, parole, mesaje, informații financiare, pot fi citite și alterate.

Un atac de tip MitM poate fi realizat și în rețelele mobile, de exemplu, folosind dispozitive de tip fake cell tower pentru a intercepta comunicațiile GSM. Impactul unui astfel de atac este sever asupra confidențialității, iar detectarea sa de către utilizator este dificilă (utilizatorul nu își dă seama că traficul său este interceptat). Protecția este asigurată prin criptarea comunicațiilor (folosirea protocoalelor HTTPS/TLS pentru site-uri sau Virtual Private Networks (VPN) pentru securizarea traficului, etc.)

Inginerie socială

Unul dintre cele mai frecvente tipuri de atac la care pot fi expuși utilizatorii de telefoane mobile este ingineria socială. Acest tip de atac nu se bazează pe tehnologie avansată, ci pe manipularea psihologică a utilizatorului. Atacatorul se prezintă drept o persoană de încredere, de exemplu, un angajat al unei bănci, al unei instituții publice sau un reprezentant al serviciului de suport tehnic al unei companii cunoscute și încearcă să convingă utilizatorul să divulge date personale sau de autentificare.

Prin apeluri telefonice, mesaje sau e-mailuri aparent legitime, victima este indusă în eroare și determinată să ofere informații sensibile precum parole, coduri de securitate sau detalii despre conturi. Acest tip de atac este eficient pentru că exploatează neatenția sau buna-credință a utilizatorului, nu neapărat vulnerabilități tehnice ale dispozitivului.

Atacuri de tip DDoS

Atacurile de tip Distributed Denial of Service (DDoS) vizează blocarea sau întreruperea funcționării unui serviciu prin suprasolicitarea acestuia cu un număr foarte mare de cereri simultane. În cazul dispozitivelor mobile, aceste atacuri nu afectează direct telefonul utilizatorului, dar pot afecta indirect aplicațiile și serviciile pe care acesta le utilizează.

De exemplu, în timpul unui atac DDoS asupra serverelor unei aplicații mobile, utilizatorul ar putea experimenta întârzieri, erori sau imposibilitatea de a accesa funcționalități de bază. Deși acest tip de amenințare este mai puțin frecvent la nivel individual, el poate avea un impact semnificativ asupra disponibilității serviciilor utilizate zilnic, cum ar fi aplicațiile bancare, cele de plată sau de comunicare.

Exploatarea vulnerabilităților

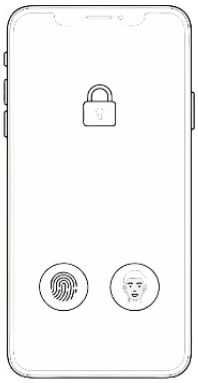
Un alt tip de risc îl reprezintă atacurile care exploatează vulnerabilități tehnice ale sistemului de operare sau ale aplicațiilor instalate pe telefon. Unele dintre aceste atacuri pot fi extrem de periculoase deoarece nu necesită nicio acțiune din partea utilizatorului. Așa-numitele atacuri „zero-click” permit compromiterea completă a dispozitivului doar prin trimiterea unui mesaj sau fișier special conceput, care este procesat automat de sistem.

De exemplu, un telefon poate fi infectat doar prin primirea unui mesaj multimedia care conține cod malițios, fără ca utilizatorul să fie nevoit să deschidă acel mesaj sau să apese pe vreun link. Aceste atacuri sunt foarte rare și presupun costuri ridicate pentru atacatori, fiind întâlnite în general în cazuri de spionaj cibernetic sau atacuri țintite asupra unor persoane de interes. Totuși, ele evidențiază cât de important este ca dispozitivul mobil să aibă sistemul de operare și aplicațiile actualizate permanent, pentru a beneficia de cele mai recente corecții de securitate.

Recomandări pentru protejarea datelor și a dispozitivelor mobile

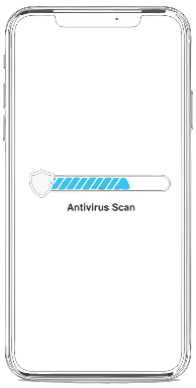
Pentru a preveni accesul neautorizat la informații și pentru a reduce riscurile cibernetice, este important ca fiecare utilizator, fie că folosește telefonul în scop personal sau profesional, să adopte un set de măsuri de bază. În cele ce urmează sunt prezentate recomandări utile pentru protejarea dispozitivului mobil, a datelor personale și a confidențialității.

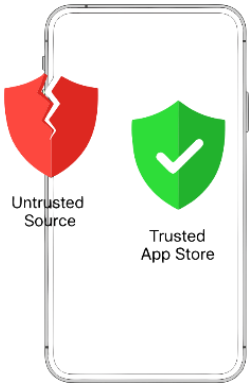
Actualizări regulate de securitate: păstrează sistemul de operare și aplicațiile instalate la zi. Activează actualizarea automată pentru a primi imediat cele mai noi îmbunătățiri de securitate. Verifică periodic dacă există actualizări disponibile și instalează-le fără întârziere, deoarece acestea corectează vulnerabilități care ar putea fi exploatate de atacatori.



Protecția ecranului de blocare: activează un cod PIN sau o parolă sigură pentru deblocarea telefonului, preferabil completate de amprentă sau recunoaștere facială. Setează blocarea automată a ecranului după câteva minute de inactivitate și activează opțiunea de ștergere a datelor după mai multe încercări greșite de autentificare. Astfel, în caz de pierdere sau furt, datele tale vor rămâne protejate.

Antivirus: instalarea unui antivirus de încredere pe telefonul mobil poate adăuga un nivel important de protecție. Acesta poate detecta aplicații periculoase, bloca accesul la site-uri de phishing și scana fișiere descărcate pentru conținut malițios. Unele soluții oferă și funcții suplimentare, precum protecție anti-furt, blocarea aplicațiilor sensibile sau alerte privind scurgerile de date. Un antivirus actualizat reduce riscul compromiterii dispozitivului în cazul unei greșeli umane sau al unei amenințări necunoscute.



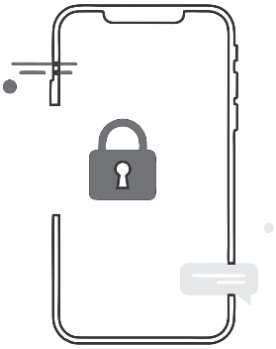


Instalarea aplicațiilor din surse sigure: instalează aplicații doar din surse oficiale, precum Google Play sau App Store, și evită aplicațiile din surse necunoscute sau modificate. Verifică ce permisiuni ai acordat fiecărei aplicații și dezactivează-le pe cele care nu sunt necesare. O aplicație simplă nu ar trebui să solicite acces la date sensibile. Șterge aplicațiile pe care nu le mai folosești pentru a reduce expunerea la riscuri.

Conexiuni sigure: evită conectarea la rețele Wi-Fi publice nesigure, cum sunt cele din cafenele, aeroporturi sau hoteluri. Acestea pot fi ușor de interceptat, iar datele transmise pot ajunge în mâinile unor persoane rău intenționate. Dacă este necesar să folosești o astfel de rețea, evită introducerea parolelor sau a informațiilor bancare. Pentru un plus de siguranță, folosește o aplicație VPN de încredere, care criptează traficul și îl redirecționează printr-un server securizat. De asemenea, dezactivează conexiunile Wi-Fi și Bluetooth atunci când nu le folosești, pentru a preveni conectarea automată la rețele sau dispozitive necunoscute.

Localizarea dispozitivului: activează funcțiile de localizare și gestionare de la distanță oferite de sistemul de operare. Android și iOS dispun de servicii precum Find My Device, care permit localizarea telefonului pe hartă, blocarea accesului și ștergerea datelor în caz de pierdere sau furt. Aceste opțiuni trebuie activate din timp pentru a putea fi folosite la nevoie. De asemenea, este recomandat să notezi codul IMEI al telefonului, care poate fi util autorităților pentru blocarea accesului la rețelele mobile.

Back-up: activează funcția de backup automat în cloud, folosind servicii precum iCloud pentru iPhone sau Google Drive pentru Android. Acestea salvează automat fotografiile, contactele și alte date importante atunci când telefonul este conectat la Wi-Fi și la încărcare. Verifică din când în când dacă sincronizarea funcționează corect. Pentru o protecție suplimentară, este recomandat să salvezi fișierele importante și pe un computer sau un hard disk extern. Astfel, îți poți recupera datele chiar dacă telefonul este pierdut, furat sau afectat de un atac cibernetic.



Confidențialitate: folosește aplicații care oferă criptarea completă a mesajelor și apelurilor (WhatsApp, Signal, iMessage), pentru a te asigura că nimeni nu poate intercepta conținutul conversațiilor. Verifică setările de confidențialitate din rețelele sociale și limitează ce informații personale sunt vizibile public, cum ar fi activitatea recentă sau locația. Dezactivează accesul la locație pentru aplicațiile care nu au nevoie reală de el și activează autentificarea în doi pași pentru conturile importante. Un manager de parole te poate ajuta să folosești parole complexe, fără să fie nevoie să le memorezi. Ai dreptul legal să soliciți ștergerea datelor tale sau să ceri informații despre modul în care sunt colectate și utilizate.

Vigilență: adoptă o atitudine precaută în fața mesajelor care promit câștiguri rapide sau te îndeamnă să accesezi link-uri necunoscute. Acestea sunt adesea tentative de fraudă. Evită să instalezi aplicații promovate prin reclame agresive sau să interacționezi cu ferestre pop-up care anunță probleme false. În browser, activează funcții de protecție precum blocarea pop-up-urilor și opțiunea „Do Not Track". Codurile QR pot ascunde adrese periculoase. Folosește o aplicație care îți arată link-ul înainte de accesare. Nu conecta telefonul la stații publice de încărcare USB, acestea pot permite accesul la datele tale. Alege o baterie externă sau un adaptor care oferă doar alimentare, nu și transfer de date.

Prin aplicarea constantă a acestor recomandări, utilizatorii își pot consolida nivelul de protecție digitală. Securitatea mobilă nu se bazează pe o soluție unică, ci pe un set de măsuri complementare și obiceiuri sănătoase. Odată integrate în rutina zilnică, aceste practici reduc considerabil expunerea la riscuri și contribuie la menținerea confidențialității și siguranței datelor personale.

Informațiile și recomandările conținute în acest document sunt furnizate „ca atare" și fără garanții. Acestea au caracter informativ și educațional și nu constituie consultanță profesională în securitate cibernetică. Referirea din prezentul document la orice produse, soluții, servicii sau metodologii de securitate cibernetică prin denumire comercială, marcă comercială, producător sau în alt mod nu constituie sau implică aprobarea, recomandarea sau garantarea eficacității acestora de către Directoratul Național de Securitate Cibernetică (DNSC).

Autori: Irina NEMOIANU, Dan ANDRIEȘ, Laurențiu Mihai ZĂBAVĂ

TLP:CLEAR se poate folosi atunci când informațiile prezintă un risc minim de utilizare abuzivă, în conformitate cu normele și procedurile aplicabile pentru publicare. Sub rezerva regulilor standard ale drepturilor de autor, informațiile TLP:CLEAR pot fi partajate fără restricții.

Glosar

Termen	Definiție
Actualizare de securitate	Pachet de modificări oferit de producător pentru a corecta vulnerabilități și a îmbunătăți protecția dispozitivului.
Autentificare în doi pași (2FA)	Metodă de protecție care combină parola cu un cod temporar trimis prin SMS, e-mail sau generat de o aplicație.
Backup	Copierea datelor într-un spațiu separat (cloud, calculator) pentru a fi recuperate în caz de pierdere sau atac.
Bluetooth	Tehnologie wireless pe distanțe scurte folosită pentru conectarea dispozitivelor (ex: căști, boxe, ceasuri).
Cod QR	Imagine care codifică un link sau text, scanabil cu telefonul; poate fi folosit și în scopuri malițioase.
Criptare	Proces de codificare a datelor pentru a preveni accesul neautorizat.
Do Not Track	Opțiune din browser care solicită site-urilor să nu monitorizeze activitatea utilizatorului.
Fake Wi-Fi	Rețea wireless falsă, creată pentru a intercepta datele utilizatorilor care se conectează la ea.
International Mobile Equipment Identity (IMEI)	Cod unic de identificare al telefonului, folosit pentru blocarea acestuia în caz de furt.
Inginerie socială	Manipulare psihologică a utilizatorului pentru a obține date sensibile (parole, coduri).
Malware	Aplicație creată cu intenția de a dăuna dispozitivului sau de a fura date, adesea deghizată în aplicații legitime.
Man-in-the-Middle (MitM)	Atac în care comunicarea dintre două părți este interceptată fără ca acestea să știe.
Permisiuni ale aplicațiilor	Accesul acordat de utilizator aplicațiilor la funcții ale telefonului (ex: cameră, contacte, locație).
Phishing	Tentativă de fraudă prin mesaje sau site-uri false ce imită entități reale pentru a fura date.
Remote Access Trojan (RAT)	Tip de malware care oferă control de la distanță asupra dispozitivului infectat.
Root / Jailbreak	Eliminarea restricțiilor impuse de sistemul de operare, cu posibile riscuri de securitate.
Secure Enclave	Componentă hardware Apple care protejează datele biometrice și cheile criptografice.
Smishing (SMS Phishing)	Phishing realizat prin SMS-uri ce conțin linkuri sau solicită informații personale.
Spyware	Software care colectează informații fără acordul utilizatorului, fără a fi detectat.
Virtual Private Network (VPN)	Serviciu care creează o conexiune criptată în Internet, protejând datele împotriva interceptării și mascând adresa IP reală.
Zero-click attack	Atac ce compromite un dispozitiv fără interacțiunea utilizatorului (ex: fără click sau accesare link).