
vidéo
mes vidéos
Now watching: Inception
The Dark Knight
2x09 : Blackwater
Chronicle
Drive
Watchmen
Happy New Yea
AGENȚIA DE APĂRARE CIBERNETICĂ

GHID DE BUNE PRACTICI PENTRU UTILIZAREA DISPOZITIVELOR DE TIP SMARTPHONE

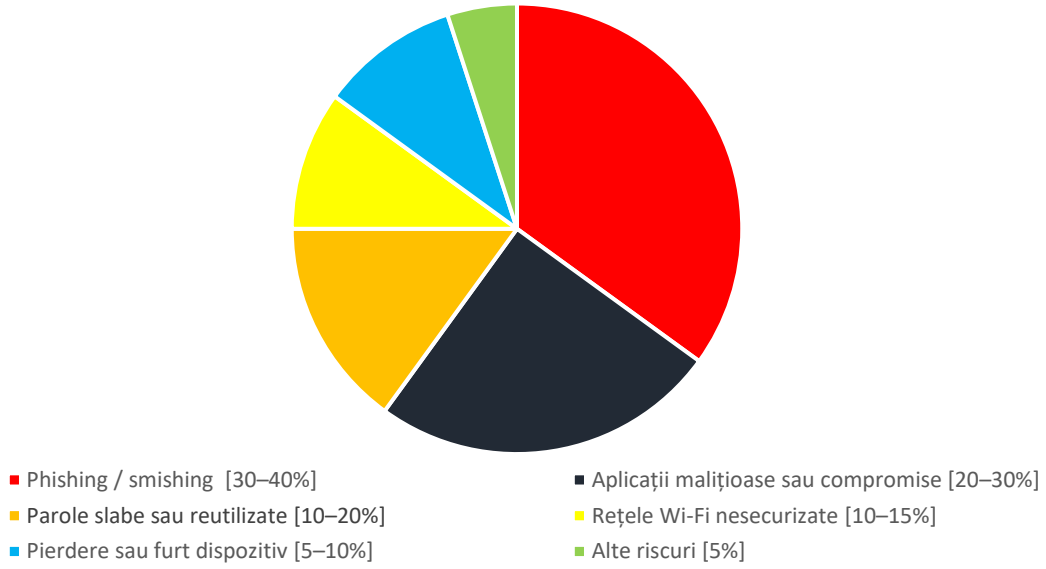
CUPRINS

INTRODUCERE

În prezent, smartphone-ul a devenit unul dintre cele mai utilizate dispozitive digitale, fiind integrat în aproape toate activitățile zilnice ale utilizatorilor. De la comunicare și acces la informații, până la autentificare și tranzacții financiare, aceste dispozitive stochează și procesează un volum semnificativ de date personale. Această evoluție a transformat smartphone-ul într-o țintă atractivă pentru persoanele rău intenționate, securitatea acestuia devenind esențială pentru protejarea identității digitale.

Graficul de mai jos oferă o imagine de ansamblu asupra principalelor tipuri de riscuri:

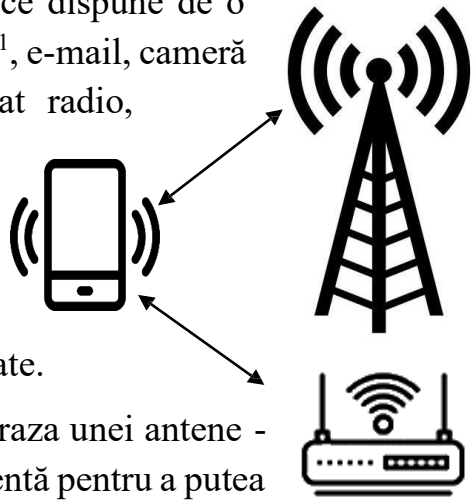
Tipuri de riscuri asociate utilizării smartphone-urilor (valori orientative)



Valorile prezentate sunt estimative și au rol ilustrativ, putând varia în funcție de context și evoluția amenințărilor cibernetice.

În ultimii ani, infractorii cibernetici s-au orientat tot mai mult către dispozitivele mobile, utilizând tehnici avansate precum phishing direcționat, aplicații compromise sau inginerie socială asistată de inteligență artificială. Acest ghid are rolul de a prezenta riscurile actuale și măsurile necesare pentru utilizarea în siguranță a dispozitivelor smartphone.

MODUL DE FUNCȚIONARE AL DISPOZITIVELOR SMARTPHONE



Smartphone-ul reprezintă un telefon mobil multifuncțional, conectat la o rețea ce dispune de o tastatură reală sau virtuală și oferă multiple funcționalități precum agendă, calendar, GPS[1], e-mail, cameră foto/video, etc. Ca principiu de comunicare acesta este foarte similar unui aparat radio, transmițând și primind constant diferite semnale.

Aceste dispozitive funcționează cu ajutorul unui sistem de operare special conceput pentru telefoanele mobile. În prezent, principalele sisteme de operare mobile sunt Android și iOS, acestea integrând mecanisme avansate de securitate precum sandboxing-ul aplicațiilor, actualizări automate de securitate și protecții hardware dedicate.

Pentru a putea comunica cu ajutorul unui smartphone acesta trebuie să se afle în raza unei antene - releu a operatorului de telefonie mobilă și să primească un semnal radio de calitate suficientă pentru a putea inița, primi sau menține o conexiune. O altă metodă prin care dispozitivul poate comunica este prin conectarea acestuia la un WAP[2], astfel încât acesta să aibă acces în Internet pentru a putea utiliza VoIP[3].

[1] GPS – Global Positioning System
[2] WAP – Wireless Access Point
[3] VoIP – Voice over Internet Protocol

Atunci când este efectuat un apel de pe telefonul mobil, acesta caută cea mai apropiată antenă a operatorului și solicită stabilirea unei conexiuni. Principiul este similar și la primirea unui apel, diferența fiind că în acest caz antena solicită stabilirea legăturii.

Dispozitivele moderne utilizează mecanisme precum criptarea implicită a datelor, autentificarea biometrică și module hardware securizate (ex: Secure Enclave sau Titan M), care contribuie la protejarea informațiilor sensibile.

TEHNOLOGII UTILIZATE

Dispozitivele de tip smartphone utilizează o varietate de tehnologii de comunicație pentru a permite transferul de date, conectivitatea la Internet și interacțiunea cu alte dispozitive. Aceste tehnologii evoluează constant, oferind performanțe îmbunătățite, dar introducând și noi provocări din punct de vedere al securității.

- **GSM (2G)** - tehnologie de bază pentru comunicații mobile, utilizată în principal pentru apeluri și SMS. Prezintă vulnerabilități ridicate de securitate;
- **UMTS (3G)** - îmbunătățește transferul de date față de 2G, însă este considerată în prezent o tehnologie depășită;
- **LTE (4G)** - oferă viteze ridicate de transfer de date și suport pentru aplicații moderne precum streaming și apeluri VoLTE;
- **5G** - tehnologie avansată care permite latență redusă și conectarea simultană a unui număr mare de dispozitive. Implică și noi riscuri de securitate la nivel de infrastructură;
- **Wi-Fi (Wi-Fi 4 / 5 / 6 / 6E / 7)** - permite conectarea la Internet prin rețele locale. Rețelele nesecurizate pot expune utilizatorii la interceptarea datelor;
- **Bluetooth (inclusiv BLE - Bluetooth Low Energy)** - utilizat pentru conectarea dispozitivelor pe distanțe

scurte, cum ar fi căști sau smartwatch-uri. Poate fi exploatat dacă este lăsat activ permanent;

- **NFC (Near Field Communication)** - permite schimbul rapid de date la distanțe foarte mici. Este utilizat frecvent pentru plăți contactless;
- **eSIM** - tehnologie care permite utilizarea unei cartele SIM digitale, eliminând necesitatea unui SIM fizic. Necesită protecție suplimentară a contului asociat;
- **UWB (Ultra Wideband**) - tehnologie utilizată pentru localizare precisă și transfer de date pe distanțe scurte, de exemplu pentru identificarea dispozitivelor.

RISCURI ASOCIATE

O mulțime de oameni utilizează în prezent cel puțin un dispozitiv de tip smartphone. Fie că sunt utilizate pentru a accesa platformele de socializare, pentru cumpărături online, pentru Internet banking sau pentru a comunica prin mesaje de tip SMS, aceste dispozitive expun utilizatorii unor riscuri majore.

Pentru majoritatea utilizatorilor este un lucru normal menținerea conturilor personale conectate pe dispozitiv, fără a lua în considerare faptul că dacă cineva reușește să acceseze smartphone-ul, acesta va avea acces la toate informațiile sensibile. De asemenea există în permanență riscul ca dispozitivul să fie pierdut, furat, distrus sau pur și simplu compromis prin intermediul paginilor web vizitate.

Potrivit cercetărilor, peste jumătate din programele malware mobile rulează în background-ul dispozitivului, fără a avea pictogramă pe ecranul de start. Acestea au rolul de a afișa reclame nedorite, de a posta recenzii false sau de a exfiltra informații sensibile care pot fi ulterior exploatate sau vândute de către persoane rău-intenționate.

Persoanele rău intenționate vizează tot mai frecvent dispozitivele mobile prin metode diverse, de la aplicații malițioase până la tehnici avansate de inginerie socială, adaptate comportamentului utilizatorilor.

- ***Acces neautorizat la dispozitiv***

În lipsa unor mecanisme de protecție adecvate, o persoană neautorizată poate accesa direct dispozitivul și implicit toate datele stocate pe acesta, inclusiv conturi de e-mail, aplicații bancare sau platforme de socializare.

- ***Compromiterea conturilor digitale***

Smartphone-urile sunt frecvent utilizate pentru autentificarea în conturi precum Google sau Apple ID. În cazul compromiterii acestor conturi, atacatorii pot obține acces la date sensibile, copii de rezervă, fotografii sau chiar pot controla dispozitivul de la distanță.

- ***Atacuri de tip phishing și smishing***

Atacatorii utilizează mesaje SMS, e-mail sau aplicații de mesagerie pentru a induce utilizatorii în eroare și a-i determina să acceseze link-uri malițioase sau să furnizeze date sensibile. În prezent, aceste atacuri includ și metode precum coduri QR malițioase (quishing).

- ***Aplicații malițioase și aplicații compromise***

Instalarea aplicațiilor din surse nesigure sau chiar din magazine oficiale compromise poate duce la infectarea dispozitivului. Aceste aplicații pot colecta date, afișa reclame abuzive sau controla anumite funcții ale telefonului.

- ***Rețele Wi-Fi nesecurizate***

Conectarea la rețele Wi-Fi publice sau nesecurizate poate permite interceptarea traficului de date sau lansarea unor atacuri de tip „man-in-the-middle”. De asemenea, atacatorii pot crea rețele false pentru a atrage utilizatorii (Evil Twin).

- ***Atacuri de tip social engineering***

Utilizatorii pot fi manipulați să divulge informații sensibile prin apeluri telefonice, mesaje sau chiar conținut generat cu ajutorul inteligenței artificiale, cum ar fi voci sau identități false.

- ***Spyware și monitorizare neautorizată***

Anumite tipuri de software pot fi utilizate pentru monitorizarea activității utilizatorului fără acordul acestuia, colectând informații precum locația, mesajele sau apelurile efectuate.

- ***Pierderea sau furtul dispozitivului***

În cazul pierderii sau furtului, datele stocate pe dispozitiv pot fi accesate de persoane neautorizate dacă nu sunt implementate măsuri de protecție adecvate.

- ***Atacuri prin intermediul porturilor USB (Juice Jacking)***

Utilizarea stațiilor publice de încărcare poate expune dispozitivul la atacuri prin care datele sunt accesate sau malware este instalat prin intermediul conexiunii USB.

CUM SE POATE INFECTA UN SMARTPHONE ?

Cele mai uzuale modalități prin care un dispozitiv se poate infecta sunt reprezentate de accesarea unui link / fișier atașat malițios sau prin instalarea unei aplicații rău intenționate.

Nu este recomandată accesarea linkurilor sau a fișierelor atașate nesolicitate primite din surse necunoscute. Atacatorii lansează o mulțime de campanii malițioase prin intermediul mesajelor de tip SMS, e-mail sau prin

intermediul platformelor de socializare. Simpla accesare a acestora poate instala automat malware pe dispozitiv.

Totodată, persoane rău intenționate pot pirata o aplicație existentă, o pot modifica și posta pe un magazin de aplicații legitim precum Google Play, astfel încât utilizatorii care descarcă aplicația să își infecteze dispozitivele.

Un alt mod prin care utilizatorii se pot expune este prin conectarea telefoanelor la un punct Wi-Fi public. Există mai multe riscuri în acest sens, cel mai semnificativ dintre acestea fiind faptul că tot traficul de date transmis prin această modalitate este necriptat, ceea ce înseamnă că o persoană rău intenționată poate intercepta în clar toate informațiile trimise sau primite de utilizator.

CARE SUNT SEMNELE SPECIFICE COMPROMITERII DISPOZITIVULUI ?

Identificarea timpurie a semnelor de compromitere a unui dispozitiv mobil este esențială pentru limitarea impactului unui posibil atac cibernetic.

- În timp durata de viață a bateriei scade în mod inevitabil, însă dacă acesta a fost infectat cu malware durata de viață scade mult mai repede. Acest lucru se datorează programului malware care folosește intens toate resursele disponibile ale dispozitivului;
- Scăderea bruscă a performanței poate fi un alt indicator al infectării smartphone-ului. Blocarea constantă a acestuia precum și repornirea spontană pot fi cauzate de infectarea cu programe malware;
- Volum ridicat de utilizare a datelor sau existența unor apeluri sau mesaje expediate de care utilizatorul nu știe nimic. În cazul utilizatorilor cu abonamente la furnizorul de telefonie, aceste lucruri se pot observa de asemenea și din creșterea costului facturii;
- Deși nu toate ferestrele pop-up sunt malițioase, apariția constantă a alertelor de acest tip poate

indica faptul că telefonul a fost infectat cu adware, o formă de malware ce are scopul de a afișa diverse pagini care generează venituri prin click-uri. Multe astfel de ferestre pot fi de asemenea linkuri de phishing;

- Activitatea neobișnuită pe unul dintre conturile conectate pe dispozitiv precum resetarea unei parole, trimiterea de e-mailuri sau înscrieri pe diferite platforme necunoscute poate indica faptul că telefonul a fost compromis;
- Încălzirea excesivă a dispozitivului chiar și atunci când nu este utilizat intens poate indica rularea unor procese malițioase în fundal;
- Apariția unor aplicații necunoscute instalate fără intervenția utilizatorului sau modificarea setărilor existente;
- Solicitarea unor permisiuni neobișnuite de către aplicații (de exemplu acces la accesibilitate, microfon sau locație fără o justificare clară);
- Notificări privind autentificări sau încercări de conectare din locații necunoscute;
- Dezactivarea sau imposibilitatea accesării funcțiilor de securitate ale dispozitivului, cum ar fi antivirusul sau setările de protecție.

BUNE PRACTICI DE SECURITATE CIBERNETICĂ

Securitatea dispozitivelor mobile nu depinde doar de tehnologie, ci în mare măsură de comportamentul utilizatorului. Majoritatea incidentelor de securitate apar ca urmare a unor acțiuni aparent inofensive, precum accesarea unui link malițios sau instalarea unei aplicații nesigure. Adoptarea unor bune practici de utilizare poate reduce semnificativ riscul de compromitere a dispozitivului și a datelor personale.

- ***Setarea unui mecanism de autentificare sigur***

Configurarea mecanismelor de protecție în cadrul smartphone-urilor este destul de intuitivă. Pentru utilizatorii Android acestea pot fi regăsite în meniul *Location & Security Settings*, iar pentru utilizatorii iOS în meniul *General*. Configurarea acestor mecanisme va mări substanțial nivelul de securitate al dispozitivului, prevenind accesul neautorizat. Se recomandă utilizarea unui cod PIN complex, a unei parole puternice sau a autentificării biometrice (amprentă sau recunoaștere facială) pentru prevenirea accesului neautorizat. Pentru un nivel suplimentar de securitate, este indicată activarea autentificării multifactor (MFA), acolo unde este posibil, pentru conturile importante.

- ***Activarea blocării automate***

Pentru a restricționa accesul asupra dispozitivului în cazul în care acesta rămâne nesupravegheat pentru o scurtă perioadă de timp sau este furat, este recomandată configurarea opțiunii de autoblocare astfel încât acesta să se blocheze automat după 15-30 de secunde de inactivitate.

- ***Actualizarea permanentă a sistemului de operare și a aplicațiilor utilizate***

Indiferent de sistemul de operare sau de aplicațiile folosite, utilizatorilor le este recomandată actualizarea constantă a acestora pentru a fi protejați împotriva noilor amenințări din spațiul cibernetic. Persoanele răuintenționate descoperă și exploatează în permanență vulnerabilitățile din cadrul acestor dispozitive din diverse motive (financiare sau reputaționale), ceea ce înseamnă că omiterea sau neactualizarea în timp util crește semnificativ riscul de a deveni victima unui atac. Fiecare actualizare lansată de companiile sistemelor de operare sau a aplicațiilor utilizate are scopul de remedia ultimele vulnerabilități descoperite și de a proteja utilizatorii.

- ***Instalarea aplicațiilor doar din surse de încredere și verificarea permisiunilor periodic***

Instalarea aplicațiilor ar trebui să fie făcută doar din surse de încredere precum Google Play sau App Store. De asemenea, înainte de a instala o aplicație se recomandă examinarea cu atenție a dezvoltatorului, a recenziilor acesteia și a permisiunilor solicitate pentru a funcționa. Spre exemplu, o aplicație simplă (lanternă) nu ar trebui în mod normal să solicite permisiunea de a accesa microfonul, locația sau contacte fără un motiv justificat.

- ***Utilizarea unei aplicații manager de parole***

Mulți utilizatori folosesc dispozitivele pe post de agendă personală, salvând în cadrul acestora diverse informații în clar, printre care și parolele conturilor online, bancare, etc. În cazul în care dispozitivul va fi compromis, implicit și aceste informații sensibile vor fi compromise. Se recomandă utilizarea unui manager de parole (exemplu: Bitwarde, NordPass, Proton Pass, 1Password) pentru generarea și stocarea în siguranță a parolelor. Acestea trebuie să fie unice pentru fiecare cont, iar acolo unde este posibil, se recomandă utilizarea tehnologiei passkeys. Parolele

sunt stocate în mod criptat ceea ce oferă un nivel de securitate ridicat. Aceste aplicații utilizează criptarea AES pe 256 de biți pentru a securiza datele de autentificare, oferind sincronizare între dispozitive, generarea de parole puternice și suport pentru chei de acces, pentru a asigura protecția împotriva încălcării securității datelor.

- ***Realizarea de backup-uri***

Realizarea de copii de siguranță (backup-uri) este importantă pentru protejarea datelor personale și profesionale. În cazul unor incidente precum atacurile de tip ransomware, erorile umane sau defectarea hardware-ului, backup-urile permit recuperarea rapidă a informațiilor fără pierderi majore. Acestea se pot face fie pe un hard extern, fie în cloud.

- ***Utilizarea în siguranță a rețelelor Wi-Fi***

Rețelele Wi-Fi publice (din cafenele, aeroporturi sau hoteluri) pot reprezenta un risc semnificativ pentru securitatea datelor, deoarece pot fi ușor interceptate de persoane malițioase. Se recomandă evitarea accesării conturilor sensibile, precum cele bancare sau conturile de e-mail, atunci când sunteți conectați la astfel de rețele. De asemenea, este important să dezactivați opțiunea de conectare automată la rețele Wi-Fi necunoscute, pentru a preveni conectarea accidentală la rețele false (de tip „evil twin”). Pentru un nivel suplimentar de securitate, se poate utiliza un VPN[4], care criptează traficul de date și îl protejează de interceptare. În plus, trebuie verificată întotdeauna autenticitatea rețelei înainte de conectare și activată criptarea HTTPS în browser.

- ***Dezactivarea funcțiilor neutilizate (Wi-Fi, Bluetooth, locație)***

Se recomandă ca funcțiile Wireless și Bluetooth să fie activate doar atunci când sunt necesare. Imediat ce utilizatorul nu mai are nevoie de acestea, se recomandă dezactivarea acestor funcții astfel încât să nu permită exfiltrarea de date sau conectarea la dispozitiv fără voia utilizatorului. Totodată, aceste tehnologii ar trebui utilizate

[4] VPN – Virtual Private Network

doar în medii de încredere precum rețeaua Wi-Fi de acasă.

Aplicațiile de socializare utilizate pot încărca imagini direct pe Internet afișând totodată și locația geografică a utilizatorului. Acest lucru permite tuturor persoanelor care vizionează fotografiile să vadă unde se află persoana respectivă în momentul respectiv, ceea ce ar putea determina o încălcare a confidențialității. Pentru a evita o astfel de situație este recomandată dezactivarea acestei caracteristici.

- ***Atenție la linkuri și mesaje suspecte***

Utilizatorii trebuie să evite accesarea linkurilor sau fișierelor atașate provenite din surse necunoscute, inclusiv cele primite prin SMS, e-mail sau aplicații de mesagerie.

- ***Phishing / Smishing / Spear phishing***

Se recomandă evitarea purtării conversațiilor sensibile pe dispozitivele personale, chiar dacă acestea au un conținut generic. Atacatorii folosesc diverse modalități pentru a colecta informații personale pentru ca ulterior să lanseze campanii de phishing, smishing sau spear phishing. Nu este recomandată deschiderea fișierelor atașate și linkurilor neașteptate provenite din surse nesigure. În cazul în care acestea provin din partea unor persoane de încredere, dar nu fac parte dintr-o conversație sau nu au fost transmise ca urmare a unei solicitări din partea dumneavoastră, înainte de deschiderea linkurilor / fișierelor atașate se recomandă contactarea acestor persoane printr-o altă cale de comunicație pentru confirmarea expedierii mesajului.

- ***Evitarea apelurilor de tip SPAM***

Există o mulțime de servicii de marketing care vor apela utilizatorii doar pentru a determina dacă numărul este utilizat de o persoană fizică. Odată ce utilizatorul răspunde la un astfel de apel, numărul acestuia va fi pus pe o listă activă, iar acesta va primi și mai multe apeluri și mesaje text de acest tip.

- ***Protejarea numărului de telefon***

Atunci când un utilizator contactează o anumită companie, numărul acestuia poate fi salvat și folosit ulterior în campaniile de marketing. Pentru protejarea numărului de telefon, utilizatorii pot folosi o aplicație precum Google Voice astfel încât aceasta va filtra și bloca pe baza unor filtre implicite orice apel de intrare care nu este în agenda telefonului și este potențial malițios

- ***Evitarea utilizării stațiilor publice de încărcare***

Sursele publice de încărcare pot expune dispozitivele inteligente pericolelor din spațiul cibernetic. Pe lângă transportul energiei electrice, cablurile de încărcare permit totodată și transferul de date. Pentru siguranța dispozitivului se recomandă utilizarea unor accesorii de încărcare originale, achiziționate de la un producător de încredere și evitarea surselor de încărcare publice.

- ***Protejarea fizică a dispozitivului***

Chiar dacă dispozitivul este protejat de mecanismele de securitate menționate anterior, există în continuare posibilitatea ca acesta să fie pierdut, distrus sau furat. Pentru securitatea fizică este recomandată utilizarea unei huse și folii de protecție și păstrarea telefonului într-un loc greu accesibil atunci când acesta nu este folosit. În cazul în care se întâmplă ca dispozitivul

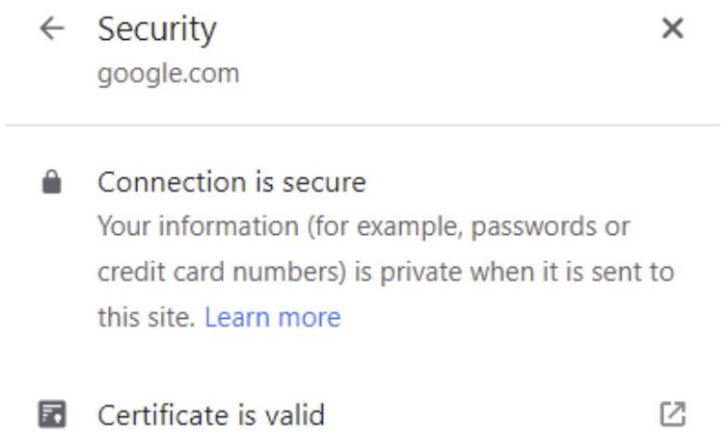
să fie pierdut sau furat, prin intermediul unei aplicații de recuperare, utilizatorul poate bloca accesul la dispozitiv sau îl poate localiza cu ajutorul semnalului GPS.

- ***Resetarea din fabrică***

Dacă un utilizator intenționează să renunțe sau să își vândă dispozitivul, se recomandă efectuarea unei resetări a datelor din fabrică astfel încât să fie eliminate toate datele și informațiile personale.

- ***Navigarea în siguranță pe Internet***

Nu este recomandată salvarea credențialelor (nume de utilizator și parolă) în browser deoarece, în cazul în care dispozitivul va fi compromis, atacatorul va avea acces la toate conturile personale ale victimei. Totodată, ar trebui accesate doar site-urile web de încredere, care dețin certificate de securitate (reprezentat de un lacăt poziționat la începutul adresei URL din bara de adrese). De asemenea se recomandă evitarea transmiterii de date sensibile, îndeosebi în cadrul site-urilor suspicioase ce solicită informații personale sau bancare. În cazul în care este necesară efectuarea unei plăți online, utilizatorilor li se recomandă deconectarea contului după finalizarea activității pe platforma respectivă.



REFERINȚE

- https://radio-waves.orange.com/ro/cum-functioneaza-un-telefon-mobil/
- https://ro.wikipedia.org/wiki/Smartphone
- https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf?utm_source=chatgpt.com
- https://www.nist.gov/publications/guidelines-managing-security-mobile-devices-enterprise-0
- https://www.govcert.gov.hk/doc/PG%20for%20Mobile%20Security_EN.pdf
- https://soti.net/resources/blog/2026/cybersecurity-best-practices-for-mobile-security-encryption/
- https://tdx.vanderbilt.edu/TDClient/33/Portal/KB/ArticleDet?ID=280
- https://www.verizon.com/articles/8-common-sense-tips-to-keep-your-smartphone-secure/
- https://ro.safetydetectives.com/best-password-managers/android/
- https://www.mcafee.com/blogs/enterprise/smartphone-security-best-practices-2/

AGENȚIA DE APĂRARE CIBERNETICĂ