
AGENȚIA DE APĂRARE CIBERNETICĂ

GHID DE CONȘTIENTIZARE A RISCURILOR UTILIZĂRII UNEI REȚELE WI-FI PUBLICE

Cuprins

Introducere

Ce este o rețea Wi-Fi publică ?

O rețea Wi-Fi publică este o conexiune la internet disponibilă, de cele mai multe ori gratuit, în locuri precum cafenele, aeroporturi, hoteluri, centre comerciale, parcuri sau biblioteci. Aceste rețele nu pun accent pe securitate, iar orice persoană aflată în raza semnalului se poate conecta fără autentificare, cu un simplu click. Datorită accesibilității, rețelele Wi-Fi publice sunt atractive pentru utilizatorii care doresc să economisească trafic de date mobile sau să lucreze din spații publice.

De ce sunt rețelele Wi-Fi publice vulnerabile ?

O rețea Wi-Fi publică este considerată vulnerabilă deoarece, în cele mai multe cazuri, nu utilizează metode moderne de criptare (precum WPA3), permite conectarea fără autentificare, nu oferă mecanisme de monitorizare a dispozitivelor conectate și este frecvent utilizată de persoane ale căror dispozitive nu sunt securizate (fără VPN, antivirus sau firewall).

În plus, atacurile cibernetice au devenit tot mai complexe, folosind tehnologii precum *Wi-Fi Pineapple*, rețele de tip *Evil Twin* și tactici de tip *phishing* bazate pe inteligență artificială (ex: *deepfake*, portaluri false, mesaje automatizate), ceea ce le face greu de detectat chiar și pentru utilizatorii avansați.

Tipuri de atacuri specifice rețelelor Wi-Fi publice

Rogue Access Point

Un *Rogue Access Point* este o rețea Wi-Fi falsă, creată intenționat de un atacator pentru a păcăli utilizatorii să se conecteze la ea în locul unei rețele legitime. Acest tip de punct de acces imită numele (ex. „Starbucks_Free”) și, uneori, chiar setările tehnice ale unei rețele publice sau private bine cunoscute, pentru a părea autentic în ochii utilizatorilor.

Cum recunoști o astfel de rețea?

- Apare brusc și nu este recunoscută de personalul locației;
- Are un nume aproape identic cu al unei rețele cunoscute (ex. „Airport_WiFi1” vs. „Airport_WiFi”);
- Nu solicită autentificare sau afișează o pagină de autentificare suspectă.

Cum te poți proteja?

- Întreabă întotdeauna personalul care este rețeaua Wi-Fi oficială a locației;
- Utilizează o conexiune VPN pentru a cripta traficul de date;
- Evită, pe cât posibil, rețelele care nu necesită nicio formă de autentificare.

Wi-Fi Pineapple

Wi-Fi Pineapple este un dispozitiv portabil creat inițial pentru testarea securității rețelelor wireless, utilizat de cercetători și specialiști în domeniul securității cibernetice. Totuși, datorită funcțiilor sale avansate, este adesea folosit și de atacatori pentru a desfășura atacuri de tip *Evil Twin*, adică pentru a crea rețele Wi-Fi false care imită rețele legitime.

Atunci când un utilizator se conectează la o astfel de rețea clonă, tot traficul său de date este redirecționat prin dispozitivul atacatorului, care poate intercepta, înregistra sau chiar modifica informațiile transmise.

Cum recunoști un astfel de atac?

- Conexiunea este neobișnuit de lentă sau instabilă;
- Site-urile securizate (*HTTPS*) devin inaccesibile sau solicită reautentificare;
- În lista de rețele disponibile apar mai multe rețele cu nume identice.

Cum te poți proteja?

- Dezactivează conectarea automată la rețele Wi-Fi de tip „open”;
- Nu introduce informații sensibile (ex. credențiale, date bancare) fără utilizarea unui VPN;
- Activează alertele pentru conexiuni suspecte (disponibile pe unele dispozitive sau aplicații de securitate).

Shoulder Surfing

Shoulder Surfing este o tehnică de spionaj fizic prin care un atacator încearcă să observe direct ecranul sau tastatura unei victime în timp ce aceasta introduce informaţii sensibile, precum parole, coduri PIN, date bancare sau mesaje private.

Atacatorii profită de neatenţia utilizatorilor în spaţii aglomerate — cum ar fi cafenele, mijloace de transport, aeroporturi sau biblioteci — şi se poziţionează discret în spatele victimei sau într-un unghi favorabil pentru a vedea tastatura ori ecranul. În unele cazuri, pot utiliza camere ascunse sau oglinzi pentru a amplifica vizibilitatea.

Cum recunoşti această tehnică?

- O persoană se apropie nejustificat de mult de tine în timp ce foloseşti un dispozitiv electronic;
- Observi că cineva pare mai interesat de ceea ce faci tu decât de propriul dispozitiv;
- Simţi că eşti urmărit în timp ce tastezi sau foloseşti ecranul.

Cum te poţi proteja?

- Nu lăsa niciodată dispozitivele nesupravegheate în spaţii publice;
- Activează autentificarea biometrică acolo unde este posibil (ex. amprentă, recunoaştere facială);
- Fii atent la împrejurimi şi acoperă tastatura atunci când introduci informaţii sensibile.

Man-in-the-Middle (MitM)

Un atac de tip *Man-in-the-Middle* se caracterizează prin interpunerea unui atacator între utilizator şi serverul cu care acesta comunică, fără ca utilizatorul să îşi dea seama. Practic, atacatorul acţionează ca un intermediar invizibil care poate intercepta datele transmise, modifica conţinutul acestora sau fura sesiunile de autentificare.

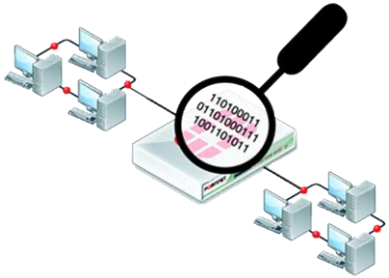
Cum recunoşti acest tip de atac?

- Primeşti alerte de securitate în browser, cum ar fi „certificatul site-ului nu este valid” sau „conexiune nesecurizată”;
- Eşti redirecţionat către pagini care arată diferit faţă de cele obişnuite (ex: un site de login cu aspect modificat);
- Browserul solicită reautentificare frecventă, chiar dacă nu ai închis sesiunea.

Cum te poţi proteja?

- Utilizează o conexiune VPN şi accesează doar site-uri care folosesc protocolul HTTPS;
- Dezactivează conectarea automată la reţele Wi-Fi;
- Evită, pe cât posibil, utilizarea reţelelor Wi-Fi deschise sau necunoscute.

Packet Sniffing



Atacurile de tip *Packet Sniffing* implică utilizarea unor aplicaţii speciale, precum *Wireshark*, pentru a intercepta pachetele de date care circulă printr-o reţea — în special atunci când aceasta este publică sau nesecurizată. Datele interceptate pot conţine informaţii sensibile, precum parole sau cookie-uri de autentificare, pe care o persoană rău intenţionată le poate folosi pentru a prelua sesiunea activă a utilizatorului.

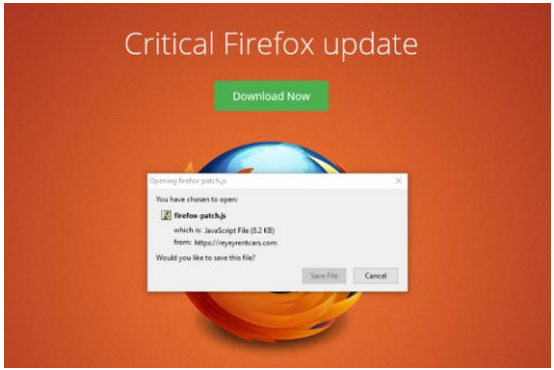
Cum recunoşti acest tip de atac?

- Primeşti notificări de conectare în conturile tale de pe dispozitive necunoscute;
- Eşti deconectat brusc de pe conturi, fără un motiv evident;
- Observi activitate neobişnuită în cont (ex: mesaje citite, comenzi plasate, modificări neautorizate).

Cum te poţi proteja?

- Activează autentificarea multifactor (MFA) acolo unde este posibil, pentru un nivel suplimentar de protecţie;
- Evită introducerea de informaţii sensibile atunci când foloseşti reţele Wi-Fi publice;
- Verifică periodic activitatea conturilor şi schimbă imediat parolele dacă observi comportament suspect.

Actualizări false



În reţelele Wi-Fi publice sau nesecurizate, atacatorii pot intercepta conexiunile şi pot livra mesaje false de actualizare (ex: update-uri de sistem, browser sau aplicaţii populare). Aceste actualizări aparent legitime pot conţine viermi, troieni sau alte forme de malware. Un simplu click pe un pop-up maliţios poate compromite întregul dispozitiv şi permite atacatorului să preia controlul asupra acestuia.

Cum recunoşti această tehnică?

- Mesaje pop-up neaşteptate care te îndeamnă să instalezi actualizări urgente sau critice;
- Încetinirea bruscă şi inexplicabilă a sistemului;
- Aplicaţii necunoscute instalate sau modificări suspecte în sistem (ex: pictograme noi, procese neobişnuite).

Cum te poţi proteja?

- Nu instala fişiere sugerate prin mesaje pop-up, mai ales în reţele Wi-Fi publice;
- Utilizează o soluţie antivirus şi un firewall actualizate;
- Instalează actualizările doar din surse oficiale (ex: site-ul producătorului, App Store, Google Play).

Quishing

Phishing-ul nu se mai limitează doar la e-mailuri sau site-uri web. În ultimii ani, atacatorii au început să exploateze canale vizuale şi fişiere aparent inofensive, precum coduri QR, fişiere PDF sau aplicaţii false disponibile în App Store ori Google Play. Toate aceste metode au în comun un element-cheie: exploatarea încrederii vizuale a utilizatorului**.**

Cum recunoşti acest tip de atac?

- Coduri QR plasate peste cele legitime — lipite fizic sau suprapuse digital în materiale promoţionale;
- PDF-uri care solicită acţiuni neobişnuite, precum instalarea de extensii, aplicaţii sau pluginuri „pentru a putea citi fişierul complet";
- Aplicaţii neoficiale, cu nume similare brandurilor cunoscute, dar publicate de dezvoltatori necunoscuţi sau cu recenzii suspicioase.

Cum te poţi proteja?

- Nu instala aplicaţii sau extensii recomandate prin fişiere necunoscute, pop-up-uri sau linkuri din mesaje;
- Activează funcţiile de protecţie anti-phishing în browserul şi antivirusul utilizat;
- Foloseşte aplicaţii de securitate care pot scana şi verifica codurile QR înainte de a deschide linkul asociat.

Captive Portal Hijacking

În multe spaţii publice, reţelele Wi-Fi redirecţionează automat utilizatorul către o pagină specială de autentificare, numită *captive portal*, înainte de a-i permite accesul la internet.

Captive Portal Hijacking apare atunci când o persoană rău intenţionată creează o versiune falsă a acestei pagini, care imită aspectul celei legitime. Utilizatorul este păcălit să introducă informaţii personale, date de autentificare sau chiar detalii bancare, crezând că urmează o procedură standard de conectare.

Cum recunoşti această tehnică?

- Adresa paginii de autentificare începe cu http:// (nu https://) sau domeniul este vag, neobişnuit ori necunoscut;
- Pagina solicită în mod nejustificat o cantitate mare de informaţii personale;
- Designul pare neprofesionist: culori neobişnuite, fonturi ciudate, greşeli gramaticale sau de ortografie.

Cum te poți proteja?

- Verifică dacă pagina de login este securizată — trebuie să folosească https:// și să aibă un certificat SSL valid;
- Fii atent la aspectul vizual al paginii: dacă pare suspectă sau nepotrivită pentru locația în care te afli, nu completa nimic;
- Nu introduce date personale sensibile, precum CNP-ul, numărul cardului sau alte informații bancare.

Practici recomandate de securitate înainte de conectarea la o rețea Wi-Fi publică

Înainte de a te conecta la orice rețea Wi-Fi, este esențial să verifici autenticitatea și siguranța acesteia. Mulți utilizatori se grăbesc să obțină acces gratuit la internet fără să-și pună întrebarea: **„Este această rețea legitimă?”**, iar atacatorii se bazează exact pe această neatenție.

Etapa de conectare este una dintre cele mai vulnerabile, deoarece un atacator poate crea o rețea falsă (ex: „Airport_Free_WiFi” sau „Hotel_Guest”), care pare legitimă, dar este configurată pentru a intercepta datele tale.

Iată câteva practici esențiale de securitate:

Alege rețele cunoscute și verificate - Conectează-te doar la rețele Wi-Fi a căror sursă o cunoști și în care ai încredere — de exemplu, cele puse la dispoziție în mod oficial de către o cafenea, un hotel, un aeroport etc. Evită rețelele cu denumiri generice precum *Free_WiFi*, *PublicWiFi* sau *ClickHere*.

Solicită denumirea oficială a rețelei de la personalul locației - Întreabă un angajat care este numele

corect al rețelei Wi-Fi. Este foarte ușor pentru o persoană rău-intenționată să creeze o rețea cu un nume similar sau chiar identic.

Dezactivează conectarea automată la rețele Wi-Fi - Majoritatea dispozitivelor salvează rețelele utilizate anterior și încearcă să se reconecteze automat ori de câte ori intră în raza de acoperire a acestora. Un atacator poate exploata această funcție, creând o rețea cu același nume (SSID) ca una folosită de tine în trecut.

Folosește dispozitivul mobil propriu ca hotspot - Dacă ai un plan de date mobile disponibil, cea mai sigură opțiune este să activezi funcția de hotspot a telefonului și să eviți complet rețelele publice. Această soluție oferă o conexiune securizată, controlată în întregime de tine.

Practici recomandate de securitate în timpul utilizării unei rețele Wi-Fi publice

Chiar și după conectarea la o rețea Wi-Fi aparent sigură, riscurile nu dispar. În timpul utilizării Internetului, datele tale pot fi în continuare interceptate, manipulate sau exploatate dacă nu iei măsurile de precauție adecvate. Atacuri precum **packet sniffing** sau redirecționări către pagini false pot avea loc fără semne evidente. Iată cele mai importante practici de urmat:

Folosește un VPN de încredere - Un VPN (Virtual Private Network) criptează tot traficul de date dintre dispozitivul tău și Internet, oferind un strat suplimentar de securitate. Astfel, chiar dacă rețeaua Wi-Fi este compromisă, datele tale rămân inaccesibile atacatorilor.

Asigură-te că site-urile utilizate folosesc HTTPS - Atunci când accesezi pagini web pe o rețea publică, verifică dacă adresa începe cu *https://*. Lipsa acestui prefix (adică *http://*) poate indica o conexiune nesecurizată.

Evită accesarea aplicațiilor bancare sau a conturilor sensibile - Chiar și atunci când HTTPS este activ, rețelele publice nu sunt recomandate pentru activități critice precum online banking, e-mailuri de serviciu sau accesul la panouri de control pentru aplicații.

Dezactivează funcțiile wireless inutile: Bluetooth, AirDrop, Sharing, Tethering - Menținerea acestor servicii active poate permite atacatorilor din apropiere să lanseze atacuri precum *Bluejacking*, *BlueBorne* sau să încerce transmiterea de fișiere malițioase către dispozitivul tău.

Practici recomandate de securitate după utilizarea unei rețele Wi-Fi publice

Chiar și după ce te-ai deconectat de la o rețea Wi-Fi publică, riscurile de securitate nu dispar complet. Rețelele publice pot lăsa urme în dispozitivul tău, precum conexiuni salvate automat sau fișiere temporare, care pot fi exploatate ulterior. De asemenea, dacă dispozitivul tău a fost expus unor atacuri în timpul conexiunii, este important să iei măsuri suplimentare pentru a preveni compromiterea datelor personale și pentru a evita eventuale atacuri viitoare.

Aplicând următoarele practici esențiale după deconectare, vei menține un nivel ridicat de securitate și confidențialitate pe termen lung, protejându-ți astfel informațiile și dispozitivul de amenințări persistente.

Șterge rețeaua Wi-Fi publică folosită din lista dispozitivului - Majoritatea dispozitivelor salvează automat rețelele utilizate pentru a facilita reconectarea ulterioară. Dezactivează această setare pentru rețelele publice sau șterge-le manual după ce nu mai ai nevoie, pentru a evita conectarea automată nedorită în viitor.

Efectuează o scanare antimalware - Este o bună practică să rulezi periodic o scanare completă a dispozitivului cu o soluție antimalware actualizată, pentru a identifica eventuale amenințări, mai ales după utilizarea unei rețele Wi-Fi publice.

Actualizează-ți regulat dispozitivul și aplicațiile utilizate - Menținerea software-ului la zi, prin instalarea tuturor actualizărilor disponibile, ajută la prevenirea vulnerabilităților cunoscute și reduce semnificativ riscul de exploatare.

Verifică periodic activitatea conturilor tale - După utilizarea unei rețele publice, acordă atenție notificărilor neobișnuite de autentificare, accesului neautorizat sau mesajelor suspecte. Dacă identifici orice suspiciune, schimbă imediat parolele tuturor conturilor.

Ce să nu faci NICIODATĂ când folosești o rețea Wi-Fi publică

1. **Să salvezi parolele în browser** – Dacă dispozitivul este compromis, parolele salvate în browser pot fi extrase cu ușurință de către atacator;
2. **Să te loghezi în conturi bancare sau servicii sensibile** – Traficul de date poate fi interceptat cu ușurință prin atacuri de tip Man-in-the-Middle, iar credențialele de acces sau cookie-urile de sesiune pot fi furate și reutilizate pentru a accesa fraudulos contul tău;
3. **Să descarci aplicații sau fișiere din surse necunoscute** – Poți instala fără să știi malware, spyware sau ransomware;
4. **Să instalezi actualizări de sistem "urgente"** – Acestea pot conține malware care oferă atacatorului acces deplin la sistemul tău informatic;
5. **Să menții active funcțiile de partajare ale dispozitivului atunci când nu le folosești** – Acestea pot fi exploatate de alți utilizatori din rețea pentru "a-ți forța" dispozitivul să accepte diferite fișiere fără permisiunea ta;
6. **Să utilizezi o parolă slabă, ușor de ghicit pe toate conturile tale** – Atacatorii pot folosi tehnici precum dictionary attacks sau brute force, acestea având capacitatea de sparge foarte rapid parolele slabe;
7. **Să trimiți informații sensibile** (ex: parole, date bancare) **prin Messenger sau conexiuni nesecurizate** – Comunicarea nesecurizată poate fi interceptată, iar datele transmise pot fi citite de terți;
8. **Să accesezi coduri QR afișate în locuri suspecte** – Codurile QR malițioase (Quishing) pot redirecționa către site-uri de phishing sau pot începe descărcări automate;

9. **Să menţii activă reconectarea automată a dispozitivului la reţelele salvate anterior** – Sistemul tău informatic se poate reconecta automat la o rețea falsă, clonată, care imită fidel o rețea legitimă;

10. **Să te conectezi la rețele Wi-Fi cu nume generice** (ex: Free_WiFi123) – Acestea pot fi rețele capcană create de hackeri în scop maliţios;

11. **Să utilizezi contul de administrator al sistemului informatic pentru activităţile zilnice** – Dacă dispozitivul tău se va infecta, malware-ul va rula cu drepturi de administrator şi va prelua mult mai uşor controlul asupra dispozitivului tău;

12. **Să ignori notificările de securitate de la sistemul de operare sau antivirus** – Mesajele de avertizare nu apar întâmplător. Un simplu „Permite” dat din reflex poate oferi acces nedorit unor aplicaţii sau site-uri periculoase. Fii atent la ce accepţi şi verifică sursa înainte să confirmi.

Toolkit de securitate recomandat

Ce este un toolkit de securitate digitală?

Un toolkit reprezintă un set esenţial de aplicaţii, servicii şi extensii care te ajută să navighezi în siguranţă pe Internet şi să îţi protejezi datele personale. La fel cum o trusă de chei te pot ajuta să repari sau să previi anumite probleme mecanice, un toolkit de securitate digitală îţi oferă instrumentele care previn accesul neautorizat, protejează confidenţialitatea şi te alertează în cazul unei breşe. Un astfel de toolkit este alcătuit din instrumente complementare, fiecare cu un rol clar în protejarea activităţii tale online.

De ce ai nevoie de un toolkit de securitate?

Un toolkit bine ales îţi asigură protecţia necesară în spaţiul cibernetic fără să fie nevoie să fii expert în IT. Aceste instrumente te ajută să îţi păstrezi datele în siguranţă şi să navighezi fără griji pe orice reţea Wi-Fi, mai ales în spaţii publice.

Ce ar trebui să conţină acest toolkit?

În centrul acestui set se află VPN-urile, care criptează traficul de reţea şi ascund locaţia reală, oferind astfel un prim strat de protecţie împotriva interceptării datelor. Navigarea devine şi mai sigură cu ajutorul unor browsere private, precum Brave sau Firefox Focus. Acestea blochează automat reclamele şi urmăritorii digitali care colectează date personale fără consimţământ.

Gestionarea parolelor este eficientizată prin password manageri ca Bitwarden sau KeePassXC, care generează și stochează parole complexe și unice pentru fiecare cont, eliminând riscul reutilizării aceloraşi parole. În plus, extensii de browser precum Privacy Badger sau HTTPS Everywhere adaugă un nivel suplimentar de protecție, blocând trackerele invizibile şi forţând utilizarea conexiunilor securizate pe site-uri.

De asemenea, un toolkit complet include şi o soluție de antivirus sau firewall cu protecție Wi-Fi, precum Windows Defender, ESET sau Kaspersky, care detectează şi blochează ameninţările cibernetice direct de pe dispozitivul tău. Împreună, aceste componente formează o barieră solidă împotriva celor mai frecvente riscuri online şi contribuie la un comportament digital sigur şi responsabil.

Ce să faci dacă securitatea ta a fost compromisă?

1. Rămâi calm

Primul şi cel mai important lucru pe care trebuie să îl faci este **să nu intri în panică**. Atacatorii mizează pe reacţii impulsive şi pe lipsa de organizare. Cu cât acţionezi mai calm şi mai calculat, cu atât vei putea limita mai eficient pagubele.

2. Acţionează rapid

Deconectează imediat dispozitivul de la Internet şi evită să mai introduci informaţii sensibile, precum parole sau date bancare, până când eşti sigur că dispozitivul este securizat. Dacă suspectezi că acesta a fost **infectat**, opreşte-l complet. În lipsa unei experienţe tehnice, apelează cât mai curând la un specialist în securitate cibernetică.

3. Schimbă parolele imediat

După ce ai securizat dispozitivul, schimbă imediat parolele tuturor conturilor importante, începând cu cele de e-mail, bancare și rețele sociale. Alege parole unice și complexe pentru fiecare cont, iar acolo unde este disponibilă, activează autentificarea multi-factor (MFA) pentru un plus de protecție.

4. Verifică activitatea recentă

Majoritatea platformelor majore (Google, Facebook, Microsoft etc.) oferă opțiuni de vizualizare a activității recente, precum logările și locațiile de acces. Verifică această activitate pentru a identifica accesări suspecte din locații sau dispozitive necunoscute. Deconectează orice sesiune care nu îți aparține și notează informațiile relevante, cum ar fi adresa IP sau ora logării, în cazul în care acestea vor fi necesare într-o investigație.

5. Anunţă serviciile afectate

Dacă este vorba despre un cont bancar, portofel digital, cont de plăţi online sau orice alt serviciu sensibil, contactează imediat instituţia responsabilă. Majoritatea băncilor au proceduri clare pentru gestionarea incidentelor de securitate şi pot bloca temporar accesul pentru a preveni pierderile. Cu cât notifici mai devreme, cu atât şansele de a limita daunele sunt mai mari.

6. Contactează autorităţile competente

În cazul în care atacul implică date cu caracter personal, informaţii financiare sau acces neautorizat, este esenţial să notifici cât mai rapid autorităţile competente. În Ministerul Apărării Naţionale poţi contacta CRISC-ul (Centrul de Răspuns la Incidente de Securitate Cibernetică) specific categoriei tale de forţe sau CRISC-P (Centrul de Răspuns la Incidente de Securitate Cibernetică Principal) la adresa de e-mail **cyber@mapn.ro** pentru raportare şi consiliere tehnică.

Checklist-uri rapide pentru creşterea nivelului de securitate

Wi-Fi sigur în 60 de secunde

- Conectează-te doar la reţele cunsocute;
- Verifică dacă reţeaua este protejată cu parolă;
- Foloseşte o conexiune VPN activă;
- Dezactivează partajarea de fişiere;
- Activează firewall-ul;
- Dezactivează conexiunea automată la reţele necunoscute.

Verificare cont compromis

- Accesează site-ul haveibeenpwned.com;
- Introdu adresa de e-mail utilizată;
- Verifică dacă adresa a fost impliată în breşe de securitate:
    - Dacă nu, felicitări! Contul tău este în siguranţă.
    - Dacă da:
        - Dacă ai folosit aceeaşi parolă pentru mai multe conturi, schimb-o de urgenţă peste tot;
        - Activează autentificarea multi-factor, dacă este disponibilă;
        - Verifică activitatea recentă a conturilor (ex: postări, mesaje sau acţiuni pe care nu le recunoşti) şi acţionează în consecinţă;

Securizare minimă telefon / laptop pentru spaţii publice

Pe telefon:

- Blochează ecranul cu PIN, parolă sau amprentă;
- Dezactivează Bluetooth-ul şi localizarea atunci când nu sunt necesare;
- Instalează aplicaţii doar din surse oficiale (ex: Google Play, App Store);
- Activează opţiunea „Găseşte-mi dispozitivul” pentru localizare şi ştergere de la distanţă.

Pentru laptop:

- Activează criptarea datelor (ex: BitLocker pe Windows, FileVault pe macOS);
- Foloseşte un cont de utilizator fără drepturi de administrator;
- Configurează blocarea automată a ecranului după 1–2 minute de inactivitate;
- Evită autentificarea în conturi sensibile (ex: bancă, e-mail) dacă nu utilizezi o conexiune VPN activă.

Glosar de termeni

Actualizare

Proces de modificare, îmbunătățire sau modernizare a unui sistem software sau hardware cu scopul de a optimiza performanța, a corecta erorile, a remedia vulnerabilitățile de securitate, a adăuga noi funcționalități sau de a asigura compatibilitatea cu alte sisteme și tehnologii.

Actualizările sunt esențiale pentru menținerea integrității și eficienței unui sistem informatic și pot fi clasificate în două categorii principale: actualizări minore (patch-uri) și actualizări majore (upgrade-uri).

AirDrop

Tehnologie de transfer de fișiere wireless dezvoltată de Apple, care permite schimbul rapid și securizat de fotografii, documente, videoclipuri, contacte sau alte tipuri de conținut între dispozitive Apple compatibile (iPhone, iPad, Mac), fără a fi necesară o conexiune la internet sau un cablu fizic. AirDrop utilizează o combinație de Bluetooth (pentru descoperirea dispozitivelor din apropiere) și Wi-Fi direct (pentru transferul efectiv al fișierelor), oferind viteză mare de transfer și criptare de tip end-to-end a datelor.

Antivirus

Tip de software specializat proiectat pentru a detecta, preveni și elimina programele malware, precum virușii, troienii, viermii sau alte amenințări cibernetice. Acest software monitorizează activitățile sistemului în timp real și analizează fișierele pentru a identifica semnele caracteristice programelor malware. Atunci când detectează o amenințare, antivirusul poate izola, remedia sau șterge fișierul sau programul respectiv, protejând astfel sistemul și datele utilizatorului. Antivirusul se bazează pe semnături ale malware-urilor cunoscute, dar și pe euristică și tehnologii de detecție comportamentală pentru a identifica și a combate noi amenințări.

Atac cibernetic

Acțiune ostilă deliberată și planificată a unui individ sau a unui grup desfășurată în spațiul cibernetic ce are ca scop obținerea de acces neautorizat, furtul de date sensibile, distrugerea sau alterarea datelor, afectarea funcționării normale a serviciilor sau manipularea sistemelor în scopuri malițioase.

Autentificare multi-factor (MFA)

Proces de securitate cibernetică care implică utilizarea a cel puțin două metode diferite de confirmare a identității unui utilizator înainte de a-i permite accesul la un sistem, cont sau aplicație. Aceste metode pot include ceva ce utilizatorul știe (cum ar fi o parolă), ceva ce utilizatorul deține (cum ar fi un dispozitiv fizic sau o cartelă de autentificare) și ceva ce utilizatorul este (cum ar fi amprenta digitală sau recunoașterea facială). MFA

creşte semnificativ securitatea, deoarece, chiar dacă o parte a factorilor este compromisă, atacatorul tot nu poate accesa contul sau sistemul fără celelalte elemente necesare autentificării.

Bluetooth

Tehnologie de comunicaţie wireless versatilă ce permite dispozitivelor să schimbe informaţii fără a mai fi necesară interconectarea acestora cu un cablu.

Captive Portal

Mecanism de control al accesului la o reţea Wi-Fi sau la internet, care redirecţionează utilizatorii către o pagină web dedicată înainte de a le permite conectarea completă la reţea. Această pagină, numită portal captiv, solicită de obicei autentificare, acceptarea unor termeni şi condiţii sau introducerea unor date de acces, precum un cod sau o adresă de e-mail. Captive portal-ul este frecvent utilizat în reţele publice, cum ar fi cele din hoteluri, aeroporturi, cafenele sau instituţii, pentru a gestiona şi monitoriza accesul utilizatorilor.

Acest sistem funcţionează prin interceptarea traficului HTTP/HTTPS iniţial şi redirecţionarea lui către portalul de autentificare, până la finalizarea cu succes a procedurii de validare.

Deepfake

Tip de conţinut digital generat cu ajutorul inteligenţei artificiale, în special prin utilizarea reţelelor neuronale profunde (deep learning), care are scopul de a modifica sau crea imagini, videoclipuri sau înregistrări audio într-un mod extrem de realist, astfel încât să pară autentice, deşi sunt false. Aceste tehnologii analizează şi învaţă trăsăturile faciale, vocale şi expresiile unei persoane, apoi le pot înlocui sau reproduce într-un alt context, generând conţinut manipulat. Deepfake-urile sunt adesea utilizate pentru a crea clipuri video în care persoane par să spună sau să facă lucruri pe care, în realitate, nu le-au spus sau făcut.

Deşi tehnologia are şi aplicaţii legitime, precum în divertisment sau educaţie, deepfake-urile sunt asociate frecvent cu riscuri de dezinformare, fraudă, defăimare sau alte ameninţări legate de securitatea digitală şi integritatea informaţiilor.

Evil Twin

Tehnică de atac cibernetic de tip reţea falsă, prin care un atacator creează un punct de acces Wi-Fi care imită un hotspot legitim, cu scopul de a păcăli utilizatorii să se conecteze la acesta. Odată conectaţi, atacatorul poate intercepta, înregistra sau modifica traficul de date al victimelor, realizând atacuri Man-in-the-Middle (MitM) sau colectând informaţii sensibile precum parole, mesaje şi date bancare.

Reţeaua „Evil Twin” foloseşte acelaşi SSID (nume de reţea) şi uneori chiar o intensitate a semnalului mai mare decât reţeaua originală, determinând dispozitivele victimelor să se conecteze automat la ea, fără suspiciuni. În unele cazuri, poate fi combinată cu pagini de tip captive portal fals pentru a fura acreditive de autentificare sau a instala malware. Acest tip de atac este frecvent întâlnit în locaţii publice cu reţele Wi-Fi gratuite (cafenele, aeroporturi, hoteluri), unde utilizatorii nu pot distinge uşor între reţeaua legitimă şi cea compromisă.

Firewall

Instrument de securitate, hardware sau software, care acționează ca o barieră între o rețea privată și o rețea publică. Scopul principal al unui firewall este de a monitoriza și controla traficul care intră și iese din rețea, în funcție de regulile predefinite. Firewall-urile reprezintă un element fundamental în securitatea cibernetică, fiind prima linie de apărare împotriva atacurilor, a accesului neautorizat sau a altor acțiuni malițioase care pot afecta integritatea și confidențialitatea datelor.

Hijacking

Acțiunea unei persoane rău-intenționate de a prelua controlul unui cont, conexiune sau sistem informativ, de obicei fără a avea permisiunea proprietarului. Hijacking-ul reprezintă o amenințare gravă la adresa securității și poate avea consecințe serioase pentru victime și pentru integritatea sistemelor sau datelor din cadrul acestora.

Hotspot

Punct de acces la internet wireless, care permite dispozitivelor mobile (laptopuri, telefoane, tablete etc.) să se conecteze la o rețea Wi-Fi prin intermediul unei conexiuni partajate, de obicei furnizată de un router, un dispozitiv mobil sau un echipament specializat.

Un hotspot poate fi:

- Public – disponibil gratuit sau contra cost în locații precum cafenele, aeroporturi, hoteluri sau biblioteci, oferind acces temporar la internet pentru utilizatori;
- Privat – creat de un utilizator individual, de exemplu prin activarea funcției de tethering pe un smartphone, care transformă conexiunea mobilă (3G/4G/5G) în semnal Wi-Fi disponibil altor dispozitive.

HTTPS Everywhere

Extensie a browserului web ce are scopul de forța browserul să utilizeze o conexiune de tip HTTPS în locul celei HTTP, atunci când un utilizator vizitează un site web. Extensia este disponibilă pentru o gamă largă de browsere web populare, cum ar fi Google Chrome, Mozilla Firefox, Opera și altele.

Hypertext Transfer Protocol (HTTP)

Protocol fundamental de comunicație utilizat în internet pentru transmiterea și recepționarea informațiilor, în special a paginilor web, între un client și un server. Acest protocol este bazat pe un model client-server, în cadrul căruia un client emite cereri HTTP către un server web pentru a accesa diferite resurse, iar serverul procesează aceste cereri și răspunde cu resursele solicitate. HTTP este considerat un protocol nesigur deoarece informațiile trimise între client-server pot fi interceptate și modificate cu ușurință de către terți neautorizați. Pentru a îmbunătăți securitatea comunicațiilor, se recomandă utilizarea protocolului HTTPS (Hypertext Transfer Protocol Secure), care criptează fluxul de informații trimis între client-server.

Hypertext Transfer Protocol Secure (HTTPS)

Versiune securizată a protocolului HTTP folosit pentru transmiterea datelor pe internet. Scopul principal al HTTPS este de a oferi un canal de comunicare sigur și criptate între un client și un server web. Acest lucru se realizează prin utilizarea unui protocol de securitate numit SSL (Secure Sockets Layer) sau succesorul său, TLS (Transport Layer Security). Aceste protocoale stabilesc o conexiune securizată între client și server, astfel încât datele să fie criptate și protejate împotriva interceptării sau modificării neautorizate în timpul tranzitului.

Man-in-the-Middle (MitM)

Tip de atac cibernetic în cadrul căruia un atacator interceptează, monitorizează sau modifică comunicarea dintre două entități fără ca acestea să știe. MitM poate avea loc în diverse medii de comunicaţii, inclusiv rețele Wi-Fi, rețele cablate, conexiuni Bluetooth sau alte canale de comunicații. Atacatorul poate folosi diverse tehnici pentru a intercepta și manipula datele, inclusiv sniffing, în care interceptează pachetele de date care trec prin rețea, sau atacuri de phishing, în care își conving victimele să acceseze site-uri web sau să descarce fișiere malware care le permit să preia controlul asupra comunicațiilor.

Password Manager

Aplicaţie software specializată, proiectată pentru a stoca, gestiona și genera parole complexe în mod securizat, ajutând utilizatorii să își protejeze conturile online fără a fi nevoiți să-și amintească fiecare parolă individual. Aceste aplicații criptează parolele într-un seif digital, accesibil printr-o parolă principală (master password) sau prin metode biometrice (amprentă, recunoaștere facială). La autentificare, managerul poate completa automat câmpurile de login, reducând riscul de tastare greșită sau reutilizare a parolelor.

Phishing

Formă de atac cibernetic în cadrul căreia o persoană rău-intenţionată pretinde că este o entitate de încredere și încearcă să obțină informații confidențiale, precum credențiale de autentificare, informații bancare sau alte date sensibile prin intermediul tehnicilor de inginerie socială.

Aceste atacuri se desfășoară adesea prin intermediul unor mesaje de e-mail, mesaje text sau alte mijloace de comunicare, care par a proveni de la instituții financiare, organizații guvernamentale sau alte entități cunoscute. Mesajele conțin adesea link-uri către site-uri web falsificate care imită site-urile autentice, astfel încât utilizatorii să fie induși în eroare și să furnizeze informațiile solicitate.

Quick Response Code (QR Code)

Matrice bidimensională de tip cod de bare care conține informații în formă de coduri alfanumerice sau binare. A fost inventat în anii 1990 în Japonia și a devenit o formă extrem de populară pentru a stoca și transmite diverse tipuri de date. Codurile QR sunt ușor de generat și pot fi utilizate într-o varietate de contexte pentru a oferi informații suplimentare sau pentru a facilita interacțiunea digitală.

Codurile QR au devenit o componentă integrală a mediului digital, fiind utilizate în diverse domenii, cum ar fi publicitatea, comerțul electronic, turismul, gestionarea inventarului, autentificarea și multe altele.

Rogue Access Point

Punct de acces wireless neautorizat, instalat într-o rețea fără aprobarea administratorilor IT. Acest tip de dispozitiv poate fi introdus fie accidental (de către angajați care vor acces Wi-Fi într-o zonă fără acoperire), fie intenționat, de către un atacator care urmărește să compromită securitatea rețelei. Un rogue access point poate permite atacatorului să intercepteze, modifice sau redirecționeze traficul de rețea, deschizând astfel posibilitatea unor atacuri de tip Man-in-the-Middle (MitM), Evil Twin, capturi de parole sau injectare de malware.

Service Set Identifier (SSID)

Identificator unic atribuit unei rețele wireless pentru a o distinge de alte rețele disponibile în zona respectivă. Practic, SSID-ul funcționează ca un fel de nume pentru rețeaua wireless, permițând dispozitivelor să o identifice și să se conecteze la ea.

Atunci când utilizatorii caută rețele wireless disponibile, SSID-urile acestora sunt afișate în lista de rețele disponibile, permițând utilizatorilor să selecteze rețeaua dorită pentru conectare. Configurarea SSID-ului este esențială pentru asigurarea unei identificări corecte a rețelei și pentru evitarea confuziilor între rețelele wireless din apropiere.

Shoulder Surfing

Tehnică de spionaj prin care o persoană încearcă să obțină informații confidențiale, cum ar fi parole, PIN-uri sau alte date sensibile, observând discret ecranul sau tastatura unei alte persoane în timp ce aceasta interacționează cu un dispozitiv electronic sau introduce date într-un sistem informatic. Această tactică poate fi folosită în diverse locuri publice sau de lucru, cum ar fi cafenelele, aeroporturile, ghișeele bancare sau birourile deschise, și poate implica observarea directă a tastelor apăsate, a ecranului dispozitivului sau chiar a mișcărilor mâinilor persoanei vizate.

Shoulder surfing poate fi utilizat de către infractori pentru a fura informații personale sau confidențiale, care pot fi ulterior folosite în scopuri frauduloase sau ilegale. Pentru a preveni acest tip de atac, este recomandat să fiți atenți la mediul înconjurător atunci când introduceți informații sensibile și să luați măsuri suplimentare de securitate, cum ar fi utilizarea ecranelor de protecție pentru a împiedica vizualizarea de către persoanele din jur sau acoperirea tastaturii atunci când introduceți parole sau PIN-uri.

Sidejacking

Tip de atac cibernetic în cadrul căruia un atacator interceptează cookie-ul de sesiune al victimei și îl folosește pentru a obține acces neautorizat la resursele sau serviciile disponibile pe un server web. Într-un astfel de atac, atacatorul nu obține parola victimei, astfel încât, atunci când victima se deconectează, este deconectat și atacatorul. Acest tip de atac este posibil atunci când un site web nu utilizează criptare completă pentru a proteja sesiunile utilizatorilor, permițând astfel unui atacator să intercepteze și să utilizeze cookie-urile de sesiune pentru a prelua controlul asupra sesiunii utilizatorului.

Pentru a preveni astfel de atacuri, este recomandat ca site-urile web să implementeze criptare HTTPS și să utilizeze metode suplimentare de securitate, precum token-uri unice sau autentificare cu doi factori.

Sniffing

Proces de interceptare și monitorizare a traficului de date din cadrul unei rețele. Acesta poate fi utilizat în scopuri legale, cum ar fi monitorizarea și îmbunătățirea securității unei infrastructuri de rețea, pentru diagnosticarea problemelor sau pentru a detecta activități neautorizate.

Cu toate acestea, sniffing-ul poate fi și folosit în scopuri ilegale, cum ar fi interceptarea și exfiltrarea de informații confidențiale fără consimțământul explicit al părților implicate. Acest lucru poate implica interceptarea datelor de autentificare, parole sau alte informații sensibile în scopuri de furt de identitate sau spionaj cibernetic. Din perspectiva securității cibernetice, este important să se implementeze măsuri de protecție împotriva sniffing-ului, cum ar fi criptarea datelor și utilizarea unor protocoale de securitate adecvate.

Tethering

Funcționalitate care permite partajarea conexiunii la internet a unui dispozitiv mobil (de obicei un smartphone) cu alte dispozitive, precum laptopuri, tablete sau alte telefoane. Astfel, dispozitivul principal acționează ca un punct de acces, oferind conectivitate prin rețeaua sa mobilă (3G, 4G, 5G).

Toolkit

Set de instrumente software specializate, concepute pentru a facilita dezvoltarea, testarea, configurarea sau administrarea altor aplicații sau sisteme informatice. Aceste instrumente sunt grupate într-un pachet unitar și pot include biblioteci, utilitare, interfețe grafice, scripturi sau componente predefinite.

Un toolkit oferă dezvoltatorilor resursele necesare pentru a accelera procesele de programare sau integrare, reducând timpul și complexitatea dezvoltării. În funcție de scop, poate sprijini realizarea aplicațiilor web, mobile, desktop sau chiar a sistemelor de securitate și automatizare.

Virtual Private Network (VPN)

Tehnologie care permite crearea unei conexiuni securizate și private între dispozitive sau rețele prin intermediul internetului. Aceasta oferă utilizatorilor posibilitatea de a accesa resursele rețelei într-un mod sigur, chiar și de la distanță.

VPN-urile sunt utilizate atât în mediile de afaceri, pentru a asigura conectivitatea sigură între filialele și angajații aflați la distanță, cât și în mediul personal, pentru a proteja conexiunile la internet în timpul navigării online. Ele pot fi implementate atât pe dispozitive individuale, cât și la nivelul întregii infrastructuri de rețea a unei organizații.

Wi-Fi

Set de tehnologii și protocoale de comunicație wireless care permit dispozitivelor să se conecteze la o rețea de comunicație fără a fi nevoie de cabluri fizice. Termenul Wi-Fi este un acronim pentru Wireless Fidelity și este folosit în mod obișnuit pentru a descrie tehnologiile bazate pe standardele IEEE 802.11, care guvernează comunicarea în rețelele fără fir.

Tehnologia Wi-Fi a devenit o componentă esențială a conectivității în lumea modernă, facilitând accesul la internet și comunicarea între dispozitive. Aceasta este utilizată într-o gamă largă de dispozitive, de la telefoane mobile și laptopuri până la electrocasnice inteligente sau alte echipamente conectate la internet.

Wi-Fi Protected Access (WPA)

Protocol de securitate dezvoltat pentru a proteja datele transmise prin intermediul rețelelor wireless. Acesta a fost creat pentru a înlocui protocolul Wired Equivalent Privacy (WEP), cunoscut pentru vulnerabilitățile sale de securitate. WPA a devenit standard de securitate pentru majoritatea rețelelor Wi-Fi, implementarea sa fiind esențială în protecția datelor și a informațiilor aflate în tranzit.

Wi-Fi Protected Setup (WPS)

Protocol creat pentru a facilita configurarea rapidă și simplificată a rețelelor Wi-Fi securizate, fără a fi nevoie de introducerea manuală a parolelor complexe. WPS permite conectarea dispozitivelor la o rețea wireless printr-un proces automatizat, folosind fie un buton fizic de pe router, un cod PIN sau NFC.

AGENȚIA DE APĂRARE CIBERNETICĂ