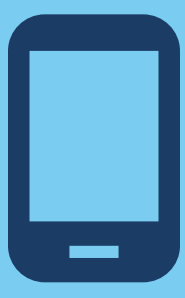
SECURITATEA REȚELELOR WI-FI PUBLICE

Recomandări pentru utilizatorii WI-Fi

ATENȚIE LA DISPOZITIVE ÎNVECHITE

Nu folosiți dispozitive cu sisteme de operare învechite, care pot fi vulnerabile și care nu sunt actualizate în mod adecvat pentru a vă conecta la rețelele publice Wi-Fi.

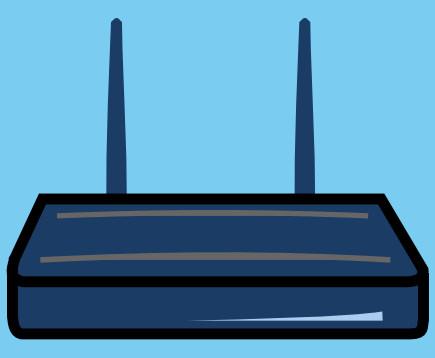


GESTIONAȚI CONECTAREA LA REȚEA WI-FI

- Nu permiteți conectarea automată la rețele Wi-Fi disponibile.
- Nu lăsați conexiunea Wi-Fi pornită atunci când nu o utilizați.

EVITAȚI REȚELELE DESCHISE

Evitați utilizarea rețelelor Wi-Fi deschise care nu sunt protejate prin parolă sau politici de confidențialitate.



ATENȚIE LA DATE SENSIBILE

Nu accesați site-urile web care dețin informațiile sensibile, cum ar fi date bancare sau de sănătate în timp ce sunteți conectat la un WI-FI public. În așa cazuri trebuie să:

- Preferați serviciul 3G / 4G / 5G al operatorului de telefonie mobilă, decât punctele publice Wi-Fi.
- Nu vă conectați la niciun cont printr-o aplicație mobilă, accessați direct site-ul web și verificați dacă folosește HTTPS înainte de logare.
- Conectați-vă printr VPN.
- Deconectați conturile la terminarea utilizării lor.

ÎN TIMP CE VĂ CONECTAȚI LA UN WI-FI PUBLIC

- Verificați SSID-ul înainte de conectare, deoarece utilizatorii rău intenționați pot configura punctul de acces cu nume SSID similare în mod intenționat cu cafenele populare, hoteluri sau locuri care oferă un astfel de Wi-Fi public.
- Evitați utilizarea terminalelor publice / partajate pentru accesarea site-urilor web care necesită introducerea informațiilor sensibile.

I.P SERVICIUL TEHNOLOGIA INFORMAȚIEI ȘI SECURITATE CIBERNETICĂ

SECURITATEA REȚELELOR WI-FI PUBLICE

Recomandări pentru proprietarii rețelei Wi-Fi

SEPARAȚI REȚEAUA

- Separați rețeaua de afaceri de rețeaua corporativă WiFi publică. Această separare poate fi efectuată fizic sau logic, prin implementarea controalelor corespunzătoare.
- Utilizați VPN pentru a transmite informații personale identificabile sau de plată pentru a oferi suficientă criptare end-to-end și control de acces.
- Actualizați regulat infrastructura wireless.

APLICAȚI MĂSURI DE SECURITATE

- Zonarea, configurarea corectă a soluțiilor de gestionare a amenințărilor ar trebui să fie puse în aplicare în conformitate cu cele mai bune practici (precum: NIST 800-41, NIST 800-53, ISO 27001, și altele);
- Utilizați IDS / IPS în cazul utilizării Wi-Fi public este sau coexistă cu rețeaua corporativă.
- Asigurați măsuri pentru detectarea, răspunsul și prevenirea punctelor de acces compromise din reteaua Wi-Fi publică.
- Utilizați SSID-uri diferite în timp ce definiți numele pentru rețeaua wireless.

GESTIONAȚI ACCESUL

- Configurați punctele de acces și routerele conform celor mai bune practici . Activați criptarea (*dacă este disponibilă).
- Eliminați/dezactivați toate conturile implicite din hardware-ul folosit, de ex. root, administrator etc.
- Modificați și actualizați parolele implicite pe switch-uri, routere și punctele de acces wireless.

MENȚINEȚI JURNALE DE ACCES PENTRU UTILIZATORI

- Jurnalele de acces trebuie să capteze: numele de utilizator (dacă este cazul), numărul mobil asociat (utilizat pentru autentificare), adresa IP, data și ora, etc., care pot identifica utilizatorul.
- Activați jurnalul de securitate pe toate dispozitivele.
- Păstrați jurnalele de securitate timp cel puțin 120 de zile.

ASIGURAȚI SECURITATEA FIZICĂ A REȚELEI

- Asigurați-vă că routerul sau AP-urile wireless sunt protejate de utilizatorii de wi-fi publici /oaspeți.
- Asigurați protecția porturiloe de rețea Ethernet de pe pereți (dacă există) și dacă nu sunt utilizate, deconectați-le de la rețea.
- Asigurați securizarea fizică a punctelor de acces de accesul fizic neautorizat sau daune fizice generale.

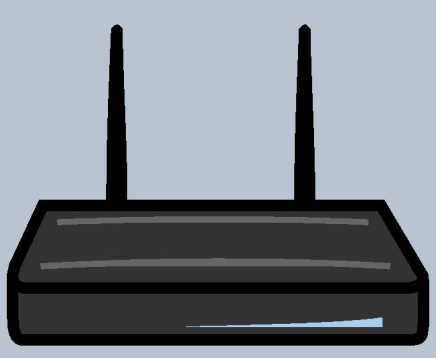
I.P SERVICIUL TEHNOLOGIA INFORMAȚIEI ȘI SECURITATE CIBERNETICĂ

SECURITATEA REȚELELOR WI-FI PUBLICE

Recomandări Furnizori Servicii Wi-Fi

SECURIZAȚI DOCUMENTELE TEHICE

Securizați corespunzător documente tehnicele, cum ar fi documentele de proiectare a rețelei, machete de rețea, detalii cu privire la adresele IP etc

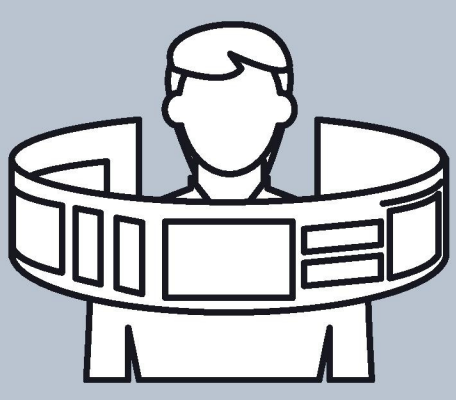


ȚINEȚI EVIDENȚA DISPOZITIVELOR NECESARE

Mențineți și documentați un inventar al tuturor dispozitivelor necesare pentru a furniza acest serviciu. Mențineți și gestionați rapoarte de activitate, statistici și rapoarte de utilizare a serviciilor

DEZVOLTAȚI UN ACORD AL UTILIZATORULUI

Dezvoltați un acord al utilizatorului privind menținerea securității informațiilor. De asemenea, stabiliți o politică de confidențialitate pentru utilizatorii Wi-Fi.



ORGANIZAȚI CONTROLUL ACCESULUI

- Orice servicii wireless ar trebui să identifice, să autentifice și să autorizeze utilizatorii înainte de a oferi acces la internet.
- Serviciul ar trebui să poată identifica și autentifica utilizatorii într-o manieră acceptabilă.
- Utilizatorul ar trebui să citească și să accepte condițiile de utilizare înainte de accesarea orice site web.

ASIGURAȚI COLECTAREA ȘI PARTAJAREA CORECTĂ A DATELOR

- Politica de utilizare trebuie să includă consimțământul pentru utilizarea informațiilor personale, care pot fi colectate de la utilizatori în timpul logării în sistem sau la utilizarea serviciilor de internet.
- Orice date colectate de la utilizatori trebuie utilizate și distribuite doar în conformitate legislația.
- Informațiile personale identificabile nu ar trebui să fie partajate cu terți decât dacă conform legislației.

I.P SERVICIUL TEHNOLOGIA INFORMAȚIEI ȘI SECURITATE CIBERNETICĂ