Govern d'Andorra

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Xarxes Wifi Públiques

Conscienciació en ciberseguretat

Abril de 2022

ÍNDEX

Aspectes a tenir en compte

Les **xarxes wifi públiques** son aquelles que no estan protegides per una contrasenya o bé estan obertes a un gran número d'usuaris (com el cas de universitats o entitats públiques) i permeten, a qualsevol usuari, connectar-se a internet de forma senzilla, còmoda i ràpida. Suposen una eina molt útil quan estem de viatje, mentre ens prenem alguna cosa en un bar… però no podem oblidar-nos que, encara que son útils, **no son xarxes segures**.

Habitualment, en les xarxes wifi públiques no es xifra (adequadament) la informació que es transmet, pel que no tenim control sobre la informació a la que accedim o compartim. Si tenim en compte que solen ser xarxes a les que estan connectats en tot moment un gran número d'usuaris, estarem exposant la nostra informació en un ampli espai susceptible de ser atacat.

- No et connectis a xarxes wifi públiques si pots evitar-lo. Algun usuari connectat podria robar-te informació. Utilitza sempre que sigui possible el VPN corporatiu o xarxes mòbils 3G, 4G o 5G.
- Si et connectes, accedeix a una xarxa amb seguretat WPA o WPA2 (això pots veure-ho en les opcions de wifi).
- Navega sempre per pàgines amb protocol https://... Assegurat revisant la URL.
- No iniciïs sessió amb usuari i contrasenya en cap servei en xarxes insegures ni tampoc utilitzis funcions de recordar contrasenya.
- Elimina les dades de xarxa memoritzades pel teu equip. Sobre tot les referents a dades personals o bancaries.

ÍNDEX

Riscos al utilitzar xarxes wifi

Robatori de dades transmeses

Si ens connectem a xarxes insegures i obertes, qualsevol atacant amb un mínim de coneixements podria arribar a accedir a informació personal i sensible transmesa des de els nostres dispositius mediant tècniques hacking.

Robatori de dades emmagatzemades al nostre equip

Al estar connectats a xarxes insegures, a les que accedeix un gran número d'usuaris, la informació emmagatzemada en els nostres equips podria quedar compromesa per la seva exposició a través d' algun recurs compartit o per un atac dirigit.

Infecció dels dispositius

Els atacants poden intentar infectar o prendre el control dels nostres equips i dispositius amb codi maliciós per diferents fins, des de una web fraudulenta o un punt d'accés a xarxes corruptes.

Riscos al utilitzar xarxes wifi

Equips intermediaris malintencionats

L'atacant, connectat a la nostra mateixa xarxa, podria fer ús de diferents tècniques amb les que poden arribar a interrompre entre la comunicació del nostre equip i un proveïdor de servei, capturant i/o modificant la informació transmesa.

El hacker "inocent"

En un moment, donat podem caure en la temptació d'utilitzar eines "hacking wifi" per connectar-nos a xarxes obertes. No sol es considera un delicte si no que deixem exposats els nostres equips a possibles atacs provinents de la mateixa xarxa.

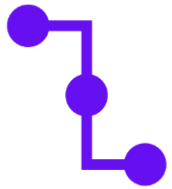
ÍNDEX

Amenaces i atacs

Quan ens connectem a xarxes wifi públiques o insegures, estem posant en risc la informació amb la que treballem, ja que accedim a xarxes compartides amb un gran número d'usuaris en les que els nostres dispositius son visibles. Això fa que els atacants exploten vulnerabilitats en la mateixa xarxa per fer-se amb la nostra informació i poder utilitzar-la en benefici. En aquest tipus de xarxes solen donar-se les següents amenaces i atacs:

Robatori de dades

Existeix un gran número i tipologia d'atacs orientats al robatoris de dades i credencials. Si aquestes dades corresponen a informació o credencials d' accés corporatives, estarem exposant la informació sensible de la nostra empresa davant aquest atacants i, dependent dels nostres privilegis en la mateixa, pot arribar a ser un risc de elevades conseqüències.



Atacs del tipus "Man in the middle"

En els que el delinqüent es cola entre la comunicació dels nostres equips amb el punt d'accés wifi, capturant la informació tramesa per fer un ús inadequat de la mateixa o bé modificar-la. Es un tipus d'atac molt difícil de detectar.

image: Flaticon es

ÍNDEX

Registres al utilitzar xarxes wifi públiques

Llocs web fraudulents

Poden existir falsos punts d'accés wifi que utilitzen un nom que genera confiança per a aconseguir que ens connectem a ells. Aquests punts solen estar infectats o donen capacitat a l'atacant de monitoritzar la nostra activitat en xarxa. En moltes ocasions redirigeixen a llocs web fraudulents infectats amb codi maliciós.

Malware

Correm el risc a exposar-nos a llocs web fraudulents o injecció de malware des del punt d'accés wifi.

Sniffers

Unit als atacs tipus “Man in the middle”, els sniffer són eines utilitzades per a la captura indiscriminada de paquets (dades del trànsit) que flueixen per la xarxa. Aquests paquets poden contenir informació sensible i/o personal que pot ser interceptada.

ÍNDEX

Recomanacions de seguretat

Instal·la, habilita i configura correctament el teu firewall
Configura el firewall perquè no permeti connexions entrants als teus equips i dispositius per part d'altres usuaris de la xarxa. Molts sistemes operatius permeten triar la manera de treball del firewall quan s'accedeix a xarxes wifi externes.

Mantingues actualitzada la teva eina antivirus i actualitzacions de seguretat
És fonamental mantenir actualitzada qualsevol aplicació, més encara l'eina antivirus. Les actualitzacions de seguretat periòdiques que llancen els fabricants aporten solucions davant els possibles atacs més recents pel que és de vital importància mantenir-los al dia.

Recomanacions de seguretat

Configura el teu equip i dispositius per a treballar segur en la xarxa
Configura el teu equip per a treballar segur en xarxes wifi públiques. Selecciona el "perfil de xarxa públic" en les propietats de la connexió perquè l'equip s'estableixi com a ocult per a altres dispositius de la xarxa.

Elimina les dades i llista de punts d'accés memoritzats
Elimina la informació memoritzada en els formularis d'accés així com comptes de correu. Elimina el llistat de punts d'accés wifi per a evitar que els equips o dispositius es tornin a connectar automàticament si entren en el seu rang. Especialment crític amb xarxes que no són de confiança.

Desactivar la connexió automàtica wifi i sincronització
Desactiva la funció de connexió automàtica a xarxes wifi per a evitar l'accés a xarxes insegures. D'igual manera deshabilita l'opció de sincronització automàtica d'informació per a evitar realitzar còpies de seguretat fora d'una connexió segura corporativa.

Recomanacions de seguretat

Evita realitzar compres online connectat a xarxes insegures

Protegeix les teves pantalles de mirades indiscretes

Comprova que la xarxa disponible es la oficial del lloc en el que estàs

Segueix els consells de seguretat i política de la teva empresa i , Navega segur!

Assegura't d'accedir sempre a webs amb certificat SSL. **(https://)**

Evita l'ús de xarxes públiques i insegures per a realitzar operacions confidencials o que continguin dades personals

Govern d'Andorra

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

ANDORRA
DIGITAL

Entitats col·laboradores

andorra
telecom

DAND
DIGITALAND by Ibermática | TAN