

AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

CONSCIENCIACIÓ EN CIBERSEGURETAT

TETHERING

Desembre 2025
Document d'ús públic

1 CONNECTA'T A INTERNET AMB LES TEVES DADES MÒBILS (*TETHERING*)

.....

2 COM POTS ACTIVAR LA COMPARTICIÓ DE XARXA AL TEU DISPOSITIU MÒBIL

.....

3 CONSIDERACIONS A L'HORA D'USAR LA COMPARTICIÓ DE XARXA AL DISPOSITIU MÒBIL

.....

4 CONNECTA'T A INTERNET USANT LES TEVES DADES MÒBILS AMB LA COMPARTICIÓ DE XARXA

.....

5 BONES PRÀCTIQUES DE CIBERSEGURETAT

.....



6 COMPARATIVA: COMPARTICIÓ DE XARXA vs. WIFI PÚBLIC

.....

7 RECORDA!



1 ■ CONNECTA'T A INTERNET AMB LES TEVES DADES MÒBILS (*TETHERING*)

Què és el *tethering*?

El ***tethering*** (compartició de xarxa) és la pràctica de compartir la **connexió de dades mòbils d'un dispositiu** (com un telèfon intel·ligent, per exemple) amb altres dispositius com ordinadors, tauletes, etc. Aquest dispositiu esdevé un **punt d'accés a internet**.

TIPUS DE *TETHERING*

Wifi

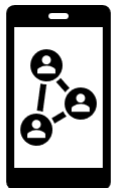
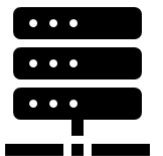
El més comú i fàcil de fer servir □ El telèfon crea una xarxa sense fils a la qual altres dispositius es connecten.

USB

Connexió directa: connecta el mòbil directament al teu ordinador mitjançant un cable USB. **Sol ser més segur i estable.**

Bluetooth

Opció menys comú, però útil quan vols compartir dades amb un baix consum de bateria.



RISCOS DE SEGURETAT

- **Accés no autoritzat:** si no es configura correctament, altres poden connectar-se al dispositiu sense permís.
- **Intercepció de dades:** especialment en connexions wifi sense encriptació forta.
- **Programari maliciós:** dispositius connectats poden introduir amenaces si no estan protegits.
- **Fuites d'informació:** si el dispositiu es perd o és robat mentre està compartint connexió.



Per què cal evitar les xarxes wifi públiques?

Les xarxes wifi públiques poden semblar una alternativa adient per connectar-se a internet, però porten associats diversos riscos per a la seguretat digital.

Motius per evitar-les

- **Xarxes falses:** poden simular ser xarxes legítimes (com WiFi_CafèGratis) per robar les teves dades.
- **Distribució de programari maliciós:** alguns atacants utilitzen aquestes xarxes per instal·lar programari maliciós al teu dispositiu quan es connecta a la xarxa.
- **Accés no autoritzat:** altres usuaris connectats poden intentar explorar el teu dispositiu si no està ben protegit.
- **Robatori de credencials:** encara que no introdueixis contrasenyes, poden interceptar sessions actives i agafar el controls dels teus comptes.
- **Manca d'criptació:** moltes xarxes no protegeixen les dades que viatgen entre el teu dispositiu i el servidor, cosa que permet que altres les interceptin fàcilment.
- **Atacs d'intermediari (*man-in-the-middle*):** un atacant es pot col·locar entre tu i el lloc web al qual accedeixes i llegir o modificar la informació sense que ho notis.



COMPTE AMB LES XARXES WIFI PÚBLIQUES

L'ús del wifi públic pot ser convenient, però, també, és una de les **VULNERABILITATS** més gran que existeixen, en termes de seguretat de la informació.

RISCOS D'UTILITZAR EL WIFI PÚBLIC

- ❖ Intercepció de dades (*sniffing*).
- ❖ Xarxes wifi falses.
- ❖ Distribució de programari maliciós.
- ❖ Robatori de la identitat digital personal.
- ❖ Robatori de dades transmeses.



COM ET POTS PROTEGIR QUAN USES WIFI PÚBLIC?

- ✓ Fes servir una **VPN**.
- ✓ Evita fer transaccions sensibles.
- ✓ Usa llocs web amb **HTTPS**.
- ✓ Desactiva l'ús compartit dels arxius i dispositius.
- ✓ Mantingues el teu dispositiu degudament actualitzat.
- ✓ Desactiva el wifi quan no el facis servir.
- ✓ Desactiva la connexió automàtica a les xarxes wifi públiques.
- ✓ Utilitza l'autenticació de múltiples factors (**AMF**).

Riscos principals d'utilitzar wifis públics

Riscos principals d'utilitzar wifis públics



1. Atacs d'intermediari

<L'atacant es posiciona entre el teu dispositiu i internet, de manera que pot interceptar o fins i tot modificar la informació que envies i que reps.



2. Xarxes falses o *honeypots* (esquers)

Xarxes wifi amb noms enganyosos (com Cafè_Gratis o Biblioteca_WiFi) que en realitat s'han creat per espiar les persones que s'hi connecten.



3. Intercepció de trànsit sense xifrar

Si accedeixes a llocs sense HTTPS, qualsevol informació que introdueixis pot ser vista per altres persones.



4. Propagació de programari maliciós

Alguns wifis públics poden redirigir-te a llocs falsos per instal·lar-te virus o programari espia.

Beneficis de compartir la connexió mòbil mitjançant la compartició de xarxa



Seguretat

Només tu tens control sobre qui accedeix a la teva xarxa. Pots protegir-la amb contrasenya forta i canviar-la quan vulguis.



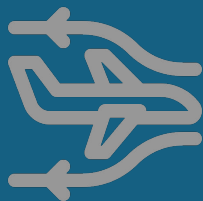
Privacitat

Les teves dades no passen per servidors de tercers sospitosos o públics, cosa que minimitza els riscos.

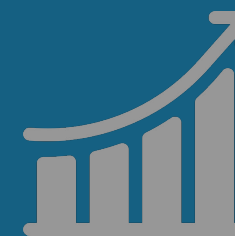


Flexibilitat

Pots connectar el teu ordinador o tauleta a una altra persona de confiança, sense dependre de xarxes externes.



Fes-ho en aeroports, cafeteries, hotels o fins i tot a l'aire lliure quan no hi hagi una xarxa wifi de confiança disponible. Ideal per a viatges.



Millora la teva productivitat

Accés estable i ràpid a reunions, classes virtuals o teletreball.

2 ■ COM POTS ACTIVAR LA COMPARTICIÓ DE XARXA AL TEU DISPOSITIU MÒBIL

Passos per a Android



Passos per a Android

Ves a **Configuració** > **Connexions** o **Xarxes i internet**.

Entra a la secció **Zona wifi/Compartir connexió** o similar.

Activa l'opció **Zona wifi mòbil**.

Personalitza el nom de la xarxa i configura una contrasenya segura.

Connecta't des del teu altre dispositiu, com si fos una xarxa wifi normal.

Ves a **Configuració** > **Dades mòbils** > **Compartir internet**.

Activa l'opció **Permetre a altres connectar-se**.

Apareixerà el nom de la teva xarxa i una contrasenya per defecte (pots modificar-la).

Altres dispositius podran veure la xarxa des del seu menú wifi.

Passos per a iOS (iPhone)



3 ■ CONSIDERACIONS A L'HORA D'USAR LA COMPARTICIÓ DE XARXA AL DISPOSITIU MÒBIL



Dades

Consulta quantes dades et queden.
Algunes tasques com videotrucades o actualitzacions automàtiques consumeixen molts megues.

Bateria

Usar compartició de xarxa pot esgotar ràpidament la bateria del teu mòbil. Tingues a mà un carregador o una bateria externa.

Senyal

La qualitat de la connexió depèn de la cobertura de la teva xarxa mòbil. Si estàs en una zona amb mal senyal, la connexió serà més lenta o inestable.



Seguretat

Canvia la contrasenya del punt d'accés wifi regularment i no utilitzis claus dèbils com «12345678».

 Desactiva-la quan no la facis servir

No deixis la xarxa activa si no uses la compartició de xarxa. Això evita connexions no desitjades i estalvia bateria.

4. ■ CONNECTA'T A INTERNET USANT LES TEVES DADES MÒBILS AMB LA COMPARTICIÓ DE XARXA

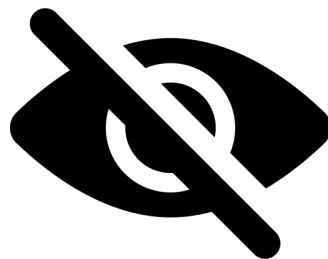


BONES PRÀCTIQUES DE CIBERSEGURETAT

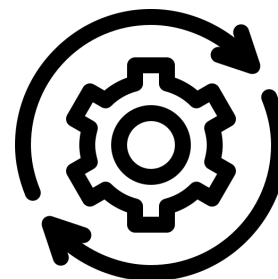
- ✓ Usa **contrasenyes robustes**.
- ✓ **Ocul**ta el **SSID** (nom de la xarxa) si no necessites que sigui visible.
- ✓ **Limita** els **dispositius connectats** i revisa qui hi accedeix.
- ✓ **Desactiva** la **compartició de xarxa** quan **no la utilitzis**.
- ✓ **Actualitza** el **sistema operatiu** i fes servir **antivirus**.
- ✓ Utilitza **VPN** si **comparteixes connexió** en espais públics.



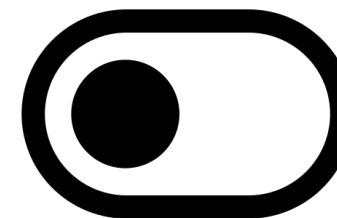
**CONTRASENYA
ROBUSTA**



OCULTA EL SSID



**ACTUALITZA SISTEMA +
ANTIVIRUS**



**DESACTIVA
COMPARTICIÓ XARXA**



USA VPN

5. BONES PRÀCTIQUES DE CIBERSEGURETAT



**Actualitza
regularment** el
sistema operatiu i
les aplicacions.

**Navega només per
llocs amb HTTPS**
(cadenat a la barra
del navegador).

**Evita transaccions
sensibles** si estàs en una
xarxa poc fiable (fins i tot
si és la teva compartició
de xarxa, però estàs en
zona pública).

**No et
descarreguis**
programari des
de fonts
desconegudes

**Usa antivirus i
tallafof** tant en el
mòbil com en el
dispositiu
connectat.

**Desactiva l'ús
compartit d'arxius**
al teu ordinador
mentre utilitzes la
compartició de
xarxa.



6. ■ COMPARATIVA: COMPARTICIÓ DE XARXA vs. WIFI PÚBLIC



CARACTERÍSTIQUES	<i>TETHERING</i> (DADES MÒBILS)	WIFI PÚBLIC
Seguretat	Alta, si es configura bé	Baixa, sense garanties
Privacitat	Alta	Molt baixa
Control de xarxa	Totalment sota el teu control	Nul
Estabilitat	Depèn de la teva xarxa mòbil	Variable i inestable
Consum de dades	Sí	No (però exposa les teves dades)
Risc de programari maliciós/espionatge	Molt baix	Molt alt

7. RECORDA!



Els wifis públics poden semblar còmodes, però representen una amenaça per a la teva informació.



La compartició de xarxa és una alternativa segura i pràctica, especialment si treballes o estudies des de diversos llocs.



Aprendre a compartir les dades mòbils de manera responsable pot protegir la teva privacitat i estalviar-te problemes.



Prioritza la seguretat digital en el teu dia a dia. No posis en risc les teves dades per una connexió gratuïta.

Avís Legal

Aquest document conté informació pública.

El seu objectiu és la conscienciació en ciberseguretat pels ciutadans, empreses i entitats d'Andorra.

© Agència Nacional de Ciberseguretat d'Andorra.