

Transformació Digital d'ANDORRA

LA CIBERSEGURETAT DURANT LES VACANCES D'ESTIU

Agost 2026
Document d'ús públic



Índex

1. Introducció

2. Riscos de ciberatac i com ens hem de protegir

3. Conclusions clau



1. INTRODUCCIÓ



Les vacances són el moment perfecte per desconnectar..., però també perquè els ciberdelinqüents aprofitin distraccions, presses i entorns poc segurs.



PER QUÈ AUGMENTA EL RISC A L'ESTIU?

- **DESPLAÇAMENT:** més xarxes públiques, més dispositius fora de l'oficina.
- **RELAXACIÓ:** menys atenció a senyals de frau.
- **COMPRES:** més exposició a botigues falses i pesca.
- **PUBLICACIONS A LES XARXES:** informació útil per a atacants.



ANDORRA
DIGITAL



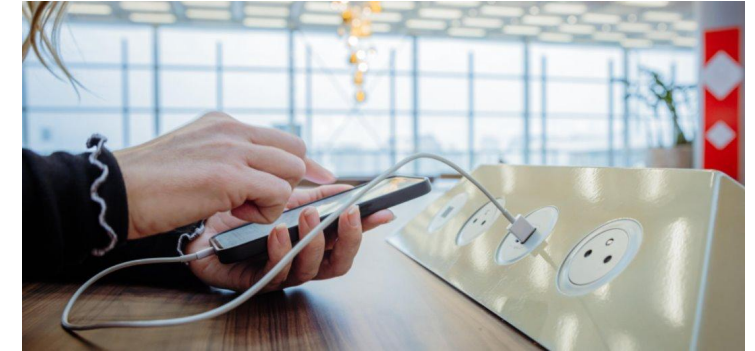
ANDORRA
DIGITAL
CIBERSEGURETAT

2. ■ RISCOS DE CIBERATAAC I COM ENS HEM DE PROTEGIR



JUICE JACKING

- Els ports USB públics es poden manipular per **robar dades** o **injectar programari maliciós** (*juice jacking*).
- Els carregadors «gratuïts» dels hotels poden incloure maquinari maliciós.



Recomanacions:

- Fes servir el **teu propi carregador i endoll**, mai un USB públic.
- Porta una **bateria externa**.
- Si no tens cap altra opció i has de fer-lo servir, utilitza un **bloquejador de dades USB**.
- Activa el mode «**només càrrega**» si el teu mòbil ho permet.



CONSELLS PER TREBALLAR SEGUR DES DE LES SEGONES RESIDÈNCIES

- Canvia la contrasenya del rúter i actualitza el microprogramari.
- Evita treballar des de xarxes wifi públiques.
- Fes servir sempre una **VPN corporativa**.
- Tingues el portàtil xifrat i amb bloqueig automàtic.
- No deixis dispositius a la vista quan surtis.

Què NO has de publicar a les xarxes quan estàs de vacances

- Dates exactes del viatge
- Ubicació en temps real
- Fotos de la casa buida
- Targetes d'embarcament
- Documents, claus, polseres d'hotel, etc.

Regla d'or: *publica quan hakis tornat, no mentre estiguis allà.*



RISCOS DE LES FOTOS EN TEMPS REAL DURANT LES VACANCES



- Les fotos inclouen **metadades** (geolocalització).
- Permeten saber que a casa teva no hi ha ningú.
- Poden revelar menors, rutines o pertinences de valor.

Solució: desactiva la geolocalització de la càmera i no publiquis en temps real.



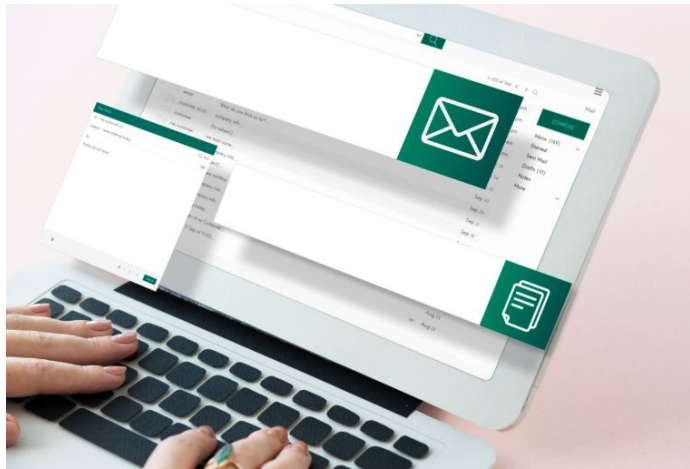


SELFIES SÍ, TARGETES D'EMBARCAMENT NO

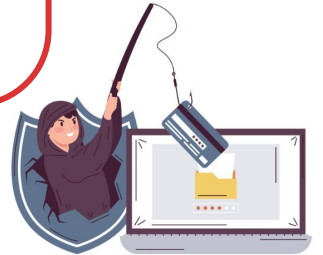


- El codi QR o el localitzador permet a un atacant:
 - Canviar el teu seient.
 - Cancel·lar el teu vol.
 - Accedir a les teves dades personals.
- Hi ha programari que permet llegir fins i tot fotos borroses.

Els atacants envien correus com:



- «*Confirmació de la teva reserva*»
- «*Problema amb el teu vol*»
- «*El teu hotel ha cancel·lat l'habitació*»
- «*La teva maleta no ha arribat*»



Com es pot detectar

- Revisa el remitent.
- No facis clic a enllaços urgents.
- Entra sempre des del web oficial.



Estafes típiques de lloguer vacacional a l'estiu

- Anuncis massa barats.
- Propietaris que «són a l'estranger».
- Sol·licitud de pagament per Bizum o transferències ràpides.
- Fotos robades d'altres webs.

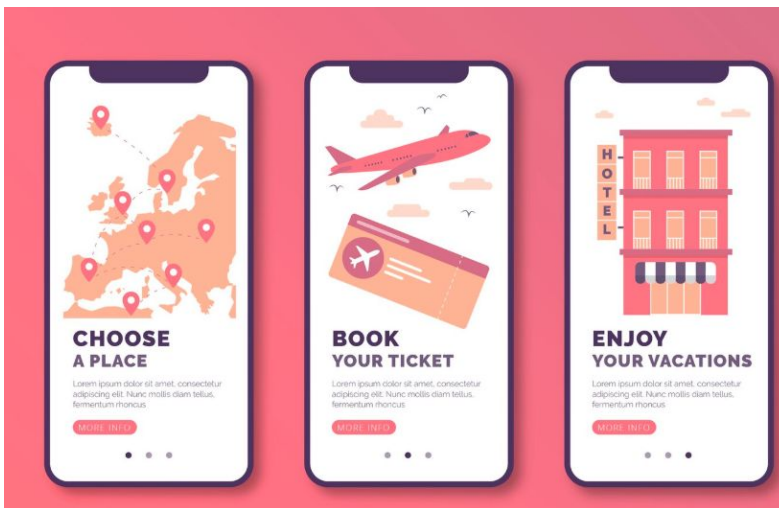


Com es pot evitar:

- Usa plataformes conegudes.
- Revisa opinions reals.
- Mai paguis fora de la plataforma.
- Demana videotrucada per verificar l'habitat



SEGURETAT EN APPS DE VIATGES I RESERVES



- Activa la verificació en dos passos.
- No desis targetes en apps desconegudes.
- Descarrega només des de botigues oficials.
- Revisa permisos: una app de vols no necessita accedir als teus contactes.

CIBERSEGURETAT DURANT LES REBAIXES D'ESTIU



- Desconfia de descomptes del 70-90 % en marques prèmium.
- Compte amb webs que només accepten targeta o transferència.
- Verifica que l'URL tingui **HTTPS** i certificat vàlid.
- Cerca opinions externes, no només les de la pàgina web en qüestió.
- Assegura't que es tracta d'una pàgina fiable (faltes d'ortografia, informació sobre l'empresa, etc.).
- Recorda: **Ningú regala res.**



PROTEGEIX EL TEU MÒBIL AQUEST ESTIU

- **Actualitza el sistema operatiu.**
- **Activa el bloqueig biomètric.**
- **Usa apps oficials.**
- **Configura l'esborrament remot.**
- **Fes una còpia de seguretat abans de viatjar.**



ACCÉS REMOT SEGUR DURANT L'ESTIU

- Usa sempre una **VPN**.
- No entris a sistemes corporatius des de xarxes públiques.
- **Activa AMF** (doble factor).
- **Evita treballar des de dispositius personals.**

- *Encripta la teva connexió.*
- *Evita l'espionatge a les xarxes públiques.*
- *Protegeix les credencials corporatives.*
- *Permet l'accés segur a recursos interns.*



COM POTS PROTEGIR LA TEVA FEINA ABANS DE DESCONNECTAR



- Tanca sessions en tots els dispositius.
- Canvia contrasenyes crítiques si toca.
- Activa respostes automàtiques sense revelar gaire informació.
- Informa el teu equip de contactes alternatius.
- Revisa permisos temporals i accessos compartits.

Suplantacions de directius durant les vacances («el CEO és fora»)

- Els atacants envien correus fent-se passar per directius absents.
- Solen demanar pagaments urgents, transferències o informació delicada.

Com es pot detectar:



- El CEO mai demana pagaments per correu electrònic.
- Verifica per telèfon o Teams.
- Revisa el domini del remitent.
- Desconfia de la urgència.





ANDORRA
DIGITAL



ANDORRA
DIGITAL
CIBERSEGURETAT

3. CONCLUSIONS CLAU





- L'estiu és un període de **risc alt**.
- La majoria dels atacs es basen en **distraccions i excés de confiança**.
- Amb algunes precaucions, pots reduir el risc més del 90 %.
- La ciberseguretat és part del teu equipatge.

