

AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

CONSCIENCIACIÓ EN CIBERSEGURETAT

LA CIBERSEGURETAT DURANT LES VACANCES D'ESTIU

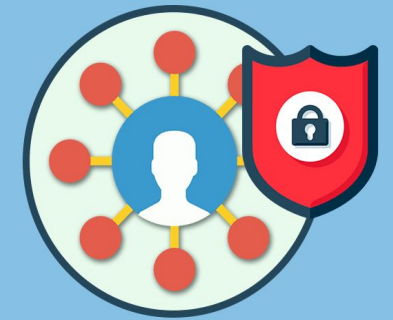
Juliol 2025
Document d'ús públic

1

CONTEXT: CONSELLS PER PROTEGIR LA TEVA INFORMACIÓ A L'ESTIU

2

RECOMANACIONS DE CIBERSEGURETAT PER A L'ESTIU



1 ■ CONTEXT: CONSELLS PER PROTEGIR LA TEVA INFORMACIÓ A L'ESTIU



Els **atacs cibernètics** augmenten considerablement durant l'**època de l'estiu**, atès que els cibercriminals aprofiten les vacances per atacar les organitzacions i les llars.

Quan naveguem per internet, hi ha moltes **amenaces** amagades darrere de cada clic que fem en una pàgina web. Per exemple, quan reservem les vacances des d'un web no oficial, quan fem transferències bancàries connectats a una xarxa wifi pública, etc.



A l'estiu, que estem menys vigilants, estem més relaxats i no anem tant amb compte, és quan podem patir més atacs (el robatori de la nostra informació personal, la propagació de virus en els nostres equips, etc.)

Per això, i amb l'objectiu que aquests atacs no t'agafin desprevingut, et proposem una sèrie de **RECOMANACIONS** que cal tenir en compte per tal que tinguis unes vacances d'estiu sense ensurts i que no pateixis cap tipus d'incident de seguretat.

1. Wifis públiques

Malgrat que molts punts d'accés a la xarxa wifi pública poden ser **segurs**, no hem d'oblidar que els ciberdelinqüents solen publicar punts d'accés de **wifi falsos**.



2. Vigila amb el que publiquess a les xarxes socials

Si tens intenció de publicar informació privada sobre les teves vacances a les xarxes socials, per exemple, la localització actualitzada o els dies que et queden per tornar a casa, és millor que ho facis a la tornada.

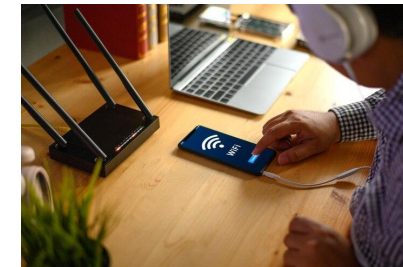
3. Canvia les teves contrasenyes quan tornis de vacances

És convenient que, un cop finalitzat el viatge o l'estada, canviïs les teves contrasenyes i posis al dia la seguretat dels teus dispositius.



4. Còpies de seguretat

Durant les vacances, **és important fer còpies de seguretat regularment i mantinguis els dispositius actualitzats**. Les actualitzacions inclouen **pedaços de seguretat** que protegeixen tant el sistema operatiu com les aplicacions contra ciberatacs.



5. Vigila amb les aplicacions mòbils que et descarregues

Descarregar aplicacions no verificades pot posar en risc la seguretat de la nostra informació. Per això, et recomanem que descarreguis només les **aplicacions de llocs web oficials**, com Apple Store i Google Play.



6. Ves amb compte amb el que connectes al teu equip

Les infeccions per USB són freqüents i representen un gran risc per als nostres equips. Et recomanem que **no connectis els teus USB en llocs desconeguts per evitar possibles contagis i fuita d'informació**, i així protegir la seguretat de la teva informació.



7. Activa l'autenticació de doble factor sempre que sigui possible

Cada dia es roben milers de comptes d'usuaris o de correus electrònics perquè la gent **no utilitza contrasenyes o les que fa servir són dèbils**. Per això, t'aconsellem que sempre que sigui possible activis l'**autenticació de doble factor**; és una **capa extra de seguretat**, ja que et demana un **CODI D'UN SOL ÚS** que s'envia al teu telèfon mòbil.



8. Compte amb els correus que reps i envies

Els **ciberatacs són cada vegada més sofisticats** i busquen obtenir dades personals i/o financeres dels usuaris aprofitant que són fora de l'oficina. Per evitar-ho, et recomanem que **no configuris la resposta automàtica de «fora de l'oficina per vacances»**, atès que els ciberdelinqüents poden aprofitar aquestes absències per suplantar la teva identitat.

9. Pèrdua dels dispositius electrònics

Et recomanem que abans de sortir de casa facis una **còpia de seguretat** i actualitzis el teu dispositiu; és una bona manera de protegir i recuperar la informació en cas que perdís el dispositiu.



10. Evita connectar-te a xarxes wifi compartides

En realitat, no som conscients dels **riscos** que implica compartir una xarxa amb una connexió a internet. Per això, et detallem una sèrie de riscos que et pots trobar i que cal que sàpigues identificar:

- Que algú que estigui connectat a una xarxa wifi pública compartida pugui veure la informació que reps o envies a través dels teus dispositius.
- Que algú que estigui connectat a una xarxa wifi pública compartida pugui accedir al teu dispositiu.
- Que algú que està connectat a aquesta mateixa xarxa et pugui robar dades personals i confidencials.

Moltes vegades és **inevitable** haver-se de connectar a una xarxa wifi pública, ja sigui perquè som fora de la zona d'**itinerància** (*roaming*) o perquè cada vegada tenim menys dades mòbils. En aquests casos, hem de ser molt prudents a l'hora d'accedir a una informació.

Per exemple, fer servir una **VPN** pot ser útil per evitar possibles atacs, malgrat que això no ens manté completament protegits, o desactivar qualsevol tipus de **connexió automàtica** dels nostres dispositius per no ser detectats per altres (per exemple, a través del Bluetooth).

2. RECOMANACIONS DE CIBERSEGURETAT PER A L'ESTIU

Virtual skimmers

Els delinqüents aconsegueixen introduir **codis maliciosos** en webs legítims per robar les dades de les targetes de crèdit quan els usuaris les utilitzen en **llocs web de confiança**.



Cal limitar el nombre de dispositius que t'emportes a la platja

Emporta't només aquells que siguin necessaris, per **minimitzar els riscos** de perdre informació confidencial que tinguis emmagatzemada en aquests dispositius.

Cal evitar els accessos no desitjats

Els telèfons mòbils i els ordinadors contenen una gran quantitat d'**informació personal i professional** de l'usuari. **NO** s'ha d'introduir mai informació personal/professional ni accedir a cap compte des de dispositius que no siguin de la teva confiança.

Robatori d'informació emmagatzemada per empreses de transport i d'allotjament

Això suposa un **perill**, ja que els usuaris tendeixen a donar l'adreça electrònica fàcilment. En cas que es produeixi una filtració, els ciberdelinqüents poden enviar **correus de pesca** per robar les credencials a aquests usuaris.

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.