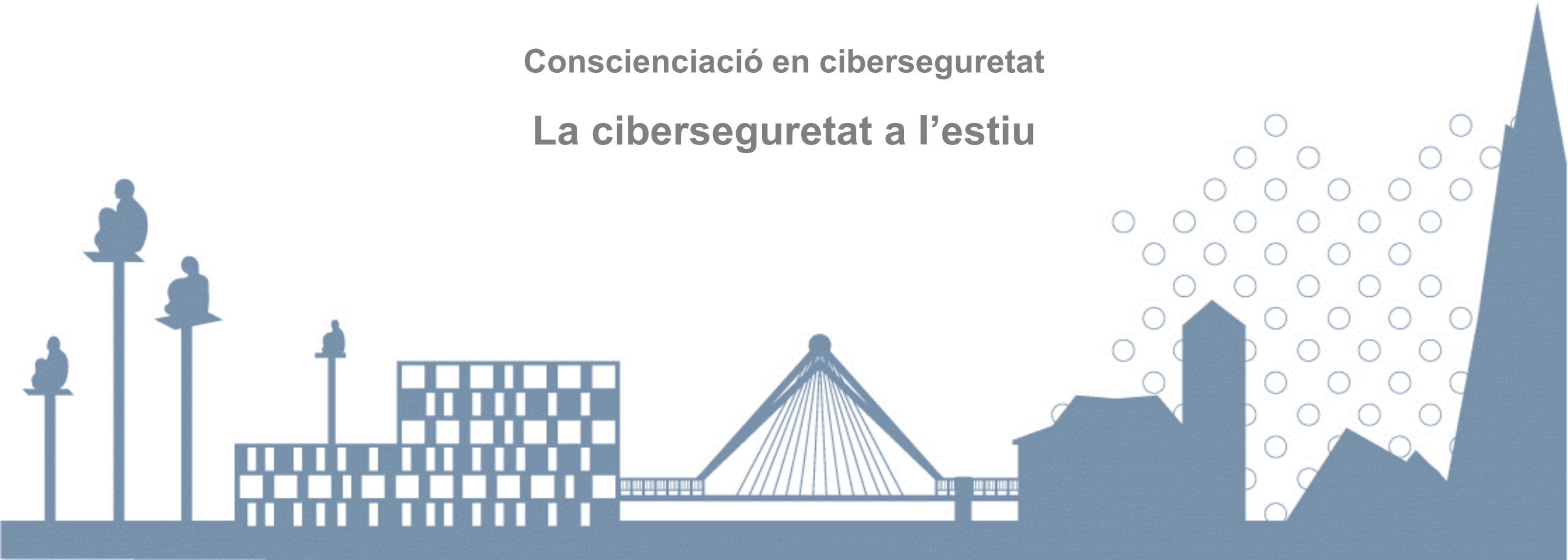
Agència Nacional de Ciberseguretat d'Andorra

Conscienciació en ciberseguretat

La ciberseguretat a l'estiu



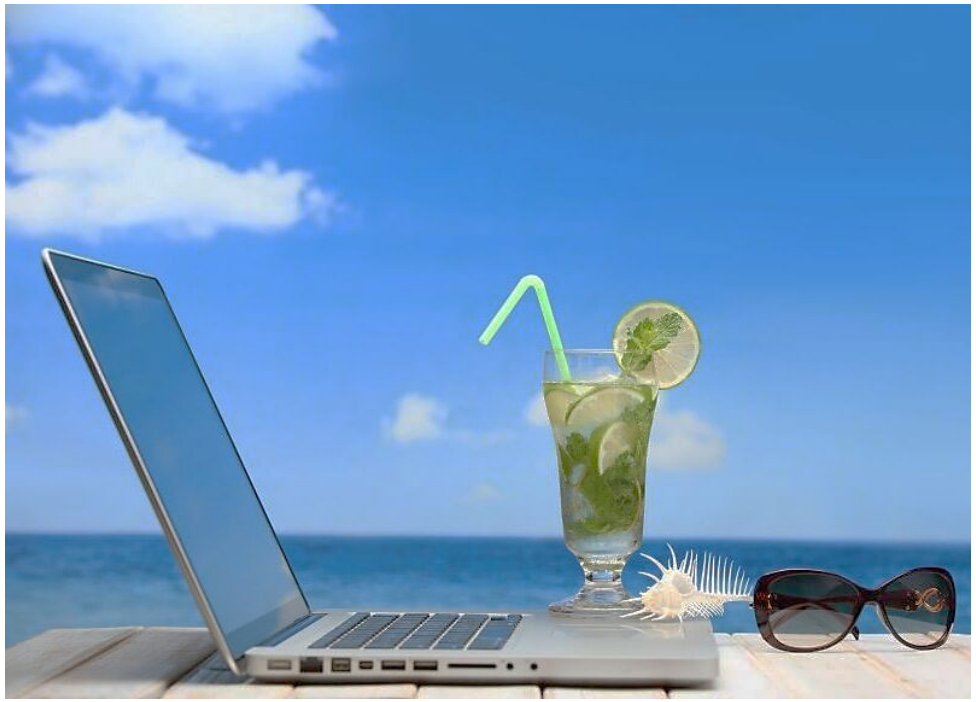
La ciberseguretat a l'estiu:

Els atacs cibernètics augmenten de manera considerable durant l'època de l'estiu, ja que els cibercriminals aprofiten les vacances per atacar les empreses i les llars.

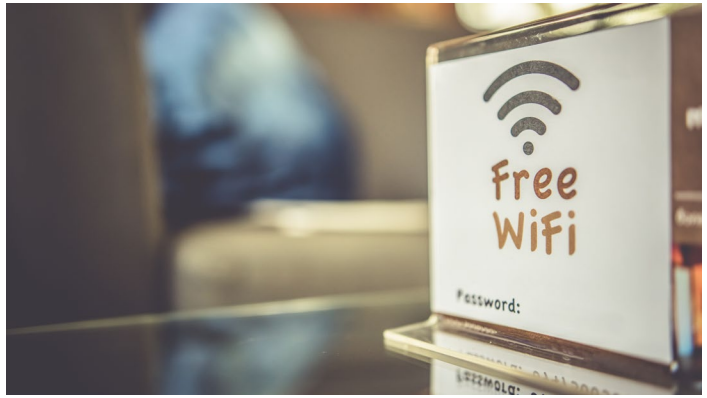
Quan navegues per Internet, són moltes les amenaces que s'amaguen darrere de cada clic que fem en una pàgina web, per exemple, quan reservem les vacances des d'una web no oficial, quan realitzem transferències bancàries connectats a una xarxa WiFi pública, quan publiquem informació privada de les nostres vacances a les nostres xarxes socials...

Aquestes conductes són molt típiques de realitzar, no només durant l'època de l'estiu, sinó també durant tot l'any. No obstant això, sembla que és a l'estiu quan estem més descuidats, relaxats i menys atents i podem patir més riscos com, per exemple, el robatori de la nostra informació personal, la propagació de virus...

Per a això, i, per tal que aquests atacs no t'agafin d'imprevist, et proposem una sèrie de recomanacions a tenir en compte, de cara que les teves vacances d'estiu estiguin lliures de sobresalts i de patir algun tipus d'incident de seguretat.



Consells per protegir-se al llarg de l'estiu:

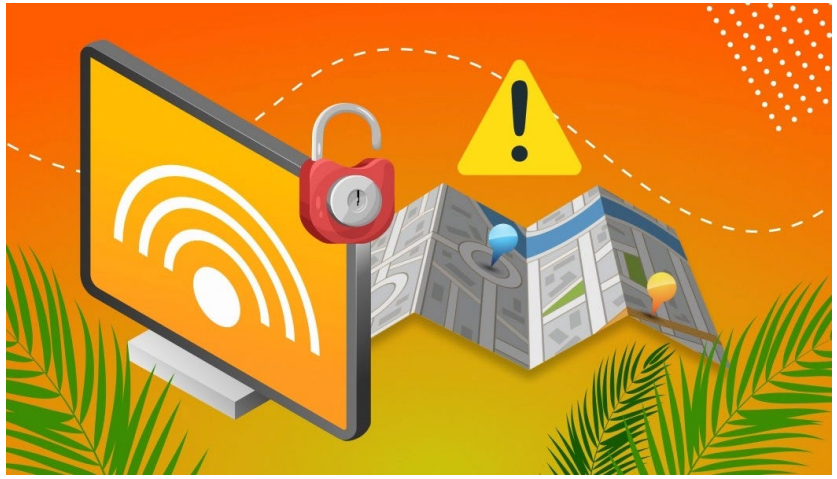


1. Xarxes WiFi públiques: Tot i que molts punts d'accés a la xarxa pública solen ser segurs, no hem d'oblidar que els ciberdelinqüents poden publicar punts d'accés de WIFI falsos. Recordeu no realitzar operacions sensibles, com per exemple, pagaments online o accedir a informació delicada/sensible des d'aquest tipus de connexió.
2. Compte amb el que publiqueu a les Xarxes Socials: Si heu de publicar informació privada de les vostres vacances a les xarxes socials, la vostra localització actualitzada o els dies que us falten per tornar a la vostra llar, és millor que ho feu quan torneu a casa. A més, és recomanable no connectar-se a aquest tipus de xarxes si voleu accedir a aplicacions, eines o informació de la companyia on treballeu.
3. Canvieu les contrasenyes a la tornada de les vacances: És convenient que, un cop hagueu finalitzat el vostre viatge o estada, canvieu les vostres contrasenyes i poseu al dia la seguretat dels vostres dispositius.

Consells per protegir-se al llarg de l'estiu:

4. Còpies de seguretat: Quan esteu de vacances i feu servir els vostres dispositius, us recomanem que realitzeu cada cert temps còpies de seguretat i actualitzeu a les últimes versions disponibles. Heu de saber que una notificació salta cada vegada que hi ha una nova actualització disponible. Així doncs, el més important és executar-la, ja sigui del propi sistema operatiu, com en les aplicacions. La majoria d'aquestes actualitzacions contenen millores de seguretat que eviten que sigueu més vulnerables als atacs cibernètics.

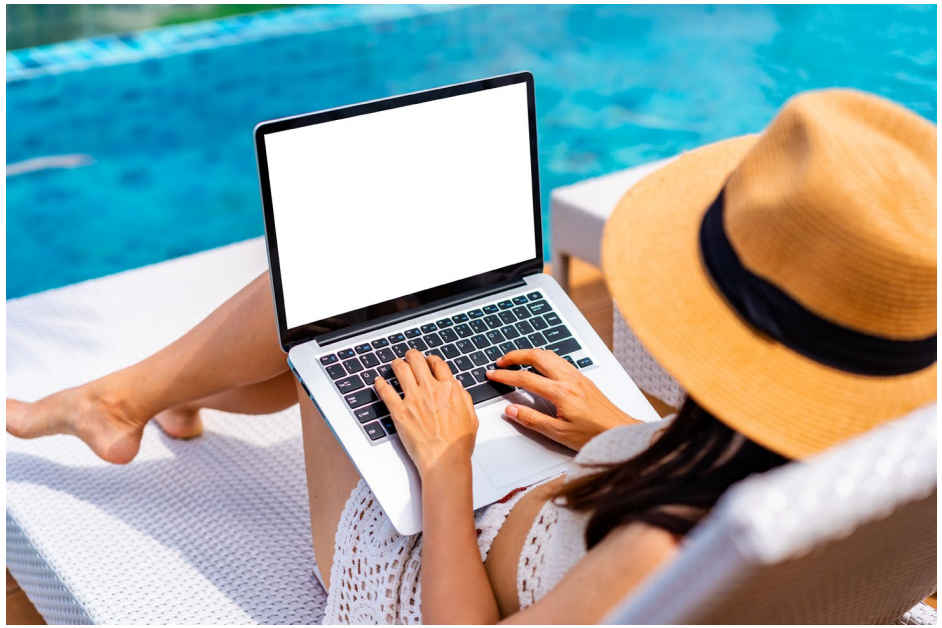
5. Compte amb les aplicacions mòbils que us descarregueu: Encara no ha estat testada la seguretat de les aplicacions mòbils que us descarregueu, ni tampoc teniu les garanties suficients del que us descarregueu pugui suposar un risc per la seguretat de la vostra informació. Recomanem, per tant, que les aplicacions que us descarregueu sempre siguin de llocs oficials, com de l'apple store i google play.



Consells per protegir-se al llarg de l'estiu:

6. Compte amb allò que connecteu als vostres equips: Les infeccions per USB són molt comunes. Cada vegada hi ha més organitzacions que prohibeixen als seus empleats que els usin a causa del seu alt risc d'infectar els dispositius. Per això, us recomanem que eviteu connectar un USB que us heu trobat al vostre equip per veure què conté o veure si podem retornar-lo al seu legítim propietari.

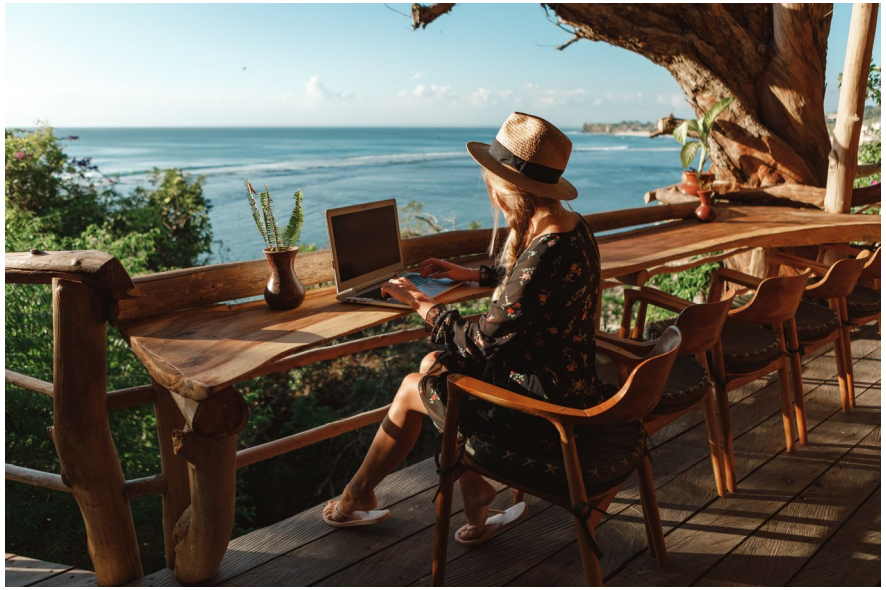
7. Activar l'autenticació de doble factor sempre que sigui possible: Tots els dies es prenen milers de comptes de xarxes socials i correus electrònics perquè la gent no utilitza contrasenyes o les que fa servir són molt febles i/o fàcils d'endevinar. Per evitar aquesta situació, el millor és activar l'autenticació de doble factor en totes les aplicacions. Això significa que cada vegada que algú intenta iniciar sessió en un compte, també necessita saber la clau que rep al seu telèfon mòbil.



Consells per protegir-se al llarg de l'estiu:

8. Compte amb els correus electrònics que rebeu o envieu: Els ciberatacs estan assolint un alt nivell de sofisticació, ja que aconsegueixen obtenir dades que després són venudes al mercat negre o serveixen per robar diners. Per exemple, un tipus d'atac comú és quan atacants envien correus electrònics a una empresa durant l'estiu per veure si els responen amb correus automàtics informant sobre absències en determinats treballadors. Això dona una gran quantitat d'informació als ciberdelinqüents quan preparen un atac per fer-se passar per algú des de dins l'empresa. El millor és no tenir aquesta mena de correus electrònics automatitzats.

9. Pèrdua dels vostres dispositius electrònics: Si durant l'estiu perdeu el vostre dispositiu i sabeu que no vau poder recuperar-lo de cap manera, recomanem que, una bona forma per recuperar la informació emmagatzemada en aquest, sigui realitzar una còpia de seguretat i actualitzar-lo abans de sortir de casa.



Consells per protegir-se al llarg de l'estiu:

10. Eviteu connectar-vos a xarxes WiFi compartides: Hom no sempre és conscient dels riscs que implica compartir una xarxa amb una connexió a Internet. Per això, detallem una sèrie de riscs que us podeu trobar i que convindria que sabéssiu identificar:

- Algú que estigui connectat a una xarxa WiFi pública compartida podria veure la informació què rebeu o envieu a través dels vostres dispositius.
- Algú que estigui connectat a una xarxa WiFi pública compartida podria accedir al vostre dispositiu.
- Algú connectat a aquesta mateixa xarxa podria robar-vos les dades personals i les més delicades.

Moltes vegades és inevitable el fet d'haver de connectar-se a una xarxa de WiFi pública, ja sigui perquè esteu fora de la zona de *roaming* o perquè les dades mòbils són cada vegada més escasses. En aquests casos, heu de ser molt cautelosos amb la informació a la qual accediu. Per exemple, usar una VPN pot ser útil per evitar possibles atacs. No obstant, això no us manté completament protegits.

El que es recomana també és desactivar qualsevol tipus de connexió automàtica dels vostres dispositius per no ser detectats per altres. Sobretot, es recomana desactivar el Bluetooth.

Consells per protegir-se al llarg de l'estiu:

11. Punts a tenir en compte abans de viatjar: Per evitar caure en alguna trampa dels ciberdelinqüents que busquen víctimes entre els futurs viatgers, tothom hauria de prendre consciència d'alguns aspectes relacionats amb la compra de vols, hotels i paquets turístics.

- Virtual skimmers: Els delinqüents aconsegueixen introduir codi maliciós en webs legítimes per prendre les dades de les targetes de crèdit quan els usuaris les utilitzen en aquests llocs de confiança. Per aquest motiu, és important revisar periòdicament els moviments de la targeta de crèdit per detectar compres o retirades de diners no autoritzades i cancel·lar-les.
- Limitar el nombre de dispositius que us emporteu a la platja: Només aquells que siguin necessaris per minimitzar els riscs de perdre informació confidencial emmagatzemada en els mateixos, per si de cas us ho roben o se us extravia.
- Furt d'informació emmagatzemada per empreses que presten serveis de transport i hotels: Això suposa un perill, ja que els usuaris tendeixen a donar el seu correu electrònic que, en cas de produir-se una filtració, els ciberdelinqüents ho poden aprofitar per preparar correus electrònics de *phishing* i prendre als usuaris les seves contrasenyes.
- Eviteu els accessos no desitjats: els telèfons mòbils i els ordinadors contenen una gran informació personal i professional de l'usuari. No es recomana mai introduir informació de tipus personal o professional ni tampoc accedir a cap compte des de dispositius que no siguin de la vostra confiança.