ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

CONSCIENCIACIÓ EN CIBERSEGURETAT

LA CIBERSEGURETAT DURANT LES VACANCES D'ESTIU

Juliol 2024
Document d'ús públic

1. LA CIBERSEGURETAT A L'ESTIU: INTRODUCCIÓ I CONTEXT

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, quan publiquem informació privada de les nostres vacances a les xarxes socials...

Aquestes conductes són molt típiques, **no només durant l'època de l'estiu, sinó també durant tot l'any**. No obstant això, sembla que és a l'estiu quan hi ha més riscos de patir un atac, atès que ens despreocupem més, estem més relaxats i no vigilem tant. Per exemple, el **robatori de la nostra informació personal, la propagació de virus**…

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**, ja sigui durant el teu temps d'oci o en el cas que hagis de teletreballar fora del teu lloc de treball/*home office* i t'hagis de connectar a la xarxa del lloc on passes les vacances.

2. CONSELLS PER PROTEGIR LA TEVA INFORMACIÓ A L'ESTIU MENTRE NAVEGUES

1. Xarxes wifi 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**. Evita fer operacions sensibles, com, per exemple, pagaments en línia o accedir a informació delicada/sensible des d'aquest tipus de connexió.

2. Vigila amb el que publiques 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. A més a més, és recomanable que no et connectis a aquest tipus de xarxes en cas que hagis d'accedir a aplicacions, eines o informació de l'empresa on treballes.

3. Canvia les 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

Quan estiguis de vacances i facis servir els teus dispositius, et recomanem que facis còpies de seguretat cada cert temps i que els actualitzis amb les darreres actualitzacions disponibles. Cada vegada que hi ha una nova **actualització** disponible, tant del sistema operatiu com d'alguna aplicació, salta una notificació; és important executar-la.

La majoria d'aquestes actualitzacions conté **pedaços** o **millores de seguretat** que eviten que siguis més vulnerable als ciberatacs.

5. Vigila amb les aplicacions mòbils que et descarreguis

Encara no s'ha testat la seguretat de les aplicacions mòbils que ens descarreguem i no tenim suficients **garanties** del que ens descarreguem en els nostres dispositius mòbils. Això suposa un **RISC** per a la seguretat de la nostra informació. Et recomanem, per tant, que sempre que et descarreguis aplicacions ho facis de llocs oficials, com **Apple Store** i **Google Play.**

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

Les **infeccions** per **USB** són molt comunes. Cada vegada hi ha més organitzacions que **prohibeixen** als seus treballadors que en facin servir a causa de l'alt risc que infectin l'equip. Per això, et recomanem que no connectis mai un USB que t'hagis trobat al teu equip per mirar què conté o per veure si el pots retornar al seu amo.

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

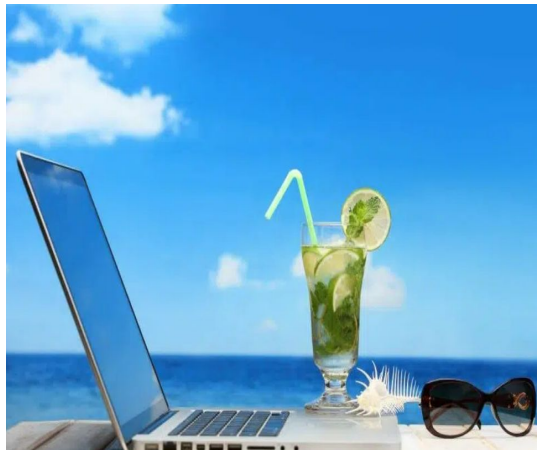
Cada dia es roben milers de comptes de xarxes socials i de correus electrònics perquè la gent no utilitza contrasenyes o les que fa servir són molt dèbils i/o fàcils d'endevinar. Per evitar-ho, el millor és **activar** l'**autenticació de doble factor** en totes les aplicacions. Això significa que cada vegada que algú intenta iniciar sessió en un compte, també necessita saber la clau que rep en el seu telèfon mòbil.

8. Compte amb els correus electrònics que rebem i enviem

Els ciberatacs estan assolint un gran nivell de sofisticació, ja que aconsegueixen obtenir dades que llavors es venen al mercat negre o, directament, roben diners. Per exemple, un tipus d'atac és enviar correus electrònics a una empresa durant l'estiu per treure informació dels correus automàtics sobre absències de determinats treballadors. Això dona una gran quantitat d'informació als ciberdelinqüents a l'hora de preparar un atac fent-se passar per algú de dintre de l'empresa. El millor és no tenir aquests correus electrònics automatitzats.

9. Pèrdua de dispositius electrònics

Et recomanem que abans de sortir de casa **actualitzis** els dispositius i facis **una còpia de seguretat** de les dades; és una bona manera de recuperar la informació que hi tens emmagatzemada, per exemple, si durant l'estiu **perds** un dispositiu electrònic i saps que no el podràs recuperar.



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 sensibles.*

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 d'anar molt amb compte 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 (desactivar, per exemple, el Bluetooth).

Per evitar caure en alguna de les trampes que ens han preparat els ciberdelinqüents que busquen víctimes entre els **futurs viatgers**, existeix una sèrie de **CONSELLS** que tothom hauria de tenir en compte abans de viatjar i que estan relacionats amb la compra de vols, hotels i paquets turístics.

✔ ***Virtual skimmers***: els delinqüents aconsegueixen introduir **codi maliciós** en webs legítims per robar 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.

✔ **Cal limitar el nombre de dispositius que t'emportes a la platja**: emporta't només els que siguin necessaris, per **minimitzar els riscos** de perdre informació confidencial que hi tinguis emmagatzemada en cas que te'ls robin o els perdis.

✔ **Robatori d'informació emmagatzemada per empreses que ofereixen serveis de transport i hotels**: això suposa un **perill**, ja que els usuaris tendeixen a donar la seva adreça electrònica i, en cas que es produeixi una filtració, els ciberdelinqüents poden intentar robar les contrasenyes als usuaris amb la tècnica de la **pesca per correu electrònic (*phishing*)**.

✔ **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 entrar a cap compte des de dispositius que no siguin de la nostra confiança**.**

Avís Legal

Aquest document conté informació pública.

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