ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

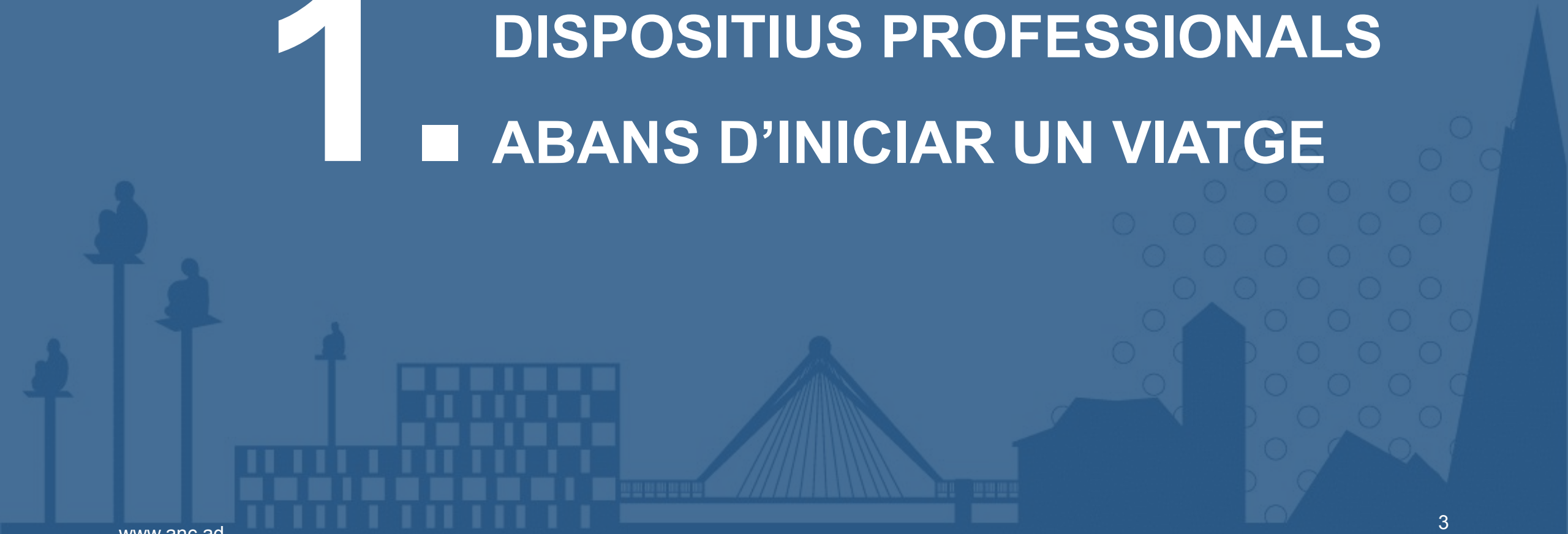
CONSCIENCIACIÓ EN CIBERSEGURETAT

LA SEGURETAT DE LA INFORMACIÓ PROFESSIONAL DURANT ELS VIATGES PROFESSIONALS I/O D'OCI

Maig 2024
Document d'ús públic

1 PREPARA ELS TEUS DISPOSITIUS PROFESSIONALS

ABANS D'INICIAR UN VIATGE



1. Prepara els teus dispositius professionals abans d'iniciar un viatge

Per reduir els riscos en general, a vegades, la millor manera de protegir els teus dispositius i les teves dades és no portar-los amb tu, però com que això no sempre és possible, et recomanem que segueixis les **INSTRUCCIONS** següents, amb l'objectiu de garantir la seguretat de la informació que hi tens emmagatzemada.

- *Emporta't només els dispositius que necessitis.*
- *És recomanable que eliminis totes les dades i els comptes confidencials que tinguis emmagatzemats en aquests dispositius.*
- *Pots fer servir una cartera o un maletí amb bloqueig RFID per desar articles que no requereixin connexió física per transmetre dades personals, com, per exemple, les targetes de crèdit, les claus de les habitacions dels hotels, etc.*

IMPORTANT: si tens algun dubte sobre quins dispositius professionals o quina informació et pots emportar, consulta-ho, si us plau, amb l'**Àrea d'IT o de Seguretat de la Informació** de la teva empresa. D'aquesta manera, tu estaràs més tranquil i ells et podran assessorar millor.

2. Fes còpies de seguretat de les dades emmagatzemades en els teus dispositius

- *Fes sempre una còpia de seguretat de les teves dades abans de sortir de viatge.*
- *Pot passar que et robin el dispositiu durant el viatge, que pateixi algun dany o que el perdis. Fes una còpia de seguretat de la informació que hi tens emmagatzemada.*

CONCLUSIÓ: abans d'eliminar qualsevol dada d'un dispositiu, assegura't que tens guardada una còpia de seguretat segura.

3. Comprova que els dispositius estiguin actualitzats

És recomanable que t'instal·lis les **últimes actualitzacions de seguretat de totes les aplicacions i serveis** que hi ha en els dispositius professionals que t'emportes en un viatge, incloent-hi els telèfons, les tauletes, els ordinadors i qualsevol altre dispositiu intel·ligent.

Per fer-ho, posa't en contacte amb l'**Àrea d'IT o de Seguretat de la Informació** de la teva empresa, en cas que tinguis algun dubte sobre l'actualització dels teus dispositius o d'alguna aplicació en particular.

4. Bloqueja el teu dispositiu professional

Utilitza el mecanisme de bloqueig més segur que estigui disponible en el teu dispositiu i, si el dispositiu disposa d'un **sistema de bloqueig biomètric** (empremta dactilar, escàner de retina, etc.), instal·la'l. Si fas servir una frase de contrasenya o un PIN, ha de ser llarg, complex i difícil d'endevinar.

5. Ves amb compte amb la informació que comparteixes a les xarxes socials

Ves amb compte amb com, quan i amb qui comparteixes informació sobre un viatge a les xarxes socials. Recomanem que consultis la política de l'empresa en relació amb aquesta qüestió, per saber què hi ha estipulat en matèria de viatges de feina i/o oci. Si vols compartir informació sobre un viatge, és més segur que ho facis un cop hagis tornat a casa.

Finalment, assegura't que els teus dispositius no estiguin publicant els llocs que visites durant els teus viatges i que no mostrin la teva ubicació, sense que ho sàpigues.

RECOMANACIÓ: et recomanem que desactivis les funcions de geolocalització o etiquetatge a les teves aplicacions per no compartir accidentalment la teva ubicació.

6. Més risc de rebre correus de pesca durant els viatges

Un correu electrònic dissenyat per enganyar-te amb l'objectiu que revelis informació confidencial, descarreguis arxius adjunts perillosos o facis clic en enllaços maliciosos. Els viatges ofereixen als estafadors una oportunitat per poder-te atacar i treure't les teves credencials.

7. Selecciona els professionals que viatgen com a possibles objectius

L'estafador envia una sèrie de missatges de pesca a aquests professionals que viatgen. Aquests missatges poden incloure, per exemple, un itinerari fals, un advertiment de viatge fals, una factura d'hotel falsa, etc.

8. Suplanta la identitat dels professionals viatgers

L'estafador espera que el professional estigui de viatge i fora de l'oficina per enviar a la seva empresa un correu electrònic de pesca que sembla un missatge autèntic enviat pel treballador.

9. Cal conèixer el país de destinació del viatge

Cada país té normatives diferents en relació amb la privacitat de les dades i amb l'ús dels dispositius. Per exemple, alguns governs insisteixen a cercar i copiar les dades de qualsevol dispositiu que entri o surti del país.

RECOMANACIÓ: abans de sortir de viatge, et recomanem que consultis a l'Àrea de IT o de Seguretat de la Informació de la teva organització les precaucions i les normes específiques del país on tens previst viatjar.

2. ALTRES RECOMANACIONS QUE CAL TENIR EN COMPTE QUAN TREBALLES FORA DE L'OFICINA

RECOMANACIONS

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**. Recorda no fer **OPERACIONS SENSIBLES** com, per exemple, pagaments en línia o accedir a informació delicada/sensible des d'aquest tipus de connexió.

2. Ves amb compte amb el que publiques a les xarxes socials

Si vols publicar informació privada de les teves vacances a les xarxes socials, per exemple, la teva localització actualitzada o els dies que queden per tornar a casa, és millor que ho facis quan arribis a casa. A més a més, és recomanable que no et connectis a aquest tipus de xarxes si has d'accedir a aplicacions, eines o informació de l'empresa on treballes.

3. Canvia les teves contrasenyes quan tornis de les vacances

És convenient que, un cop hagis acabat el teu viatge o estada, **CANVIÏS LES 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 cada cert temps facis còpies de seguretat i actualitzis els dispositius amb les últimes actualitzacions disponibles. Cada vegada que hi ha una **ACTUALITZACIÓ** disponible del sistema operatiu o d'alguna aplicació surt una notificació, és important que l'executis. La majoria d'aquestes actualitzacions contenen **PEDAÇOS** o **MILLORES DE SEGURETAT** que eviten que siguis més vulnerable als atacs cibernètics.

5. Compte amb les aplicacions mòbils que et descarregues

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. Per tant, recomanem que sempre que et descarreguis una aplicació sigui 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 cop hi ha més organitzacions que en **PROHIBEIXEN** l'ús als seus treballadors per l'alt risc d'infecció de l'equip. Per això, et recomanem que no connectis un USB que t'hagis trobat al teu equip per veure què conté o per mirar si el pots tornar al seu legítim amo.

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

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

8. Ves amb compte amb els correus electrònics que reps i envies

Els ciberatacs cada vegada tenen un nivell més alt de sofisticació: aconsegueixen obtenir dades que després 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 mitjà de les respostes dels correus electrònics automàtics s'obté informació sobre l'absència de determinats treballadors. Això aporta una gran quantitat d'informació als ciberdelinqüents quan es prepara un atac per fer-se passar per algú des de dins de l'empresa. El millor és no tenir aquests correus electrònics automatitzats.

9. Pèrdua dels teus dispositius electrònics

Per exemple, si durant l'estiu **PERDS** el teu dispositiu electrònic i saps que no el podràs recuperar de cap manera, una bona manera de recuperar la informació que hi tens desada és si has fet una **CÒPIA DE SEGURETAT** i l'has **ACTUALITZAT** abans de sortir de casa.

10. Evita connectar-te a xarxes wifi compartides

En realitat, no som conscients dels **RISCOS** que implica compartir una xarxa amb connexió a internet. Per això, t'expliquem 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 estigui connectat a aquesta mateixa xarxa et pugui robar dades personals i sensibles.*cibernètics.

Avís Legal

Aquest document conté informació pública.

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