



#AprenemCiberseguretat

PROTECCIÓ DE LA IDENTITAT DIGITAL

Identitat digital

TOTA INFORMACIÓ IDENTIFICATIVA (NOM, DIRECCIÓ, DATA DE NAIXEMENT...) EXPOSADA EN INTERNET. BONA PART D'AQUESTA INFORMACIÓ L'EMMAGATZEMEM I LA TRACTEM A TRAVÉS DE DISPOSITIUS MÒBILS COM EL TELÈFON INTEL·LIGENT, LA TAULETA TÀCTIL, ELS RELLOTGES INTEL·LIGENTS O LES XARXES SOCIALS.

Conseqüències

Robatori d'identitat

Es produeix quan un atacant obté informació personal d'una persona física o jurídica i la utilitza il·legalment, per exemple, per cometre algun frau o delictes.



PÈRDUA ECONÒMICA



SUPLANTACIÓ D'IDENTITAT



CIBERASSETJAMENT

BONES PRÀCTIQUES EN DISPOSITIUS MÒBILS

1

CODI D'ACCÉS ROBUST ASSOCIAT A UNA PANTALLA DE BLOQUEIG

10

REALITZEU CÒPIES DE SEGURETAT PERIÒDIQUES DELS CONTINGUTS DEL DISPOSITIU MÒBIL

2

NO DONEU PERMISOS INNECESSARIS O EXCESSIUS A LES APLICACIONS

3

DESHABILITEU INTERFÍCIES DE COMUNICACIONS SENSE FILS

4

NO CONNECTEU DISPOSITIUS MÒBILS A XARXES WIFI PÚBLIQUES OBERTES.

5

NO CONNECTEU DISPOSITIUS MÒBILS A PORTS USB DESCONEGUTS.

6

MANTENIU ACTUALITZATS SISTEMA OPERATIU I APLICACIONS

9

USEU CAPACITATS NATIVES DE XIFRATGE DEL DISPOSITIU MÒBIL PER PROTEGIR DADES

8

NO INSTAL·LEU CAP APLICACIÓ MÒBIL QUE NO PROVINGA D'UNA FONT DE CONFIANÇA.

7

USEU PROTOCOL HTTPS. NO ACCEPTEU MISSATGES D'ERROR DE CERTIFICAT DIGITAL INVÀLID.



BONES PRÀCTIQUES EN XARXES SOCIALS



1

Protegiu l'accés als perfils en xarxes socials amb **CONTRASENYES ROBUSTES** utilitzant el factor doble d'autenticació on siga viable.

2

LIMITEU LA INFORMACIÓ donada en la creació del perfil en xarxes socials. Empleu un pseudònim.

3

Actualitzeu regularment la **CONFIGURACIÓ DE SEGURETAT** en totes les plataformes per assegurar-se que sempre estiguen establertes en el nivell més estricte.

4

NO COMPARTIU CONTINGUTS SENSIBLES sobre la vida personal pròpia o d'altres en xarxes socials: documents identificatius, números de telèfon, adreces postals, localitzacions exactes, identificadors de vehicles, etc.

5

NO FEU CLIC EN CONTINGUTS L'ORIGEN O EL PROPÒSIT DELS QUALS NO ES TINGUEN CLARS. Augmenteu la cautela davant missatges d'identitats desconegudes.

6

CONTROLEU LA GEOLOCALITZACIÓ de perfils i continguts en xarxes socials. Desactiveu la geolocalització per defecte en el menú de configuració dels perfils.

7

Comproveu la **CONFIGURACIÓ DE LA PRIVACITAT** tant en el perfil com en els continguts que es comparteixen. Davant qualsevol dubte, manteniu accessible la informació privada només per a amigats /contactes.

8

NO DIFONEU INFORMACIÓ PRIVADA d'altres persones **SENSE EL SEU CONSENTIMENT**. No etiqueteu sense sol·licitar prèviament el seu permís.

9

Manteniu **EN PRIVAT LA LLISTA DE CONTACTES**. Analitzar les sol·licituds d'amistat de desconeguts.

WWW.UV.ES/UVSTIC

VNIVERSITAT
DE VALÈNCIA

UVstic

Vicerektorat d'Estratègia, Qualitat i
Tecnologies de la informació
Conscienciació en la seguretat de la informació