HABILITATS PER FER SERVIR LA TECNOLOGIA MÒBIL DE FORMA EFICAÇ, SEGURA I INTEL·LIGENT

apdcat
Autoritat Catalana de Protecció de Dades
apdcat.cat

ÚS i NAVEGACIÓ SEGURA

Falsa sensació de seguretat, a causa del domini que tenim de la tecnologia.

Un dispositiu mòbil ens connecta amb el món, però també comporta **certs riscos** (aplicacions malicioses, virus, programari espia, exposició pública de la nostra informació privada, enganys, estafes...).

GEOPOSICIONAMENT

On ens trobem i els llocs que freqüentem són **informacions que no hem de donar a desconeguts.**

Recomanacions:

-**No informem** de la localització de les fotos i de les nostres publicacions **a les xarxes socials**.

-En aplicacions per "buscar els meus amics", **només** compartim la nostra ubicació **amb persones de molta confiança** (pares, germans, el nostre millor amic...).

DESCÀRREGA D'APLICACIONS

Les aplicacions que ens descarreguem **poden contenir virus** o funcionalitats no desitjades (espiar-nos, enviar missatges amb cost extra, accedir a la nostra informació privada...).

Què hem de fer?

-**Baixar només aplicacions des de llocs fiables** (Appstore o Google Play) que passen un primer filtre de seguretat.

-**Llegir opinions d'altres usuaris**, mirar quantes persones se l'han baixat i quina puntuació rep.

VALIDACIÓ DE PERMISOS

Ens hem d'**assegurar que les aplicacions no accedeixen a parts del dispositiu que no necessiten per funcionar**. Es podria utilitzar per a finalitats no legítimes.

Per tant:

-Abans de descarregar una aplicació, ens hem de **qüestionar si els permisos que ens demana tenen sentit** per a la funció que fa.

-Quan l'aplicació ens demani un permís nou, **només l'hem d'acceptar si pensem que el necessita**.

-**Posteriorment, podem revisar els permisos** que té cada aplicació **i modificar-los**.

DETECCIÓ DE SITUACIONS DE RISC i RECOMANACIONS

-**Si ens contacten persones estranyes** que volen saber informació nostra o afegir-se al nostre cercle d'amistats, desconfiem-ne i **no les acceptem!**

-**Les promocions i campanyes en línia** que prometen vals o participació en concursos i **que ens demanen les nostres dades** per divulgar-les **solen ser enganys** que les exposen i que volen viralitzar-se. **No hi caiguem!**

-**Si ens demanen que cliquem un enllaç o que descarreguem un arxiu, pensem primer si coneixem qui ens l'envia**, si se sol expressar tal com ho fa, si realment l'estàvem esperant o si podria tractar-se d'un esquer per fer que ens descarreguem algun **contingut maliciós**.

-Sempre que accedim als nostres comptes des del dispositiu o l'ordinador d'un amic, **recordem de tancar les sessions per evitar que algú suplanti la nostra identitat o xafardegi les nostres converses**.

QUI TÉ ACCÉS AL QUE ENVIEM O PUBLIQUEM?

El nostre mòbil o tauleta són finestres al món, però també **pissarres al món**. Utilitzem-los tenint sempre això present i **no exposem innecessàriament massa dades personals nostres ni del nostre entorn**.

El que enviem o publiquem a la xarxa s'hi quedarà **per sempre**. En un futur aquesta informació o aquestes imatges **es poden utilitzar en contra nostra**. Algunes imatges poden revelar massa informació privada, es poden acabar distribuint entre persones que no volem que les vegin, es poden utilitzar per assetjar-nos a nosaltres o a una altra persona, poden sortir a la llum quan siguem més grans i busquem feina…

És recomanable **activar les opcions de privacitat dels nostres comptes a les xarxes** socials de manera que els configurem com a comptes **privats** i puguem **controlar i restringir qui hi té accés**.

De tota manera, encara que només publiquem entre la nostra xarxa privada d'amistats, **no sabem quin ús en faran els altres**. I si se'n fan còpia i ho difonen? Tot i així, voldríem publicar aquell contingut?