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

apdcat
Autoritat Catalana de Protecció de Dades
apdcat.cat

PROTECCIÓ DELS DISPOSITIUS

Podem **reforçar la seguretat** del nostre dispositiu configurant-lo de manera adequada.

Per contra, certes pràctiques poden debilitar-la i deixar la **porta oberta a possibles atacs**.

ANTIVIRUS

Què són: Els antivirus **permeten detectar i netejar el nostre dispositiu** de determinats programes que suposen un risc i que ens poden haver infectat pel simple fet de baixar algun arxiu, clicar un enllaç, baixar un adjunt o simplement visitar una pàgina web.

Riscos a què estem exposats: revelar a tercers el contingut de les nostres comunicacions, segrest del dispositiu a partir del seu xifrat (ransomware), bombardeig publicitari o seguiment de la nostra navegació web (adware),...

Opcions: Com que **iOS** funciona en un entorn més tancat, **Apple** no ofereix opcions d'antivirus a la seva Appstore.

A través de **Google Play** ens en podem descarregar per a dispositius **Android**.

El fet de tenir un antivirus instal·lat no ens protegeix de tots els riscos i per tant haurem de **seguir sent curosos** en la utilització del nostre telèfon o tauleta.

Una opció interessant és el programa gratuït **Conan Mobile**, que ofereix una **eina de protecció integral**: ens avisa de configuracions insegures del nostre dispositiu i ens informa dels permisos que sol·liciten les aplicacions que tenim instal·lades.

(!) No hem de fer cas de pantalles emergents o avisos de pàgines web que pretenen espantar-nos i fer-nos creure que el nostre dispositiu està infectat per un virus (scareware). El que realment pretenen és que descarreguem programes maliciosos disfressats d'antivirus o que paguem diners per fer veure que netegen de virus el nostre terminal.

És molt important **mantenir constantment actualitzat el sistema operatiu i les aplicacions que tenim instal·lades** per assegurar-nos que les millores en seguretat que posen al nostre abast els fabricants estan al dia.

WiFi

A diferència de les wifis privades, com la que puguem tenir a casa nostra, les wifis públiques gratuïtes o compartides solen tenir **mesures de seguretat molt baixes o nul·les**.

Correm el **risc que les nostres comunicacions siguin espiades**, modificades o redirigides a pàgines web falses, sovint amb l'objectiu de robar-nos contrasenyes o informació molt privada.

Per tant, mai **no enviarem informació sensible** (noms d'usuari, contrasenyes, dades que no vulguem que ningú sàpiga) **a través d'una wifi pública. Esperarem a poder-nos connectar a una xarxa segura** o utilitzarem les dades mòbils (3G/4G).

ACCÉS AL DISPOSITIU

Resulta de gran importància **protegir l'accés al nostre dispositiu amb un codi**, un patró o definir la nostra empremta digital.

Cal **activar el bloqueig del dispositiu** per a l'encesa i per després de cert període d'inactivitat.

Android ofereix també la possibilitat d'establir un codi d'accés per a les aplicacions per **evitar que algú** que utilitza el nostre telèfon **pugui xafardejar** en excés.

SELECCIÓ I EMMAGATZEMATGE DE CONTRASENYES DELS NOSTRES COMPTES (CORREU, XARXES SOCIALS)

Cal utilitzar **contrasenyes robustes i diferents** per a cada compte. Així, si les credencials (usuari i contrasenya) d'un compte són descobertes, no comprometem altres serveis nostres.

No hem de compartir ni difondre les nostres contrasenyes i cal **guardar-les en llocs segurs**.

En relació amb la contrasenya del nostre correu electrònic, és important configurar com a sistema de recuperació en cas d'oblit el correu/telèfon dels pares o de germans més grans.

XIFRAT DEL DISPOSITIU

Quan xifrem un dispositiu el que estem fent és convertir tota la seva informació en un format que **no pot ser llegit** de cap manera **per qui no tingui la clau** per desxifrar-lo.

Els dispositius **Apple** ja estan **xifrats per defecte** a partir de la versió d'iOS 8 sempre que activem el **bloqueig per codi**.

En **Android** els terminals també venen **xifrats per defecte** a partir del sistema Marshmallow.

Cal que pensem a **xifrar també la targeta SD externa**.
Si no, algú podria evitar fàcilment la protecció per contrasenya del dispositiu **inserint-la a un altre telèfon o directament a un ordinador!**

RISCOS DEL ROOTEIG O JAILBREAK DEL DISPOSITIU

Dur a terme un rooteig o jailbreak del dispositiu suposa d'alguna manera **"piratejar-lo" amb la finalitat d'alliberar-lo d'una determinada operadora telefònica**, poder instal·lar-nos determinats jocs gratuïtament i, en el cas dels entorns iOS, poder tenir aplicacions de fora de l'Appstore.

Els nostres **telèfons i tauletes porten una configuració de seguretat** per defecte que evita que ens baixem aplicacions de fonts no fiables. **A través del rooteig o jailbreak estem deshabilitant aquesta configuració**.

A banda que podem perdre la garantia, també ens **podem instal·lar aplicacions que no han passat un control previ i que, per tant, poden contenir virus** o programari espia, poden deixar portes obertes per accedir a les nostres credencials, enganyar-nos fent-nos creure que desactivem un permís quan en realitat l'estan activant...