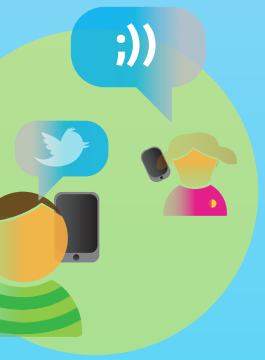


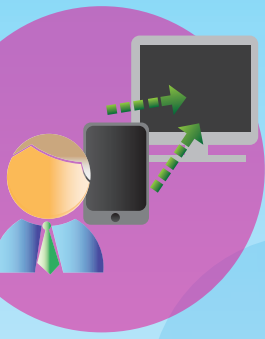
Perquè no hi hagi fuites involuntàries d'informació:

Conèixer les opcions relatives a la privacitat del nostre dispositiu i configurar-lo segons les nostres preferències, a banda de mantenir les precaucions pròpies per a l'ús segur d'Internet i xarxes socials. Conèixer les possibilitats de configuració del nostre dispositiu i desactivar aquells permisos que no són necessaris.

Perquè les teves dades no circulin per la xarxa sense el teu permís:

Ser conscients d'on estan emmagatzemades les dades, amb quines restriccions d'accés i nivell de protecció, i com es transmeten a través de la xarxa.

En el cas de la informació personal a la qual permetem que altres accedeixin, hem d'intentar controlar qui la té i per a què pot utilitzar-la, així com conèixer els nostres drets d'accés, modificació, cancel·lació i com podem exercir-los.



Per no perdre la informació que hi tens emmagatzemada:

Fer còpies de seguretat periòdiques i relativament freqüents, i emmagatzemar-les en un lloc segur.

Realitzar un esborrat complet de la informació que conté el nostre terminal quan el canviem, el cedim o el venem mitjançant la funcionalitat de "restauració a la configuració de fàbrica".

Per si, malgrat tot, te'l roben o el perds:

Demanar a l'operadora el bloqueig de totes les trucades de sortida i el bloqueig del terminal, o bé, si ho teníem configurat així, realitzar un bloqueig remot i esborrat remot de dades.

Igualment, és convenient canviar les contrasenyes que poden estar emmagatzemades al dispositiu.

Podeu consultar altres guies com aquesta a
www.internetsegura.cat
Seguiu-nos a

Guia ràpida per a un ús segur del mòbil

internet + segura

Cada cop és més habitual el robatori o la pèrdua de dispositius mòbils, i també la filtració o fuita de la informació que hi tenim emmagatzemada, però hem de saber que es poden prendre mesures per, si més no, mitigar l'impacte d'aquesta possible pèrdua, fuita o robatori. Abans de res, però, **cal fer una reflexió sobre per a què utilitzem el nostre mòbil, quines prestacions té, quina informació hi emmagatzemem i què ens suposaria, tant personalment com professional, la seva pèrdua o robatori, o la filtració de la informació que hi tenim emmagatzemada.** Cal tenir present a més, que els mòbils més utilitzats actualment, del tipus smartphones, tenen pràcticament les mateixes prestacions i, per tant, els mateixos riscos de seguretat, que els ordinadors portàtils o de sobretaula. És en funció d'aquestes reflexions que caldrà aplicar un nivell més o menys alt de seguretat, però en tot cas, aquestes són algunes de les recomanacions bàsiques per a un ús segur del nostre mòbil:

Perquè no accedeixin a les teves dades personals:

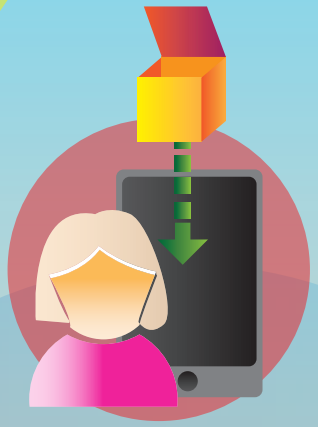
Sospitar de les trucades i SMS des de números desconeguts i ocults i no donar dades personals fins a tenir la certesa que és un tràmit legítim.

Desconfiar de trucades i SMS de números desconeguts o de difícil verificació, encara que tinguin una aparença d'autenticitat. Aplicar el sentit comú i no proporcionar cap tipus de dades si no estem realment segurs de qui hi ha altre costat de la línia o qui és l'emissor de l'SMS.

Perquè no te'l prenguin:

Protegir l'accés físic al dispositiu tenint-lo en tot moment controlat, com qualsevol altre objecte de valor.

No donar a conèixer a tothom el tipus de mòbil que tenim ni fer-ne ostentació, sobretot si es tracta d'un terminal de gamma alta. Utilitzar el mode vibrador en l'avís de trucada (sempre que sigui possible), i ser discrets quan efectuem o contestem una trucada.



Per evitar que s'infecti:

No instal·lar cap aplicació al nostre mòbil que no coneguem o de la qual no tinguem referències sòlides.

Utilitzar sempre que sigui possible les aplicacions proporcionades pel proveïdor oficial i instal·lar preferiblement software original. Llegir els permisos que demanen les aplicacions que instal·lem per evitar que puguin accedir a informació i utilitzar-la de manera que no sigui la desitjada. Finalment, les solucions de seguretat per a mòbils inclouen una protecció equivalent als antivirus dels ordinadors i pot ser molt eficaç per evitar usos fraudulents.
Abans d'instal·lar-ne cap, però, cal validar que la font de l'aplicació és de confiança, perquè existeixen una sèrie de falsos antivirus que s'utilitzen per robar dades o realitzar fraus.

Perquè només tu puguis activar-lo:

Protegir el desbloqueig del terminal, demanant la introducció d'un PIN, contrasenya o patró gràfic per poder interactuar amb el terminal quan aquest es trobi bloquejat.

Activar el bloqueig automàtic del dispositiu després d'un cert temps d'inactivitat i mantenir sempre actiu el bloqueig de la targeta SIM d'accés a la xarxa mòbil, de manera que s'hagi d'introduir el PIN cada vegada que s'encén el telèfon. Canviar les contrasenyes per defecte en les aplicacions que les incloguin per una contrasenya segura. No introduir números PIN ni contrasenyes a la vista de tothom.

Per navegar segur amb el mòbil:

Evitar sempre que sigui possible connexions amb xarxes WiFi desconegudes o controlades per tercers, de les quals en desconeixem el propietari.

En cas de connectar-se a xarxes no segures o desconegudes, no activar l'opció de "desar connexió" o "connexió automàtica". Sobretot quan ens connectem a llocs sensibles com ara bancs en línia, procurar realitzar l'accés des de xarxes fiables, assegurar-nos que la connexió és segura (xifrada amb SSL) i tancar sessió explícitament en el lloc web.

internet +segura