

Guia ràpida per a un ús segur de les xarxes socials corporatives en dispositius mòbils



Generalitat
de Catalunya



El contingut d'aquesta guia és titularitat de la Fundació Centre de Seguretat de la Informació de Catalunya i resta subjecte a la llicència de Creative Commons BY-NC-ND. L'autoria de l'obra es reconeixerà a través de la inclusió de la menció següent:

Generalitat de Catalunya

Autoria: Centre de Seguretat de la Informació de Catalunya

Obra titularitat de la Fundació Centre de Seguretat de la Informació de Catalunya.

Llicenciada sota la llicència CC BY-NC-ND.

Aquesta guia es publica sense cap garantia específica sobre el contingut.





Aquesta llicència té les particularitats següents:


Vostè és lliure de:

 Copiar, distribuir i comunicar públicament l'obra.

Sota les condicions següents:

 **Reconeixement:** S'ha de reconèixer l'autoria de l'obra de la manera especificada per l'autor o el llicenciador (en tot cas, no de manera que suggereixi que gaudeix del suport o que dona suport a la seva obra).

 **No comercial:** No es pot emprar aquesta obra per a finalitats comercials o promocionals.

 **Sense obres derivades:** No es pot alterar, transformar o generar una obra derivada a partir d'aquesta obra.

Avís: En reutilitzar o distribuir l'obra, cal que s'esmentin clarament els termes de la llicència d'aquesta obra. El text complet de la llicència es pot consultar a <https://creativecommons.org/licenses/by-nc-nd/4.0/deed.ca>

Aquesta guia ràpida s'ha redactat amb l'objectiu d'informar als treballadors públics encarregats de gestionar comptes corporatius de xarxes socials de les principals recomanacions per garantir la seguretat en l'accés i en la gestió dels seus continguts.

1. Pineja'l

El dispositiu ha d'estar protegit amb un PIN a l'hora de connectar-se a la xarxa. Per desbloquejar-lo després d'un temps d'inactivitat, hauràs d'introduir una **contrasenya**, **PIN** o **patró gràfic** que el retorni a l'activitat normal. Recorda també de canviar les contrasenyes de les aplicacions per defecte amb **contrasenyes segures**. Si utilitzes un ordinador o portàtil per fer aquesta funció, assegura't que el dispositiu queda blocat després d'un temps d'inactivitat i que cal una credencial per iniciar la sessió.

Consell:

No introdueixis ni números PIN ni contrasenyes a la vista de tothom.



2. Vacuna'l

Consell:

Si tens dubtes sobre quines solucions de seguretat són més recomanables per al teu dispositiu, informa't sobre les més adequades. Per exemple, ves amb compte amb els falsos antivirus que s'utilitzen per robar dades o realitzar frauds. Algunes aplicacions fraudulentas (*keylogger*) s'ha demostrat que poden enregistrar l'entrada de contrasenyes des del teclat.

No instal·lis cap aplicació de la qual no en tinguis referències sòlides, i sempre que sigui possible proporcionades pel proveïdor oficial. Compte amb els permisos requerits per algunes aplicacions: poden accedir a la nostra informació i utilitzar-la de manera no adequada. Si fas servir un dispositiu fix, posa't en contacte amb els responsables TIC per actualitzar les darreres versions de navegador.



3. Connecta't amb seguretat

Evita les connexions a xarxes wi-fi desconegudes o controlades per tercers, de les quals moltes vegades en desconeixem el propietari.

Consell:

Si malgrat tot has d'utilitzar una d'aquestes xarxes, assegura't de no activar l'opció 'desar connexió' o 'connexió automàtica'.

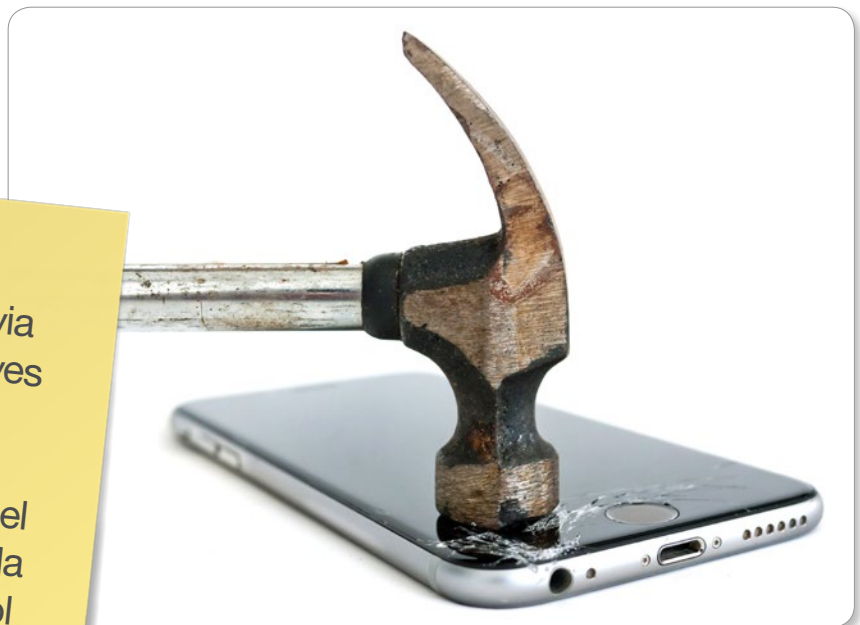


4. Actua en remot

Si el dispositiu s'espatlla, el perds o te'l roben, fes de seguida un bloqueig remot i un esborrat remot de dades. I, sobretot, comunica la incidència al teu coordinador al més aviat possible.

Consell:

Per precaució, canvia totes les contrasenyes emmagatzemades i tingues sempre una còpia de seguretat del dispositiu per poder-la restaurar en qualsevol moment.



1. Travessa dues portes




La funció de gestió d'equips a TweetDeck permet que diferents usuaris hi accedeixin amb el seu propi compte de Twitter. És convenient que habilitis la verificació d'inici de sessió (*login verification*) del teu compte per ajudar a mantenir segurs tots els comptes compartits (el teu personal i tots els que gestonis des de TweetDeck). És necessari que introdueixis un codi de sis dígitos quan vulguis accedir al compte.

Seguretat

Verificació d'entrada Comprova les sol·licituds d'entrada
Un cop entris, el Twitter t'enviarà un missatge SMS amb un codi que necessitaràs per accedir al teu compte.

Verificació del restabliment de la contrasenya Demana informació personal per restablir la contrasenya
Per a més seguretat, quan restableixis la contrasenya se't demanarà que confirmis l'adreça electrònica o el número de telèfon.

Com funciona la verificació d'entrada

-  Hauràs de proporcionar un codi quan iniciis sessió.
-  Se t'enviarà el codi d'entrada per SMS.
-  Quan entris el codi d'entrada, sabem que de veritat ets tu.

Inicia

2. No estiguis a més d'un lloc alhora

Si comparteixes l'accés des de diversos dispositius o són compartits, assegura't que, després de cada ús, tanques la sessió i no queden dades emmagatzemades. També pots esborrar l'historial del navegador (CTRL+H) amb les contrasenyes desades, la memòria cau, etc. És interessant fer servir la navegació privada amb els navegadors per tal de no deixar rastre de les pàgines visitades. Així evites que algú pugui accedir accidentalment al teu compte.

Consell:

Tingues el mòbil sempre a mà i no el deixis desbloquejat.



3. No obris als desconeguts

A Twitter, cal ser molt curós amb les formes escurçades <http://t.co> dels missatges directes, ja que poden camuflar algun contingut nociu.

Si reps un enllaç des de l'escurçador bit.ly, pots comprovar-ne la seguretat afegint el símbol + al final de la seqüència.

Per exemple: bit.ly/heidud+

Consell:
Estigues alerta amb els missatges d'advertència de Twitter.



4. Vigila qui i què autoritzes

Hi ha unes quantes app desenvolupades per Twitter (Periscope, Klout...) a les quals ens connectem amb les credencials d'aquesta xarxa. Poden ser molt útils, però també poden comprometre la seguretat dels comptes que gestionem.

Consell:

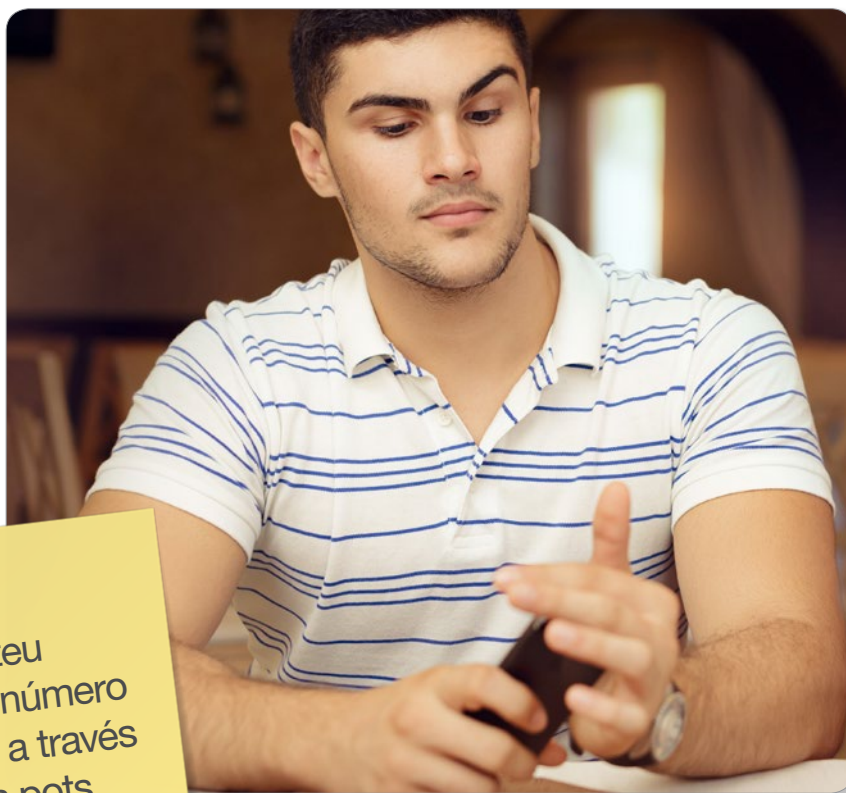
Revisa els termes de l'aplicació i els permisos que atorgues a cada una.

A més permissivitat, més intrusió. Si detectes algun problema, reinicialitza amb freqüència.



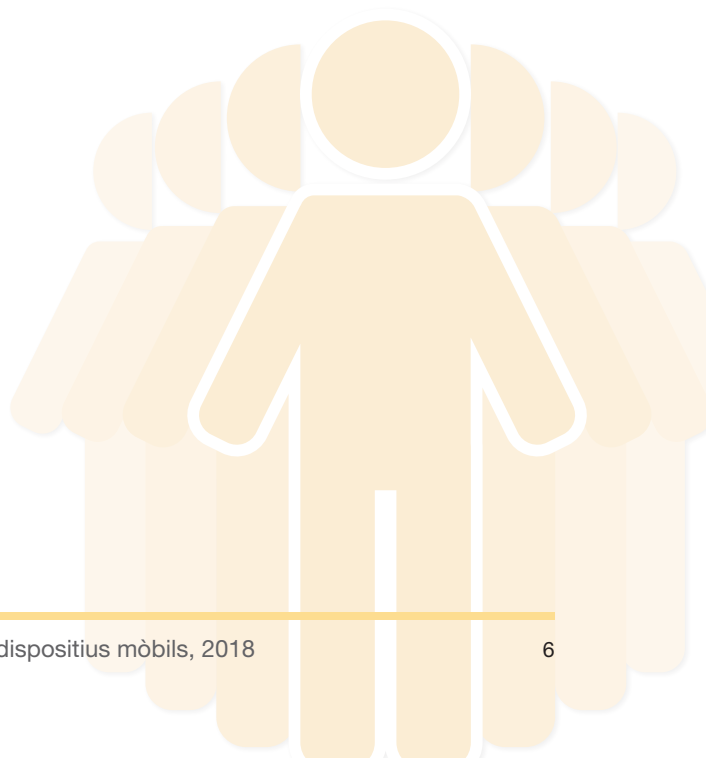
5. Parla amb el teu dispositiu

És important saber quines són les possibilitats de configuració dels nostres dispositius mòbils i destriar les funcions necessàries de les innecessàries (per exemple, la geolocalització).



Consell:

No comparteixis el teu compte de correu i número de mòbil personals a través de Twitter. Si ho fas pots revelar la identitat del gestor del compte corporatiu.



1. Travessa dues portes

Empra un mètode d'autenticació de doble factor dels que hi ha disponibles:

Consell:

Investiga totes les possibilitats de seguretat que t'ofereix Facebook mateix.

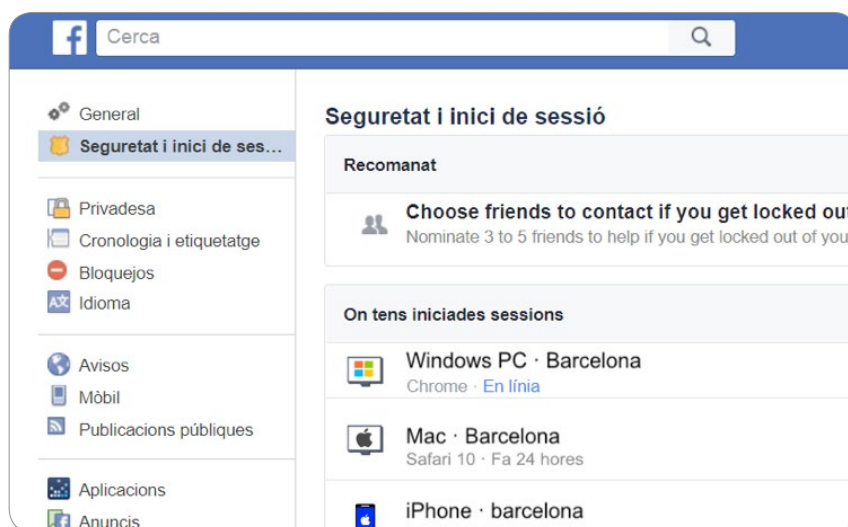


2. No estiguis a més d'un lloc alhora!

Si comparteixes l'accés des de diversos dispositius, assegura't que, després de cada ús, tanques la sessió i no queden dades emmagatzemades.

Consell:

Pots controlar les últimes sessions obertes a l'apartat Configuració/Seguretat i Inici de sessió/On tens iniciades sessions.



També pots desconnectar les sessions que ja no gestiones a la pàgina de Facebook. I pots configurar Alertes (*Get alerts about unrecognized logins*) sobre entrades no acreditades en altres navegadors o dispositius al correu electrònic o al mòbil.

3. Vigila qui i què autoritzes

Hi ha unes quantes app (Thunderclap, Instagram, Klout, Polldaddy Polls, Doodle.com, Pinterest...) i jocs desenvolupats per Facebook (<https://www.facebook.com/settings?tab=applications>) als quals ens connectem amb les credencials d'aquestes xarxes. Poden ser molt útils, però també poden comprometre la seguretat dels nostres comptes.

Consell:

Revisa la configuració de l'aplicació i si atorgues permisos de publicació automàtica a cada una d'aquestes (a l'apartat *This app can*). A més permissivitat, més intrusió. Si detectes algun problema, limita'n l'ús.



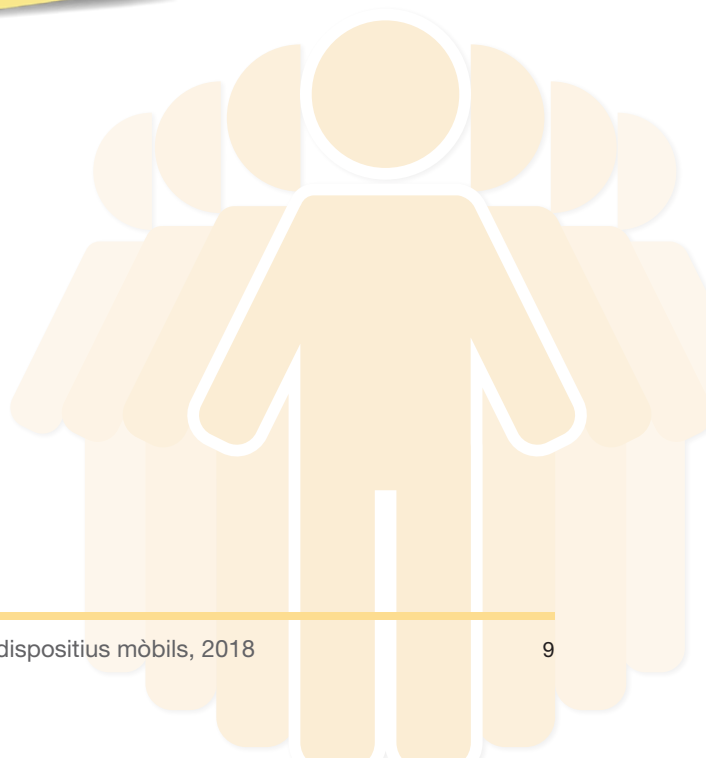
4. Parla amb el teu dispositiu

Les app de la família de Facebook (WhatsApp, Instagram, Facebook Messenger) fan servir les galetes emmagatzemades en el dispositiu (per exemple, la localització), fotografies o contactes. I això segmenta els anuncis en funció del teu comportament o interessos.



Consell:

Revisa quines són les empreses que deixen galetes en els teus dispositius i valora les que creus que no et convenen. Un recurs molt interessant és: <http://www.youronlinechoices.com/es/>.



□ Fes dissabte

Quan canvies el terminal, quan el cedeixes o, fins i tot, quan el vens, has d'assegurar-te d'esborrar completament tota la informació associada a aquest aparell. L'operació és molt senzilla. Simplement has de cercar de restaurar la configuració de fàbrica i tornaràs l'aparell a la configuració que tenia quan el vas treure de la caixa original.

Per a Android:

Ajustos > Sistema > Restablir ajustos > Restablir dades de fàbrica.

Per a iPhone:

Ajustos > General > Restablir > Esborrar continguts i ajustos

□ Pregunta't si les teves dades poden estar més segures

Investiga si entre les opcions de configuració del teu dispositiu hi ha el xifratge de les dades que emmagatzema. Assessorat al web oficial de com pots fer-ho: segur que te'n surts!

□ Mira sempre les ombres

Si detectes qualsevol incident o mal funcionament que creus que pot comprometre la seguretat, i que no hem tractat en aquesta guia, adreçat a xarxes@gencat.cat



Generalitat de Catalunya