

**I tu? protegeixes la teva
informació al mòbil?**



Anem a fer un diagnòstic de la configuració de privacitat del teu mòbil.



Estigues atent a les següents 13 preguntes i ves anotant un punt per cada resposta afirmativa.





1. Per entrar al teu mòbil
necessites contrasenya,
empremta, patró,...?



2. El teu mòbil es bloqueja
automàticament quan no el fas
servir?



3. Els teus missatges queden
ocults quan la pantalla està
bloquejada?

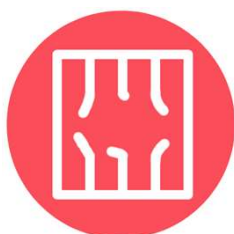


4. Tens limitat l'accés a totes les funcions quan està bloquejat?

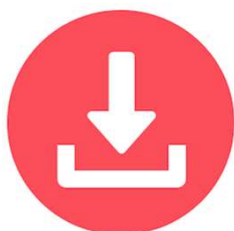
(accés a Siri, a l'agenda, respondre missatges o trucades perdudes)



5. Tens el mòbil sempre
actualitzat?
(sistema operatiu i aplicacions)



6. Ets conscient del perill de
piratejar el teu mòbil?
(realitzar un “jailbreak” o “rooteig”)



7. Descarregues les apps sempre
des dels mercats oficials?
(App Store o Google Play)



8. Abans de descarregar una app, mires els comentaris d'altres usuaris?



9. Verifiqueu que els permisos
que les apps et sol·liciten són
necessaris pel seu ús?

(accés a contactes, localització, micro,...)



10. Evites enviar informació sensible
a través de xarxes WiFi públiques?
(les de centres comercials, hotels, cafeteries,...)

Informació sensible (contrasenyes,...)



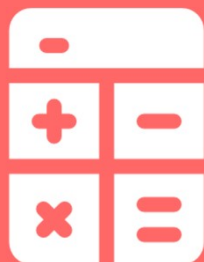
11. Fas regularment còpies de seguretat del teu mòbil?



12. Tens anotat el número
IMEI del teu mòbil?



13. En cas de pèrdua o robatori,
sabries localitzar remotament el
teu mòbil?



Suma els punts obtinguts

Resultat:



0-7
punts



8-10
punts



11-13
punts



Anem a veure com millorar la configuració del teu mòbil per protegir la teva privacitat.

1. Bloqueig d'accés al mòbil



Amb el mòbil desbloquejat qualsevol persona podria:

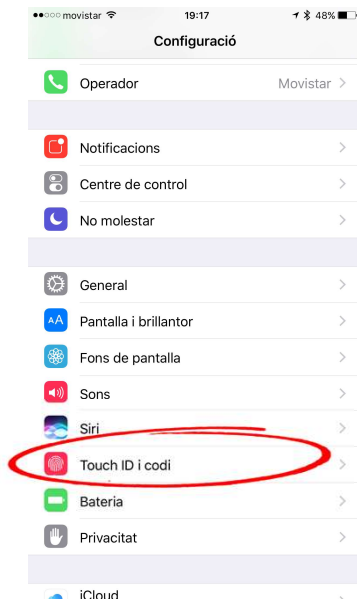
- Accedir a la teva informació.
- Fer-se passar per tu i publicar en nom teu.

1. Bloqueig d'accés al mòbil



És molt important tenir configurat algun sistema que limiti l'accés al teu mòbil (una contrasenya, un patró, la nostra empremta,...)

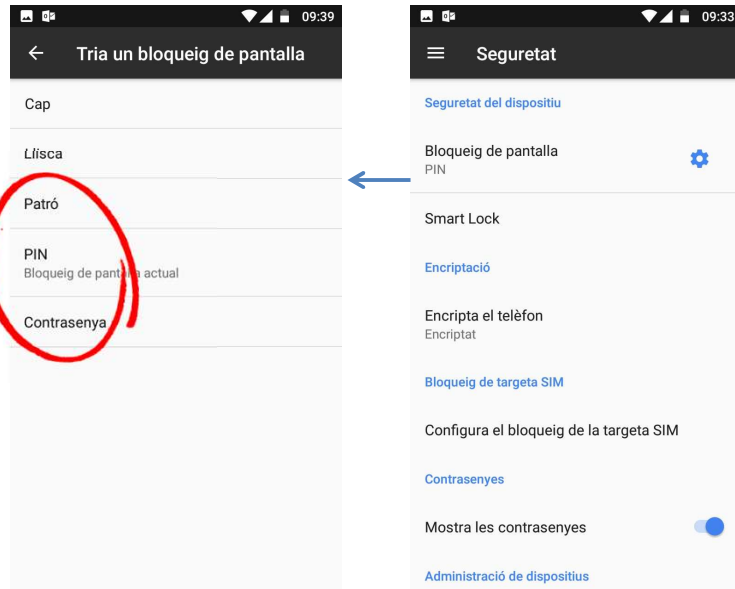
1. Bloqueig d'accés al mòbil



Configuració / Touch ID i codi

En el cas que NO tinguéssim cap codi activat, ens donaria l'opció a activar-lo

1. Bloqueig d'accés al mòbil



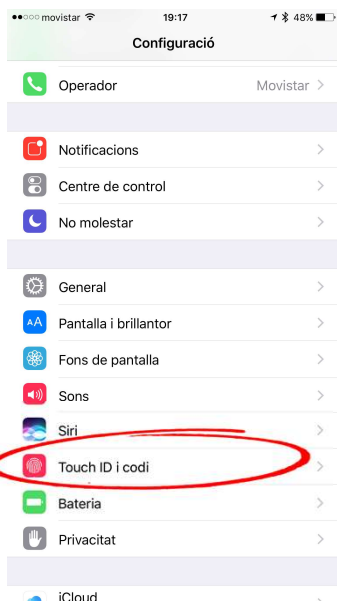
Configuració / Seguretat / Bloqueig de pantalla -> Establir tipus de bloqueig

2. Bloqueig automàtic



Si actives l'opció de bloqueig automàtic del teu mòbil, evites l'accés d'altres persones al seu contingut.

2. Bloqueig automàtic



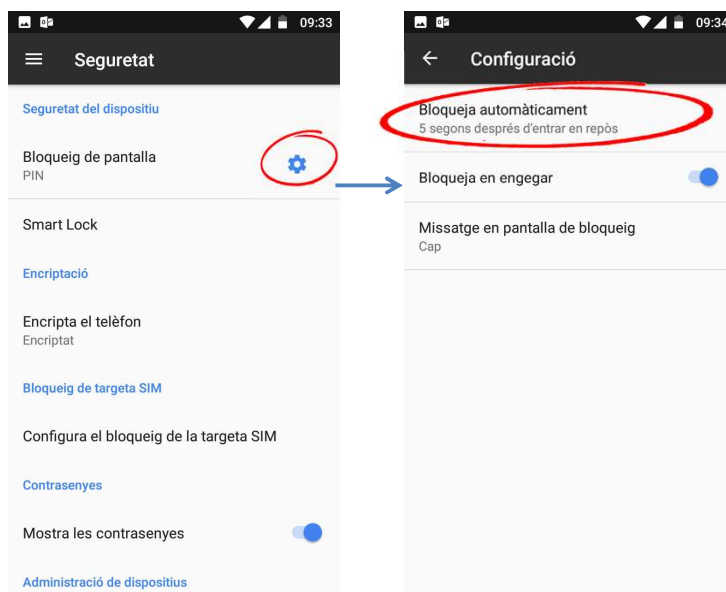
apdcat
Autoritat Catalana de Protecció de Dades



Configuració / Touch ID i codi

Il·liscar avall i ens apareix “Codi obligatori” – immediatament (per activar el bloqueig automàtic)

2. Bloqueig automàtic



Configuració / Seguretat / Bloqueig de pantalla (rodeta) -> Establir bloqueig automàtic

3. Restricció de notificacions en pantalla



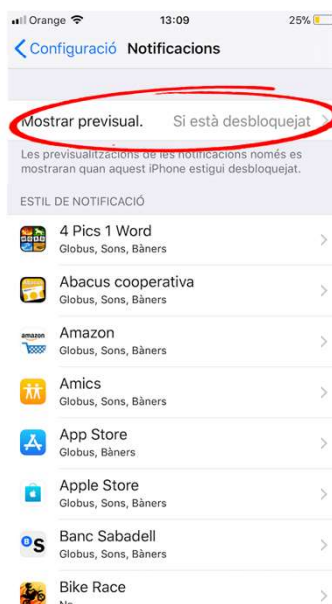
Per defecte, els missatges que rebem al mòbil poden llegir-se sense necessitat d'haver de desbloquejar la pantalla.

3. Restricció de notificacions en pantalla



Anem a veure com podem restringir les notificacions de missatges.

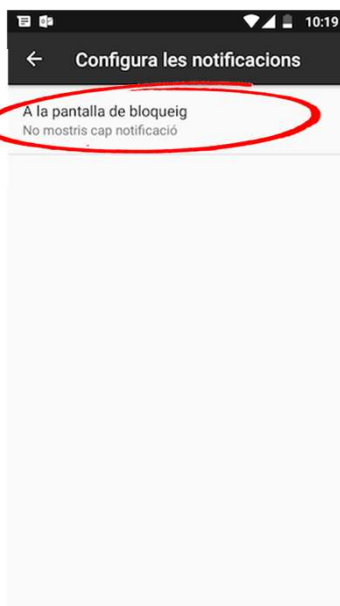
3. Restricció de notifikacions en pantalla



Sempre	
Si està desbloquejat	☒
mai	

Configuració / Notifikacions / Mostrar previsual. "Si està desbloquejat"

3. Restricció de notificacions en pantalla



No mostris cap notificació
Mostra tot el contingut de les notificacions
Amaga el contingut sensible de les notificacions..

Activar “No mostris cap notificació” o bé “Amaga el contingut sensible de les notificacions” de manera que el contingut del text notificat no es previsualitzi.

4. Limitació funcions amb pantalla bloquejada



Certs mòbils permeten l'accés a algunes funcions quan la pantalla està bloquejada.

4. Limitació funcions amb pantalla bloquejada



Anem a veure perquè no convé deixar
gaire portes obertes...

4. Limitació funcions amb pantalla bloquejada



En algunes ocasions Siri ha demostrat ser un mètode que permet saltar-se el bloqueig de pantalla o donar accés a informació sensible (on vivim, contactes, darreres trucades,...).



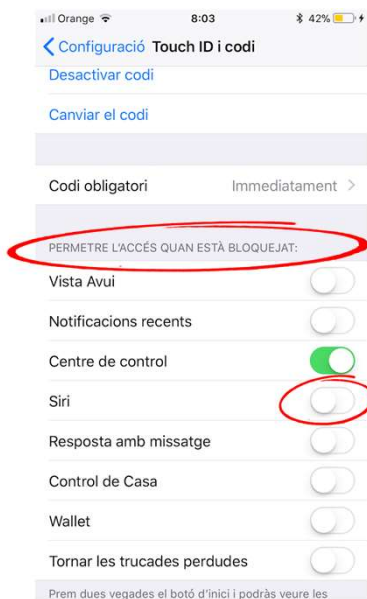
ATENCIÓ HI HA UN VÍDEO (està configurat per reproduir-se automàticament en passar el ratolí per sobre)

Si li diem a Siri que ens porti a casa, per exemple, s'activarà la navegació i ens indicarà sobre un plànol on es troba la nostra casa.

Si li demanem que truqui a algú dins la nostra agenda de contactes també ho farà.

És preferible forçar Siri sempre a demanar el desbloqueig del dispositiu.

4. Limitació funcions amb pantalla bloquejada



Convé limitar al màxim l'accés a funcionalitats del nostre telèfon quan tenim la pantalla bloquejada.

Configuració / touch ID i codi / anar desactivant opcions, en especial Siri, agenda,...

5. Actualitzacions de programari



Actualitzar el sistema operatiu i les apps garanteix que el nostre mòbil té instal·lades les versions més segures.

5. Actualitzacions de programari

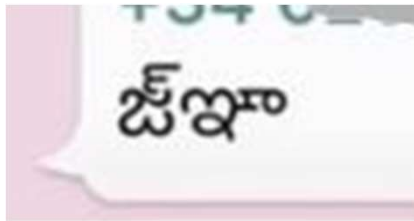


Convé instal·lar-les tan aviat com estiguin disponibles. Per això és bo activar la descàrrega automàtica de les actualitzacions.

5. Actualitzacions de programari



En versions antigues d'iOS, si rebies aquests caràcters hindús al teu mòbil, el mòbil quedava inutilitzable.



apdcat
Autoritat Catalana de Protecció de Dades

Fa uns mesos, si rebies aquests caràcters hindús en algun xat, els mòbils iOS quedaven inutilitzables (apareixia de manera contínua la poma a la pantalla). Només els mòbils actualitzats solucionaven aquesta errada de programació i eren “immunes” a aquest problema.

En altres ocasions, els errors de programació impliquen problemes de seguretat. Per tant, només si tenim l'última versió del sistema operatiu i de les aplicacions estarem protegits al màxim front als darrers errors detectats.

5. Actualitzacions de programari



Ens indica que tenim una actualització disponible



Quan tinguem una actualització disponible ens apareixerà una notificació a la icona de configuració.

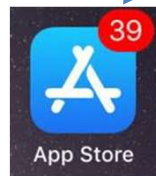
Seguim la ruta Configuració / General / Actualització de programari.

Premem "Descarregar i instal·lar".

5. Actualitzacions de programari



Ens indica que tenim actualitzacions pendents



Quan tinguem actualitzacions d'aplicacions pendents ens apareixerà una notificació a la icona de l'App Store.

Accedirem a l'App Store i a l'apartat d'actualitzacions seleccionem "Actualitzar-ho tot".

5. Actualitzacions de programari

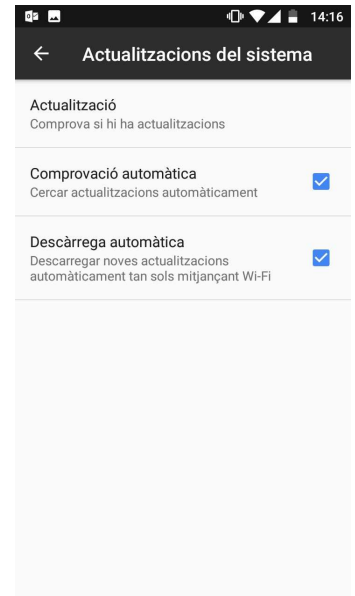
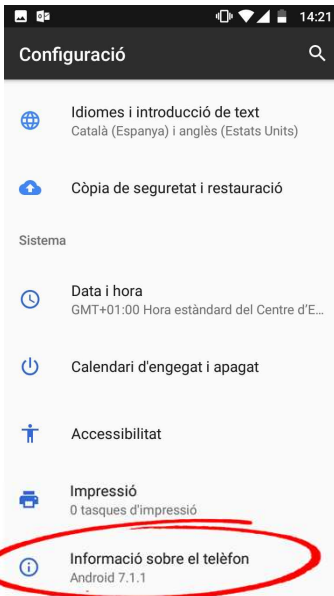


És preferible que les actualitzacions es descarreguin de manera automàtica i així evitem haver d'estar-hi pendents.



És preferible que les actualitzacions es descarreguin de manera automàtica i així evitem haver d'estar-ne pendents.
Seguirem la ruta Configuració / iTunes Store i App Store.
Activarem la descàrrega automàtica de les actualitzacions.

5. Actualitzacions de programari

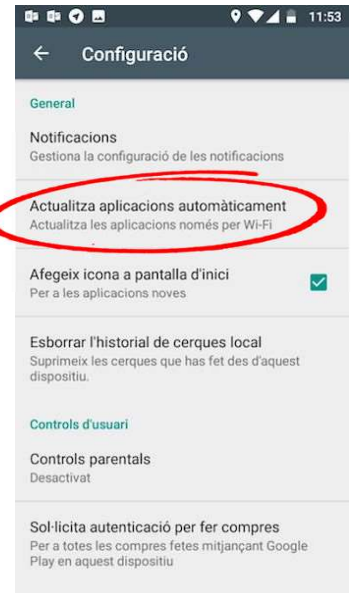
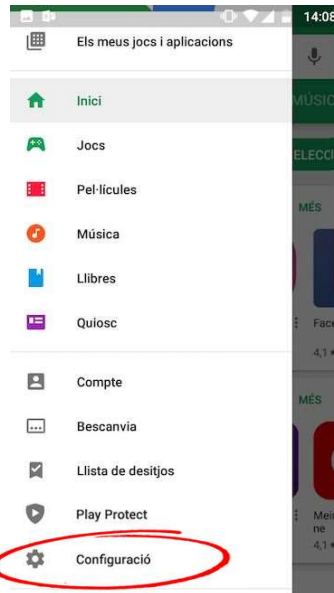
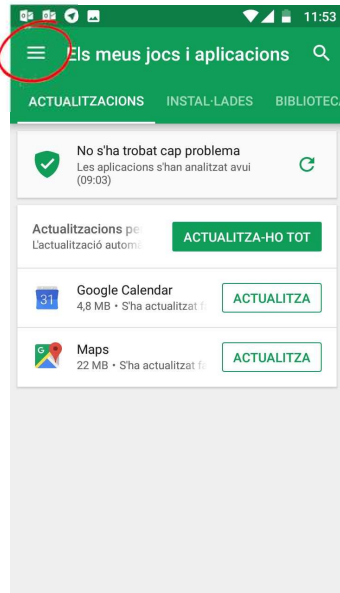
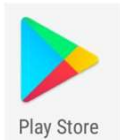


Des de la configuració del telèfon seguint la ruta:

Informació sobre el telèfon / Actualitzacions del sistema

- Podrem comprovar si tenim actualitzacions pendents
- Podrem activar la 'comprovació i descàrrega automàtica'

5. Actualitzacions de programari

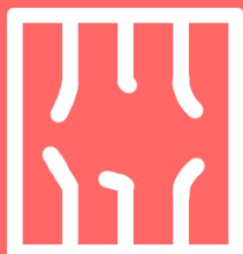


És preferible que les actualitzacions es descarreguin de manera automàtica i així evitem haver d'estar-hi pendents.

Des de la Play Store veurem quines actualitzacions tenim pendents.

- Podrem demanar que s'actualitzin en aquell mateix moment.
- Podrem definir que s'actualitzin de manera automàtica (recomanat)

6. Jailbreak del mòbil



Dur a terme el “jailbreak” o “rooteig” del nostre mòbil suposa piratejar-lo, alliberant-lo del sistema operatiu original.

La majoria de nosaltres estem satisfets amb el nostre telèfon tal com ens ve donat. Hi ha però persones que volen alliberar-se de les restriccions que els fabricants ens imposen i poder “tunejar” lliurement el mòbil, eliminar aplicacions preinstal·lades, descarregar aplicacions de fora de l’App Store en el cas dels iPhones, etc... Com es fa el jailbreak o rooteig d’un mòbil? doncs canviant el software que controla el telèfon o tauleta

6. Jailbreak del mòbil



Aquesta pràctica implica abandonar el model de seguretat del mòbil i comporta riscos.

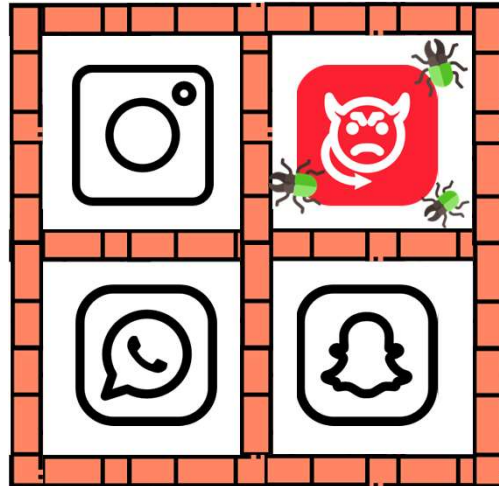
La majoria de nosaltres estem satisfets amb el nostre telèfon tal com ens ve donat. Hi ha però persones que volen alliberar-se de les restriccions que els fabricants ens imposen i poder “tunejar” lliurement el mòbil, eliminar aplicacions preinstal·lades, descarregar aplicacions de fora de l’App Store en el cas dels iPhones, etc... Com es fa el jailbreak o rooteig d’un dispositiu? doncs canviant el software que controla el telèfon o tauleta

6. Jailbreak del mòbil



El **model de seguretat** dels nostres mòbils es basa en l'aïllament de les aplicacions entre elles.

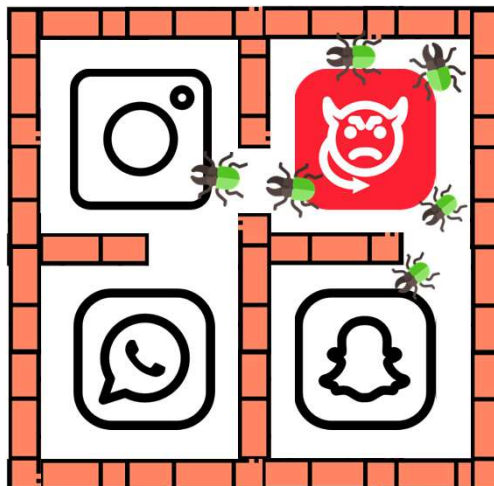
Una aplicació maliciosa no podrà interactuar o afectar a d'altres.



6. Jailbreak del mòbil



Si realitzem “jailbreak” o “rooteig” del mòbil, ens “alliberem” del sistema operatiu que ens ve imposat però alhora ens exposem a que tota la informació del nostre mòbil quedi compromesa.



6. Jailbreak del mòbil



Conseqüències de realitzar “jailbreak” o “rooteig”:

- Quedem fora del model de seguretat del fabricant.
- Pèrdua de garantia.
- Comportament menys estable del dispositiu.
- Menor durada de la bateria.

Pots estar deixant obertes portes d'accés a la teva informació personal, contrasenyes,...

Més probable que el dispositiu tingui un comportament poc estable, s'apagui més sovint, algunes apps no funcionin en el nou entorn i que la vida de la bateria es vegi escurçada.

6. Jailbreak del mòbil



Robadas más de 225.000 cuentas de Apple

Juan Miguel Revilla, 31 de agosto de 2015, 20:18

SEGURIDAD VIRUS



Las credenciales fueron robadas a través del malware KeyRaider, que se distribuye con la popular herramienta de jailbreak para iOS Cydia.

apdcat
Autoritat Catalana de Protecció de Dades

Notícia completa:

<https://www.itespresso.es/robadas-225-000-cuentas-apple-141921.html>

7. Descàrrega d'aplicacions



Els mercats oficials (App Store i Google Play) ofereixen garantia que les aplicacions que ens instal·lem han passat un procés de verificació.

7. Descàrrega d'aplicacions



Convé fugir dels mercats alternatius ja que són menys estrictes en requeriments de seguretat.

7. Descàrrega d'aplicacions



Descarregar aplicacions des de mercats alternatius pot comportar riscos:

- Permisos abusius
- Adware
- Enganys



CYBERSECURITY

12 Sep 2018 · 7 mins read

Fortnite Android App Investigation: Spyware Risks

We analyzed over 30 Fortnite Android app files downloaded from unofficial marketplaces, including Amazon, and found over 20% of them could be used to spy on you. We discovered apps that can access your camera, track your location, monitor calls, read your contacts and more. Only a minority were actually legitimate apps of any sort as a further 40% were either thinly-veiled adware or scams.

apdcat
Autoritat Catalana de Protecció de Dades

-Concessió de permisos excessius (activar-te la càmera en qualsevol moment, prendre't els contactes, realitzar trucades, baixar-se altres aplicacions, localitzar-te).

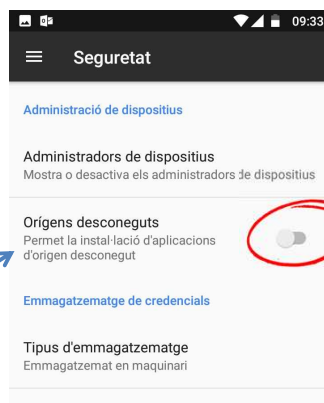
-Adware: Instal·lació d'apps que pretenen bombardejar-te amb anuncis.

-Apps que busquen enganyar-te perquè els donis les teves dades i després les venen.

Notícia completa:

<https://www.top10vpn.com/privacy-central/cybersecurity/fortnite-android-app-investigation-spyware-risks/>

7. Descàrrega d'aplicacions



No convé tenir activada aquesta opció que permet descarregar aplicacions des de mercats alternatius en mòbils Android



És important descarregar les aplicacions només des dels mercats oficials (App Store i Google Play).

Configuració / Seguretat / Orígens desconeguts (no permetre)

Alliberar el nostre dispositiu fent jailbreak o rooteig el fa molt més insegur i vulnerable.

8. Verificació de comentaris



És convenient informar-se de la fama i reputació que una aplicació té a la xarxa.

8. Verificació de comentaris



L'experiència d'altres usuaris pot ser molt útil per evitar descarregar-nos aplicacions de “dubtosa procedència”.

8. Verificació de comentaris



En ocasions, als mercats oficials s'hi han "colat" apps malicioses (en especial a Google Play).



Una versió maliciosa de WhatsApp va aconseguir colar-se a Google Play i va assolir un milió de descàrregues. Tenia permisos per descarregar-se altres aplicacions i a partir d'aquí podia comprometre el nostre dispositiu

8. Verificació de comentaris



En ocasions, als mercats oficials s'hi han "colat" apps malicioses (en especial a Google Play).

Aquesta app, per exemple, prometia fer-nos guanyar *likes* i *followers* a Instagram

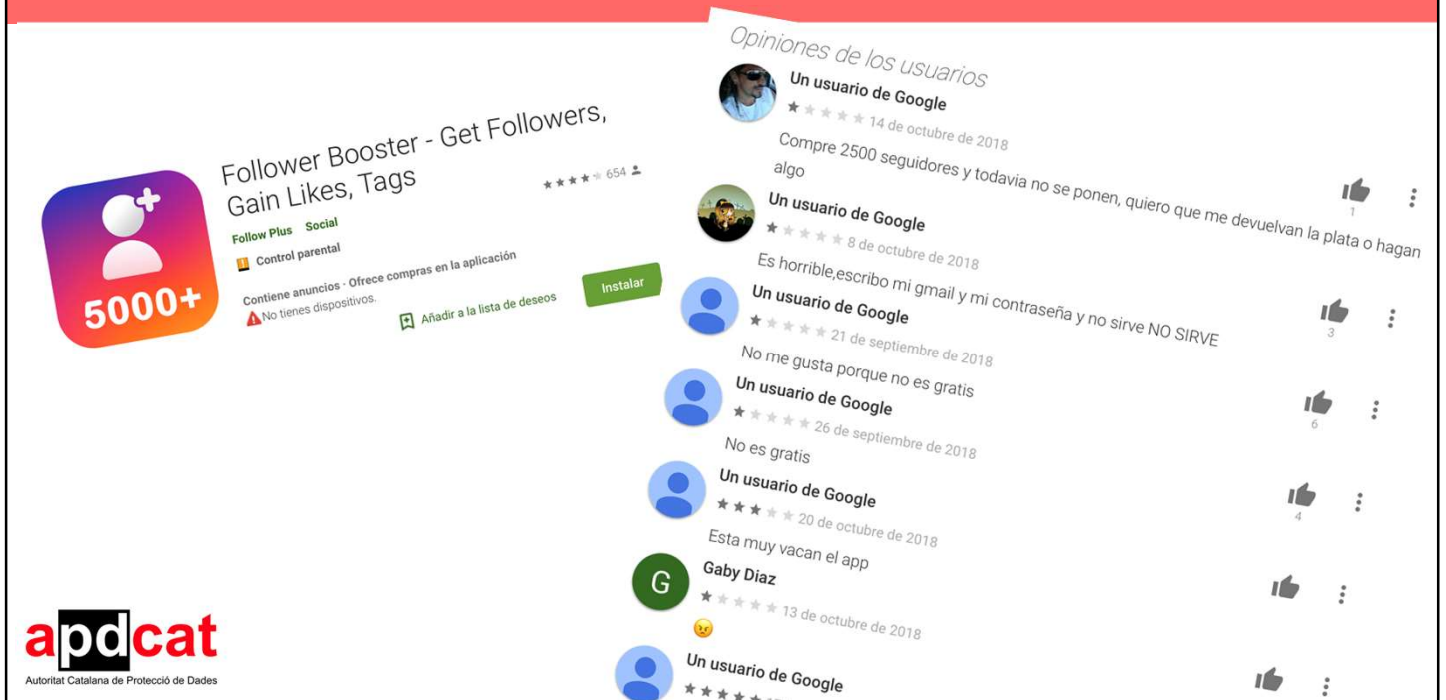
Nuevos ladrones de credenciales de Instagram descubiertos en Google Play
POR LUKAS STEFANKO PUBLICADO 9 MAR 2017 - 10:53AM
AMENAZAS INFORMÁTICAS



Los usuarios de Instagram se convirtieron en el objetivo de varias apps nuevas utilizadas para robar credenciales, que aparecen en Google Play como herramientas para administrar o incrementar el número de seguidores en la red social.

L'aplicació per guanyar followers i likes a Instagram robava credencials (usuaris i contrasenyes).

8. Verificació de comentaris



Aquí veiem un exemple del tipus de comentaris que els usuaris donen a una app per guanyar followers i likes. Si els mirem abans de descarregar-la ens estalviarem uns quants disgustos...

9. Validació de permisos



Per tal de funcionar, una aplicació necessita accedir a determinades funcionalitats del nostre mòbil.

9. Validació de permisos



Quan una aplicació ens demana permís per accedir a algun lloc del nostre mòbil, convé que ens preguntem si realment ho necessita.

9. Validació de permisos



Aneu a la vostra app store i reviseu els permisos que demanen aplicacions que fan de llanterna



Flashlight Free: No Permissions

Humberto Tools

★★★★★ 1,951

PEGI 3

You don't have any devices.

Add to Wishlist

Install



Brightest Flash LED Lights

Flashlight Group Productivity

★★★★★ 124,772

PEGI 3

Contains Ads

You don't have any devices.

Add to Wishlist

Install

Linterna LED - La Más Brillante Para Android

Flashlight Group

- control flashlight
- full network access
- close other apps
- run at startup
- draw over other apps
- control vibration
- prevent device from sleeping
- modify system settings
- toggle sync on and off
- install shortcuts
- uninstall shortcuts



Al instalar actualizaciones de Linterna LED - La Más Brillante Para Android, es posible que se añadan automáticamente funciones adicionales en cada grupo. [Más información](#)

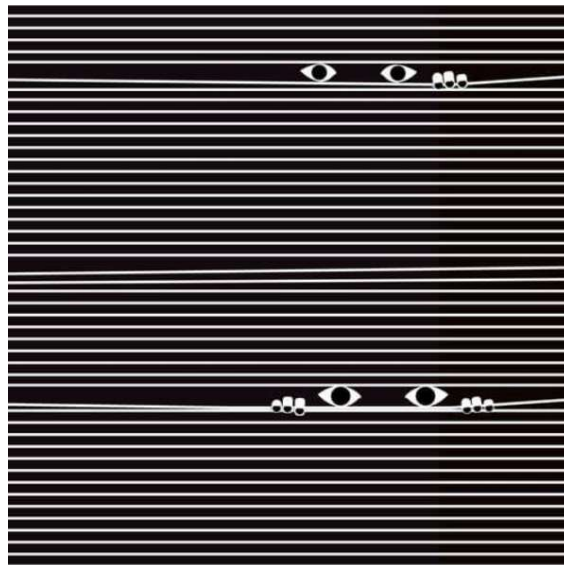
Cancelar

apdcat
Autoritat Catalana de Protecció de Dades

9. Validació de permisos



- Cal revisar els permisos que les aplicacions ens demanen abans d'instal·lar-les.
- Podem concedir o revocar permisos amb posterioritat des de configuració del dispositiu.
- Si veiem que una app demana més permisos del compte, convé no instal·lar-la o esborrar-la.

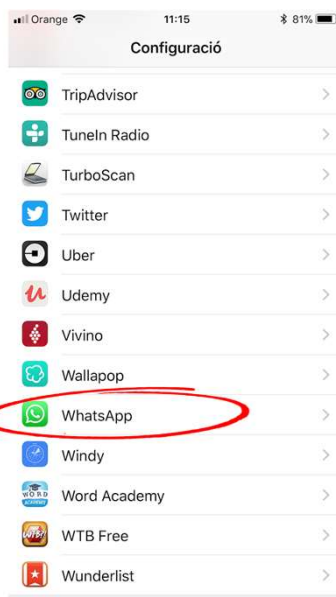


9. Validació de permisos



Podem revisar
aplicació per aplicació
quins permisos té i
modificar-los.

apdcat
Autoritat Catalana de Protecció de Dades



Configuració / Nom de l'app -> apareixen els permisos concedits

9. Validació de permisos



O bé podem anar mirant, permís a permís, quines apps l'utilitzen.

apdcat
Autoritat Catalana de Protecció de Dades



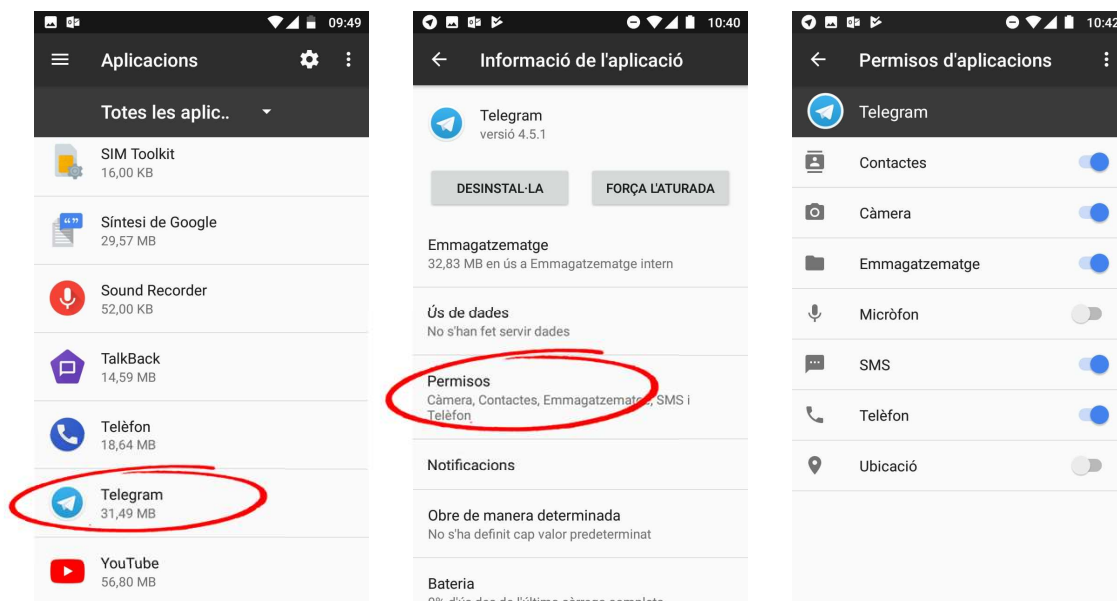
Configuració / Privacitat / Tipus de permís -> Veurem quines aplicacions en fan ús

9. Validació de permisos



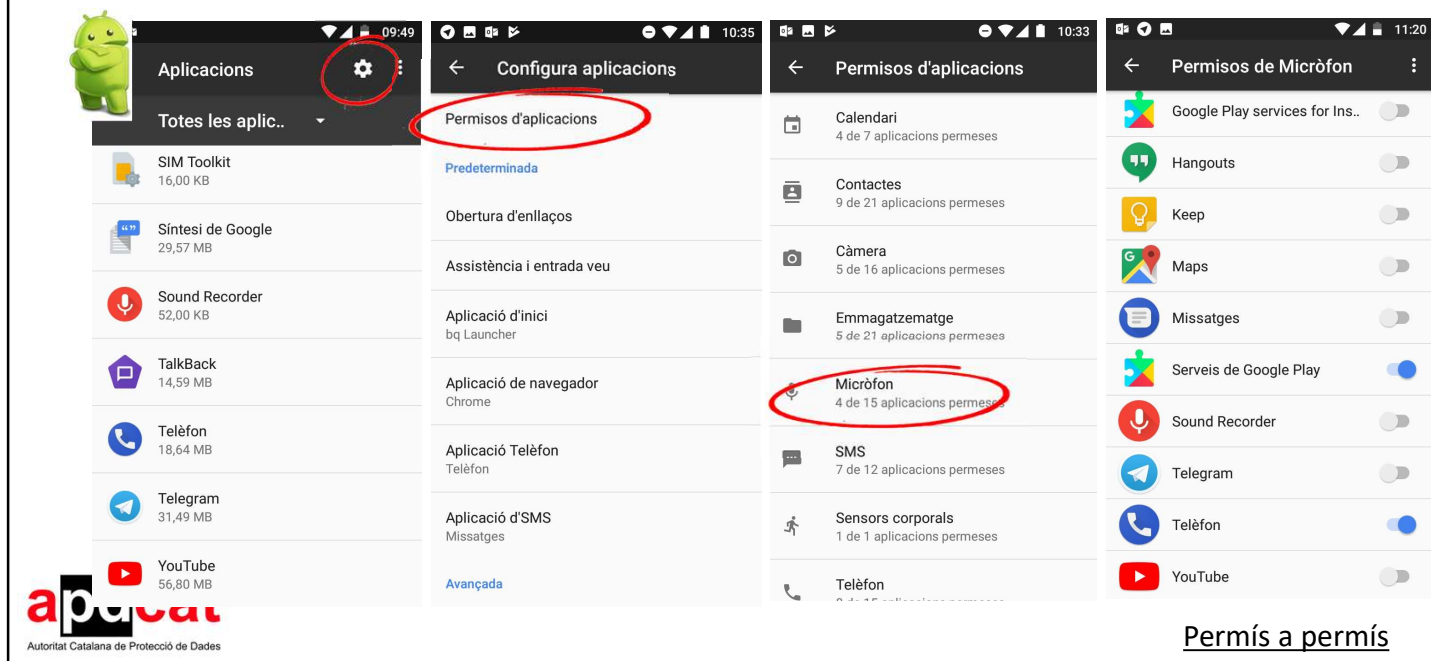
Aplicació per aplicació

apdcat
Autoritat Catalana de Protecció de Dades



Configuració / Aplicacions / Nom de l'aplicació -> Veurem quins permisos té

9. Validació de permisos



Configuració / Aplicacions / "rodeta" / Permisos d'aplicacions / Tipus de permís ->
Veurem quines aplicacions en fan ús

10. Xarxes públiques



Les xarxes obertes dels hotels, aeroports, centres comercials i altres llocs públics, no solen estar configurades de manera segura.



MÉS INFO PER ENTENDRE EL TEMA:

Oficina de Seguridad del Internauta (INCIBE)
<https://www.osi.es/es/wifi-publica>

Vídeo explicatiu:
<https://www.youtube.com/watch?v=0g-rbuKTByw>

Vídeo Chema Alonso que comentàvem de com creava un punt d'accés fals a l'aeroport i monitoritzava el trànsit.
<https://www.youtube.com/watch?v=hpF7LhMXu5I>

10. Xarxes públiques



Això implica que algú que comparteixi la mateixa xarxa podria estar “escoltant” les nostres comunicacions.

Contrasenyes per exemple

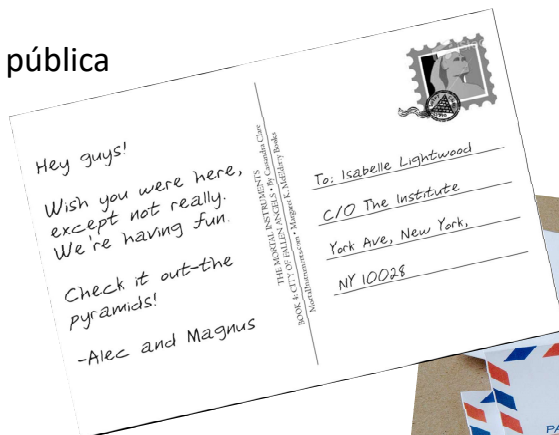
10. Xarxes públiques



10. Xarxes públiques



WiFi pública



WiFi privada



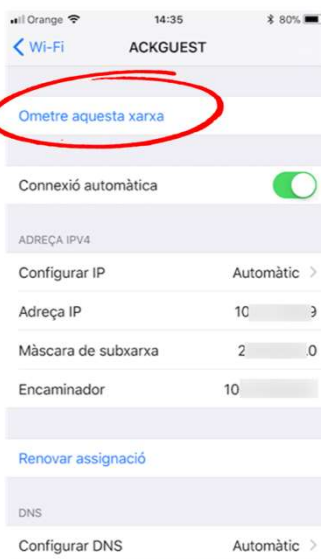
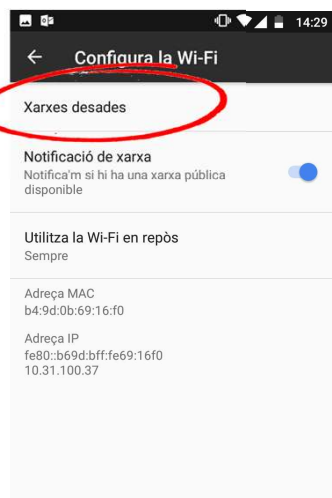
10. Xarxes públiques



Recomanacions:

- Cal evitar utilitzar xarxes WiFi públiques per rebre o transmetre informació sensible. Alerta, estem en “mode postal”!
- Les dades mòbils són una alternativa més segura (3G/4G).
- És recomanable desactivar la connexió WiFi quan no la necessitem.
- Convé esborrar les WiFi públiques (no segures) dels nostres mòbils.

10. Xarxes públiques



A iOS podem esborrar-les només mentre hi estem connectats

Sinó caldrà que reiniciem la configuració i s'esborraran totes

Android permet esborrar-les en qualsevol moment.

iOS només permet esborrar una xarxa quan hi estem connectats. Si volem fer net de les xarxes no segures que tenim desades, haurem de reiniciar la configuració de xarxa del nostre mòbil.

11. Còpies de seguretat



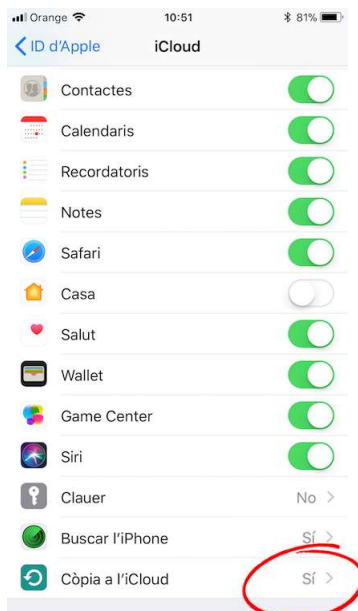
Si mai perdem, ens roben o se'ns espatlla el mòbil, només podrem recuperar el seu contingut si disposem d'una còpia de seguretat recent.

11. Còpies de seguretat



Les còpies poden guardar-se a l'ordinador o, per més comoditat, podem emmagatzemar-les al núvol i activar còpies automàtiques.

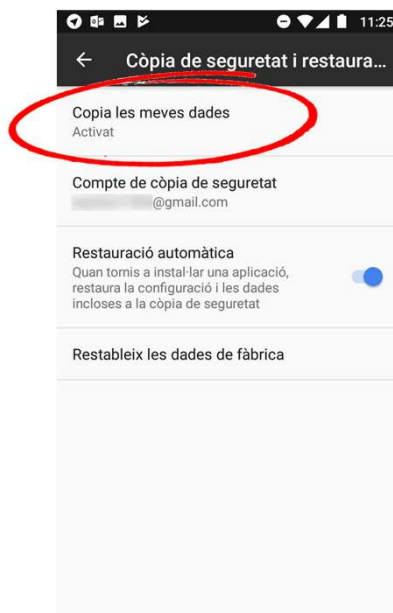
11. Còpies de seguretat



Configuració / clicar sobre el nom del propietari / iCloud / activar Còpia a l'iCloud

La còpia s'emmagatzemarà al nostre compte d'iCloud.

11. Còpies de seguretat



Configuració / Còpia de seguretat i restauració / Copia les meves dades activat

La còpia s'emmagatzemarà al nostre compte de Google.

12. Número IMEI



El número IMEI és la “matrícula” del nostre mòbil.

12. Número IMEI



Si el tenim anotat podrem, en cas de pèrdua o robatori, acreditar que el mòbil és nostre.

12. Número IMEI



Una manera fàcil de conèixer el número IMEI és marcar la següent seqüència:

***#06#**



És el número que apareix a la caixa del mòbil. En els mòbils amb bateria extraïble sol aparèixer en una etiqueta que hi ha darrera la bateria. Podem fàcilment esbrinar l'IMEI del nostre mòbil marcant la seqüència ***#06#**. Ens apareixerà en pantalla i aleshores convé apuntar-lo o fer una captura i guardar aquella imatge fora del mòbil.

13. Localització remota



Si tenim activada la localització remota del mòbil, en cas de pèrdua o robatori el podrem ubicar sobre un mapa, fer-lo sonar, bloquejar-lo, o fer aparèixer un missatge en pantalla. Tot això de manera remota.

13. Localització remota

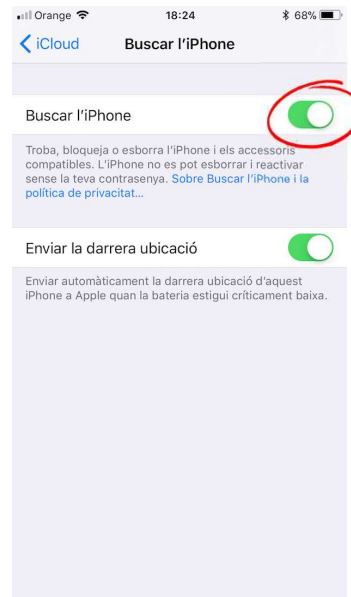


Anem a veure com configurar-ho abans de la pèrdua i com localitzar-lo un cop perdut.

13. Localització remota

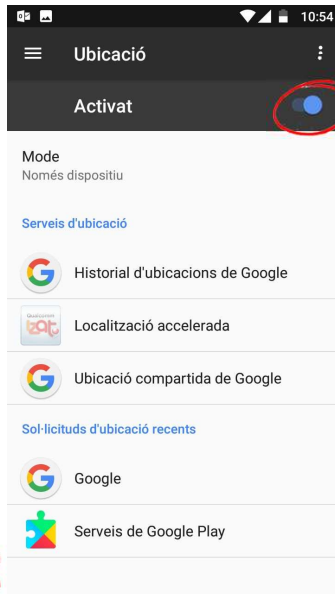


Prèviament, hem de
tenir activada l'opció
de Buscar l'iPhone



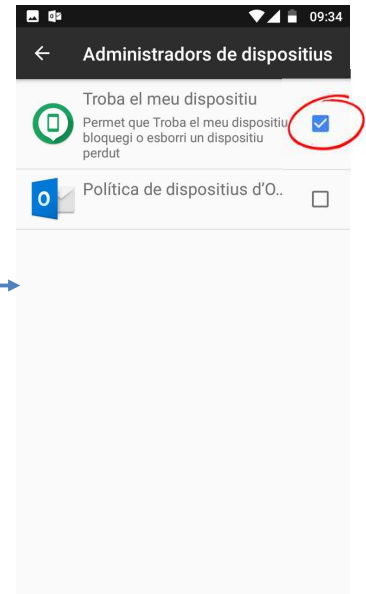
Configuració / clicar sobre el nom del propietari / iCloud / activar Buscar l'iPhone

13. Localització remota



A Android farem dues coses:

- 1) Activarem la ubicació.
- 2) Habilitarem l'opció de "Troba el meu dispositiu".



Configuració / Ubicació -> Activat

Configuració / Seguretat / Administradors de dispositius -> Activat

13. Localització remota



Ara, si ens desapareix el mòbil,
podrem...

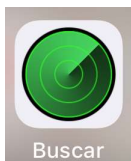
Configuració / Ubicació -> Activat

Configuració / Seguretat / Administradors de dispositius -> Activat

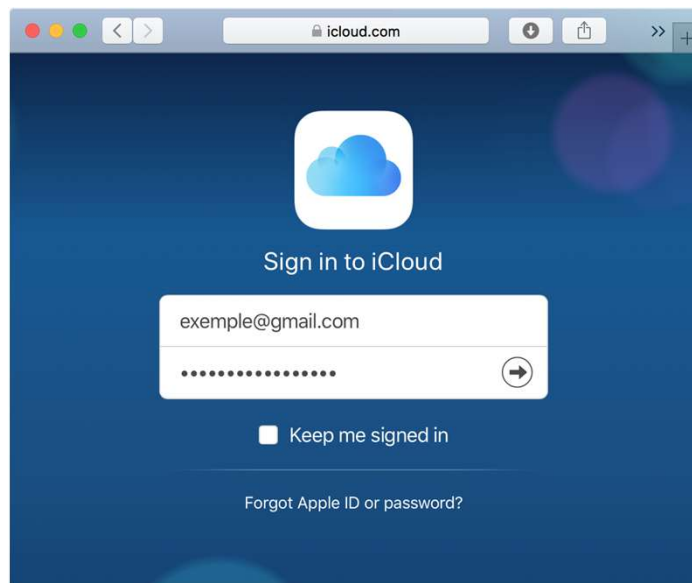
13. Localització remota



Des d'un altre dispositiu iOS o des de www.icloud.com ...



apdcat
Autoritat Catalana de Protecció de Dades



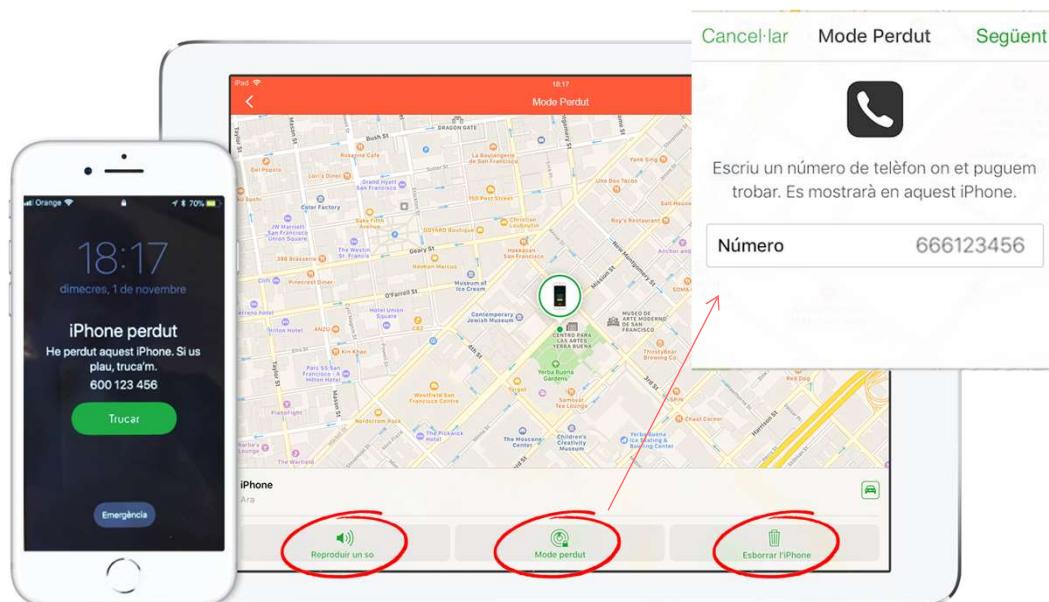
13. Localització remota



... realitzar les
següents accions:



apdcat
Autoritat Catalana de Protecció de Dades



13. Localització remota



Des de

www.android.com/find



apdcat
Autoritat Catalana de Protecció de Dades

Google Troba el meu dispositiu

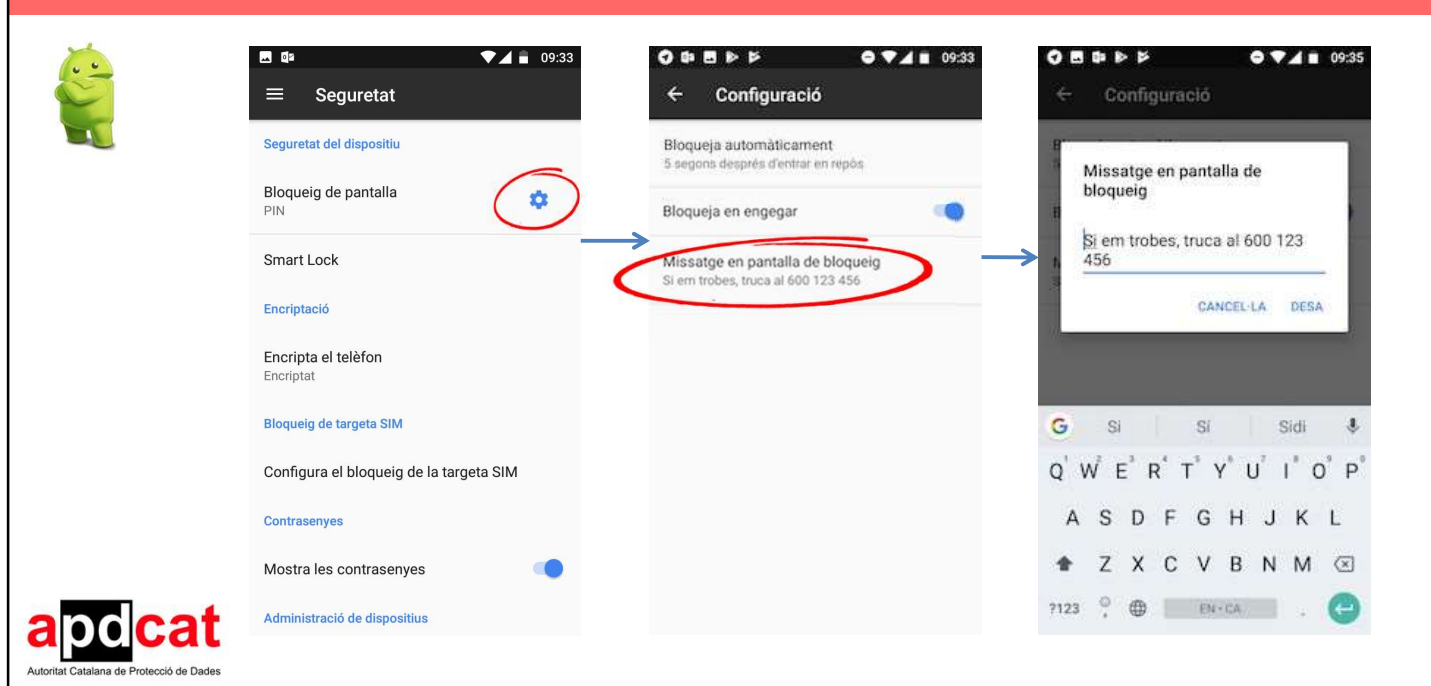
Huawei Y635-L01
Última connexió a les 4 hores amb la **Cronologia de Maps**

REPRODUUEIX UN SO
El dispositiu sonarà durant cinc minuts, encara que estigui en silenci.

BLOQUEJA
Bloqueja el dispositiu i mostra un missatge o un número de telèfon.

ESBORRA
Esborra tot el contingut del dispositiu. Després, ja no el podràs localitzar.

Android: Informació de contacte del propietari



Configuració / Seguretat / Bloqueig de pantalla (rodeta) / Missatge en pantalla de bloqueig

Els dispositius Android permeten fer aparèixer un missatge a la pantalla bloquejada. Això no és possible als dispositius iOS on hauríem d'establir com a foto de pantalla de bloqueig una imatge que haurem editat amb el missatge que volem incloure.



Fem un repàs de totes les configuracions i recomanacions que cal tenir presents:





Ara la informació al teu mòbil està
millor protegida!

Moltes gràcies



Autoritat Catalana de Protecció de Dades



Generalitat de Catalunya