

mossos d'esquadra



**Ús Responsable de les Noves
Tecnologies**

**Material Didàctic
Consells Seguretat**

RECORDEU:

1. Configureu el vostre perfil adequadament: Limiteu qui pot contactar amb vosaltres i quines persones podran tenir accés a la vostra informació.

2. Mantenir només els contactes de confiança. No incorporeu contactes indiscriminadament. No accepteu “amistats” de desconeguts. A Internet és molt fàcil dir mentides i fer veure que ets una altra persona. A més, **no obriu missatges de correus no coneguts i tampoc els arxius adjunts**, poden contenir elements no segurs amb els quals accedir a la vostra màquina per tal de dur a terme accions il·legals i/o perilloses. En aquests casos esborreu el missatge i elimineu-lo de la paperera, directament i sense obrir-los.

3. Utilitzar paraules clau o secretes per identificar els coneguts.

4. Elimineu aquells contactes que no coneixeu personalment.

5. Eviteu proporcionar dades personals reals com l'adreça i el número de telèfon.

6. No pengeu informació que no voleu que la gent pugui veure. Un cop penjada en perdem el control.

7. Desconnecteu la càmera web quan acabeu la sessió. Si aquesta està incorporada a l'equip tapeu-la amb un gomet, paper etc.

8. No pengeu informació que no voleu que la gent pugui veure. Un cop penjada en perdem el control.

9. Creeu una adreça de correu electrònic específica per utilitzar-la únicament dins de l'àmbit de la xarxa social, així si algun dia us voleu donar de baixa i no rebre comunicacions de la xarxa no rebreu missatges al vostre correu personal habitual.

n cas de sostracció de contrasenya el primer pas a seguir és **informar a l'administrador de la web** mitjançant enllaços directes de denúncia. Independentment d'això o si fent l'anterior no s'obté una solució satisfactòria al problema i ho creieu convenient, hauríeu de realitzar una denúncia formal a qualsevol comissaria de la PG-ME o de la PL, si algú fa o ha fet un ús inadequat de les vostres dades personals, us provoquen algun tipus de dany, us arriben amenaces, injúries, o fins i tot poden atemptar contra el dret a la vostra intimitat i al dret a la pròpia imatge.

- **Canvieu sovint les vostres contrasenyes.** Es considera una contrasenya segura aquella de més de 8 caràcters i que combina lletres i números, majúscules i minúscules.
- Si utilitzeu el mòbil per accedir a les xarxes socials cada cop que hi accediu feu-lo utilitzant l'usuari i la contrasenya.

10. Cal expressar-se educadament, respectant a tothom. S'ha de tenir “netiqueta”, o sigui, bones maneres a la xarxa.

ALTRES:

No responeu a sol·licituds de claus o informació sensible. Tota sol·licitud rebuda a través de la xarxa, relacionada amb dades personals, dades sobre contrasenyes, dades bancàries, sol·licitud de diners, etc., les quals no esteu esperant que siguin sol·licitades, sempre, abans de respondre-la s'hauria de contactar personalment amb l'entitat oficial o particular, presumpta demandant de la informació sensible o diners per fer la comprovació oportuna.

Si algú fa un ús abusiu de les xarxes notifiqueu als administradors. Aquests s'encarregaran de portar a terme les actuacions pertinents previstes en les seves condicions de servei.

Si us doneu d'alta en una xarxa social llegiu la política de privadesa i les condicions de servei associades a l'ús de la xarxa social per part de l'usuari. D'aquesta manera, sabreu de primera mà quins són els vostres drets i quins els de l'empresa que controla la xarxa social.

CONCLUSIÓ:

En definitiva, a les xarxes socials hauríem d'actuar amb la mateixa prudència amb què actuem en el nostre dia a dia i no fer als altres allò que no ens agradaria que ens fessin a nosaltres.



COM XATEJAR DE FORMA SEGURA

Recordeu:

- 1) Ves amb compte en qui confies en línia i recorda que alguns "amics" en línia són realment estranys. Esquiva'ls.
- 2) Manté en secret la teva informació personal en completar el teu perfil o xat en línia (nom, adreça, número de telèfon, número de mòbil, adreça de correu electrònic privat, fotografia), encara que te la demanin.
- 3) No descarreguis arxius adjunts (fotografies, documents, música, ...) que t'enviïn per xat persones desconegudes. Poden infectar el teu equip i prendre el control d'aquest.
- 4) Recorda que sempre pots sortir del xat per evitar situacions no desitjades, o canviar el teu nom d'usuari.
- 5) Bloqueja les persones amb qui no vulguis xatejar.
- 6) Pensa abans de contestar als missatges privats.
- 7) No utilitzis el teu nom real - sinó un àlies (però pensa'l bé perquè no cridi l'atenció de forma equivocada).
- 8) Actua si creus que els teus amics es troben en perill.
- 9) Aprèn a mantenir / guardar una còpia de la conversa en el xat - això pot ser útil si has de denunciar d'alguna situació que es produeixi.
- 10) Denuncia qui viola les regles que estableix la sala de xat.
- 11) Ves en compte si vols quedar amb persones que només coneixes d'un xat. Si finalment decideixes fer la trobada, demana a un familiar o amic que t'acompanyi - si més no en la primera trobada. Queda sempre en un lloc públic. Porta sempre un telèfon mòbil que estigui connectat. Tingues cura de les teves pertinences personals.

PREN DECISIONS:

- **Si trobes persones excessivament amables.** Casualment tenen els mateixos gustos per la música, les pel·lícules, actors... Els assetjadors són amables al principi i canvien sobtadament a desagradables.
- **Atura en sec la comunicació** quan sospitis que hi ha moltes contradiccions i inconsistències amb les històries d'un nou amic (de sobte resulta ser més gran del que deia al principi).
- **Si sospites d'alguna cosa estranya**, segueix la teva intuïció i comenta-ho a un adult de confiança.
- Es diu que els adolescents que parlen de sexe amb estranys a la xarxa tenen més probabilitats d'entrar en contacte amb els assetjadors sexuals. **Quan per qualsevol excusa surt el contingut sexual hauries d'avisar-ho a algun adult de confiança o aturar en sec la conversa.**
- **Compteu amb adults de confiança** (pare, mare o educadors) si us sentiu amenaçats per algú que us contacta per la xarxa. Els mossos sempre us ajudaran i els interessa saber el lloc web en qüestió on això passa per evitar altres casos.



DECÀLEG XARXES SOCIALS

1. Ves amb compte en qui confies en línia i recorda que alguns "amics" en línia són realment estranys.
2. Mantén en secret la teva informació personal en completar el teu perfil o xat en línia (nom, adreça, número de telèfon, número de mòbil, adreça de correu electrònic privat, fotografia), encara que te la demanin.
3. Recorda que sempre pots donar-te de baixa per evitar situacions no desitjades, o canviar el teu nom d'usuari.
4. Sigues educat en els xats. Unes paraules no mesurades poden enfilars a situacions no desitjades. Alerta amb les bromes i els comentaris despectius/irònics amb amics amb qui no tens massa confiança. Pensa abans de contestar als missatges privats.
5. No utilitzis el teu nom real - sinó un àlies (però pensa'l bé perquè no cridi l'atenció de forma equivocada).
6. Actua si creus que els teus amics es troben en perill.
7. Aprèn a mantenir / guardar una còpia de la conversa en el xat - això pot ser útil si has de denunciar d'alguna situació que es produeixi.
8. Utilitza els canals de denúncia disponibles quan algú viola les regles del proveïdor de xat.
9. Ves en compte en quedar amb persones que només coneixes en línia.
10. En cas que hagi decidit que sí, cal que demanis a un familiar o amic que t'acompanyi si més no en la primera trobada. Queda sempre en un lloc públic. Porta sempre un telèfon mòbil que estigui connectat. Tingues cura de les teves pertinences personals.



Com evitar l'assetjament a la xarxa

1. No siguis xafarder!!

Evita la difusió de rumors sobre companys o coneguts. No cal enviar missatges de text, sobretot si aquest fa referència a la vida personal dels altres.

2. No t'hi tornis!!

Ignora els missatges ofensius o amenaçadors. Bloqueja al qui ho envia i denúncia aquests comentaris a professors, pares o a la mateixa policia.

3. Els espectadors també són culpables..

Si observes com els teus amics fan comentaris ofensius o denigrants a un company de classe o conegut i no dius res, ets tan culpable com ells. Pensa que denunciar aquests fets és un acte de valentia.

4. Neteja el teu perfil personal

Borra qualsevol cosa de la teva pàgina que sigui molt personal, vergonyós o il·legal. Pensa que aquella fotografia rodejat d'ampolles buides durant una festa no es veuran tan bé quan enviïs sol·licituds a la universitat.

5. Pensa les coses dues vegades, posa't roba!!

Recordes d'aquelles fotografies en les quals gairebé no portes roba, envies petons o fas flexions davant del mirall? Potser penses que són molt "sexy" però la llei no ho considera així. Fes-te un favor, no les enviïs ni les passis a ningú més.

6. Protegeix el teu espai

Utilitza les configuracions de seguretat i no acceptis a qualsevol persona com a amic. Comprova qui és?, per què series el seu amic?

7. Reconeix la diferència entre “maco” i “pervers”

Pensa-ho bé, un home gran que vol tenir una cita amb un menor és simplement sinistre. No és afalagador, és il·legal!

8. Parla amb els teu pares, no són tan rígids com sembla

Algunes vegades els adults s'escandalitzen pel que estàs fent en línia perquè mai els hi expliques res. Aprèn ha explicar les coses perquè puguin confiar en tu.

Consells per prevenir l'enviament de SMS amb contingut sexual

1. PENSA EN LES CONSEQÜÈNCIES...

de fer, enviar o reenviar una fotografia amb contingut sexual d'un altra persona, inclòs la teva. Aquesta imatge podria suposar perdre oportunitats de futur, ser víctima d'humiliacions i comentaris per part dels teus companys, o fins i tot ser objecte d'una investigació policial.

2. MAI FACIS...

fotografies de tu mateix que no voldries que tots (companys de classe, professors, família...) veiessin.

3. ABANS D'ENVIAR ALGUNA COSA...

Recorda que no pots controlar fins on pot arribar aquesta imatge. El que envies al teu nòvio/a pot acabar fàcilment entre els seus amics i els amics dels seus amics i així successivament.

4. SI REENVIAS...

una fotografia amb contingut sexual d'algú sense el seu consentiment, estàs violant la seva confiança i creant un ambient hostil al seu entorn. No ets tu qui decideix les persones que han de veure el seu cos, així que no renviis la seva imatge a ningú.

5. SI ALGÚ ET PRESIONA...

perquè enviïs una fotografia amb contingut sexual, no cedeixis i parla amb un adult de confiança. Recorda que algú que intenta aconseguir que facis quelcom amb el que no et sents còmode, probablement no és de confiança.



CONTRASENYES SEGURES

Característiques d'una contrasenya segura

Una contrasenya segura ha de tenir al menys tres d'aquestes quatre característiques:

- Tenir números
- Tenir lletres
- Tenir majúscules i minúscules
- Tenir símbols (!, \$, %, &, #, etc.)

També ha de complir els següents requisits:

- Longitud no inferior a vuit caràcters
- No ha de formar-se amb números i lletres consecutius al teclat.
- No ha de contenir informació fàcil d'endevinar, com ara la informació personal
- No ha de contenir paraules existents en cap idioma

I per últim, però igual d'important, s'ha de:

- Tenir una contrasenya per a cada servei
- S'ha de canviar amb certa freqüència
- Guardar la contrasenya en un lloc segur i no donar-la a ningú

Tècnica per crear una contrasenya segura (exemple)

1) Trieu una frase fàcil de recordar i tanqueu-la amb un símbol. Un bon mètode per crear una contrasenya sòlida és pensar una frase fàcil de memoritzar, un refrany, el títol d'una pel·lícula que haguem vist fa poc temps, un llibre que ens hagi agradat, etc.

Visc al carrer Estoril número 9!

2) Seleccioneu la primera lletra de cada paraula, i escriviu el resultat alternant majúscules i minúscules.

VaCeN9!

3) Ara només heu d'afegir la terminació del compte al qual pertanyerà la contrasenya i tancar-la amb un altre símbol.

Google+: *VaCeN9!g+?*

Facebook: *VaCeN9!fk?*

Twitter: *VaCeN9!tr?*

Outlook: *VaCeN9!ol?*

Ja tenim la nostra contrasenya per als diferents comptes, fàcil de recordar, difícil d'endevinar i 100% segura!



Privacitat a les xarxes socials

Avui en dia l'ús d'Internet i les xarxes socials s'ha generalitzat, i amb aquest tipus d'aplicacions web els usuaris poden compartir amb altres usuaris les seves experiències, les seves dades personals, i les seves aficions. Tota aquesta informació és molt compromesa i hem d'anar amb molta cura a l'hora de publicar-la. Per això és important donar molta importància a les pautes i normes de seguretat personal a l'hora de publicar, és a dir, saber què hem de publicar, què hem de compartir i amb qui.

En aquest sentit, resultarà útil tenir clares unes pautes d'actuació en aquestes plataformes pel que fa a la privacitat:

Formació

Cal aprendre a gestionar contactes i a publicar tota mena de continguts a les xarxes. Per exemple saber què hi podem publicar, el temps que hi romandrà o disposar de l'autorització de terceres persones que apareguin a les imatges. I, a més, hem de conèixer que algunes xarxes són especialment intrusives amb els drets d'explotació de tot el que s'hi publica.

Regulació i Responsabilitat

Les persones usuàries de les xarxes socials han d'assumir les responsabilitats inherents al medi (Internet). Per exemple, etiquetar fotografies d'una tercera persona sense el seu consentiment vulnera el dret a la pròpia imatge. Tot el que es fa, té unes conseqüències.

Identificació

Cal tendir a la identificació dels usuaris per evitar l'anonimat a les xarxes socials.

L'agència Catalana de Protecció de Dades recomana als usuaris que aprenguin a gestionar la identitat pròpia i que s'assegurin que tenen totes les opcions de privacitat activades. Vigilar qui s'afegeix a la llista d'amics és clau, però també ho és no publicar el telèfon, ni l'adreça, ni detallar quan no s'és a casa, ni passar informació d'amics i de familiars. L'agència recorda que no s'han de publicar fotografies compromeses ni de menors, ni d'amics sense consentiment d'aquests.



COM PROTEGIR LA PRIVACITAT A FACEBOOK

1. **Comprovacions inicials:** Com veuen el meu perfil els altres usuaris? Qui pot trobar-me al Facebook o contactar amb mi? Com controlem la difusió del que publiquem? Comproveu-ho!

Configuració de privacitat / Privadesa / Eines i configuració de privacitat

2. **Etiquetat o “tagging”:** configureu aquesta opció per a mantenir a ratlla la vostra reputació a Facebook.

Configuració de privacitat / Cronologia i etiquetatge

3. **Hem de decidir a qui permetem veure el nostre perfil.**

Només accepteu com amics a persones que coneixeu.

Les amistats dubtoses podeu posar-les a la llista de restringits, on només podran veure la informació i les publicacions que es facin públiques.

Si es trobeu amb un contacte que no desitgeu, podeu deixar de tenir-lo com amic i, a més, podeu bloquejar l'accés d'aquesta persona al compte.

Configuració de privacitat / Bloquejos

4. **Configurar l'ús de les nostres dades en anuncis:** Les fotos i el nom d'usuari del vostre perfil poden usar-se per fer anuncis dels serveis que heu dit que us agraden. Configureu que **ningú** pugui veure aquestes dades en l'apartat d'anuncis: tant als proveïdors tercers com a anuncis a amistats.

Configuració de privacitat / Anuncis

5. **Dedica una mica de temps en assegurar-te que tenim activats els ajustaments de seguretat que ofereix l'aplicació, per tant activa :** la navegació segura (https), avisos per SMS o correu electrònic quan iniciem les sessions, la recollida dels dispositius reconeguts per entrar al compte (ordinador de casa, portàtil, mòbil, altres dispositius...), la recollida de les sessions actives (ubicacions –casa, wi-fi oberts, escola...- i tipus de dispositiu)

Configuració del compte /Seguretat

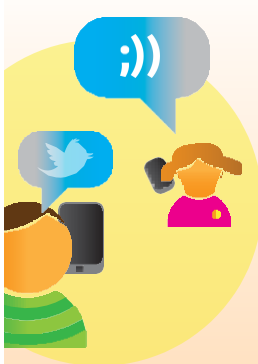


COM PROTEGIR LA INFORMACIÓ QUE TINC AL MEU MÒBIL

Als nostres **smartphones**, la quantitat d'informació i el nivell de confidencialitat s'equipara cada vegada més a la d'un ordinador. Així doncs, cal aplicar principis de seguretat i mesures per protegir-los: antivirus, connexions segures, aplicacions oficials... La naturalesa de mobilitat dels dispositius i la mida reduïda us ha de fer ser encara més responsables.

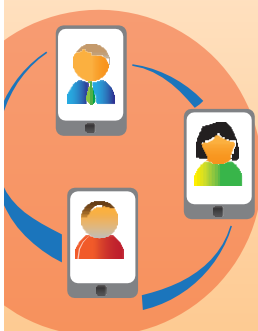
Recordeu els següents consells:

- Exploreu les possibilitats de configuració dels dispositius i desactiveu les funcions que no necessiteu.
- Afegiu a contactes els números de telèfon de confiança amb qui habitualment teniu comunicació.
- Desconfieu de la resta de trucades (números no controlats i ocults), SMS/MMS que no sabem d'on provenen i què volen
- Activeu l'opció de bloqueig automàtic perquè després d'un cert temps d'inactivitat s'hagi de desbloquejar de nou usant una clau, el mateix pin, un patró visual o reconeixement facial.
- No introduïu números PIN i contrasenyes a la vista de tothom.
- Sospita de les trucades des de números desconeguts i ocults, i, no donis dades personals fins a tenir la certesa que és un tràmit legítim.
- Tanca sessió en llocs webs sensibles després d'una sessió de navegació.
- Eviteu aparellaments amb *bluetooth* amb dispositius desconeguts! Si no utilitzeu aquesta funció, desactiveu-la.
- No activeu l'opció de connexió wi-fi automàtica.
- Eviteu la connexió amb xarxes wi-fi desconegudes o controlades per tercers, de les que no coneixem el propietari
- Si heu de connectar el mòbil a altres dispositius (ordinadors o de qualsevol tipus) és imprescindible tenir la seguretat que són segurs, ja que existeix el risc d'infecció del nostre terminal.
- Realitzeu còpies de seguretat.



Perquè no hi hagi fuites involuntàries d'informació:

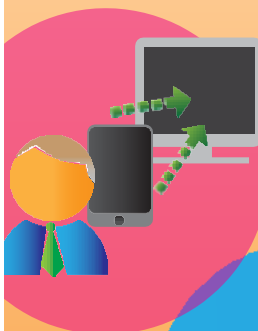
Conèixer les opcions relatives a la privacitat del nostre dispositiu i configurar-lo segons les nostres preferències, a banda de mantenir les precaucions pròpies per a l'ús segur d'Internet i xarxes socials. Conèixer les possibilitats de configuració del nostre dispositiu i desactivar aquelles funcions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



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:

Demandar 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 la guia completa
"Guia per protegir i utilitzar de forma segura el mòbil"
al nostre web www.cesicat.cat

Seguiu-nos a



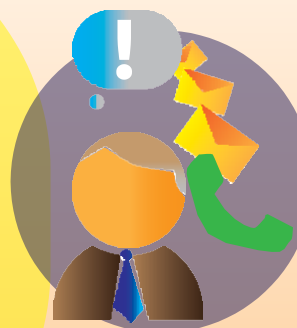
Guia ràpida per a un ús segur del mòbil



cesicat

Centre de Seguretat de la
Informació de Catalunya

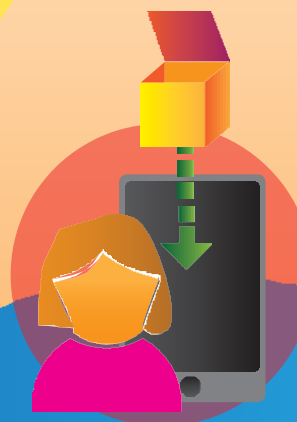
Cada cop és més habitual el robatori o la pèrdua de dispositius mòbils, i també la filtració o fuga de la informació que hi tenim emmagatzemada, però hem de saber que es poden prendre mesures per, si més no, mitigar l'impacte d'aquesta possible pèrdua, fuga o robatori. Abans de res, però, **cal fer una 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.

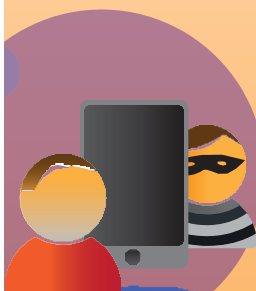
Desconfiar de trucades i SMS de números desconeguts o de difícil verificació, encara que tinguin una aparença d'autenticitat. Aplicar el sentit comú i no proporcionar cap tipus de dades si no estem realment segurs de qui hi ha altre costat de la línia o qui és l'emissor de l'SMS.



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 tradicionals dels ordinadors de sobretaula que pot ser molt eficaç. 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 frauds.



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.

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 desconeguem 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.