

• GUIA •

PER A LA PRÀCTICA D'UNS

HÀBITS -CIBER- SALUDABLES

- FEM UNA INTERNET MÉS SEGURA -



Benvolgudes i benvolguts,

Vivim immersos en una **revolució digital** que està transformant molts aspectes de la nostra vida. Avui, més que mai, hem de prendre consciència que navegar per Internet també pot generar riscos que hem de conèixer. La millor manera de prevenir-los és, justament, generant uns bons **hàbits cibersaludables**.

La guia que teniu a les mans és un recull de consells i de bones pràctiques amb l'objectiu de fer de la xarxa un **espai segur, de respecte i de convivència**.

La tecnologia ens farà canviar, però també és cert que nosaltres podem fer canviar la tecnologia. En aquest sentit, tenim un gran instrument de país com és el programa **Internet Segura** del Centre de Seguretat de la Informació de Catalunya (CESICAT). Es tracta del programa oficial de la Generalitat en matèria de conscienciació i formació a la ciutadania amb la mirada posada en la seguretat digital.

Aquest serà un **segle digital i ciutadà**. Des del Govern treballem amb la voluntat de tenir una ciutadania digitalment apoderada, capacitada i protegida sobre la qual bastir la Catalunya del segle XXI.

Jordi Puigneró
conseller de Polítiques Digitals
i Administració Pública



- 01 -

**Crea contrasenyes
llargues amb lletres,
números i símbols**

**Evitaràs que les endevinin
i accedeixin a les teves dades**

Parlem de... dades segures

Les dades personals, en el món digital, són béns molt preuats. I, per tant, aquestes dades han d'estar ben assegurades i copiades en un entorn protegit. Igual que no deixem les claus de casa al pany, no s'ha d'abandonar una contrasenya en un *post-it*.

Com fer-ho?

- Fes servir contrasenyes llargues, amb lletres, números i símbols com ara %, #, & o /.
- Aplica una contrasenya diferent per a cada servei o aplicació: no la reutilitzis.
- Utilitza, sempre que puguis, el doble factor d'autenticació: sabràs que, en cas que algú sàpiga la contrasenya, no podrà accedir al teu compte perquè usa un dispositiu no reconegut.
- Fes diverses còpies dels continguts (fotos, documents...) i guarda-les en llocs segurs.

I tu?

Encara ets dels que tens les contrasenyes apuntades en una llibreta a la taula?
Tens totes les fotos de la teva vida en una única carpeta a l'ordinador?





- 02 -

**Abans de donar les
teves dades, assegura't
de quin ús se'n farà**

Protegeix la teva privacitat

Parlem de... privacitat

Fotos, comentaris, vídeos... tot allò que publiquem ho pot veure tothom. O no. Som responsables de la nostra privacitat. Saps qui veu la teva darrera foto a Instagram?
O aquella publicació pujada de to a Facebook?
O aquell missatge polèmic que vas escriure a Twitter?

Com fer-ho?

- Tot allò que deixes anar a raig a la xarxa es manté al llarg del temps. La identitat digital no s'esborra: n'has de tenir cura.
- Totes les pàgines que visites i les cerques que fas queden registrades. Si vols controlar la teva privacitat, esborra les dades de navegació periòdicament.
- Revisa les dades i permisos que et demanen les aplicacions que t'instal·les al mòbil. Sigues conscient de la informació que cedeixes a canvi de res.
- Controla la privacitat dels teus perfils de xarxes socials: tu tens el control de qui veu què.

I tu?

Encara t'emprenyes si reps publicitat personalitzada quan navegues?
Saps qui pot veure les publicacions que fas a les xarxes socials?





WIFI



- 03 -

**Quan compris
en línia, no utilitzis
wifis obertes**

**Les dades mòbils sempre
seran més segures**

Parlem de... frau digital

L'àmbit digital cada vegada és més utilitzat pels delinqüents per dur a terme tot tipus de fraus. A mesura que la societat esdevé més connectada, aquest tipus de pràctiques augmenten. És per això que cal anar molt en compte per no caure en paranys que poden costar molt cars.

Com fer-ho?

- Comprova que l'adreça on et connectes tingui la icona del forrellat i l'*https*: les dades només les veuràs tu i el destinatari.
- Si has de fer operacions amb diners o qualsevol altra dada personal sensible, fes servir les dades mòbils i no pas una wifi oberta (amb poca confiança de qui la controla).
- Instal·la un antivirus a tots els teus dispositius per estar ben protegit.
- Vés amb compte amb els missatges que et prometen regals espectaculars o descomptes fabulosos: solen ser enganys.

I tu?

Comproves, abans de clicar, si les adreces on et dirigeixes poden ser malintencionades?
Encara et creus els anuncis emergents que t'alerten que estàs infectat i et proposen la solució miraculosa?





DENUNCIA
LA PUBLICACIÓ



- 04 -

Actua contra l'assetjament a les xarxes

Fem del món digital un espai
de respecte i convivència

Parlem de... civisme digital

En l'entorn digital, igual que en la nostra vida quotidiana, el respecte ens ha d'acompanyar a l'hora d'utilitzar la xarxa. Tractar tothom com vols que et tractin a tu és una màxima que ens serveix sempre com a referència.

Com fer-ho?

- Les teves accions a les xarxes tenen incidència en la teva comunitat. Per tant, pensa bé en les conseqüències que tot això comporta.
- Si ets espectador de qualsevol comportament inapropiat, no et quedis callat i reporta-ho. Les pròpies aplicacions i xarxes socials t'ho posen a l'abast de manera ràpida i senzilla.
- Si has estat víctima d'una suplantació d'identitat o de robatori de dades personals o diners, recull totes les proves que tinguis i denuncia-ho formalment.

I tu?

Has estat víctima d'algun comportament d'aquestes característiques i no has fet res?
Has publicat o comentat alguna cosa que hagi pogut fer sentir malament algú?





- 05 -

**Mantingues al dia
els dispositius
i les seves aplicacions**

**Els protegiràs contra virus
i programes no desitjats**

Parlem de... dispositius al dia

Els vehicles de motor han de passar periòdicament la inspecció tècnica, igual que les calderes de gas. De la mateixa manera, els ordinadors, les tauletes, els mòbils i qualsevol altre dispositiu han d'estar actualitzats per garantir-ne el bon funcionament i, sobretot, la seguretat.

Com fer-ho?

- Fes cas, quan t'ho recordin, que cal actualitzar el sistema operatiu i els programes amb les darreres versions disponibles.
- Sempre que sigui possible, configura actualitzacions automàtiques al mòbil i la tauleta: faràs neteja d'errors interns i optimitzaràs el rendiment del dispositiu.
- Abans d'obrir un dispositiu extern, passa l'antivirus per comprovar que està lliure de qualsevol tipus d'infecció.

I tu?

Encara vas pel món sense antivirus pensant que a tu no et passarà?
Retardes sistemàticament l'actualització del sistema operatiu perquè et fa mandra?



#InternetSegura

internetsegura.cat

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.







**Descarrega't la guia capturant aquest codi QR o a:
<https://internetsegura.cat/habits-ciber-saludables>**