

Formació interna de centre

Ciberseguretat

2022 | 2023



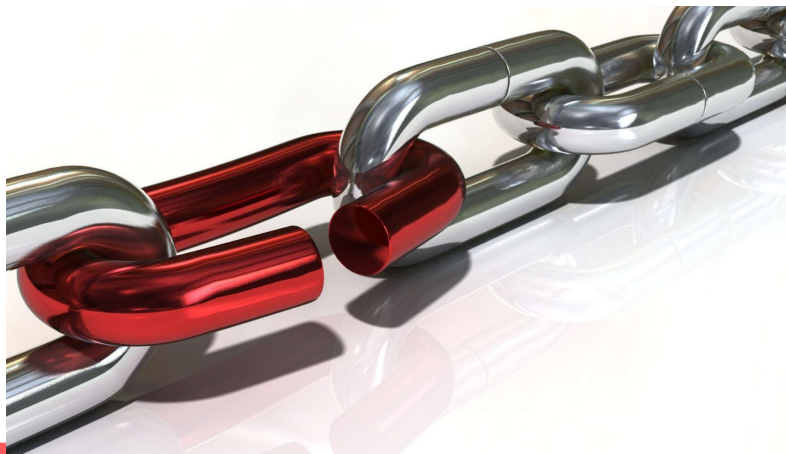
Generalitat de Catalunya
Departament d'Educació



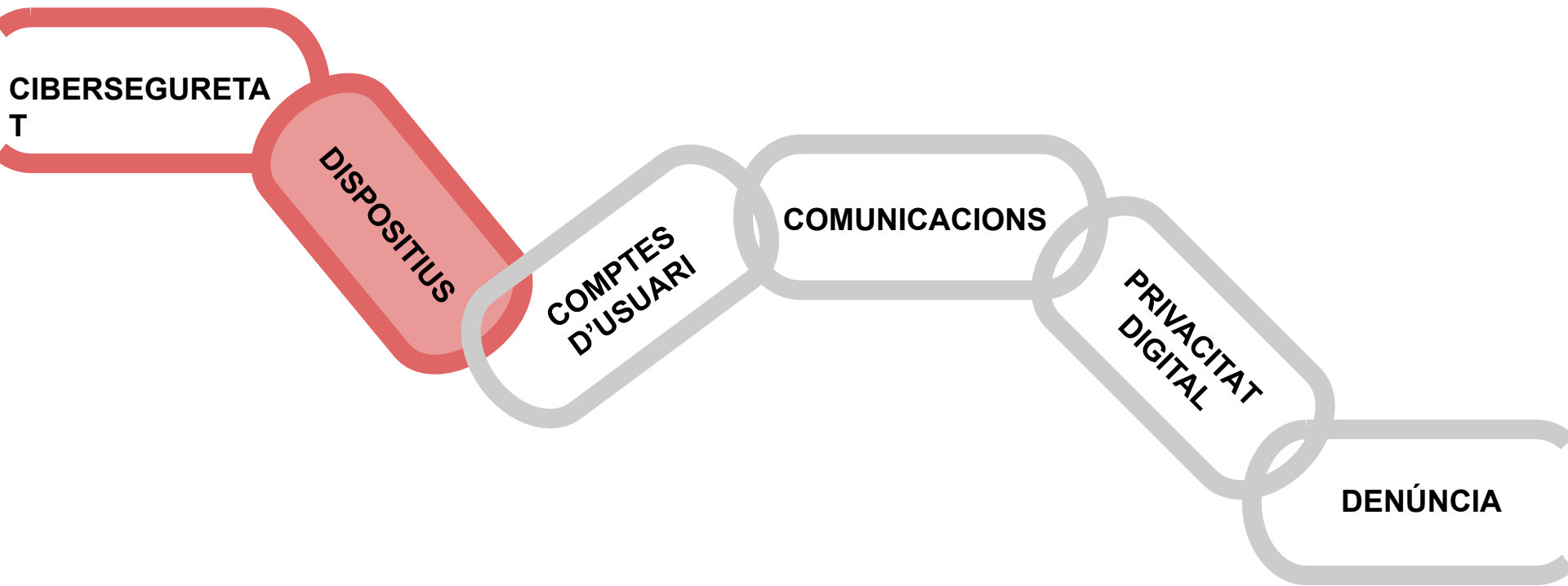
De què parlem quan parlem de ciberseguretat?

La ciberseguretat és la seguretat en la informàtica.

Sovint es compara amb una cadena.



Es **trenca** si una de les baules és dèbil, i la cadena deixa de ser útil.





Als nostres dispositius hi ha informació molt important.

- Personal.
- Professional.

Si s'apoderen del dispositiu poden:

- Obtenir informació, esborrar-la o manipular-la.
- Fer-se passar per nosaltres.



Un “virus” us ha esborrat mai el dispositiu?

Doncs, què volen de nosaltres?

Habitualment volen benefici econòmic a través de:

- Robar o segrestar dades.
- Aprofitar la connexió i potència del nostre dispositiu.



Els virus anomenats 'ransomware' **encripten les dades i demanen un rescat econòmic** per recuperar-les.

Podem evitar la pèrdua d'aquestes dades fent una **còpia de seguretat**:

- Dispositiu físic extern. Cal encriptar si conté dades confidencials.
- Al núvol.





Com podem evitar que ens infectin?

Actualitzacions

Antivirus

Tallafocs

Bones pràctiques

Què t'instal·les?

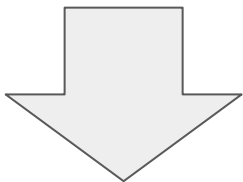
Quines pàgines
visites





Minimització infeccions en els dispositius

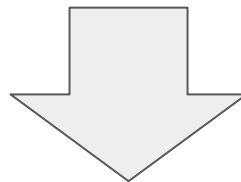
Ordinadors portàtils i
Chromebooks del **PEDC**
(docents i alumnat)



Els elements de seguretat estan
configurats d'acord amb els
criteris de l'Agència de
Ciberseguretat, **no cal intervenir**

Recomanat!

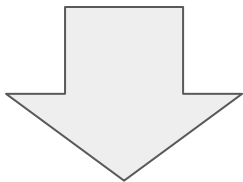
Altres dispositius on
l'usuari té el rol
d'administrador



**Cal configurar tots els
elements de seguretat**
(antivirus, tallafocs, programari
instal·lat ...)



Altres dispositius on l'usuari té el rol d'administrador



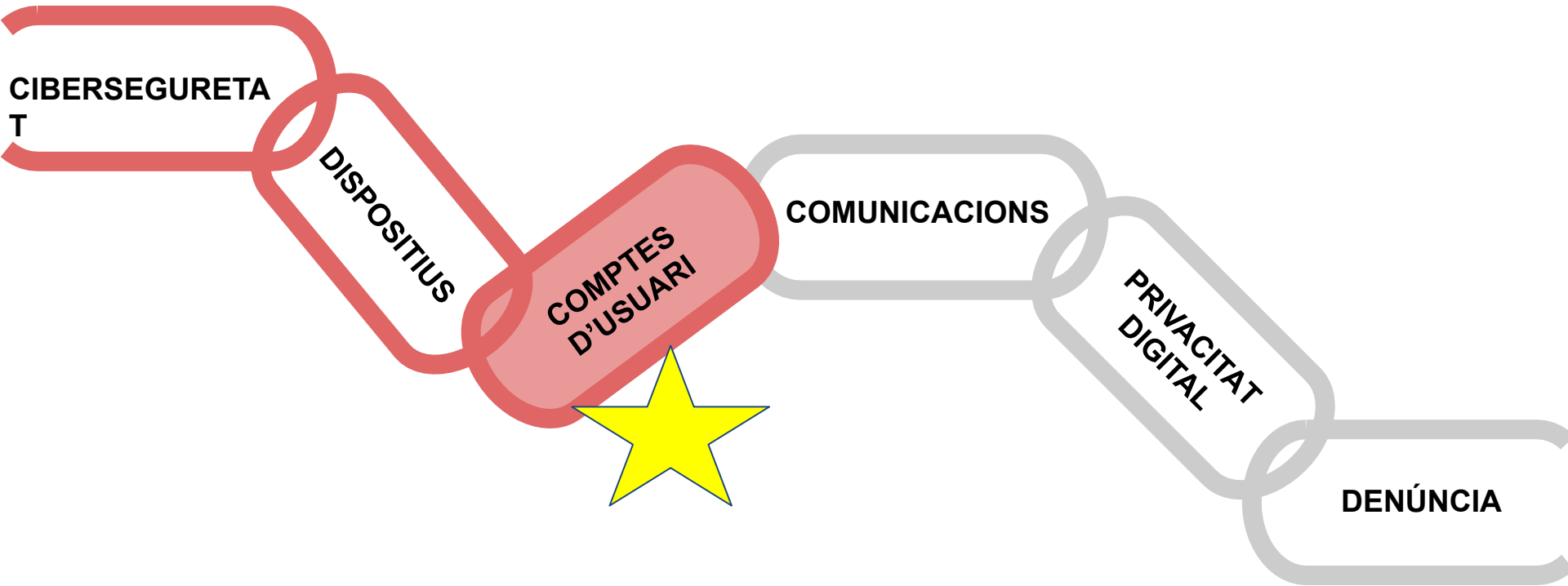
Cal configurar tots els elements de seguretat
(antivirus, tallafocs, programari instal·lat ...)

MATERIAL EXTRA

- [ANTIVIRUS: Programació d'anàlisi setmanal i excloure carpetes i arxius.](#)
- [Com restaurar o eliminar els arxius en quarantena a Windows Defender.](#)
- [Les còpies de seguretat](#)
- [Configuració del tallafocs](#)







L'accés als nostres **comptes d'usuari**, es fan habitualment a través de nom d'usuari i contrasenya.

Les contrasenyes són les claus que **donen accés a la teva vida digital:**

- Informació personal.
- Accés als teus serveis habituals:
- correu electrònic, comptes bancaris, xarxes socials, etc.





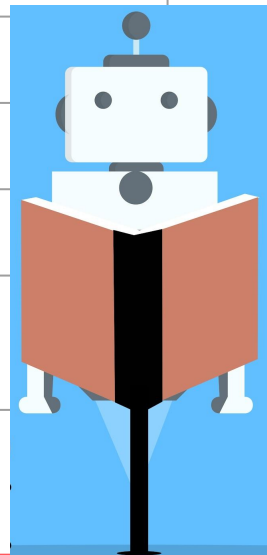
Quins errors cometem durant la gestió de contrasenyes?

- Utilitzar sempre la mateixa per tots els comptes.
- No canviar-la regularment.
- Compartir l'usuari i contrasenya.
- Apuntar-la en un post-it i enganxar-ho a sota el teclat o a la pantalla.
- Permetre que algú accedeixi als teus dispositius.
- Contrasenya dèbil: curta o amb paraules de diccionari.



Ens calen contrasenyes segures, però com les creem?

Truc	Exemple
Mateix patró , petites variacions	ATRI: K8542sd\$ A XTEC: K8542sd\$ X
Camel : Alternar majúscules i minúscules	CaMeL
Utilitzar Caràcters regionals o especials	ç ñ ! ~
Canviar lletres per números	c0ntr4s3ny4
Regles mnemotècniques	Qui no té cap, ha de tenir cames -> QNTCHDTC



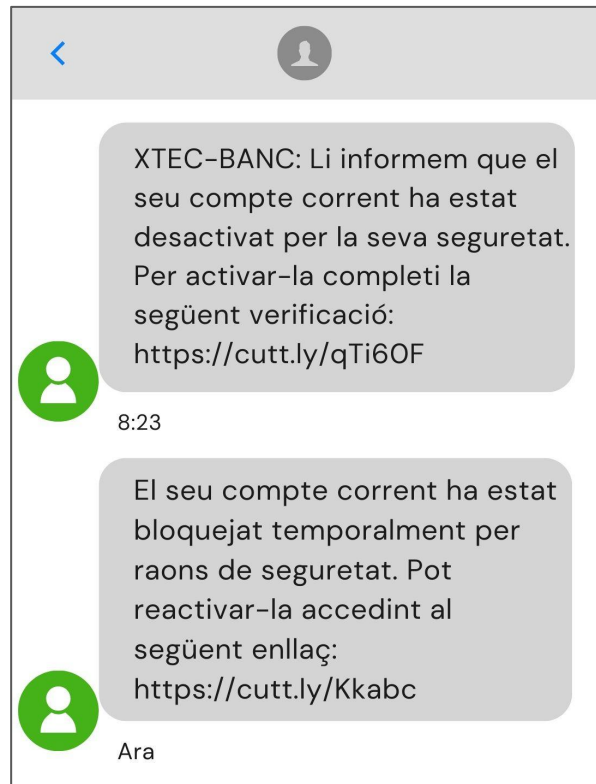


Activitat. Creació de contrasenyes segures

Un atac habitual és utilitzar **enginyeria social** per aconseguir accés al teu compte d'usuari.

Però com poden suplantar-nos les identitats?

- **Phishing:** La “pesca” busca enganyar a través de missatges fraudulents, per obtenir les nostres dades personals (per exemple les dades bancàries).
- **SIM Swapping:** Es duplica la targeta SIM del mòbil d'una persona per suplantar el seu número de telèfon. Això permet als atacants obtenir, per exemple, els codis de confirmació de transferències o contractacions dels bancs que es confirmen via SMS.





I per què la gent “pica” durant aquesta pesca?

- Excés de confiança.
- Desconeixement.

*Es coneixen con a
atacs d'enginyeria
social.*

Com podem evitar-los?

Formació! Tant dels docents com de l'alumnat.



Formació de l'alumnat.

L'agència de ciberseguretat de catalunya ofereix recursos per infants i adolescents, que els docents poden projectar a l'aula quan sigui convenient.

★ https://xtec.gencat.cat/ca/recursos/tecinformacio/internet_segura/



Gestors de contrasenyes



KeePass



BitWarden

LastPass...

Doble factor d'autenticació



Bloqueig de pantalla





Gestors de contrasenyes



KeePass



BitWarden

LastPass...



- ★ [Com configurar els navegadors.](#)
- ★ [Utilització d'un gestor de contrasenyes, a triar entre el KeePass \(instal·lació \) o Bitwarden \(gestor al núvol\).](#)



Doble factor d'autenticació



Es recomanem en els comptes en línia més sensibles, com ara el banc, el correu electrònic o serveis de compra en línia. Això ens protegeix fins i tot del robatori de contrasenyes, ja que, sense aquest segon factor d'autenticació, els criminals no podran tenir accés als nostres comptes encara que coneguin les nostres credencials.

El segon factor d'autenticació hauria de ser d'algun d'aquests tipus:

- Quelcom que saben: paraula o frase de pas.
- Quelcom que tenim: dispositiu mòbil, token o dispositiu electrònic per generar codis d'un sol ús.
- Quelcom que som: identificació biomètrica o similar.

★ [Activar un segon factor d'autenticació a Gmail.](#)

★ [Activar un segon factor d'autenticació a Twitter.](#)



Bloqueig de pantalla



Per configurar el bloqueig de pantalla hem de tenir en compte el temps d'espera de la pantalla, el mètode de desbloqueig i la informació que es pot veure quan la pantalla està bloquejada.



PATRÓ

PIN

CONTRASENYA

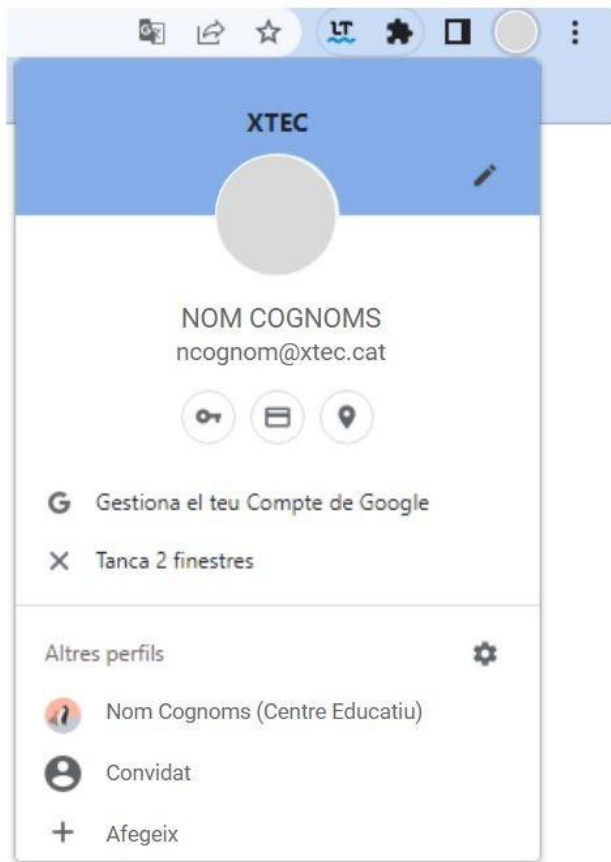
BIOMETRIA



CONTRASENYA



BIOMETRIA



Els navegadors més habituals, permeten tenir **perfils** en funció de diferents comptes d'usuari.

Es pot definir més d'un compte en un sol navegador:

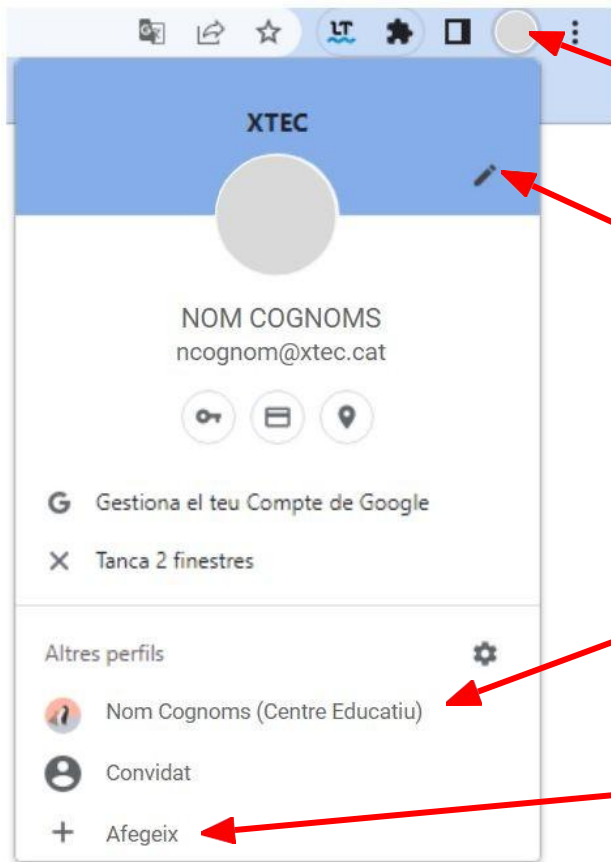
- Personal
- XTEC
- Centre (@nomdelcentre.cat)



Cal anar en compte en configurar aquests perfils. Només s'ha de fer en dispositius d'ús personal, que només hi tinguem accés nosaltres. Tancar sessió d'aquests usuaris no és immediat i, si ens oblidem, deixariem el nostre correu i totes les altres contrasenyes o targetes de crèdit que tinguéssim configurades obertes per al següent usuari que vingüés darrera.



Comptes d'usuari: perfils de navegadors



Clicant sobre la imatge, accedeixes a les opcions de configuració del perfil.

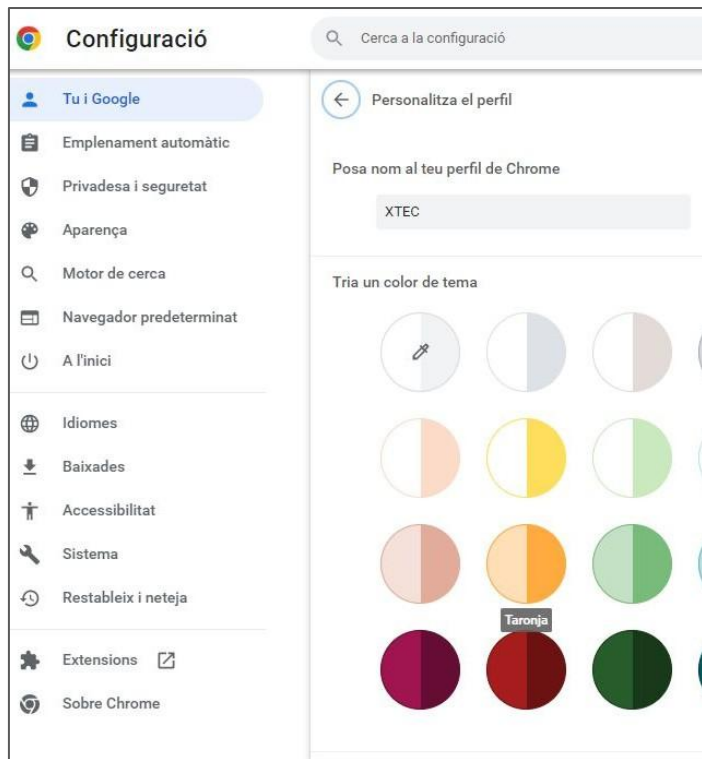
Editar el perfil actiu.

Canviar de perfil actiu.

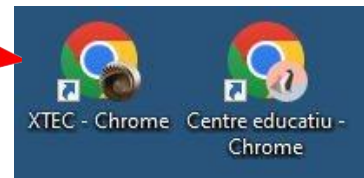
Afegir perfils.



Comptes d'usuari: perfils de navegadors



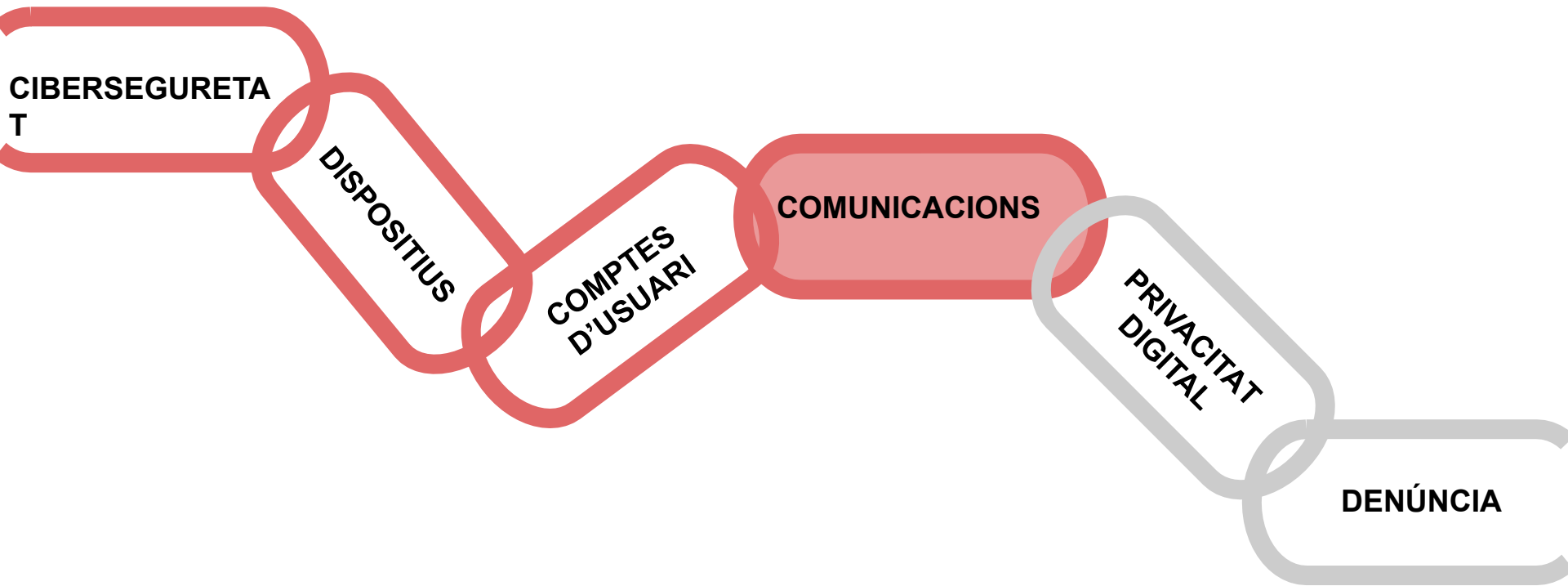
- Cada perfil de navegador **és independent** dels altres, i s'obre en una nova finestra.
- Cada perfil tindrà **les seves pròpies dades** d'aplicacions, extensions, historial de navegació, marcadors, contrasenyes desades i pestanyes obertes.
- Permet moltes opcions de configuració del navegador com per exemple les de privadesa i seguretat.
- El compte XTEC té limitat la sincronització entre dispositius.
- Es poden crear **accessos directes** als perfils a l'escriptori.





Activitat. Gestió de perfils del navegador.

- ★ Perfils del navegador Chrome:
<https://ateneu.xtec.cat/wiki/form/wikiexport/cmd/tac/treballaralnuvol/treballalaula/chrome>
- ★ Perfils del navegador Mozilla:
<https://support.mozilla.org/es/kb/usar-el-administrador-de-perfiles-para-crear-y-eli>
- ★ Perfils del navegador Microsoft Edge:
<https://support.microsoft.com/es-es/topic/iniciar-sesi%C3%B3n-y-crear-varios-perfiles-en-microsoft-edge-df94e622-2061-49ae-ad1d-6f0e43ce6435>





Bluetooth y otros dispositivos

Agregar Bluetooth u otro dispositivo

Bluetooth

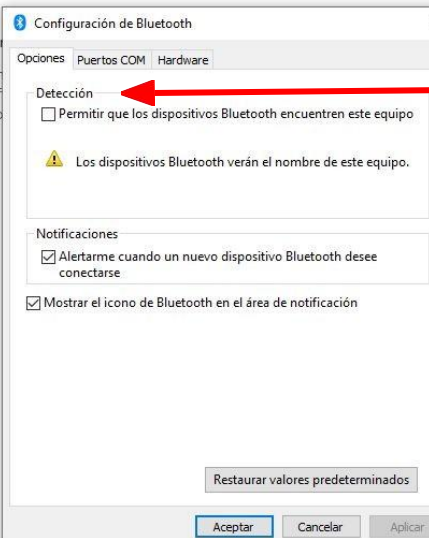
☐ Desactivat

☒ Mostrar notificaciones para la conexión con el Emparejamiento rápido

Cuando esta opción está seleccionada, puedes conectarte a dispositivos Bluetooth compatibles rápidamente cuando están cerca y en modo de emparejamiento.

☐ Descargar a través de conexión Bluetooth

Durante conexiones de uso masivo para evitar la descarga de software (controladores, información de dispositivos adicionales).



Recomanacions sobre l'ús del **Bluetooth**

Desactiveu-lo si no el feu servir

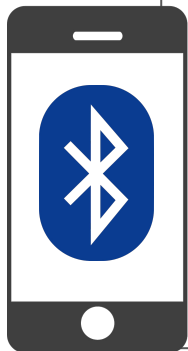
Eviteu operacions Bluetooth en llocs públics

Utilitzar-lo en ocult (alguns mòbils no ho permeten)

No connectar-se a dispositius sense verificar la font

Canvieu el pin per defecte (si hi ha l'opció)

Reviseu els permisos de les apps (mòbils)





Wifi Oberta

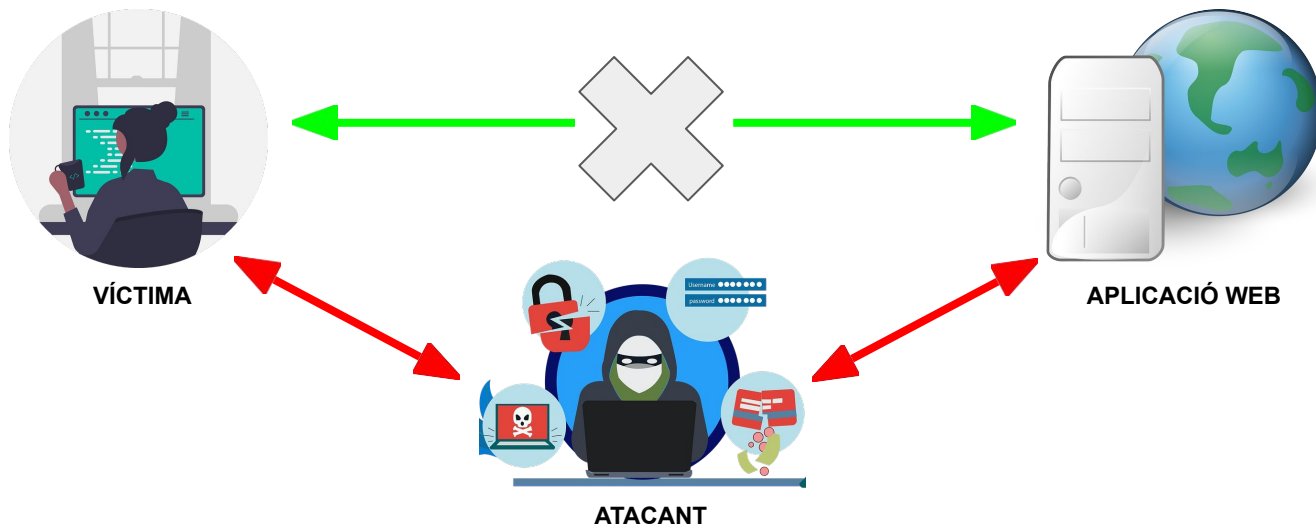


Wifi Oberta amb identificació



Wifi Xifrada

- Les xarxes públiques són aquelles que pot utilitzar qualsevol persona.
- Es consideren amb més risc perquè no se sap:
 - Si els paràmetres de seguretat estan ben configurats.
 - Qui està connectat a la xarxa.





A CASA VOSTRA (PRIVADA)

- Activeu la seguretat **WPA2** de la WiFi.
- Establiu una contrasenya robusta.
- Comproveu quins dispositius estan connectats.
- Definiu una llista “blanca” dels vostres dispositius.

FORA DE CASA (PÚBLICA)

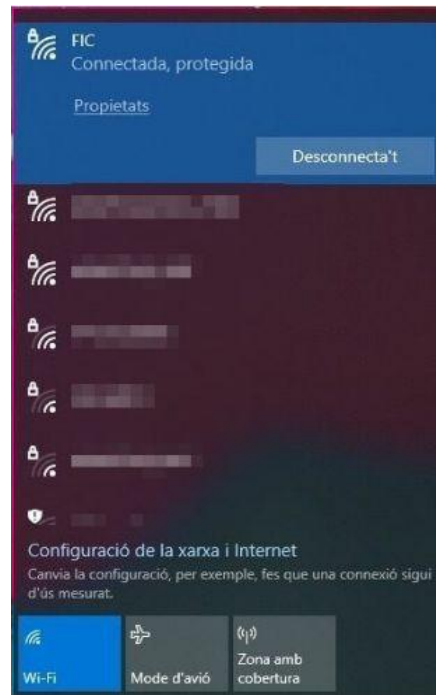
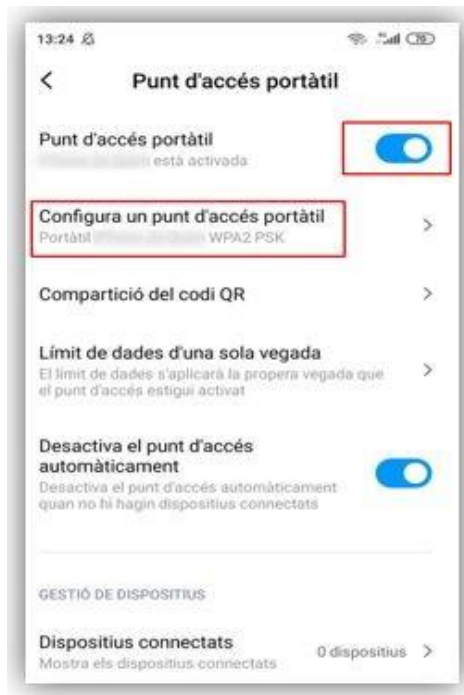
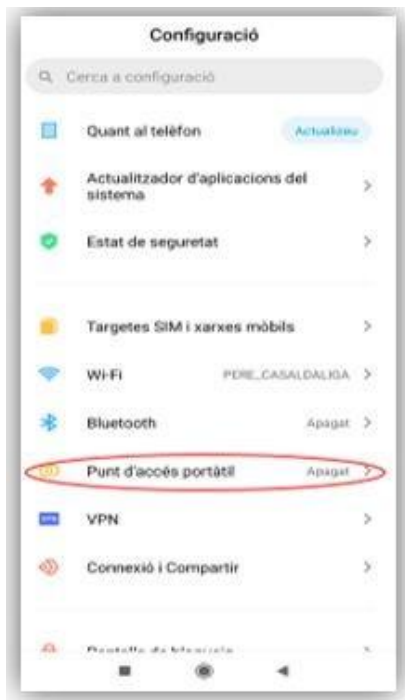
- Eviteu connectar-vos a xarxes WiFi públiques.
- Feu servir el vostre mòbil com a punt d'accés WiFi, amb una contrasenya robusta.
- Eviteu operacions amb dades personals o bancàries.
- Assegureu que la connexió sigui encriptada.



- Utilitzeu una **VPN** (Virtual Private Network).

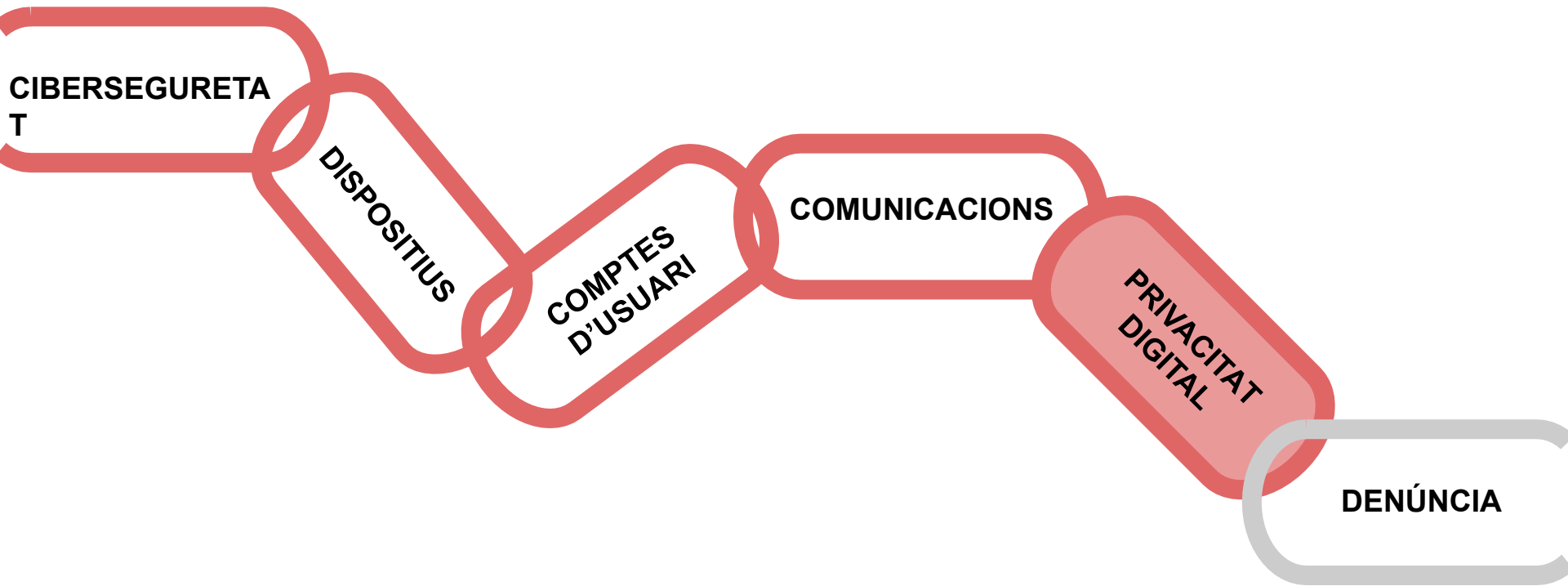


Utilitzar el “Punt d'accés portàtil” del nostre telèfon mòbil





Activitat. El mòbil com a
punt d'accés a Internet.



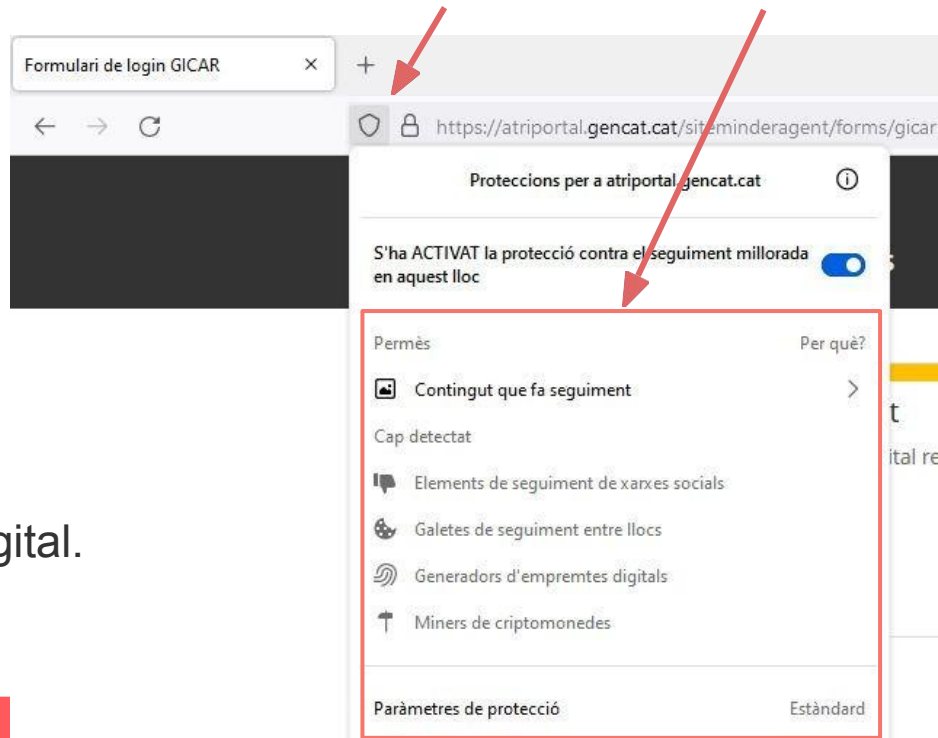
- **Privacitat digital** és el control que un usuari pot exercir sobre les seves dades a Internet.
- Aquestes dades **tenen un valor comercial**, i les empreses volen explotar-les.
 - Historial de navegació, localització, edat, gènere, preferències, etc.
 - Utilitzen tècniques de seguiment (**tracking**), recol·lectant els llocs que visites i analitzant el teu comportament.
- Les **cookies** són uns fitxers que es guarden en el teu ordinador quan navegues, i que desen les teves preferències per quan tornis a la pàgina.
 - Algunes empreses les utilitzen per fer un seguiment de l'usuari.



Els navegadors disposen de mecanismes de seguretat i privacitat.

- Filtres d'accés a pàgines malicioses.
- Filtres de publicitat.
- Limitació de pàgines emergents.
- Extensions del navegador.
- Configuració de formularis.
- Configuració de contrasenyes.
- Utilització d'un proxy.
- Incorporació de certificats d'identitat digital.
- Gestió de cookies (galetes).

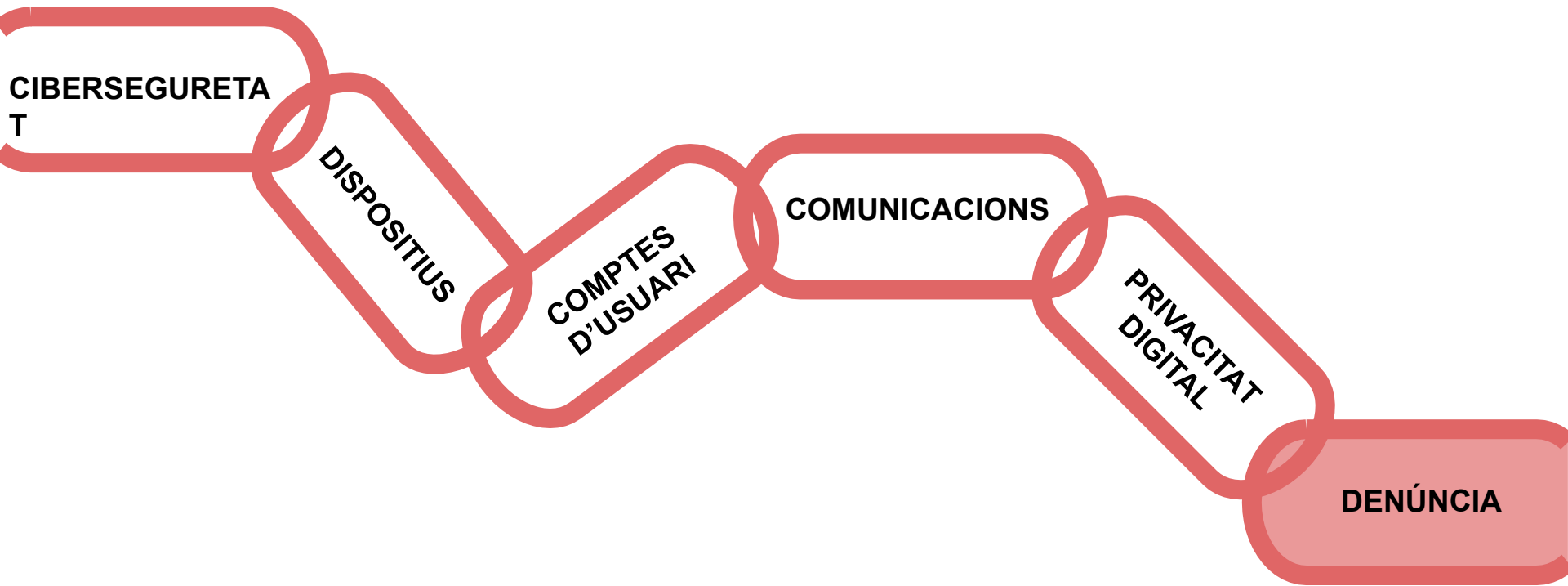
Proteccions a Mozilla Firefox





- El **mode incògnit** és una funció de privacitat del navegador web.
- El navegador crea una sessió temporal, aïllada de la sessió principal.
- D'aquesta manera dificulta que et facin un seguiment.
- Quan es tanca el navegador, s'esborren totes les dades.
- És útil si utilitzes el teu compte en un ordinador que no és teu.
 - És habitual oblidar-se de tancar la sessió en els ordinadors compartits, treballar en mode incògnit facilita que en tancar el navegador no es quedi la sessió oberta.
 - Per exemple si fas servir l'ordinador d'aula per una hora de classe, o a la sala de professorat.





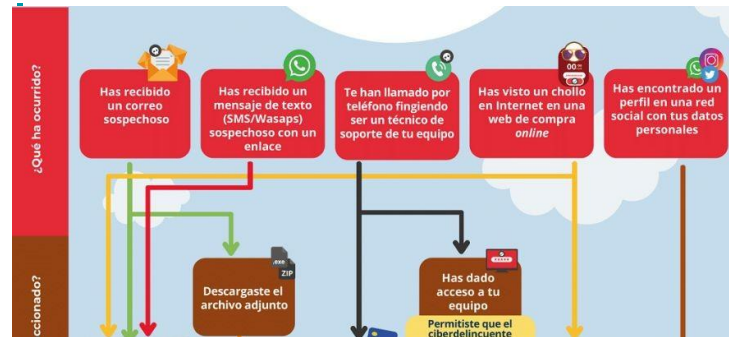
- Un **delicte informàtic** és un delicte que es realitza en un entorn digital.
- Com en tots els delictes, la víctima ha de [denunciar-ho](#).
 - Recopilar informació i registres sobre el delicte.
 - Es pot denunciar en jutjats de guàrdia o a la [comissaria més propera](#).
- En el cas de necessitar assessorament:
 - Correu: internetsegura@gencat.cat
 - Formulari de contacte: [Internet Segura](#)



- Contacta amb la web o el servei:

- Google: <https://support.google.com/accounts/answer/6294825?hl=es-419>
<https://support.google.com/mail/contact/abuse/>
- Instagram: <https://help.instagram.com/446663175382270/>
<https://help.instagram.com/368191326593075/>
- TikTok: <https://www.tiktok.com/safety/resources/hacked-account?lang=es>
- Facebook: <https://es-es.facebook.com/help/fakeaccount>
<https://es-es.facebook.com/help/1216349518398524/>
- Twitter: <https://help.twitter.com/en/forms/authenticity/impersonation>

- Infografia “Què fer si ets víctima d'un frau”.





Materials complementaris
per treballar-ho a l'aula.



Recursos, guies didàctiques i
notícies sobre ciberseguretat



Recursos, guies didàctiques i
notícies sobre ciberseguretat



Recursos per l'aula

Altres recursos:

- [Instituto nacional de tecnologías educativas y de formación del profesorado](#)
- [Diagnòstic de la privacitat en dispositius mòbils](#)
- [Internet segura for kids \(is4k\)](#)
- [Oficina de Seguridad del Internauta \(OSI\)](#)
- [Instituto nacional de ciberseguridad \(avançat\)](#)