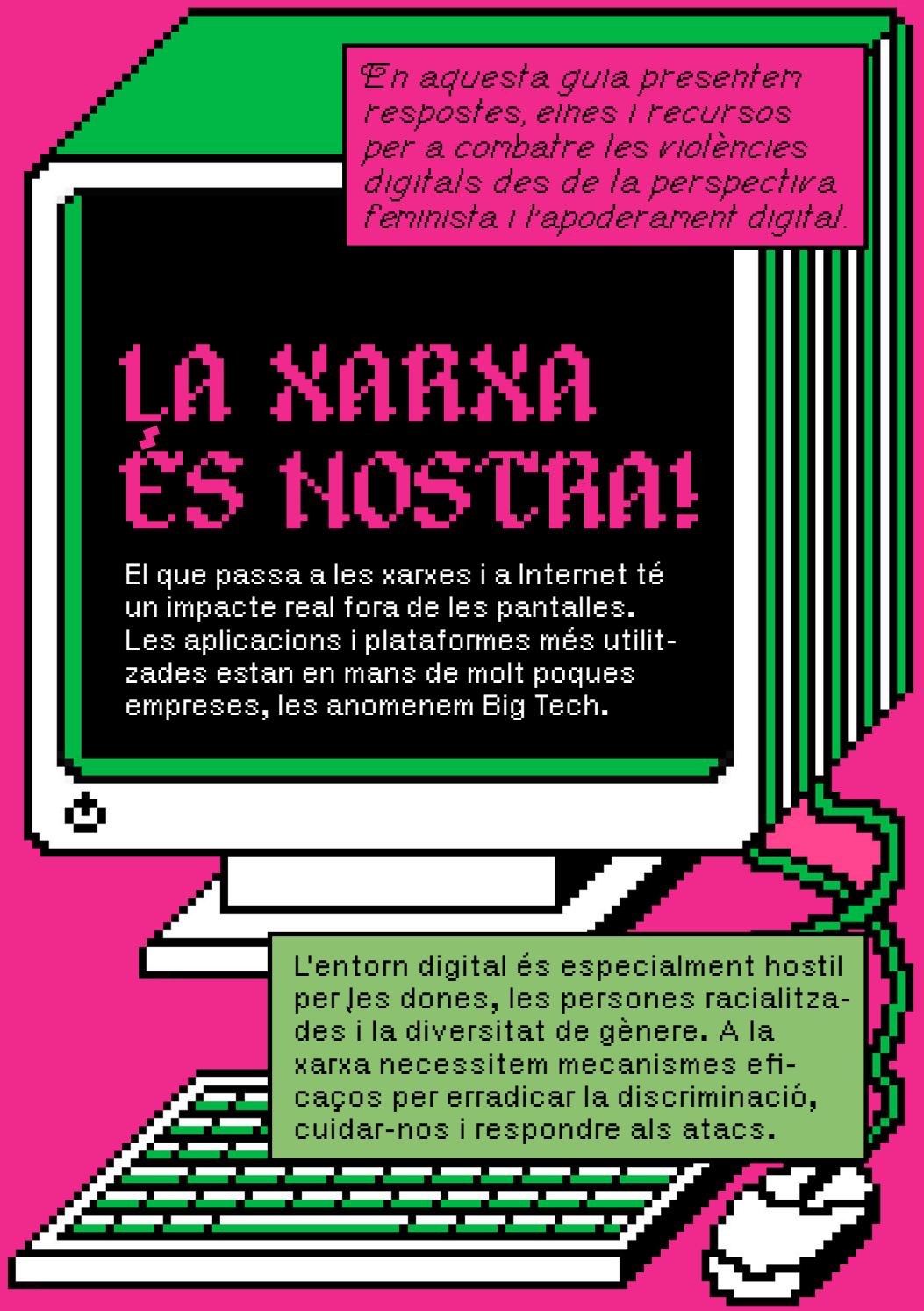

Kit d'autodefensa digital feminista ràpida
Millora la privacitat
Sèxting segur <3
Control i vigilància

En aquesta guia presentem respostes, eines i recursos per a combatre les violències digitals des de la perspectiva feminista i l'apoderament digital.

LA XARXA ÉS NOSTRA!

El que passa a les xarxes i a Internet té un impacte real fora de les pantalles. Les aplicacions i plataformes més utilitzades estan en mans de molt poques empreses, les anomenem Big Tech.



L'entorn digital és especialment hostil per les dones, les persones racialitzades i la diversitat de gènere. A la xarxa necessitem mecanismes eficaços per erradicar la discriminació, cuidar-nos i respondre als atacs.

Reforçar la privacitat és un escut que permet prevenir els atacs!

1/Configura les opcions de privacitat dels navegadors, xarxes socials i sistemes operatius que més utilitzes.

2/Configura els permisos! No totes les apps han de tenir accés a la càmera, micro, ubicació, contactes...

3/Utilitza navegadors de programari lliure, com Mozilla Firefox.

4/Cerca informació per Internet sense rastres amb Startpage.

5/Utilitza extensions per bloquejar anuncis (adblock) i per bloquejar rastrejadors (privacybadger.org/es/)

6/Desactiva la localització sempre que no la necessitis.

Les tecnologies digitals no són neutres. Han estat creades per persones (la majoria homes blancs, occidentals, cisheterosexuals i de classe alta), i en conseqüència no estan lliures de biaixos i desigualtats. La bretxa digital de gènere és molt notoria en qui produeix i decideix sobre tecnologia.

Control i vigilància

Creus que hi ha algú observant-te?

Creus que algú podria estar accedint als teus comptes i dispositius?

Revisa les aplicacions instal·lades als teus dispositius. N'hi ha alguna que no coneguis o que ja no necessitis? Aprofita aquesta oportunitat per fer neteja i desinstal·la-les!

1/ Identifica quins comptes compartits tens amb aquesta persona (plataformes d'streaming, xarxes socials, pàgines de compra en línia...).

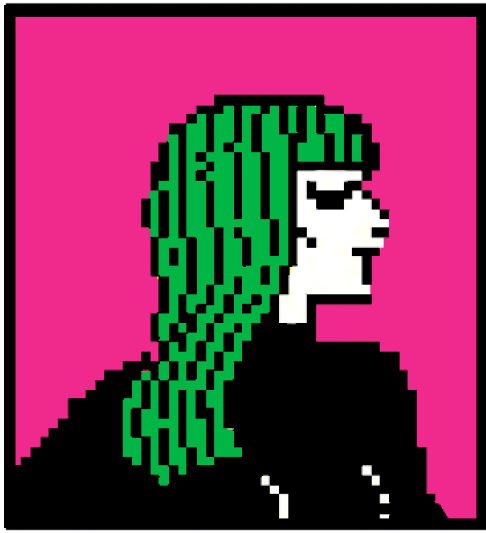
Tanca els teus comptes en qualsevol dispositiu al qual aquesta persona pugui tenir accés i obre'n de nous dels quals en tinguis el control de manera exclusiva.

Revisa la configuració de seguretat i privacitat de les teves xarxes socials i activa, sempre que sigui possible, la verificació en dos passos.

2/ Pensa si algú podria endevinar les teves contrasenyes, o si pot haver tingut accés físic als teus dispositius.

Canvia les contrasenyes dels comptes i els codis d'accés (PIN) que utilitzes per desbloquejar els teus dispositius (mòbils, ordinadors, tauletes). També pensa en els dispositius connectats a casa (com ara el router i els assistents de veu). Recorda fer servir contrasenyes segures!

Contrasenyes segures



La contrasenya ha de ser diferent en cada compte, servei i dispositiu.

Ha de contenir, com a mínim, 16 caràcters. Utilitza majúscules i minúscules, números i caràcters especials.

Ni any de naixement, ni lloc de residència: no usis cap dada que es pugui associar a la teva identitat.

Recorda canviar les teves contrasenyes regularment.

3/ Pregunta't si actualment estàs connectada a cap compte o dispositiu compartit, i desconnecta't si pots (auriculars sense fil, assistents de veu, tauletes...).

Segueix aquests consells i fes

sèxting segur!

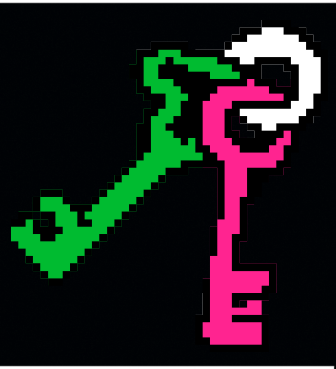
El sèxting consisteix en l'enviament d'imatges de contingut sexual amb el consentiment de totes les persones que hi participen. Aquesta pràctica sexual, com qualsevol altra, es pot donar o no en una relació, i no ha d'implicar cap judici de valor.

1/ Estableix pactes de confidencialitat, i unes regles bàsiques que promoguin la seguretat i que minimitzin els riscos!

2/ Fes-les efímeres: amb el mode autodestrucció o amb un temporitzador perquè desapareguin en X segons.

3/Encripta!

Les fotos xifrades dificulten l'accés a terceres persones. Pots utilitzar hat.sh. Només cal crear les teves claus i usar-les cada vegada que vulguis enviar contingut íntim o arxius privats.



4/ Si vols guardar les teves fotos, fes-ho en una carpeta xifrada! Encripta amb una contrasenya segura amb Cryptomator (sense registre, de codi obert i compatible amb tots els sistemes operatius).

5/ Utilitza canals segurs. No utilitzis WhatsApp, Telegram, Facebook, Instagram, Tinder o aplicacions que mostrin el teu telèfon o que permetin descarregar les imatges compartides amb els altres.

Wire, Confide o Wickr, són canals més segurs que dificulten les captures de pantalla i et permeten saber si algú ho intenta. No requereixen número de telèfon per a fer el registre.

Evita vincular els teus comptes en aquestes aplicacions amb el compte de correu personal o el teu perfil d'IG o FB, ja que així les teves imatges quedaran deslligades de la informació personal més identificativa.

6/ Anonimitza, no mostris parts del teu cos que t'identifiquen (un tatuatge, cicatrius, marques de naixement, etc.). Tampoc incloguis en les imatges part del teu mobiliari o del lloc on estàs.

7/Regla cara/cul

Per a pixelar o difuminar la teva cara, altres parts del cos o el fons de fotos i vídeos pots fer servir Obscuracam i Photo Exif Editor. Evita que s'enviïn metadades (com l'hora i la localització) a través de les teves imatges i vídeos.

Kit d'autodefensa digital feminista ràpida

Aquesta guia d'autodefensa digital feminista és una eina per a totes les persones que busquen protegir-se en línia i garantir la seva seguretat al món digital. Aquesta publicació recull consells pràctics i eines útils per a protegir la privacitat en línia, el control de les nostres imatges íntimes o privades i la prevenció i resposta en casos de control i vigilància.

L'autodefensa digital feminista és una forma de resistència i d'empoderament. En prendre mesures per a protegir la nostra privacitat i seguretat en línia, també desafiem les normes patriarcals i reclamem el nostre dret a existir sense por al món digital.

Esperem que aquesta guia sigui útil per a totes aquelles persones que busquen protegir-se en línia i que juntes construïm un món digital més segur i equitatiu per a tothom.

Tota la informació:
stopviolenciesmasclistesonline.org

Guió: Violeta Zamora Úbeda
Il·lustracions: Clara Iris Ramos
Disseny: Tina Araüna Baró
Continguts: Donestech.net i Fembloc.cat

Ideat i impulsat per: F5 Donestech

Amb la col·laboració de: Ministerio de Igualdad · Secretaría de Estado de Igualdad y contra la Violencia de Género · Delegación del Gobierno contra la Violencia de Género

Ajuntament de Barcelona


Com recuperar comptes robats. Fembloc.
Si vols saber més sobre les metadades:
"¿Qué son los rastros digitales?" a myshadow.org
"¿Por qué me vigilan, si no soy nadie?" Marta Peirano
Moltes aplicacions i plataformes a nivell mundial estan en mans de molt poques empreses, són les GAFAM o BigTech. Saps que fan amb les teves dades?
Revisa els teus rastres a Internet a myshadow.org
Contrasenyes segures. Fembloc.
Si vols eliminar les metadades de les imatges que enmagatzema el vostre telèfon, comparteix-les fent servir Scrambled Exif.
"Hot on your trail" de cironline.org
En el cas de que això et fos igual: "7 coses que sabem què diràs":
Desconecta de la teva ex-parella. Fembloc.
Autodefensa digital feminista
Lluita contra els rastrejadors i millora l'ecosistema web per a proporcionar privadesa a tothom amb Cover your Tracks!
Big Tech
Control i vigilància
Hi ha algú accedint als teus comptes o dispositius? Si alguna cosa no va bé, valora si vols més autonomia en la teva privacitat i desconnecta si et cal!
Sèxting segur
Regla cul/cara:
Si mostres el cul, no mostris la cara, si mostres la cara, no mostris el cul!
Si les imatges o vídeos han estat allotjades a alguna plataforma (xarxa social, servei de missatgeria, pàgina web, etc..) exigeix que siguin retirades immediatament:
Pixela i evita l'enviament de metadates amb:
Obscuracam
Photo Exif Editor
Si algú difon de manera pública o privada les teves fotos i/o vídeos sense el teu consentiment:
Pots fer-ho directament reportant a les plataformes:
Pots fer-ho mitjançant el Canal Prioritari de l'AEPD:
Safer Nudes, una guia sensual de seguretat digital:
Si vols conèixer les lleis que t'amparen: https://acoso.online/espana/
Guarda proves per si vols denunciar, no n'hi ha prou amb les captures de pantalla. Necessitaràs certificar la prova, ja sigui en una empresa de certificació digital o a través d'una notaria.
Aquí t'ho expliquem amb més detall: "Com documentar proves", Fembloc.
LA XARXA ÉS NOSTRA!