¡Fortalecer la privacidad es un escudo que permite prevenir los ataques!

1/Configura las opciones de privacidad de los navegadores, redes sociales y sistemas operativos que más utilices.

2/Configura los permisos! No todas las apps tienen que tener acceso a la cámara, micro, ubicación, contactos...

3/Utiliza navegadores de software libre, como Mozilla Firefox.

4/Busca información por internet sin rastros con Startpage.

5/Usa extensiones para bloquear anuncios (adblock) y para bloquear rastreadores (privacybadger.org/es/)

6/Desactiva la localización siempre que no sea necesaria.

Las tecnologías digitales no son neutrales. Han sido creadas por personas (mayoritariamente hombres blancos, occidentales, cisheterosexuales y de clase alta), y en consecuencia no están libres de sesgos y desigualdades. La brecha digital de género es muy notoria en quien produce y decide sobre la tecnología.

Kit de autodefensa digital feminista rápida

Esta guía de autodefensa digital feminista es una herramienta para todas las personas que busquen protegerse en línea y garantir su seguridad en el mundo digital. Esta publicación recoge consejos prácticos y herramientas útiles para proteger la privacidad en línea, el control de nuestras imágenes íntimas o privadas y la prevención y respuesta en casos de control y vigilancia.

La autodefensa digital feminista es nuestra forma de resistencia y empoderamiento. Tomando medidas para proteger nuestra privacidad y seguridad en línea, también desafiamos las normas patriarcales y reclamamos nuestro derecho a existir sin miedo en el mundo digital.

Esperamos que esta guía sea útil para todas esas personas que busquen protegerse en línea y que juntas construyamos un mundo digital más seguro y equitativo para todo el mundo.

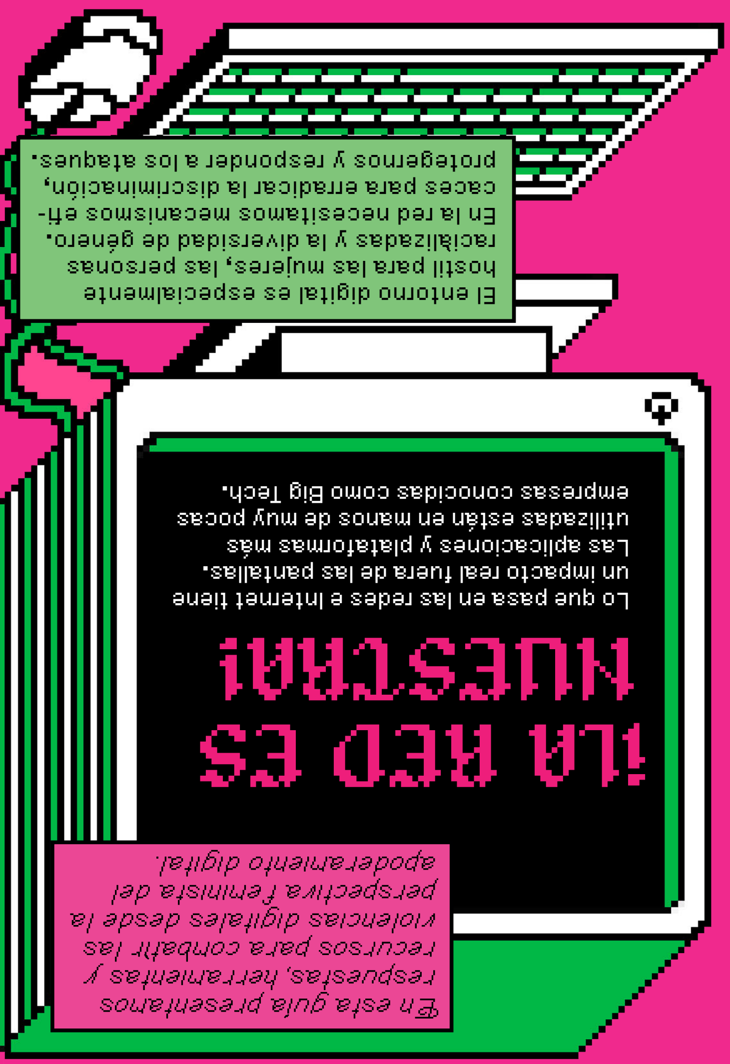
Tota la informació:
@stopvmo / stopviolenciesmasclistesonline.org

Guión: Violeta Zamora Úbeda
Ilustraciones: Clara Iris Ramos
Diseño: Tina Araüna Baró
Contenidos: Donestech.net y Fembloc.cat

Ideado e impulsado por: F5 Donestech

Con la colaboración 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



Control y vigilancia

¿Crees que alguien te observa?

¿Crees que alguien podría estar accediendo a tus cuentas y dispositivos?

Revisa las aplicaciones que tienes instaladas en tus dispositivos. ¿Hay alguna que no conozcas o ya no necesites? ¡Aprovecha la oportunidad para limpiar y desinstalar!

1/ Identifica qué cuentas compartes con esa persona (plataformas de streaming, redes sociales, páginas de compra en línea...)

Cierra tus cuentas en cualquier dispositivo al cual esta persona tenga acceso y abre cuentas nuevas que tengan tu control exclusivo.

Revisa la configuración de seguridad y privacidad de tus redes sociales y activa, siempre que sea posible, la verificación en dos pasos.

2/ Piensa si alguien podría adivinar tus contraseñas, o si puede haber tenido acceso físico a tus dispositivos.

Cambia las contraseñas de las cuentas y los códigos de acceso (PIN) que uses para desbloquear tus dispositivos (móviles, ordenadores, tablets). Piensa también en los dispositivos conectados a la casa (como router y asistentes de voz). ¡Recuerda utilizar contraseñas seguras!

Contraseñas seguras

Las contraseñas tienen que ser diferentes en cada cuenta, servicio y dispositivo.

Tienen que tener, como mínimo, 16 caracteres. Usar mayúsculas y minúsculas, números y caracteres especiales.

Ni año de nacimiento, ni lugar de residencia: no uses ningún dato que pueda relacionarse con tu identidad.

Recuerda cambiar las contraseñas regularmente.

3/ Pregúntate si actualmente estás conectada a cualquier dispositivo compartido y desconéctalo si puedes (auriculares sin cable, asistentes de voz, tablets...).

¡Sigue estos consejos y haz sexting seguro!

Sexting consiste en enviar imágenes de contenido sexual con el consentimiento de todas las personas involucradas. Esta práctica sexual, como todas, se puede dar o no en una relación, y no tiene implicaciones de juicio de valores.

1/ Establece pactos de confidencialidad, y unas reglas que promuevan la seguridad y minimicen los riesgos.

2/ Haz las fotos efímeras: con modo autodestrucción o temporizador para que desaparezcan en X segundos.

3/¡Encripta!

Las fotos cifradas dificultan el acceso a terceras personas. Puedes usar hat.sh. Solo tienes que crear tus llaves y usarlas cada vez que quieras enviar contenido íntimo o archivos privados.

4/ Si quieres guardar tus fotos, hazlo en una carpeta cifrada. Cifra con una contraseña segura usando Cryptomator (sin registro, de código abierto y compatible con todos los sistemas operativos).

5/ Utiliza canales seguros. No uses WhatsApp, Telegram, Facebook, Instagram, Tinder o aplicaciones que muestren tu número de teléfono o permiten descargar las imágenes compartidas con los demás.

Wire, Confide o Wickr, son canales más seguros que dificultan las capturas de pantalla y te permiten saber si alguien lo intenta. No requieren número de teléfono para registrarse.

Evita vincular las cuentas de esas apps a tu correo personal o tu perfil de IG o FB, y así separarlas de la información personal más identificativa.

6/ Anonimiza, no muestres partes de tu cuerpo que te identifiquen (tatuajes, cicatrices, marcas de nacimiento, etc.). Tampoco expongas partes del mobiliario o del sitio donde estás.

7/Regla cara/culo

Para pixelar o difuminar tu cara, otras partes del cuerpo o el fondo de fotos y vídeos puedes usar Obscuracam i Photo Exif Editor. Evita enviar metadatos (como la hora y la localización) a través de tus imágenes y vídeos.

¡Si muestras el culo, no muestres la cara. Si muestras la cara, no muestres el culo!

Cómo recuperar cuentas robadas Fembloc.

Contraseñas seguras. Fembloc.

Desconecta de tu expareja. Fembloc.

Si quieres saber más sobre metadatos:

"¿Qué son los rastros digitales?" a myshadow.org

Si quieres eliminar metadatos de las imágenes almacenadas en tu teléfono, compartelas usando: Scrambled Exif.

"¿Por qué me vigilan, si no soy nadie?" Marta Peirano

Muchas aplicaciones y plataformas a nivel mundial están controladas por muy pocas empresas, las GAFAM o Big Tech. ¿Sabes qué haces con tus datos?

"Hot on your trail" de cironline.org

En caso de que todo esto te dé igual: "7 coses que sabem què diràs":

Revisa tu rastro en internet con myshadow.org

Lucha contra los rastreadores y mejora el ecosistema web para proporcionar privacidad a todos con Cover your Tracks!

Autodefensa digital feminista

Control y vigilancia

¿Hay alguien accediendo a tus cuentas y dispositivos? Si algo no funciona, valora si quieres más autonomía en tu privacidad y desconecta si hace falta!

Big Tech

Sexting seguro

Regla cara/culo: Si muestras el culo, no muestres la cara, si muestras la cara, no muestres el culo!

Si las imágenes o vídeos han sido alojadas en cualquier plataforma (redes sociales, servicios de mensajería, páginas web, etc) exige que sean retiradas inmediatamente:

Puedes hacerlo directamente reportando las plataformas:

Puedes hacerlo mediante el Canal Prioritario del AEPD:

Si alguien difunde de forma pública o privada tu fotos y/o vídeos sin tu consentimiento:

Pixela y evita enviar metadatos con:

Obscuracam

Photo Exif Editor

Safer Nudes, una guía sensual de seguridad digital:

Si quieres conocer las leyes que te amparan: http://acoso.online/espana/

Guarda pruebas por si quieres denunciar, las capturas de pantalla no son suficientes. Necesitarás certificar las pruebas en una empresa de certificación o a través de una notaría. Aquí te lo contamos con más detalles: "Com documentar proves", Fembloc.

LA RED ES TUYA!