Completa guía de seguridad en Internet para mujeres

Sara Levavi-Eilat Investigadora de ciberseguridad

Índice

- Estar segura en Meetup.com
- Cómo evitar la violencia doméstica
- Apps de SOS

¿Alguna vez has sido acosada en la calle? ¿Recibido un mensaje grosero en una aplicación de citas? ¿Un compañero de trabajo te ha hecho un comentario que no estaba bien sobre tu apariencia?

No eres la única.

Con el movimiento #MeToo, es fácil iniciar sesión en Twitter o Facebook y ver la cantidad de mujeres que son víctimas de acoso sexual. Ya sea en persona u online, mujeres de todas partes lo han sufrido de un modo u otro. Y con todos los nuevos modos de comunicarse que ha abierto Internet, **el acoso online es más frecuente que nunca.**
Según un estudio por Pew Research Center, **la mayor parte del abuso en Internet tiene lugar en redes sociales**. Aunque los hombres también están sujetos al acoso en Internet, el cual incluye insultos, burlas y amenzas físicas, el estudio concluyó que en Internet **las mujeres son más del doble de propensas a sufrir acoso sexual que los hombres.**
Además, **más de la mitad de las mujeres de entre 18-29 afirman haber recibido imágenes sexuales explícitas sin su consentimiento.**
Esta cifra está creciendo, y aunque el 70% de las mujeres considera el acoso online un grave problema, no muchas saben cómo evitarlo.

Las mujeres suelen sufrirlo simplemente por ser mujeres. Los ataques suelen ser sexuales o misógenos, y la retórica suele centrarse en sus cuerpos y ser violencia sexual. Esto daña tanto física como emocionalmente, y **las mujeres suelen ser intimidadas y responder con silencio, prefiriendo ignorar el tema a ponerse en un riesgo mayor.**
Sin embargo, existen modos de protegerte.

Esta guía está escrita con la intención de dar poder a las mujeres para que puedan navegar por Internet sin miedo. En ella hablamos de hechos comunes en los que las mujeres están sujetas a acoso en su vida diaria (en redes sociales, en el trabajo, en una cita...) y ofrecemos consejos sobre cómo tomar el control.

Es importante mencionar **que parte de los consejos aquí mostrados recomiendan el anonimato** en lugar de arriesgarse a ser un objetivo. Aunque podría parecer que es opuesto a animarles a expresarse, creemos que todas las mujeres deberían elegir por sí mismas.
Nuestro trabajo es ofrecerte las herramientas que necesitas para hacerlo.

Esperamos que esta guía anime a mujeres de todas partes a **defenderse y protegerse, y a plantar cara frente al acoso sexual tanto en Internet como fuera.**

El acoso en las redes sociales

La mayor parte del acoso online tiene lugar en redes sociales, cosa que tiene sentido dado el tiempo que pasamos hoy en día en estas plataformas. Redes sociales amplias combinadas con anonimato dan lugar a una realidad en la que cualquier cosa que publiques, tuitees o compartas te expone a abuso pontencial.

A continuación profundizamos en las plataformas de redes sociales más populares y te mostramos cómo protegerte de pesados, trolls y *stalkers* (acosadores).

Twitter

Debido a su naturaleza pública, **Twitter es una de las redes sociales en las que más tiene lugar el acoso.** Y no hablamos sólo de celebridades y personalidades públicas; existe infinidad de historias de personas corrientes que han sido atacadas, a menudo simplemente por expresar su opinión respecto a cuestiones políticas o feministas.
De hecho, Amnistía Internacional publicó un informe criticando a Twitter por no tomar las medidas adecuadas respecto al acoso a mujeres. El estudio muestra a docenas de mujeres que relatan el abuso que sufrieron en Twitter, muchas citando respuestas inaceptables de la red social tras haber informado de los incidentes.
A menudo **el resultado suele ser el silencio, optando las mujeres por simplemente no plantar cara por miedo a recibir aún más acoso**. Muchas mujeres acaban censurándose a sí mismas o abandonando la plataforma; para algunas personas, especialmente periodistas y activistas, **esto puede ir en detrimento de sus carreras.**

Las cosas se alcanzaron un punto álgido en octubre de 2017 cuando **una serie de alegaciones de asalto sexual de personas famosas apareció bajo el hashtag viral #MeToo.** El hashtag, utilizado por mujeres para identificarse a sí mismas como víctimas de acoso y/o asalto sexual, circuló por todo Twitter en cuestión de horas y dejó muy claro lo frecuente que son estos incidentes.
Poco tiempo después, la cuenta de la actriz Rose McGower fue suspendida temporalmente tras haber tuiteado una serie de alegaciones en contra del depredador sexual Harvey Weinstein y varios peces gordos de Hollywood que ella afirmaba que se lo permitían. La violación del servicio citó que uno de sus tuits incluía un número de teléfono privado.

Pero con tantos tuits abusivos contra las mujeres que no acaban en cuentas suspendidas, muchas mujeres tuvieron suficiente. La ira resultante dio lugar al **hashtag #WomenBoycottTwitter, el cual animaba a las mujeres a boicotear la plataforma durante un día en señal de solidaridad.**
Twitter afirma haber mejorado su sistema de tratamiento de informes de abusos, pero el problema sigue existiendo; no obstante, existen medidas que las mujeres pueden tomar para reducir las posibilidades de ser objetivo de acoso.

5 Formas de protegerte en Twitter

1.Utiliza varios perfiles

Las mujeres cuya carrera depende de mantener un perfil público pueden encontrar útil utilizar varias cuentas.

Al contrario que para otras plataformas de redes sociales, para Twitter esto es perfectamente aceptable según sus términos del servicio. De hecho, las empresas suelen hacerlo con el fin de dirigirse a audiencias diferentes.

Te interesa crear un perfil personal y uno público.
Tu perfil personal debería tener los ajustes de privacidad más estrictos. Dado que por defecto un perfil de Twitter es público, tendrás que establecerlo manualmente.
Normalmente, cuando tus tuits son públicos, cualquiera puede verlos - incluso las personas que ni siquiera tienen cuenta en Twitter. Sin embargo, **cuando tus tuits están "protegidos", sólo los seguidores que hayas autorizado**

podrán verlos y nadie podrá retuitearlos. Asegúrate de sólo permitir que te sigan a aquellas personas que conozcas y en quienes confíes.

Cómo cambiar tus ajustes de privacidad en Twitter:
Haz clic en tu perfil y ve a Settings y Privacy>Privacy and safety>Protect your Tweets.

Hacer este cambio también protege retroactivamente tus tuits anteriores. Dicho esto, cabe mencionar que dado que Twitter no tiene control sobre los motores de búsqueda externos, **los tuits anteriores a este ajuste pueden seguir siendo visibles en Internet.** Por tanto, si quieres anonimato de verdad, deberías abrirte un nuevo perfil personal y proteger tus tuits desde el principio. También merece mención el hecho de que tus respuestas a otros tuits y menciones también estarán protegidas, por lo que sólo serán visibles para tus seguidores autorizados. Esto obviamente hace que sea **mucho más difícil participar en el tipo de discusiones y debates públicos por los que Twitter es famoso**, por lo que tendrás que decidir si tener un perfil privado merece la pena para ti.

Para crear una cuenta adicional, haz clic en el icono de tu perfil. A continuación haz clic en el signo de intercalación junto a tu nombre, donde tendrás la opción de crear una nueva cuenta.

Este segundo perfil será tu perfil público. Si utilizas Twitter con fines laborales, **este será el que te represente profesionalmente**, así que asegúrate de no tuitear de ninguna cosa demasiado personal.
Otra opción consiste simplemente en mantener anónimo este perfil. Eso significa **no utilizar tu nombre real ni fotos de ti, ni tuitear nada que pueda ser utilizado para descubrir dónde vives o trabajas.**
Ten en cuenta que **no puedes tener ambas cuentas abiertas en el mismo navegador al mismo tiempo.** Si quieres tener ambas abiertas, puedes utilizar navegadores diferentes o utilizar la app soportada por Twitter, TweetDeck.
2.Bloquea a todo aquel que acose y abuse de otros e informa de ellos
Si recibes un tuit abusivo, puedes bloquear a la persona que lo envió.

Cómo bloquear a alguien en Twitter:

Haz clic en el signo de intercalación de la esquina superior derecha del tuit y elige "block the user" (bloquear al usuario).

Uno de los problemas del bloqueo es que es muy fácil para los usuarios crearse cuentas nuevas, conocidas como "sock puppets", que aún no hayan sido identificadas.

Una forma de lidiar con esto es con la app Block Together. Block Together bloqueará automáticamente a cualquier cuenta que intente seguirte que tenga menos de 7 días de actividad, menos de 15 seguidores o que tus seguidores hayan bloqueado. Es muy útil cuando estás siendo atacada por numerosos trolls.

Además de bloquear a los usuarios, también puedes informar de incidentes abusivos a Twitter.

Cómo denunciar a alguien en Twitter:
Simplemente haz clic en el signo de intercalación de la esquina superior derecha del tuit o de la cuenta, selecciona *report* (denunciar) y sigue las instrucciones.

Por desgracia, aunque el acuerdo de usuario de Twitter no permite el acoso, la plataforma es conocida por no tomar todas las medidas que podría para limitar la mala conducta.

De hecho, según un análisis de la ONG Women Action and the Media (WAM), **el 67% de las mujeres que denunciaron abusos afirmó que ya había informado a Twitter al menos una vez en el pasado.**
Aún así, sigue mereciendo la pena denunciar tuits y cuentas abusivas dado lo fácil que es hacerlo.

Twitter no ofrece actualmente una forma de comprobar el estado de las denuncias de abuso. Dicho esto, a fecha de enero de 2018, Twitter te informa de su evaluación una vez la denuncia ha sido procesada.

3.No etiquetes ubicaciones
El *geotagging* es cuando **tu publicación incluye la ubicación desde la que fue enviada**. Para mantenerte a salvo de *doxing* y *stalking*, lo mejor es no

utilizar la función de etiquetar tu ubicación. Afortunadamente, etiquetar la ubicación requiere que optes voluntariamente a ello, por lo que por defecto no se muestra.
Cuando redactas un tuit, verás un botón de ubicación en la parte inferior (parece un pin boca abajo). Si lo pulsas tendrás la opción de añadir tu ubicación a tu tuit.

No lo hagas.

Ten también en cuenta que **podrías revelar tu ubicación incluso sin etiquetarla simplemente mencionando dónde te encuentras.** Sabemos que es divertido contar a la gente en un momento determinado que estás disfrutando de una nueva galería o pasándolo en grande durante una noche de fiesta, pero a veces es mejor esperar y publicar más tarde, cuando ya no estés allí, lo bien que lo PASASTE (en pasado).

4.Evita el *doxing*

El *doxing* es la forma más extrema de acoso en Internet. *Doxing* es cuando la información personal de alguien, como su dirección, número de teléfono, lugar de trabajo, información bancaria o incluso información de sus familiares, se publica online como **llamada a que otros les acosen.**
Puede que hayas oído el término por primera vez en 2014 con los informes de #gamergate. Gamergate fue un movimiento impulsado por el furioso ex de la desarrolladora de juegos Zoe Quinn, quien escribió una entrada de blog acusándola de haberse acostado con un periodista a cambio de un análisis positivo de su juego.

A pesar del hecho de que nunca se escribió tal análisis, **una gran cantidad de personas, principalmente gamers varones y blancos, tomaron la publicación como una llamada al acoso al entender que no sólo su pasatiempo favorito sino su libertad de expresión y masculinidad estaban bajo ataque** por los llamados "guerreros de justicia social".
¿El resultado?

No sólo Quinn sino las mujeres que la defendieron, incluyendo la desarrolladora de videojuegos Brianna Wu y la periodista Anita Sarkeesian, recibieron ataques incensantes por parte de trolls de Internet que las inundaron

de **una oleada diaria de amenazas de muerte y de violación**, principalmente vía Twitter.

Ellas también sufrieron *doxing*.

Los efectos en la industria de los videojuegos fueron escalofriantes, **y las mujeres siguen tomando precauciones extra por miedo a convertirse en objetivos.**

Por ejemplo, Tessa, una analista de inteligencia cuyo trabajo requiere que interactúe con gamers, **conoce a varias mujeres en la industria que han sufrido acoso**, y a menudo sufre comportamiento irrespetuoso ella misma. Dado que muchas interacciones tienen lugar a través de Skype, es imposible ocultar el hecho de que es mujer. Aun así, Tessa **toma medidas serias para ocultar que trabaja directamente para la industria de los videojuegos** y no revela ninguna información personal sobre ella como su nombre real o dónde vive.

Claro está, las mujeres de la industria de los videojuegos no son las únicas en peligro de sufrir *doxing*. El clima político incendiario de hoy ha resultado en que **muchos han perdido sus trabajos y han tenido que dejar sus hogares tras haber sufrido *doxing* por haber asistido a concentraciones de derecha alternativa.**

Pero no tienes que participar en actividades políticas controvertidas para sufrir *doxing*. **Algunos han sido víctimas de *doxing* "accidentalmente".** Por ejemplo, tras los atentados de la Maratón de Boston, un estudiante de la Brown University sufrió *doxing* al ser identificado por error como el autor; asimismo, tras la concentración de Charlottesville Unite the Right, un ingeniero de la Universidad de Arkansas sufrió *doxing* al ser identificado erróneamente como participante.

4 Formas de evitar sufrir *doxing*

1. **Búscate en Google.** Una búsqueda simple te mostrará qué tipo de información existe por la red sobre ti. Si esta incluye información que puede utilizarse para identificarte, mira a ver si puedes quitarla de Internet. Los perfiles de redes sociales tienen ajustes de privacidad que pueden resetearse fácilmente, y muchas webs como las *White Pages* (páginas blancas) te dan la opción de no mostrarte. Por desgracia, podría ser imposible eliminar toda tu

información de Internet, pero con una búsqueda por lo menos podrás ver qué pueden encontrar otros sobre ti.

2. **Suscríbete a un servicio que te elimine de webs "broker" de datos:** Si encuentras tu información en una web como *White Pages*, lo más probable sea que también aparezcas en otros directorios de Internet, muchos de los cuales no serán fáciles de encontrar. Por tanto, si tienes motivos para creer que puedes ser objetivo de *doxing*, considera pagar por un servicio como PrivacyDuck o DeleteMe.
3. **Comprueba que tu cuenta de email no haya estado involucrada en una fuga de información;** también puedes utilitar la herramienta https://haveibeenpwned.com/ para ver si tu dirección de email y contraseña pueden haber estado expuestas a una de las fugas a gran escala que han ocurrido en los últimos años. Si ha sido así, cambia tu contraseña y considera añadir autenticación de dos factores a tu cuenta. Esto ofrecerá una capa de seguridad adicional al requerir información adicional (aparte de tu contraseña) para iniciar sesión.
4. **Utiliza una VPN:** Utilizando una VPN o red privada virtual puedes cifrar toda tu actividad de Internet para protegerte de hackers. Las VPNs funcionan desviando tus datos de internet a través de un túnel a un servidor de terceros, evitando que se muestre tu dirección IP (y ubicación real). Aquí tienes algunas VPNs que recomendamos.

5.Evita que hackers se hagan con tu cuenta de Twitter

Desde el antiguo presidente Obama a Britney Spears, durante los años la cuenta de Twitter de múltiples celebridades ha sido hackeada por individuos que quisieron dañar sus reputaciones y causar caos. Dicho esto, a muchas personas corrientes también le han hackeado su cuenta con una frecuencia alarmante.

4 Formas de evitar que hackeen tu cuenta de Twitter

1. **Crea una contraseña robusta:** Suena obvio, pero te sorprendería la cantidad de personas que utilizan contraseñas débiles y fáciles de averiguar (o tal vez no). Para crear una contraseña robusta, asegúrate de que es larga, tiene mayúsculas y mínusculas, e incluye números y símbolos.

2. **Habilita la verificación de inicio de sesión:** Esto proporciona una capa de seguridad adicional a la hora de iniciar sesión. En lugar de simplemente tener que introducir tu contraseña, también tendrás que introducir un código que Twitter envía a tu dispositivo móvil. Para habilitarla, haz clic en el icono de tu perfil>Account>Security>Login verification. En la misma pestaña también puedes activar que se solicite información personal para cambiar la contraseña.
3. **Desconfía de cualquier app de terceros que requiera acceso a tu cuenta:** Si tienes dudas sobre si una app es legítima o no, no la instales. Para ver qué apps tienen acceso a tu cuenta de Twitter, haz clic en el icono de tu perfil y ve a Apps. Para eliminar una app, haz clic en "Revoke access".
4. **Ten cuidado con las URLs acortadas:** Debido al límite de 280 caracteres de Twitter, tiene sentido que muchas personas utilicen URLs acortadas para los enlaces al exterior de la plataforma. El problema es que es difícil saber el destino de estos enlaces y si llevan a una web maliciosa. Por tanto, te interesa ser muy cauta; no hagas clic en enlaces que veas publicados en tuits de otras personas.

Una buena indicación de que alguien ha estado manipulando tu cuenta es si descubres actividad inusual, como seguir a personas nuevas o envío de tuits que no recuerdas. Si ves algo así, lo primero que tienes que hacer es cambiar tu contraseña. También deberás informar de ello a Twitter - puedes hacerlo acudiendo a su centro de asistencia y enviando un ticket.

También deberías enviar un ticket si **alguien ha creado una cuenta nueva con tu nombre**. Para ayudar a Twitter a saber que tú realmente eres tú, tendrás la opción de subir una imagen de un documento identificativo emitido por el gobierno u otra forma de identificación.

Facebook

Rachel no se lo pensó dos veces cuando hizo clic afirmando estar interesada en acudir a un concierto de uno de sus grupos favoritos durante una sesión habitual en Facebook. Se emocionó muchísimo cuando uno de los miembros del grupo le pidió amistad y **empezó a enviarle mensajes privados.**
La conversación empezó como algo casual, pero pronto él empezó a hablar de su foto de perfil, diciéndole que le gustaba que a ella no le importara que se le viera el pezón.

Espera... ¿Qué?

En su foto de perfil no se le veía el pezón. ¿O sí? Rachel **llevaba dos años con esa foto de perfil** y nadie nunca le había dicho nada. Rachel examinó cuidadosamente la foto. ¿Tal vez lo que vio fue una sombra de su top?
Le dijo que se equivocaba e intentó explicar la sombra, otorgándole el beneficio de la duda. Pero él seguía insistiendo y **pronto comenzó a pedir fotos de desnudos.**
Mirando atrás, Rachel sabía que debió haber terminado la conversación ahí y bloquearle, pero en aquel momento sólo parecía un malentendido. Al fin y al cabo era una foto provocativa, ¿no? **Tal vez debería haber esperado este tipo de reacción.**

Ella intentó dirigir la conversación una vez más hacia el tema musical y del concierto, pero él era como un perro con su hueso y no dejó de pedir más fotos. Finalmente ella dejó de contestar, pero se sintió extraña durante unos días, **preguntándose qué habría estado pensando la gente de ella todo ese tiempo.**

La historia de Rachel no es tan sorprendente: no es violenta ni se violó a nadie. Más bien suena como un encuentro habitual en redes sociales. No obstante, es la banalidad de la situación lo que hace que sea tan triste. **Todos los dias las mujeres sufren peticiones extrañas de desconocidos y acaban preguntándose qué hicieron para ocasionarlo**, y tienen que seguir adelante sabiendo que aunque sólo están intentando vivir sus vidas, otros las miran como objetos.

Los estudios muestran que **el impacto de este tipo de interacciones es especialmente severo para las mujeres; es más del doble de probable que las mujeres describan su última experiencia de acoso como MUY traumática en comparación con los hombres.**

Y pedir fotos subidas de tono sólo es una de las miles de caras del acoso por Facebook. **Las mujeres a menudo reciben mensajes abusivos y fotos de penes no solicitadas**, y no es poco común ser etiquetadas en **fotos degradantes** o incluso que se creen perfiles falsos con sus nombres y fotos.

5 Formas de protegerte en Facebook

1.Controla exactamente quién ve cada cosa

En los últimos años, Facebook ha puesto mucho de su parte por actualizar la plataforma y permitirte personalizar estas opciones, incluso **permitiéndote ocultar tu información de personas determinadas.**

Cómo controlar lo que la gente ve en tu perfil de Facebook:

En tu ordenador, haz clic en el signo de intercalación de la esquina superior derecha de la página y selecciona configuración. En el panel de la izquierda, haz clic en Privacidad. Desde ahí podrás gestionar exactamente quién puede ver tus publicaciones y cómo pueden los demás contactar contigo.

A continuación, ve a Historias y Etiquetas. Esto te permite controlar quién puede publicar en tu muro y quién puede ver las publicaciones en las que estás

etiquetada. Aquí también puedes cambiar tus ajustes para que **analices y apruebes cualquier etiqueta antes de que se haga efectiva.**

Otra herramienta útil que puedes usar es la que **te permite ver exactamente lo que ven los demás cuando visitan tu perfil.** De ese modo puedes estar segura de que ciertas personas no verán información personal si no quieres que lo hagan.

2.No permitas que acosadores potenciales sepan dónde estás

Como mencionamos arriba, etiquetar tu ubicación en publicaciones y fotos puede ser un modo mediante el cual te pueden encontrar los acosadores. En Facebook, cuando escribes una publicación tienes la opción de añadir tu ubicación actual para que tus amigos la vean. Es mejor no utilizar esta función. No obstante, **las etiquetas de lugar no son la única forma de la que se te puede encontrar.**

¿Alguna vez te has dado cuenta de que, después de acudir una tienda determinada, de repente empiezas a ver anuncios de ella en Facebook? ¿O de que conoces a alguien en una fiesta y al día siguiente Facebook te muestra a esa persona en sugerencias de amistad?

El modo que tiene Facebook para saber estas cosas es que si tienes instalada su app para móviles y llevas tu dispositivo contigo por ahí (como hacemos la mayoría), **Facebook conoce tu ubicación en todo momento.**

Si quieres, puedes ver exactamente dónde te ha estado rastreando Facebook. Esta información no es pública, así que no te preocupes de que otros usuarios de Facebook puedan usarla para saber dónde estás.

Cómo ver dónde ha rastreado Facebook tu ubicación:

Ve a configuración. Haz clic en ubicación en el panel de la izquierda, y luego haz clic en ver historial de ubicaciones. Aparecerá un mapa junto con un **registro que muestra tu ubicación durante todo el tiempo que has tenido activados los ajustes de ubicación. Para algunos, ese registro se remonta a años atrás.**

Cómo borrar tu historial de ubicaciones:

Haz clic en las tres barras de la esquina superior derecha de la pantalla (o inferior derecha si usas un iPhone). Selecciona configuración de la cuenta>

ubicación. Pulsa para desactivar Servicios de ubicación, y debajo desplázate a la izquierda para desactivar Historial de ubicaciones.

Para borrar todo tu historial pasado, haz clic en Ver tu historial de ubicaciones y selecciona los tres puntos de la esquina superior derecha. Ahí tendrás la opción de borrar el historial completo. Tendrás que introducir tu contraseña para hacerlo (cambiar tu contraseña es otro modo genial de evitar que otros accedan a tu ubicación o a tu cuenta de Facebook en general).

3.Bloquea a los acosadores y pon a los individuos molestos en tu lista de personas restringidas.

Otra opción útil de esta página es la de **poner a ciertas personas en una lista de personas restringidas.** Estando en ella, se mostrarán como amigos pero sólo podrán ver la información que compartas públicamente. Esto especialmente útil si quieres evitar la confrontación con alguien que temes que intentará intimidarte o aprovecharse de ti.

Aunque es fácil de decir que deberías ser directa y poder decirle a alguien a la cara que no quieres que vea las cosas personales que publicas, **todos sabemos lo rápido que se puede descontrolar una situación cuando un tipo de hombre determinado se siente rechazado.**

Por tanto, la próxima vez que conozcas a un hombre en un bar que *insista* en hacerse tu amigo en facebook *y* se quede mirando cómo aceptas su solicitud de amistad, escaquéate al baño un minuto y ponlo en tu lista de personas restringidas.

4.Denuncia las cuentas falsas

Aunque va en contra de sus términos de servicio, Facebook estima que actualmente existen **66 millones de cuentas falsas en la plataforma.** Un motivo que tiene la gente para crear cuentas falsas es hacerse pasar por otros usuarios. Al utilizar tus fotos y nombre real, **un impostor es capaz de hacerse amigo de personas de tu círculo social y después publicar contenido dañino y falso sobre ti.**

Si descubres una cuenta falsa que utiliza tus fotos e información personal, puedes denunciarla a Facebook y el servicio la cerrará.

Cómo denunciar un perfil falso en Facebook:

Ve al perfil falso, haz clic en los tres puntos de la esquina superior derecha de la página y selecciona Report (denunciar) > Report this profile > They're pretending to be me or someone I know.

Dicho esto, **un impostor inteligente te bloqueará para que no puedas ver la cuenta falsa.** Si lo hace, haz que un amigo denuncie la cuenta por ti.

Facebook se esfuerza por ser proactivo en la identificación de cuentas impostoras, y recientemente ha anunciado una iniciativa que utiliza **software de reconocimiento facial para marcar fotos de perfiles nuevos en las que aparezcan usuarios existentes.**

Cabe mencionar, no obstante, que el software sólo escaneará las cuentas nuevas, por lo que **si ya existe un perfil falso tuyo, a menos que tú o alguien que conozcas lo encuentre y lo denuncie, no hay forma de descubrirlo.** Además, las únicas fotos que se escanearán en busca de tu cara son aquellas dentro de tu red de amistades o amistades de amistades - en lugar de todos los usuarios de la plataforma.

Esto nos hace pensar sobre la efectividad real de esta táctica, especialmente considerando cómo de comunes **son los perfiles falsos, no con fines de venganza personal sino para estafar dinero a la gente o promocionar productos o agendas políticas.** Específicamente, encuestas sobre las elecciones presidenciales de EE.UU. de 2016 revelaron toda una industria de actividad en Facebook generada artificialmente para influenciar la opinión pública.

En estos casos, un modo simple de protegerte consiste en **hacer privadas casi todas tus fotos.** Si la persona que crea la cuenta falsa no tiene acceso a tus fotos, serás un objetivo mucho menos atractivo de cara a la suplantación de identidad.

5.Evita el "porno de venganza"

En los últimos años, el *sexting* se ha convertido en un modo habitual de flirteo. De hecho, según un estudio el 88% de los adultos encuestados afirmó haber enviado mensajes o imágenes sexualmente explícitas al menos una vez. Esto no es necesariamente malo; el mismo estudió mostró una **correlación entre el *sexting* y la satisfacción sexual**, y descubrió que a las mujeres les gusta especialmente.

Dicho esto, enviar fotos reveladoras puede ser arriesgado si caen en manos equivocadas. Demasiadas mujeres han sido víctimas de campañas de humillación, en las cuales **algún ex en busca de venganza enviaba imágenes íntimas a sus familiares, amigos o incluso jefes.**
Afortunadamente, Facebook ya tiene un **algoritmo que identifica y elimina las imágenes explícitas.** Sin embargo, en noviembre de 2017 Facebook también anunció un nuevo y novedoso modo de hacer frente a esta epidemia del "porno de venganza". La idea, que se está probando primero en Australia, va a generar inquietudes.
Básicamente, si sospechas que se puede subir una imagen determinada a Facebook sin tu consentimiento, **rellenas un formulario explicando el asunto y envías la imagen por ti misma utilizando la app Facebook Messenger.** Despúes de estudiar el informe y la foto, Facebook la borrará. Dado que Facebook es propietario de Instagram, esto evitará que la imagen también se difunda en dicha plataforma.

Este enfoque tiene algunos problemas. Primero, tienes que saber que las imágenes están circulando por ahí (a veces se sacan fotos y vídeos sin el conocimiento ni consentimiento de la víctima). En segundo lugar, tienes que tener las imágenes (podría no ser el caso si se sacaron con la cámara de otra persona). Por último, **tienes que confiar en Facebook y aceptar que una persona real de la compañía verá las imágenes que tú explícitamente no quieres que circulen por ahí para consumo público.**
Para muchos, saber que algún técnico *friki* tiene acceso a sus fotos íntimas, incluso durante poco tiempo, contribuirá al trauma y la ansiedad que ya están sufriendo.

Instagram y SnapChat

Las fotos no fueron lo único que cambió cuando Instagram se lanzó en 2010 y SnapChat en 2012. El acoso en Internet también lo hizo.

Al hacer tus fotos públicas, **cualquiera puede comentar en ellas.** Aunque es difícil entender por qué dedicaría alguien su tiempo a ser un troll, existen personas que se pasan el día buscando fotos para insultar a otras personas. Comentarios humillantes públicos y DMs (la versión de Instagram de los mensajes privados) con lenguage vulgar y explícito plagan millones de cuentas cada día.

Además de al *trolling*, **muchas mujeres son susceptibles al "porno de venganza", fotos de penes, y otra fotografía explícita no consentida.**

Con diferentes técnicas puedes contraatacar e incluso evitar que se ocurran algunos de estos escenarios. Sí, los *trolls* y los imbéciles encontrarán un modo de atacarte si son suficientemente persistentes, pero tomando las siguientes medidas puedes hacérselo mucho más difícil.

3 Formas de protegerte en Instagram y SnapChat

1.Comprueba tus imágenes en busca de información que pueda identificarte

Hay varias cosas simples que puedes hacer para que tus fotos y tu cuenta sean algo más seguras.

Digamos que estás en un restaurante y quieres publicar una foto de tu plato en Instagram. Es normal etiquetar al restaurante porque aumenta el tráfico; no obstante, **al etiquetar el restaurante te sitúas en su ubicación.**
Ahora cualquier acosador sabe dónde estás.

De forma similar, si activas los ajustes de *geolocation* o ubicación geográfica, tu riesgo es aún mayor. Si haces un *snap* de una foto de tu *caramel latte* de Starbucks puedes estar en cualquiera de los 27.339 Starbucks de todo el mundo, pero **si tienes activada la ubicación geográfica todo aquel que vea tu foto sabrá exactamente dónde te encuentras.**
Snapchat reveló una nueva característica en junio de 2017 llamada SnapMap, la cual muestra las ubicaciones de todos tus amigos en un mapa. Aunque podría parecer inocente, en realidad permite a otros rastrearte constantemente. **Desactiva la característica SnapMap y te ahorrarás un montón de situaciones potencialmente feas.**

2.No utilices tu información real

Cuando te registras en SnapChat, la plataforma requiere que proporciones tu fecha de nacimiento, número de teléfono y dirección de email - algo bastante estándar en las aplicaciones de redes sociales. Sin embargo, **cualquiera con unos mínimos conocimientos técnicos puede encontrar esa información a través de tu cuenta de SnapChat.** Esto hace que sea extremadamente fácil que alguien lleve su acoso al email, WhatsApp y muchas otras plataformas.

La mejor forma de proteger tu información es ocultándola. **Crea una dirección de email nueva para registrarte.** Utiliza también un número de teléfono falso (como el que le darías en una discoteca a un pesado que no quieres que te llame) e invéntate una fecha de nacimiento diferente.

Otro truco sencillo que hace que sea mucho más difícil para los trolls acceder a ti consiste en **cambiar tu cuenta de pública a privada.** Esto se aplica tanto para Instagram como para SnapChat. Cambiar tu cuenta a privada limitará las personas que pueden ver tus publicaciones a amigos, familiares o cualquiera que tú apruebes.

Cómo convertir tu cuenta en Privada en SnapChat:

Ve a Settings>View My Story>My Friends/Custom. En Settings puedes cambiar quién puede ponerse en contacto contigo y quién puede ver tu ubicación.

Cómo convertir tu cuenta en Privada en Instagram:

Ve a Settings>Private Account (desliza a la derecha para activar).

Si necesitas utilizar estas apps para promocionar un producto, tu empresa o a ti misma, te recomendamos crearte una cuenta diferente. Así tus fotos personales no se mezclarán con tus fotos públicas.

Dicho esto, incluso si tomas todas estas medidas, es posible que se cuelen comentarios groseros. En ese caso, necesitas saber cómo...

3.Bloquear pesados - Tanto Instagram como SnapChat tienen la opción de bloquear a otros usuarios. Mediante esta técnica puedes bloquear a un usuario y después borrar sus comentarios

Cómo bloquear a alguien en Instagram:

Selecciona la persona a la que quieras bloquear, pulsa los tres puntos de la esquina superior derecha y después pulsa block (bloquear).

Cómo bloquear a alguien en SnapChat:
Selecciona la persona a la que quieras bloquear, pulsa las tres líneas de la esquina superior derecha y después pulsa block.

Acoso en el trabajo

Por desgracia, el acoso también es común en el entorno laboral. Según un estudio, **una de cada tres mujeres de edad entre 18-34 ha sufrido acoso en el trabajo.** 25% de esas mujeres fueron acosadas por mensajes de texto o emails, y el 71% de ellas no denunció el hecho.
Sólo podemos especular sobre los motivos, pero uno podría ser que el acoso sexual no está claramente definido.

Sin embargo, algunos ejemplos de acoso sexual incluyen:

1.Compartir imágenes o vídeos sexualmente inapropiados.

2.Enviar cartas, textos o emails con contenido sugerente.

3.Contar chistes obscenos o anécdotas sexuales.

Pero ¡hasta estas cosas son ambiguas! Si alguien envía una foto de un pene, eso claramente es acoso sexual, pero en el caso de un comentario podría tratarse de malinterpretación.

Por tanto, ¿cómo saber si podría tratarse de acoso sexual?

Para cuando no estés segura, piensa en cómo te sientes. **¿Te hizo sentir incómoda el comentario?** ¿Hay algo raro detrás de él? Si fue así, lo más probable sea que exista una intención subyacente que podría considerarse acoso sexual.

Acoso sexual en el trabajo

El acoso sexual tiene muchas formas, y cuando es en Internet suele ser aún menos obvio - pero ocurre. Si te encuentras en una situación profesional en la que te sientes incómoda, deberías empezar a grabarla inmediatamente. **A menudo, los incidentes mayores surgen a raíz de una serie de incidentes menores, los cuales si no se documentan adecuadamente no serán útiles como pruebas.**

Incluso si no estás segura de si un encuentro cuenta como acoso o no, es mejor tratarlo como tal por si la situación empeora y eventualmente decides tomar acción.

Cómo denunciar acoso en el trabajo

1.Documenta todos los encuentros

Cualquier comentario, email inapropiado u otra correspondencia que pueda clasificarse como acoso debe ser registrado y almacenado en algún lugar al que sólo tú tengas acceso (no en el Google Drive de la empresa, por ejemplo). Puede ser que un comentario haya sido involuntario, pero si se repite podrás ir documentando el caso.

Si un encuentro implica algo dicho verbalmente o un contacto inapropiado, escríbete a ti misma lo antes posible un email (desde tu cuenta personal) describiendo el incidente con la mayor precisión posible. Incluye la fecha, la hora y la ubicación del incidente.

2.Monitoriza la situación

Saca capturas de pantalla, anota las fechas y las horas, guarda los emails y mantén un archivo de todo lo que te haga sentir incómoda.

3.Denúncialo

Una vez tengas pruebas, es momento de presentar una denuncia. Aunque a veces es incómodo, denunciar acoso en la oficina es una de las formas más productivas de detenerlo.

Envía tus pruebas al departamento de RR.HH., el cual con suerte tendrá una política sobre cómo proceder. Si tu empresa no tiene departamento de recursos humanos, deberás construir un email muy detallado y enviarlo al departamento de gestión o a tu jefe (siempre y cuando no sea la persona que te acosa).

Cómo escribir un email que denuncia acoso sexual:

Puede ser desalentador crear ese primer email, por lo que hemos incluido una plantilla que puedes utilizar.

Asunto: Queja oficial sobre acoso sexual

Estimados [RR.HH.] y [jefe]:

Les escribo este email para informarles de que [nombre del acosador] ha estado acosándome sexualmente durante los últimos [x cantidad de tiempo].

Durante ese tiempo, han ocurrido los siguientes incidentes:

- [Ejemplo 1: Describe lo que ocurrió y cuándo. Intenta incluir la mayor cantidad de hechos posible.]
- [Ejemplo 2: Describe el segundo incidente que te hizo sentir incómoda. Recuerda incluir si se lo contaste a alguien más en el trabajo].
- [Ejemplo 3: Adjunta cualquier documento o prueba que sirva para tu caso.]

[Si es aplicable, incluye qué medidas debería tomar la empresa. Por ejemplo, puedes poner: "Me gustaría ser transferida a un departamento diferente" o "Me gustaría que se estudiase este caso y recibir una queja formal de parte de [nombre del acosador]."]

Gracias por su atención. En caso de necesitar más información, no duden en solicitarla.

Saludos cordiales,

[Tu nombre]

Tu oficina debería tener una política sobre cómo evaluar la situación y tomar medidas al respecto.

Si crees que tu queja no se analizó con la debida atención, recuerda que **siempre puedes buscar consejo legal en el exterior.** Un profesional versado en leyes en tu zona debería ser capaz de guiarte a través de los pasos siguientes.
También debemos mencionar que para muchas personas **denunciar el incidente internamente no es una opción, ya que muchas mujeres son freelancers o autónomas.** En este caso tienes que tomar cartas en el asunto por ti misma.

Acoso sexual cuando trabajas por cuenta propia

Si eres autónoma y sufres un encuentro inapropiado, dado que no hay a quién informar, **tienes que gestionar la situación por ti misma.**

Esto es exactamente lo que le ocurrió a Ariel, una música que recibió mensajes sexuales de otro profesional de su sector. Tras recibir comentarios sobre cómo se mueve cuando toca, Ariel respondió "no seas un capullo", a lo que el acosador contestó "Me encanta cómo hablas."

Aunque Ariel decidió no avergonzarlo públicamente, sí respondió que sus comentarios eran provocativos y agresivos. El acosador discrepó y ahí se quedó el asunto.

Ariel sintió que enfrentarse al acosador de cara fue fortalecedor y motivador. A otras personas podría parecerles que el mejor modo de salir bien paradas es ignorar a los acosadores; **no existe una foma correcta o incorrecta de abordar el acoso en este escenario.** Es decisión tuya.

Acoso sexual en LinkedIn

LinkedIn, una plataforma online profesional y de negocios, por desgracia también se ha convertido en un medio en el que se da el acoso sexual. **Aunque la política de LinkedIn prohibe toda forma de acoso, no hay modo de que la plataforma lo evite**; por desgracia, el acoso sexual sigue ocurriendo en ella a diario.

Al ser una web de contactos (profesionales), **algunos la tratan como una web de citas.** Entre otras quejas, mujeres han denunciado a hombres que les enviaban mensajes inapropiados y hacían comentarios obscenos sobre su apariencia basándose en su foto de perfil.

Otro problema potencial: tu currículum.

Muchas personas suben su currículum sin considerar que **su dirección de email y número de teléfono aparecen en la cabecera.** A menos que quieras que todo Internet tenga acceso a esa información, elimínala de la versión que publicas en la red.

Para algunos hombres, llamadas de teléfono pidiéndoles una cita podría no parecerles acoso sexual, pero en el caso de mujeres que reciben llamadas de desconocidos, desde luego lo es.

Ese es el problema. Ya que la mayoría del acoso no es tan descarado, es más difícil para las mujeres validarlo y denunciarlo. No obstante, aunque no puedes evitar que hombres pesados te envíen mensajes en LinkedIn, existen formas de protegerte.

4 Formas de protegerte en LinkedIn

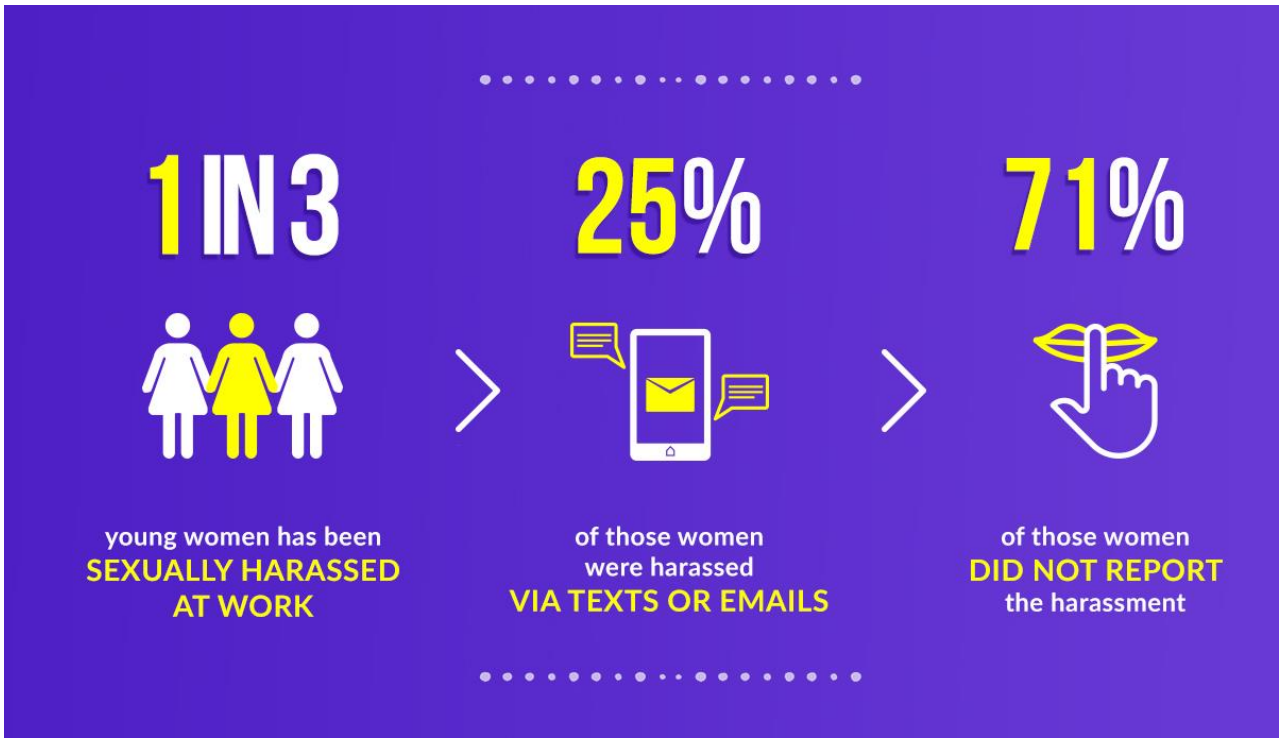
1.Antes de aceptar una conexión en LinkedIn, comprueba tu relación con la persona. ¿Tienes conexiones en común? ¿Trabaja en tu sector? Si no es así, no aceptes.

2.Si recibes un mensaje no deseado, puedes decidir bloquear al remitente. Simplemente haz clic en los tres puntos de la parte superior derecha y haz clic en *Report this conversation* (denunciar esta conversación).

3.También puedes bloquear a esa persona para que no vea tu perfil ni contacte contigo. Ve al perfil de la persona en cuestión, haz clic en More>Report/Block y sigue las instrucciones.

4.Si subes tu currículum, comprueba que tu dirección de casa, número de teléfono y otra información de contacto no se muestra en él. Si alguien quiere contactarte por trabajo, puede hacerlo a través de LinkedIn.

No hay garantía de que estas sugerencias te vayan a proteger al 100%, pero te ofrecen más control sobre quién puede ponerse en contacto contigo.



Las citas en Internet y el acoso sexual

Kylie* llevaba un mes chateando con Marco tras haber conectado en OKCupid, pero aún no se habían visto en persona. Una noche, después de una hora de mensajes cada vez más coquetos, Marco sugirió pasar a un contacto más visual - quería tener sexo a través de Skype.

Al día siguiente, Kylie se horrorizó cuando uno de sus amigos la llamó para contarle que había recibido una grabación del encuentro. Una hora después, **Kylie recibió un mensaje de Marco: o pagaba o la grabación sería enviada a más personas de su círculo social.**

En el mundo de las citas online es donde las mujeres son más vulnerables a acoso cibersexual.

Esto se debe a que, a diferencia de la mayoría de redes sociales, **los sitios de citas son donde acudes con el propósito específico de conocer extraños y potencialmente tener contacto íntimo.** Mientras que en otras webs ajustes de privacidad estrictos pueden actuar como escudo, en las webs de citas estas formas de mantenerte segura resultarían en otro solitario sábado por la noche. Aunque se supone que las aplicaciones de citas deben ser divertidas, también son famosas por dar lugar a algunos encuentros bastante incómodos.

Por ejemplo, Esme* conoció a Raphael en la app Happn. Después de chatear en la app, la conversación paso a WhatsApp, pero cuando Esme echó un vistazo a su foto de perfil, se dio cuenta de que Raphael **era distinto y su perfil no coincidía con el de la app de citas.** Al no querer una confrontación, Esme dijo a Raphael que tenía algunos temas personales que tratar antes de estar lista para quedar en persona. En lugar de aceptar su explicación, él comenzó a bombardearla con preguntas agresivas sobre dónde estaba y con quién.
Al final, Esme terminó bloqueándolo y denunciándolo a Happn. Sabiendo que él la buscaría en redes sociales, Esme también lo bloqueó en Facebook, WhatsApp e Instagram. Y cuando intentó llamarla, también bloqueó su número. Tanto si Raphael finalmente lo entendió (improbable) o simplemente le resultó demasiado difícil mantener el contacto, Esme fue capaz de detener el abuso - pero no todas las mujeres tienen esta suerte.

Lo que le ocurrió a Esme es conocido como ***catfishing*** **- cuando alguien se hace pasar por otra persona en Internet utilizando fotos y perfiles falsos.** Aunque Esme fue capaz de ver que la persona del perfil de Happen era diferente de la persona del perfil de WhatsApp, la mayoría de *catfishers* son suficientemente listos para ocultar mejor sus huellas.
De forma similar, es bastante fácil **convertirse en cómplice de un *catfisher* sin saberlo.** Observemos el caso de Cori*, por ejemplo. Un día recibió una llamada de una amiga diciéndole que **su foto de perfil de Facebook estaba siendo usada en el perfil de citas de otra persona.** Cori denunció el perfil falso y éste fue borrado, pero ¿quién sabe cuántas personas vieron su cara y la información hasta ese entonces?
Por desgracia, no existe forma de conocer gente en Internet y al mismo tiempo estar segura de que nunca vas a ser víctima. Sin embargo, existen formas de protegerte a ti misma.

3 Formas de protegerte en webs de citas

1.Comprueba el pasado de la persona

Cuando conectes por primera vez con alguien en Internet, búscalo en Google, Facebook y otras apps de citas si estás en ellas. Busca inconsistencias en las fotos y descripciones de perfil. Si encuentras alguna, denuncia el perfil a la app.

2.Conoce a la persona a través de la app

Chatea en la app antes de pasar a otra plataforma. Esto te permite tener una ligera impresión de quién es antes de mostrar más información sobre tu vida personal. Una vez te sientas suficientemente cómoda para trasladar la conversación a otra plataforma, sé consciente de lo que se puede ver en ella. Por ejemplo, tanto WhatsApp como Telegram permiten fotos de perfil, WhatsApp permite estados y Telegram permite escribir una pequeña bio. Ambas aplicaciones tienen una característica de "última conexión" que muestra a tus contactos la última vez que estuviste en la app. Si no quieres que alguien vea esta información, cambia tus ajustes de privacidad. Y, si acabas quedando en persona, **asegúrate de quedar en un lugar público e informa a un amigo/a de dónde vas a estar.**

3.Haz privadas las fotos y cuentas de tus redes sociales

Esto minimiza las posibilidades de que alguien robe tus fotos y las use en plataformas de citas.

Sexting seguro

La mayoría de adultos están familiarizados con el sexo seguro, pero seguro que no dedican el mismo cuidado al tener *sexting* seguro.

Esto es especialmente importante en la actualidad dado que el *sexting* es cada vez más popular. De hecho, según un estudio, **casi la mitad de los adultos encuestados afirmaron practicar el *sexting***.

Sin embargo, el hecho de que muchas personas lo hagan no significa que no tenga riesgos. Las historias de "porno de venganza" y de hacks que han expuesto fotos íntimas son muy comunes. No es difícil imaginar cómo podría afectar a tu vida profesional y personal que tus fotos íntimas cayeran en las manos equivocadas.

La respuesta fácil sería decirte que dejaras de hacer *sexting*, pero no vamos a hacer eso. **El *sexting* puede ser una parte divertida y gratificante de tu relación o vida privada** y no estamos aquí para evitarte buenos momentos.

Lo que vamos a hacer es ofrecerte unos consejos sencillos sobre cómo hacerlo de forma segura. Algunos parecerán de sentido común, pero **también vamos a profundizar en soluciones más técnicas para que puedas relajarte cuando tu smartphone *empiece a calentarse*.**

7 Formas de protegerte cuando hagas *sexting*

1.No incluyas tu cara u otras características que te puedan identificar

Tu primera línea de defensa si tus fotos se vuelven públicas es la negación plausible. Esto significa asegurarte de que tus fotos no incluyan tu cara, marcas de nacimiento singulares o tatuajes.

2.No hagas *sexting* cuando tengas más copas de la cuenta

Puede que después de un par de margaritas te salga el lado salvaje, pero eso no significa que sea el mejor momento de desabrocharte el top y sacar la cámara.

Afortunadamente, existen varias apps que pueden evitar arrepentimientos del día después. Por ejemplo, **Drunk Locker es una app muy completa para cuando sabes que vas a salir de fiesta.** Aparte de encontrarte un chófer, **también puede bloquear ciertos contactos** para que no puedas ponerte en contacto con ellos vía mensajes de texto, llamadas ni redes sociales.

3.Haz que tus fotos se autodestruyan

La app **Disckreet está específicamente diseñada para el *sexting***, y requiere que tanto el emisor como el receptor introduzcan una contraseña para ver una imagen enviada. El principal beneficio que ofrece Disckreet es que **te permite borrar tus imágenes del teléfono de la persona a quien se las enviaste.** Dicho esto, no hay nada que evite que la persona que recibe tus fotos saque una captura de pantalla y las guarde de ese modo.

Una app que más o menos aborda el problema de las capturas de pantalla es la popular **SnapChat, que borra automáticamente las fotos unos segundos después de que se abren.** Aunque SnapChat permite las capturas de pantalla, te enviará una notificación cuando se toma una. Dicho esto, no es la solución perfecta, ya que buscar un poco en Google te muestra varias formas de eludir la notificación - por lo que sigue siendo posible para alguien guardar tu foto sin que lo sepas.

Confide, una app muy bien cifrada que borra mensajes y fotos automáticamente, **no permite a los receptores sacar capturas de pantalla.** Pero, de nuevo, si alguien está decidido a guardar tus fotos íntimas encontrará el modo de hacerlo.

4.Protege tus teléfonos y fotos con contraseña

Para asegurarte de que nadie ve nada cuando te deslices por tu galería o la del teléfono de tu pareja, ambos deberían proteger sus teléfonos con contraseña.

También puedes descargar una app que **almacenará tus fotos sexys en una carpeta aparte protegida por contraseña.** Algunas opciones son KeepSafe y Gallery Lock. Una de las mejores cosas de Gallery Lock es que puedes elegir que el icono se mantenga oculto, por lo que otras personas no caerán en la cuenta de que tienes la app en tu teléfono. Además, si alguien intenta iniciar sesión y falla varias veces, la app le sacará una foto.

Ten en cuenta, no obstante, que **no todas estas apps ofrecen cifrado**, lo que significa que podrías correr el riesgo de que tus fotos se roben mediante hacking.

5.Guarda tus fotos de forma segura

Si mandas un *snap* de una foto en la que se ve tu trasero como la obra de arte que es, puedes optar por guardarla en lugar de que se autodestruya. En ese caso, es mejor **guardarla en un ordenador** que en un dispositivo móvil, el cual es más propenso a perderse o ser robado.

Ten en cuenta que incluso en un ordenador es posible ser hackeado, por lo que deberías **guardar tus fotos delicadas en un fichero cifrado.** VeraCrypt es un programa gratuito de código abierto que te permite cifrar archivos determinados en tu Mac o PC.

Sin embargo, ten en cuenta que una vez tus fotos se encuentran en una carpeta cifrada, **sigues teniendo que borrarlas de forma permanente de tu ordenador.** No es suficiente con enviarlas a la papelera y vaciarla.

Hasta que esos datos se reescriben por datos nuevos, siguen existiendo y pueden ser encontrados por un hacker. Afortunadamente, existe software para borrar archivos de forma permanente. Una de las opciones gratuitas más populares para Windows es Eraser, y para Mac puedes utilizar Permanent Eraser.

6.No sincronices tus fotos

Si tienes un Android, seguramente tus fotos se guarden automáticamente en Google Photos, y si tienes un iPhone, en la iCloud.

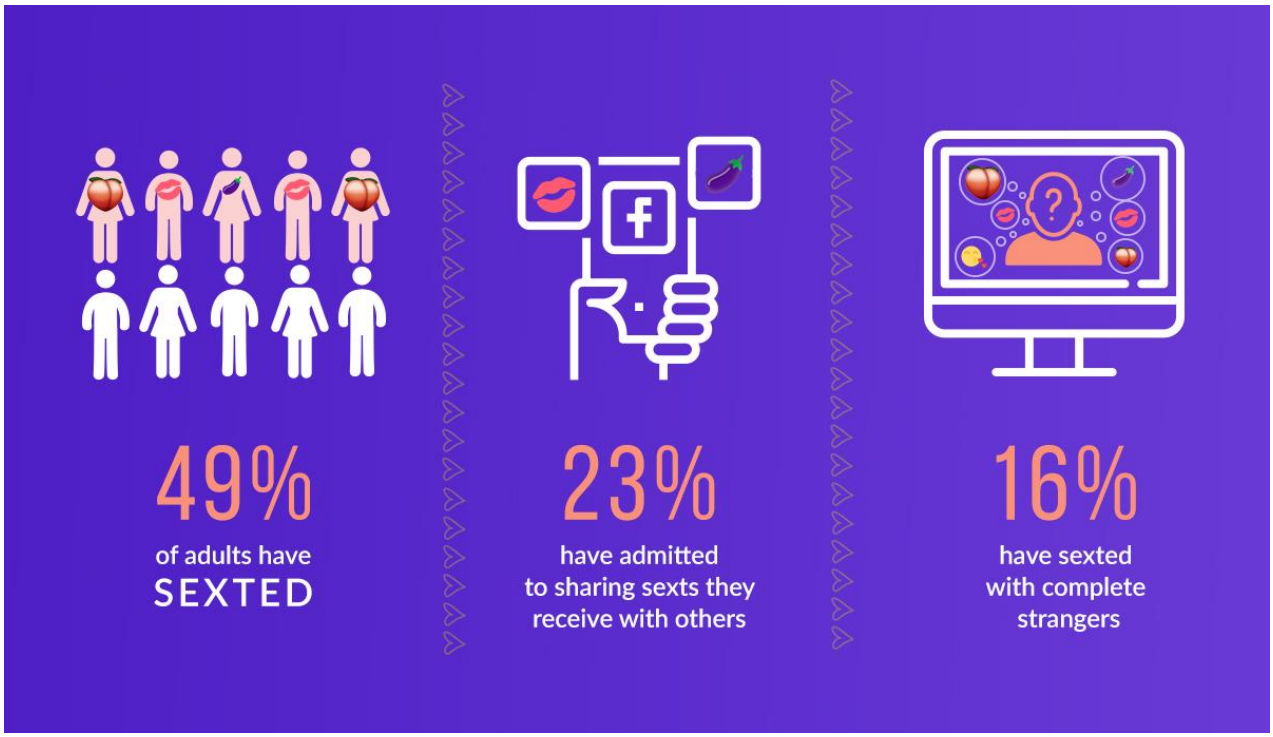
Puede que recuerdes el famoso hack de iCloud de 2014, en el cual **fotos privadas de varias celebridades (principalmente mujeres), incluyendo las de Jennifer Lawrence y Kirsten Dunst, se filtraron** tras un ataque de *phishing*. Como no quieres que eso te ocurra a ti, lo mejor es **mantener tus fotos sensibles fuera de la nube.**

Dicho esto, no recomendamos desactivar la sincronización automática ya que puede causar que pierdas tu información si te roban o pierdes tu teléfono. En vez de eso, deberías entrar en Google Photos o iCloud y **borrarlas una por una**. No obstante, ten en cuenta que **si tienes la sincronización automática activada, esta podría ocasionar que la foto también se borre de tu teléfono la próxima vez que se sincronice.** Por tanto, si quieres guardar la foto, guarda una copia en algún otro lugar - preferiblemente en una carpeta cifrada (ver arriba).

7.No envíes fotos a personas en las que no confíes

Lo sabemos, parece muy obvio, pero dado que **el 16% de la gente afirma haber hecho *sexting* con desconocidos**, es importante decirlo.

Es especialmente importante no enviar fotos potencialmente comprometedoras a alguien que no conozcas demasiado, ya que como habrás visto en este artículo, **no existen condones para el *sexting*, por lo que no hay forma de estar totalmente segura.** Toma las precauciones que puedas y elige bien a tus compañeros de *sexting*.



Ataques IRL (en la vida real)

Obviamente, los ataques a las mujeres no sólo ocurren en Internet. A menudo se extienden al mundo real, al utilizar los perpetradores tecnología que les ayuda a perseguir y abusar de sus víctimas. De hecho, una encuesta de proveedores de ayuda a víctimas reveló que el 79% de ellos trató con víctimas que habían sido vigiladas mediante redes sociales.

En ocasiones los perpetradores son personas que conocemos, **como un compañero controlador.** Otras, **los ataques son fruto de oportunidades**, como el robo de un teléfono móvil o el aprovechamiento de alguien que simplemente está en el lugar equivocado en el momento equivocado.

En cualquier caso, existen precauciones que puedes tomar para mantenerte a salvo, como informar a un amigo/a de dónde vas a estar, cifrar los datos de tus dispositivos móviles y tener contraseñas seguras y bien almacenadas.

Cómo utilizar una app de transporte compartido de forma segura

En 2014, una mujer fue violada en Nueva Delhi por su chófer de Uber. Después de que se revelara que el conductor tenía antecedentes penales desde hacía una década que incluían agresión sexual, algunas personas solicitaron que la aplicación de transporte compartido se prohibiera por completo.

Después de una serie de noticias dañinas, Uber tiene ahora un nuevo CEO a la cabeza. Y **parece que la empresa ya está lista para tomarse en serio la seguridad de los pasajeros** lanzando algunas iniciativas nuevas.

La principal que ya ha sido implementada te permite informar de tu viaje a hasta cinco contactos de confianza. Esto significa que **tus amigos pueden monitorizar tu viaje y ver que has llegado a tu destino.** Si quieres, también es posible optar por que esta característica de Contactos de confianza sólo esté habilitada para los viajes nocturnos.

La característica Contactos de confianza es similar a la característica Send ETA de Lyft, la cual te permite enviar tu ruta y hora estimada de llegada a un amigo. **Tanto en el caso de Uber como en el de Lyft, estos mensajes incluyen marca y modelo de coche, matrícula y foto del conductor.**

Uber también está trabajando en una **característica 911** (112) que te permitirá llamar a los servicios de emergencia con sólo pulsar un botón, **proporcionándoles también tu ubicación en tiempo real**. Otras iniciativas que Uber tiene planeadas incluyen la comprobación de los antecedentes del conductor y análisis de nuevas DUI y delitos penales de su lista de conductores.

Mientras tanto, aquí te mostramos algunos pasos que puedes realizar para mantenerte segura.

5 Formas de protegerte cuando uses una app de transporte compartido

1.Asegúrate de que te subes al coche adecuado

Antes de lanzarte a la carretera, comprueba la matrícula, marca y modelo del coche y el nombre y la foto del conductor para asegurarte de que todo está correcto.

2.No hagas saber a tu conductor si tu destino es tu casa o lugar de trabajo

De hecho, en caso de ser así, te podría interesar tener una pequeña charla y contar una mentira piadosa que le haga pensar otra cosa. Por ejemplo, si pregunta cómo estás, podrías decir "genial, con muchas ganas de ver a mis amigos". Otra opción es la de dar otro lugar cercano como tu destino en lugar de tu dirección exacta, y caminar un par de calles.

3.Comprueba las valoraciones del conductor

Una característica muy buena de las apps de transporte compartido es que permiten a los pasajeros valorar a los conductores. Si el tuyo tiene valoraciones negativas, cancela el viaje y busca otro conductor. Para no tener que esperar demasiado, ten un par de aplicaciones instaladas en tu teléfono para que puedas utilizar la que te consiga antes un conductor fiable.

4.Monitoriza tu ruta

Si estás familiarizada con la zona a la que vas a acudir, te darás cuenta si el conductor toma la ruta equivocada. Pero si no lo estás, abre la aplicación de mapa de tu teléfono y sigue tu ruta para asegurarte de que estás yendo al destino que solicitaste. Si la ruta parece extraña, dilo.

5.Si sientes que algo no está bien, bájate

Sí, puede que llegues tarde a tu cita y pierdas unos dólares, pero si no te sientes segura, pide al conductor que pare y bájate del coche. **Con demasiada frecuencia, las mujeres se ponen en situaciones peligrosas porque creen que seguir sus instintos dará lugar a una situación incómoda.** Al carajo; no importa.

Qué hacer si pierdes o te roban el teléfono

Para muchos de nosotros es como si nuestras vidas estuvieran en nuestro teléfono. Nuestros teléfonos contienen nuestros contactos, nuestras fotos y las apps que utilizamos para circular, estar al día de las noticias, organizar nuestra agenda personal y de trabajo, y mantenernos conectados con amigos y familiares; es **muchísima información personal que no queremos que caiga en las manos de un extraño.**

Afortunadamente, existe una serie de pasos sencillos que puedes realizar para protegerte en caso de perder tu teléfono o de que te lo roben.

4 Formas de proteger el contenido de tu teléfono

1.Protege tu teléfono con contraseña

Para evitar que alguien obtenga acceso inmediato al contenido de tu teléfono una vez está en su poder, lo mejor es tenerlo protegido por contraseña.

El modo exacto de establecer una contraseña dependerá del dispositivo, pero en el caso de Android probablemente tengas que ir a Settings>Security>Screen lock type. Aquí puedes elegir desbloquear tu teléfono utilizando un patrón, un pin o una contraseña.

Una contraseña es la opción más segura, pero también la más molesta ya que hay que introducirla cada vez que quieras mirar tus notificaciones de Facebook. También es posible que tengas la opción de que tu teléfono sólo se desbloquee con tu huella dactilar.

Otra característica interesante es el *smart lock* o bloqueo inteligente. Con *smart lock*, el teléfono no se bloqueará cuando lo tienes encima si te encuentras en ciertos lugares (por ej. en tu casa), o si estás cerca de otros dispositivos de confianza. Algunos teléfonos incluso te ofrecerán las opciones de reconocimiento de voz o reconocimiento facial.

2.Ubica tu teléfono

Una de las mejores cosas de tener GPS en el teléfono es que si se pierde puedes rastrear su ubicación. Sin embargo, **para que esto funcione tienes que configurarlo de antemano.**

Si tienes un Android, tienes varias opciones. Algunos dispositivos, como Samsung, tienen esta característica integrada - aunque para acceder a ella tienes que crearte una cuenta Samsung. Activando esta característica podrás conocer la ubicación de tu teléfono visitando https://findmymobile.samsung.com/ desde otro dispositivo e iniciando sesión. Otra opción es descargar la **app Find My Device de la Play Store de Google**. Esta app funciona igual que la de Samsung y sólo requiere que tengas una cuenta Google. Además, si has perdido tu teléfono en algún lugar de tu casa, la app puede hacerlo sonar incluso si está en modo silencio. Ve a https://myaccount.google.com/intro/find-your-phone, inicia sesión y podrás ver la ubicación de tu teléfono en un mapa. Desde ahí también podrás resetear la contraseña del teléfono.

Ten en cuenta, no obstante, que si tienes un Android **sólo podrás localizar tu dispositivo si tus servicios de ubicación están activados y estás conectado a Internet.** Un ladrón listo desactivará estas funciones para que no puedas rastrear dónde se encuentran él y tu teléfono.

Si tienes un iPhone, tienes que descargar la app Find My iPhone. Una vez instalada, podrás localizar tu dispositivo en un mapa visitando https://www.icloud.com/#find e iniciando sesión en iCloud.

Desde ahí también puedes establecer tu teléfono en modo *Lost Mode* (perdido), lo que lo bloqueará. *Lost Mode* también te permite enviar un mensaje a la pantalla bloqueada, por lo que si tu teléfono simplemente está perdido, puedes escribir algo del estilo de "Teléfono perdido. Por favor, llame al 212-555-1234 para devolverlo." O, si sabes que tu teléfono ha sido robado, puedes escribir "Que te den".

3.Borra tus datos

Esta es la opción nuclear. Si estás seguro de que no vas a recuperar tu dispositivo, **puedes utilizar las apps Find My Device/Find My iPhone para borrar todos los datos del teléfono de forma remota**, por lo que incluso si el ladrón consigue superar tus protecciones por contraseña no podrá acceder a tu información personal.

Ten en cuenta que cuando haces esto, ya que todas tus cuentas personales serán borradas, **ya no podrás rastrear tu teléfono remotamente.**

Dicho esto, tu teléfono seguirá pudiendo recibir servicio de tu proveedor de telefonía, lo que significa que quien lo tenga podrá llamar desde tu número y utilizar tu plan de datos. Para evitarlo, **llama a tu proveedor de servicios de telefonía e infórmale de que tu teléfono ha sido robado.**

Saber que puede que un día tengas que borrar los datos de tu teléfono es otro gran motivo para **realizar una copia de respaldo del contenido de tu teléfono** (cosa que deberías tener siempre). Si tienes un Android, la forma más fácil de realizar dicha copia es utilizar la nube de Google; si tienes un iPhone, utiliza la iCloud.

Pero, ¿qué pasa si no tienes la prudencia de instalar las apps Find My Device/Find My iPhone de antemano y ahora no puedes cambiar tus contraseñas, bloquear tu teléfono o borrar tus datos remotamente? En ese caso deberías...

4.Cambiar las contraseñas de todas tus apps

Haz una lista de las apps que tienes en tu teléfono que requieren contraseña, utiliza otro dispositivo y empieza a cambiar tus contraseñas. Entre éstas seguramente se incluyan tu email, cuentas de redes sociales, cuentas bancarias y *app stores*.

Estar segura en Meetup.com

Una de las cosas geniales de Internet es que puede conectar a completos desconocidos que tienen algo en común pero nunca se habrían conocido si no fuera por la red.

Una forma de hacerlo es a través de la web Meetup.com, la cual permite a los usuarios **crear y unirse a eventos y actividades de temas que les interesan.** Algunas categorías populares de los *meetups* (encuentros) incluyen cine, salud y bienestar, LGBT o mascotas. Es una forma fantástica de hacer nuevos amigos y cultivar tus intereses.

Pero ¿no te decía siempre tu madre que no hablaras con extraños? ¿Te lo decía con motivos, o sólo eran paranoias?

Un poco de ambas cosas. Claramente deberías salir ahí fuera y disfrutar de la vida... pero tomando algunas precauciones.

3 Formas de protegerte en Meetup.com

1.No incluyas demasiada información personal en tu perfil

Ten en cuenta que la página de tu perfil es completamente accesible a cualquiera con Internet, por lo que incluye solamente información que no te importe que sea pública.

Si te apasiona la comida y estás impaciente por encontrar encuentros culinarios en tu ciudad, desde luego deberías mencionar el nuevo puesto de tacos con el que estás obsesionada. Pero no digas que se encuentra justo en la puerta de tu edificio en el 333 de Main Street, que vives en el piso 4D y, ya que estamos, que no tiene cerrojo.

Si te interesan los encuentros familiares, escribe que tienes hijos de diez y seis años, pero no incluyas que se llaman Timmy y Sue, que van al colegio Lincoln y que vuelven a casa caminando solos a las 2:30 pm.

2.Conoce a la gente en la vida real antes de comunicarte con ellos en privado

Meetup tiene un sistema de reenvío de emails, por lo que puedes recibir los mensajes que te envíen los miembros en tu email sin que ellos tengan tu dirección de email.

Aun así, si no te interesa que la gente contacte contigo antes del encuentro y de conocerla en la vida real, **puedes optar por bloquear los mensajes de los usuarios** y sólo recibir mensajes de organizadores de eventos. Simplemente ve a tu cuenta y haz clic en Settings>Privacy.

Ahí **puedes elegir si quieres que tu perfil muestre tus grupos o intereses.** También puedes elegir quién puede contactarte en Meetup: organizadores, miembros de tus encuentros o cualquiera de la web.

3.Informa a un amigo de dónde vas a estar

En cualquier situación en la que vayas a quedar con desconocidos, es buena idea decirle un amigo adónde vas y fijar una hora para escribirle y que sepa que llegaste a casa sana y salva. Además, **si en el encuentro habrá bebidas, nunca pierdas de vista tu vaso.**

Cómo evitar la violencia doméstica

La violencia doméstica (siglas en inglés: IPV), afecta a casi un tercio de las mujeres estadounidenses. Aunque la tecnología puede ofrecer herramientas a las víctimas (por ej. para recopilar pruebas contra un maltratador), lamentablemente también puede ser utilizada por los maltratadores. Esto se debe a que el control es un elemento integral de la violencia doméstica, y **el uso incorrecto de la tecnología puede ofrecer a los maltratadores un medio de ejercer control sobre sus víctimas.**

Según un estudio reciente, aunque muchos maltratadores utilizan tecnología diseñada específicamente para la vigilancia, es mucho más común el uso de otro tipo de apps con esta finalidad. Algunas de esas apps incluyen las de tipo ***find my phone*** (encuentra mi teléfono) **y apps de monitorización familiar y de niños.**

El problema de esto es que es que los activistas en contra de la violencia doméstica no pueden ir tras las empresas que producen estas aplicaciones, y

las app stores no las pueden bloquear ya que, la mayor parte del tiempo, se usan con fines totalmente legítimos.

Muchas de estas apps permiten a los maltratadores **realizar un seguimiento de la ubicación de la víctima**, **leer sus mensajes** haciendo que sean reenviados a un dispositivo diferente, e incluso **observarla y escucharla remotamente** al activar la cámara y el micrófono del teléfono.
Como mencionamos arriba, también existen apps que se anuncian explícitamente como **apps para vigilancia no consentida**. Aunque es raro encontrar este tipo de apps en una *app store* legítima, existe una gran cantidad de ellas en los rincones de Internet. Y aunque la mayoría de teléfonos vienen con ajustes que bloquean las apps que no son de *app stores* legítimas, en Internet es posible encontrar guías para anular estos ajustes.
Uno de los elementos más nefarios de este tipo de apps es que pueden ser configuradas para que el icono de la app esté oculto, haciendo **prácticamente imposible que la víctima la detecte en su teléfono.**
Podrías pensar que la solución sería escanear el teléfono en busca de spyware, pero lamentablemente, algunos de los nombres más conocidos de la industria como son Symantec, Kaspersky y Avast, han demostrado ser ineficaces a la hora de detectar estas apps.

Por tanto, ¿qué puedes hacer para protegerte?

3 Formas de evitar que te monitorice una pareja abusiva

1.Ten el teléfono en tu poder en todo momento

Prácticamente todas las apps estudiadas requieren que el abusador tenga acceso físico al teléfono de la víctima al menos una vez.

2.Sé prudente al utilizar cualquier teléfono que no hayas obtenido por ti misma

Los abusadores con mucho control sobre sus víctimas a menudo también controlan su dinero, por lo que son ellos quienes compran los nuevos teléfonos de las víctimas. En estos casos no sólo pueden preinstalar apps de doble propósito, sino también pueden incluso *rootear* el dispositivo, permitiéndoles instalar las apps más nefarias. Incluso existen empresas que venden teléfonos ya *rooteados* o con software de vigilancia y monitorización preinstalado.

3.Protege tu teléfono con contraseña y no compartas tu contraseña con nadie

Como mencionamos arriba, tener tu teléfono bloqueado por contraseña es la primera línea de defensa para mantener a salvo su contenido. Si sospechas que tu pareja está accediendo a tu dispositivo, cambia inmediatamente tu contraseña. Elige una larga y compleja y asegúrate de no utilizar elementos que puedan adivinar, como tu cumpleaños o el nombre de tu mascota.

Dicho esto, no somos ingenuos y no podemos ignorar la realidad de que **muchas víctimas de violencia doméstica son obligadas a revelar su contraseña** o "permitir" que se instale este tipo de apps peligrosas en sus teléfonos.

Estés o no en posición de proteger tu dispositivo, **si eres víctima de violencia doméstica, existen recursos que pueden ayudarte a salir de la situación.** Estas sólo son alguna de las organizaciones cuya misión es ayudar a las víctimas:

National Network to End Domestic Violence: https://nnedv.org/

The National Domestic Violence Hotline: 1-800-799-7233, http://www.thehotline.org/resources/

Family and Youth Services Bureau: https://www.acf.hhs.gov/fysb/resource/help-fv

Apps de SOS

En general, es buena idea tener instalada una app de emergencia en tu teléfono por si las moscas. Estas te permiten **notificar a amigos o familiares cuando sientes que estás en peligro y/o contactar con los servicios de emergencia.**

Algunos tipos de teléfonos vienen con estas funciones incluidas, así que merece la pena ver si el tuyo lo tiene. Si no es así, echa un vistazo a estas apps, todas disponibles tanto para Android como para iOS.

1. ICE, siglas en inglés de *In Case of Emergency* (en caso de emergencia), **te permite enviar un mensaje y tu ubicación GPS a contactos determinados** cuando quieres que tus amigos o familiares estén al tanto de tu paradero. **También puedes configurar que el mensaje se envíe a una hora concreta**, de

modo que, por ejemplo, si no vuelves de un paseo cuando anochece, en ese momento recibirán el mensaje.

2. React Mobile hace lo mismo que ICE pero también tiene un botón "SOS Help Me" (ayúdame) que notifica a tus contactos previamente seleccionados por email y texto, y también **publica un mensaje en Facebook y Twitter** si así lo estableces. Al mismo tiempo, la app **contacta automáticamente con los servicios de emergencia locales.**
3. Siren GPS no se pondrá en contacto con tus amigos o familiares, pero con sólo un botón alertará a los servicios de emergencia y les proporcionará tu ubicación. También puedes **crear un perfil personal con información relevante que se facilite a las autoridades en caso de emergencia.** Este puede incluir tu estado de salud e información de contacto en caso de emergencia. La app también te da la opción de llamar al departamento de bomberos, una ambulancia o a la policía.

También puedes **mostrar la información que quieras en tu pantalla de bloqueo** para que se utilice en caso de darse una situación en la que no seas capaz de proporcionar la información por ti misma. Por ejemplo, puedes escribir algo como "En caso de emergencia, llamen a [nombre de alguien]", seguido de su número de teléfono. O, si tienes un problema de salud específico como una alergia severa o epilepsia, puedes incluir información relevante ahí.
Cómo establecer un mensaje en la pantalla de bloqueo dependerá del modelo de teléfono que tengas.

Conclusión

La tecnología e Internet juegan un gran papel en nuestras vidas tanto positivo como negativo. Como mujeres, somos un objetivo en Internet por varios motivos, pero eso no quiere decir que tengamos que desconectarnos o aislarnos.

Esperamos que esta guía te proporcione las armas para protegerte y defenderte en Internet y en persona, y que las herramientas que ofrecemos te sean de ayuda.

Si esta guía te ha resultado útil, agradeceríamos que la compartieras con otras personas para que más mujeres puedan aprender a estar más seguras tanto dentro como fuera de la web.