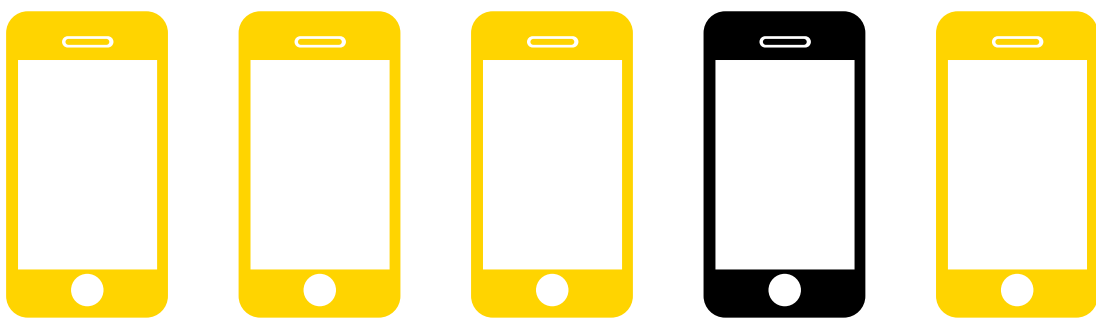
HOJA DE RUTA DE SEGURIDAD: CIBERACOSO



CONSTELACIÓN DE TELÉFONO MÓVIL

CONEXIONES

Los hotspots de Wi-Fi y las conexiones bluetooth pueden revelar tu ubicación y hacer que sea más fácil hackear tu teléfono.

i. SMS/Llamadas

Si un acosador puede conseguir tu número de celular, puede acosarte mediante mensajes de texto o llamadas. Puede usarlo en combinación con un GPS para revelar que conoce tu ubicación. También puede usar spyware para interceptar tus mensajes y llamadas.

GPS

Los GPS pueden decirte qué cafeterías están cerca, pero también pueden hacerle saber a otros dónde estás. La aplicación Girls Around Me, que afortunadamente ya caduca, era un perfecto aluvión de información de GPS y desarrolladores inescrupulosos.

i. Fotos

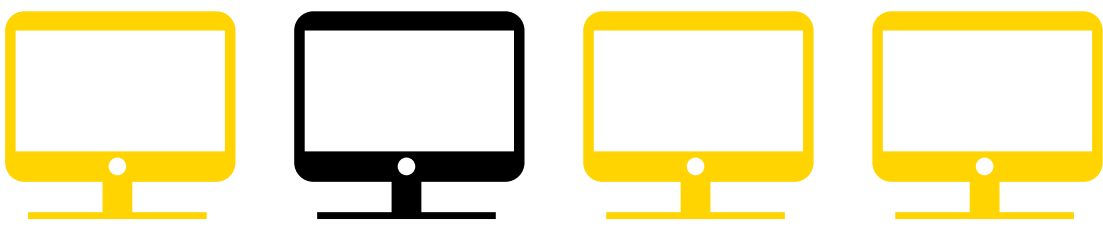
Las fotos llevan información incrustada en sus propiedades que incluye cuándo y dónde se tomaron. También es posible deducir la ubicación en base a lo que muestra la imagen.

CONTRASEÑAS

Si tu teléfono no está protegido con contraseñas, cualquier persona que lo tome puede acceder a tu información. El hackeo de contraseñas es común y cuanto más sepa de ti el acosador, más posibilidades tiene de adivinar tu contraseña. Además, las contraseñas más comunes son fáciles de divinar, como “123456”, “abc123” y “(nombre propio)”

APLICACIONES

Hay aplicaciones maliciosas que contienen spyware. Cuantas más funciones tenga tu smart phone, como GPS, más pueden utilizarse esos extras en tu contra.



CONSTELACIÓN DE LAPTOP

CONEXIONES

Los hotspots de Wi-Fi y las conexiones bluetooth pueden revelar tu ubicación y hacer que sea más fácil hackear tu dispositivo.

REDES SOCIALES

De las entradas y fotos que publicas resulta muy fácil deducir información, sobre sobre dónde vives, los lugares que visitas regularmente y las personas que te interesan. A veces tus amistades también pueden revelar, sin quererlo, información sobre ti.

CHATS EN LÍNEA

En las salas de chat puede haber acoso desde los contactos. Además, si utilizas la opción “recordar la contraseña automáticamente”, cualquiera que use tu computadora puede entrar a tus servicios de mensajería.

BLOGS

A los acosadores les gusta meterse en los espacios para comentarios para publicar amenazas e insultos. Esto es común cuando el acosador es un desconocido.

CORREO ELECTRÓNICO

Las direcciones de correo electrónico a menudo están vinculadas a nombres y perfiles reales y los acosadores pueden servirse de esto para contactarte de manera directa. Una vez más, pueden usar spyware para acceder a tu dirección electrónica privada.

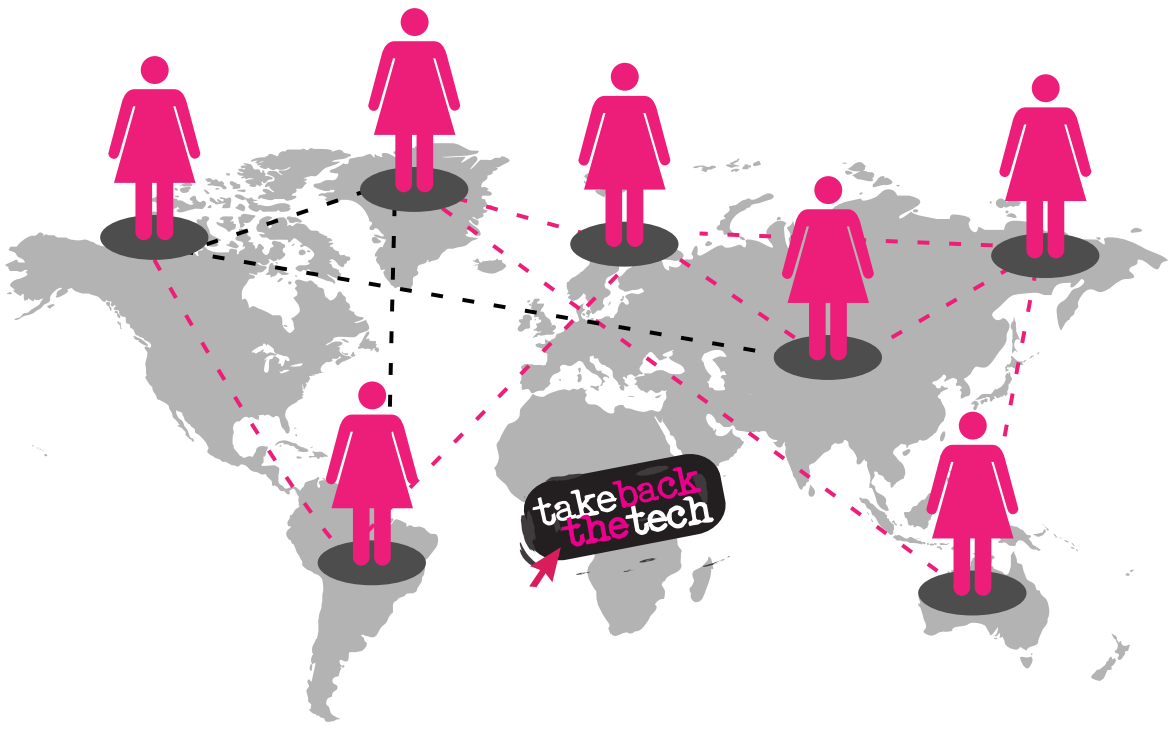
CÁMARAS WEB

Los acosadores pueden usar spyware para acceder a las cámaras web y filmar a personas sin su consentimiento.

CONTRASEÑAS

Si tu dispositivo no está protegido con una contraseña, cualquiera que la use puede acceder a tu información. El hackeo de contraseñas es común y cuanto más sepa de ti el acosador, más posibilidades tiene de adivinar tu contraseña. Además, las contraseñas más comunes son fáciles de divinar, como “123456”, “abc123” y “(nombre propio)”.

RELATED RIGHTS



YOUR RIGHT TO FREEDOM OF EXPRESSION

ARTICLE 19, UNIVERSAL DECLARATION OF HUMAN RIGHTS: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media regardless of frontiers."

Cyberstalking is often used to silence women and girls. Whether bloggers, gamers, tweeps or general users, women are often intimidated into leaving online spaces and closing their computers. But women have the same rights as men to access those spaces and be heard on any issue.

You have the right to express yourself freely online and off, which makes cyberstalking a free speech issue.

YOUR RIGHT TO PRIVACY AND FREEDOM FROM DEFAMATION

ARTICLE 12, UNIVERSAL DECLARATION OF HUMAN RIGHTS: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

People who stalk women online take advantage of the anonymity the internet can give them. Some of the same people who violate women's privacy online do so while fiercely maintaining their own right to privacy.

An APC study looking at recent legislation in South Africa, New Zealand and Canada reflects the need for internet intermediaries and others to play a role in preventing and rectifying online violence. The legislation recognises that the internet makes it easy for stalkers to be anonymous and holds internet service providers accountable to reveal information about the identity of the harasser, cease providing service to the harasser and/or remove harmful content.

In Europe, there is also a Right to be Forgotten, which can be used to demand that search engines remove links with personal information because it is irrelevant. Interestingly, the burden of proof is now on the search engine to prove that the data cannot be deleted because it is still relevant. The law applies to all companies, including those outside the EU, which serve European citizens.

YOUR RIGHT TO FREEDOM FROM VIOLENCE

UNITED NATIONS DECLARATION ON THE ELIMINATION OF VIOLENCE AGAINST WOMEN: "States should condemn violence against women and should not invoke any custom, tradition or religious consideration to avoid their obligations with respect to its elimination. States should pursue by all appropriate means and without delay a policy of eliminating violence against women... [This includes] any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life."

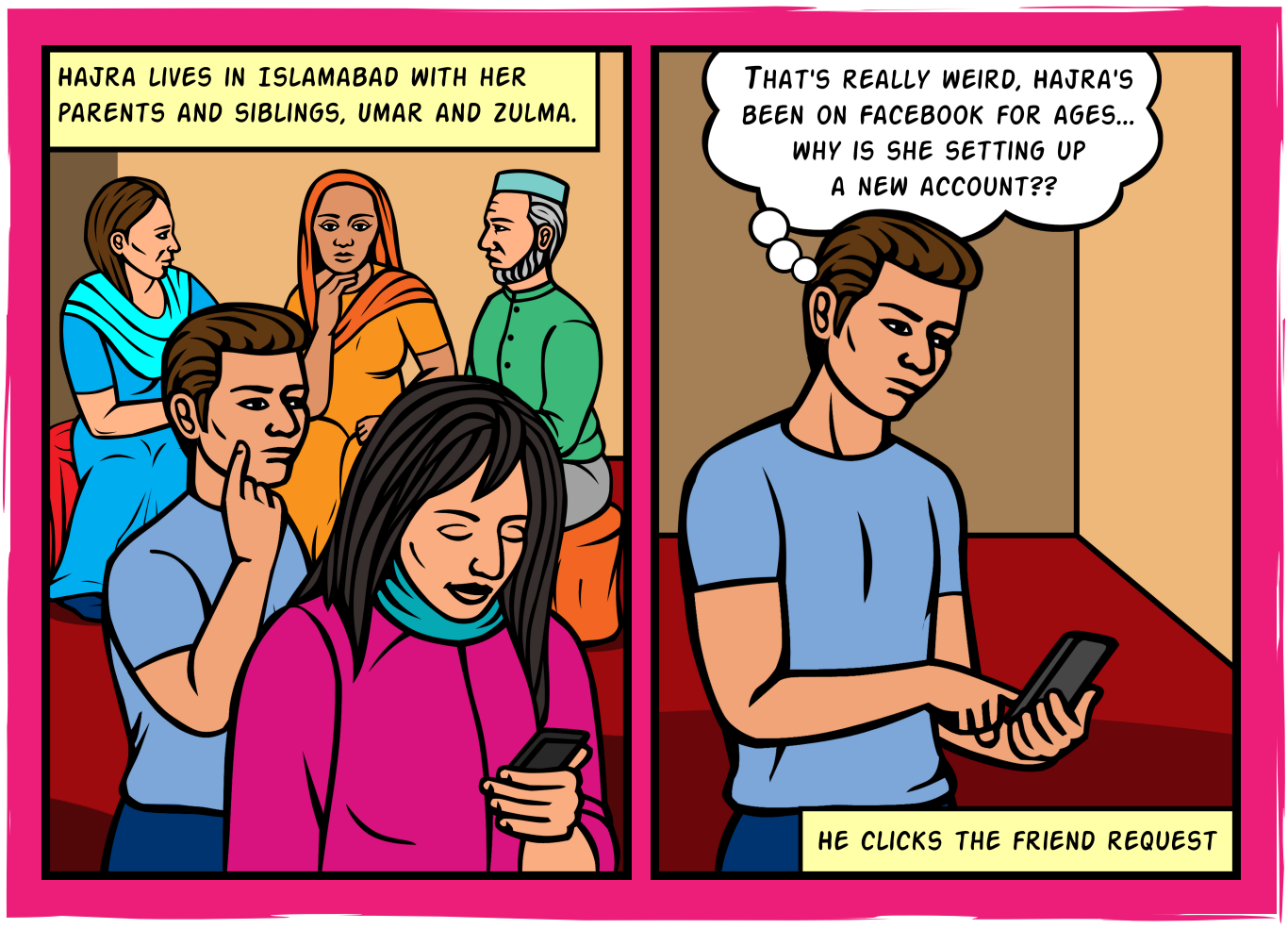
COUNCIL OF EUROPE CONVENTION ON PREVENTING AND COMBATING VIOLENCE AGAINST WOMEN AND DOMESTIC VIOLENCE: "Parties shall take the necessary legislative and other measures to promote and protect the right for everyone, particularly women, to live free from violence in both the public and the private sphere."

Recent domestic legislation specifically tackling online violence against women recognises:

- the need to provide practical redress to targets of harassment
- the responsibility of websites and internet providers in cyber-harassment cases
- the need for public education

In South Africa, New Zealand, California and Nova Scotia, for instance, all new legislation recognises that harm caused by online harassment includes emotional distress even when there is no actual physical harm.

CYBERSTALKING



1 2 3 4

EL CIBERACOSO ES UN ATAQUE A UNA PERSONA A TRAVÉS DE LA TECNOLOGÍA POR RAZONES DE ENOJO, VENGANZA O CONTROL.

Un informe de Working to Halt Online Abuse que cubre el período 2000-2013 revela que la mitad de las personas que respondieron habían sufrido algún tipo de ciberacoso de parte de alguien con quien tenían algún tipo de relación, mientras que la otra mitad no había tenido ninguna relación con el perpetrador. Del primer grupo, la conexión más común era un/a ex (39.5%), seguido de un/a conocido/a en línea (16.25%) y algún/a amigo/a (12.5%).

La mujeres tienen más probabilidades de experimentar ciberacoso, en especial de un compañero íntimo. La mayoría de las acosadas por un compañero íntimo también enfrentan algún ataque físico de esa persona

El ciberacoso incluye, aunque no se limita a:

- hostigamiento, humillación e injurias a la persona tomada como blanco
- acoso a la familia, amistades y empleadores para aislar a la persona
- tácticas para atemorizar a la persona
- adoptar la identidad de la otra persona
- vigilar (p.ej., usando las notificaciones de Facebook para averiguar a dónde va la persona, usando spy ware, activando GPS)

El ciberacoso puede ser difícil de enfrentar debido a:

- el anonimato del acosador
- la presunción de las autoridades de que un acosador que está lejos no viajará para concretar las amenazas
- el acosador incita a sus amigos en línea para que participen del acoso, para aumentar la angustia de la persona acosada