¿Cómo evitar la filtración de imágenes privadas?

Descripción

Hace unos días hackers filtraron fotos privadas de famosas desnudas en internet, algo que causo revuelo y que provocó cuestionarse ¿dónde se están guardando las fotos y quién tiene acceso a ellas? ¿Qué tan vulnerables somos al robo de nuestra información? Hoy te contamos cómo evitar que tus fotos se filtren en la web

Claudia Kompatzki
ckompatzki@todomujeres.cl
Follow @clau_kom

SANTIAGO.- Jennifer lawrence, Kim Kardashian, Vanessa Hudgens y Emma Watson, son algunas de las famosas que sufrieron la filtración de sus fotografías privadas tras una supuesta ruptura de seguridad de la nube de almacenamiento ICloud, la cual ha sido negada por la empresa Apple.

Sin embargo esto es algo más común de lo que parece, día a día nos sacamos fotos y no sabemos con exactitud si nuestro dispositivo móvil está siendo algún registro de la información en otro lugar o si está siendo intervenido.

Para ponerle un poco de picor a nuestras relaciones o simplemente lucirnos frente a los chicos, puede ser qué más de una vez nos hemos sacado fotografías subidas de tono y si es con tu novio y hay confianza no pensamos en que algo malo pueda suceder….pero lo cierto es que la filtración de las fotos es una posibilidad que no podemos ignorar. Y para no pasar por esa vergüenza aquí algunos consejos que compartió Manu Contreras (@mcontreras), Editor jefe de tecnología de @betazeta y Editor en @fayerwayer y @fayerwayer, en su artículo "Las 3 cosas que debes saber si decides hacerte fotos comprometedoras con tu móvil" para cuidarnos del mal rato y las consecuencias que nos puede traer la filtración de una fotografía prohibida.

Comprueba dónde se guardan tus fotos

Muchas de estas famosas cuyas fotos personales se han visto compartidas por millones de personas

se encontraban en **iCloud**, el servicio de sincronización y copia de seguridad de Apple. Pero estamos descubriendo que mucha gente no sabe exactamente qué es iCloud o que directamente sus fotos estaban copiadas en algún otro sitio. Comprueba donde están tus fotos. Si usas un iPhone o un iPad revisa si tus fotos se están copiando a iCloud. Si tienes instalado OneDrive, Dropbox o cualquier aplicación de almacenamiento en la nube, comprueba que las fotos no se están subiendo automáticamente.

Si usas Android, comprueba que la función de subida de fotos de Google+ no está activa, aunque para esto lo primero que tienes que saber es que existe algo llamado Google+.

Cuando subas una foto, ten en cuenta que estas fotos no sólo están en tu móvil o en la nube, muchos de estos servicios además **copian esas fotos a otros dispositivos como portátiles o tablets**. Ya no vale el borrar una foto de tu móvil, tienes que asegurarte que está borrada de todo dispositivo que tengas.

ICloud guarda instantaneamente tus archivos en todos los dispositivos registrados con tu mail

Contraseñas y miente, miente muchísimo

Por favor, cuando te registres en algún servicio en internet donde guardas documentos, vídeos o fotos: **miente**. Si, miente. Cuando te pregunten por el nombre de tu primera mascota, ¡no pongas el nombre de tu mascota! Usa otro nombre que vayas a recordar. De un amigo, de alguien de tu familia, de un famoso, de lo que sea pero **nunca el nombre real.**

Se cree que gran parte de las filtraciones se consiguieron gracias a hackeo de ingeniería social, mediante *phishing* se lograban correos y contraseñas. Parece básico, pero hay que recordarlo: no des tu usuario y contraseña a nadie que no sea el verdadero servicio. ¿Cómo sabes eso? Sencillo, revisa que la URL sea el dominio de Apple, Google, Microsoft, de tu banco o del servicio que sea, y siempre que sea mediante conexión segura (“https” o una señal verde en la barra de direcciones).

Y en temas de contraseñas, hay decenas de formas de crear contraseñas seguras. Desde webs como Strong Password Generator y aplicaciones que generan aleatoriamente contraseñas y además las almacena como es1password. Comprueba cuál fácil es te romper la seguridad de tu contraseña con How Secure Is My Password

.

¿Una técnica para siempre acordarte de una contraseña? Genera una frase larga, como de 10 palabras. Por ejemplo “El caballo del príncipe mató el zorro de la duquesa mientras tomaban café”, una frase sin sentido pero fácil de recordar. Ahora es cuestión de jugar con ella. Por ejemplo una contraseña podría ser usar la primera letra de cada palabra (*ecdpmezdldmtc*), o usar la segunda letra, alternar mayúsculas y minúsculas, agregar espacio o símbolos. Sé creativo pero siempre con una larga frase sin mucho sentido aparente.

Control de daños

Digamos que te da igual todo, que te haces estas fotos, que no tienes interés por tu seguridad y que tus fotos, por alguna razón acaban en internet. Primera regla: **que no te entre el pánico.**

Lo primero que debes hacer es informar al servicio donde están alojadas las fotos y pedir su retirada inmediata. Después debes denunciar ante las autoridades pertinentes. Policia Nacional, Policia Federal, Guardia Civil… sea cual sea el cuerpo de seguridad de tu país, **debes interponer una denuncia** para que el responsable o responsables sean encontrados y puestos a disposición de la justicia.

Investiga de dónde han salido las fotos, si tú las tomaste revisa aplicaciones instaladas, redes sociales o incluso quién ha tenido acceso a tu móvil. Puede darse el caso que haya sido una persona de tu confianza quien las haya publicado (como en el “porno de venganza”).

Pero si hay algo importante que todo el mundo debe entender de internet es esto: **internet tiene memoria y nunca olvida**. En la mayoría de las ocasiones las fotos siempre acaban en algún servicio perdido, quizá no tenga tu nombre o nadie sepa quién es la persona de la fotografía, pero hay muchísimos sitios de internet que comparten este tipo de contenido sin importar quién o qué sale en ellas.

Cuando accedes a internet, sobre todo cuando decides usar redes sociales o tener dispositivos conectados a internet, tienes que entender que **la seguridad es y siempre será una ilusión**. No existe servicio perfecto o sistema de seguridad irrompible.

La mejor solución es siempre la más obvia. Si no quieres que algo aparezca en internet, no lo hagas. No es una prohibición, pero siempre ha sido la mejor de las soluciones.

¿Cómo andan las cosas en Chile?

Valentina Roth ha sufrido varias veces la filtración de sus imágenes

Para contextualizar el tema y traerlo directamente a nuestro país, entrevisté a Pablo Peréz Quinteros (@pabloperezq), Periodista y Social Media Strategist en laUniversidad Andres Bello.

¿Recuerdas algún caso de filtración de imágenes privadas memorable en Chile?

Hay un caso memorable, el de Valentina Roth y la filtración de su video en un lobby, también el de Macarena Venegas y la otra notable, que tuvo mucho de farándula, porque estuvo metida también la Fiera, el caso de la Alejandra Álvarez Pero ese puntual fue más fuerte, puesto que el culpable (que aún no se tiene certeza de quién es) fue publicado en un sitio de foro, Portalnet.

¿En que terminó la mayoría de estos casos?

La mayoría quedan en las disculpas del caso y se levanta la medida cautelar.

¿Qué puedo hacer si me están amenazando con publicar mis “fotos prohibidas”?

Tú, como dueño de tu imagen, puedes negarte tajantemente a que se publiquen tus fotos, ahora bien, si se publican, puedes tener la oportunidad de demandar a los responsables de la filtración.

Luego tienen que aplicarse los diversos elementos. Si las fotos fueron tomadas en el ámbito público, nada que hacer. Si las fotos son tuyas y alguien las tomó sin tu consentimiento y las divulgó, corre sanciones, muchas veces son sanciones pecunarias, es decir, plata. Muy pocas veces es penal.

¿Crees que efectivamente funciona la justicia en cuanto a sancionar por la filtración de imágenes privadas?

La justicia se basa más bien en los hechos que presentan las partes. Luego de investigar dan a conocer el veredicto. En este caso, las instituciones cumplen su labor y, de acuerdo a las pericias y, muchas veces, a las negociaciones, las situaciones, por lo general, llegan a buen puerto

¿Algún consejo para poder enviar una imagen "subida de tono" pero hacer que desaparezca y que no se filtre? ¿se puede o mejor no arriesgarse?

Lo más recomendable es simplemente no tomar fotografías subidas de tono. Internet tiene memoria y, a pesar de que a lo mejor pudiste borrar la imagen en su momento, alguien pudo haber guardado una copia y volvió a subirla, o si lo haces, con una cámara personal. Observarlas y borrarlas.

Una experiencia personal

Daniela (22 años)

Mi experiencia fue con mi ex, a el le encantaba que nos tomáramos fotos, nunca entendí porqué pero yo me encontraba en un estado físico que me gustaba sacarme fotos, yo feliz posaba para él. Pero después de unos meses terminamos y nunca más supe de él…. Antes de que dejáramos de vernos, yo siempre le pedía que borrara las fotos que me tomaba pero la verdad es que nunca supe con certeza si realmente lo hizo…

Nunca sabrás si él borró las fotos…

Brigada del CiberCrimen de la PDI

La policía de investigaciones chilena y su división de CiberCrimen dan consejos para cuidarnos mientras navegamos por internet:

Sobre el fraude en la red, especialmente el phishing y el pharming.

1. Realizar operaciones en sitios seguros (https://)
2. Tener conocimiento que los bancos no solicitan actualizaciones de datos por correo electrónico o teléfono.
3. Verificar la barra de direcciones en el navegador, cuando se esté operando en sitios de Bancarios.

Respecto del correcto uso de claves en mail y redes sociales.

1. Sólo deben ser de conocimiento del usuario, y jamás compartirlas con terceros desconocidos.
2. Cambiarlas con frecuencia y siempre utilizar de preferencia claves que contengan, letras, número y símbolos.
3. Jamás dejarlas escritas en algún lugar visible como mecanismo recordatorio, dado que cada uno es responsable de la misma.

Sobre los peligros de la pedofilia y el abuso sexual impropio.

1. Protege tu intimidad, especialmente frente a individuos o personas que no conoces y contactadas vía Internet. No entregar datos personales como nombre, apellidos, direcciones, datos de tu colegio y familia.
2. Si recibes un correo electrónico o ingresas algún perfil de una red social, que te parezca raro, cuéntale a tus padres de inmediato, y en especial es registrar inmediatamente el nombre de identificación ya sea del perfil o la casilla electrónica que se ha comunicado contigo.
3. No dejes que tu webcam muestre elementos que puedan identificarte (como diplomas con tu nombre, fotos de tu casa o ciudad, etc)
4. Recuerda que tienes la libertad de decir que “NO”, y dejar de establecer contactos con alguien o ver algo que te provoque sensaciones desagradables o vergüenza.
5. Establecer la ubicación física del equipo computacional, en un lugar donde los adultos puedan mantener vigilancia de la navegación de los menores de edad, y evitar que naveguen en sus habitaciones a puerta cerrada.

Excitarle el día a tu pareja con una foto picarona puede ser muy fácil pero siempre ten en mente que puede que la imagen termine en un lugar que no quieres y que eso te traiga más de un problema. Sigue los consejos que los expertos te dieron para evitarte el mal rato.

Fecha de creación
septiembre 2014