Universidad Veracruzana

Seguridad en redes sociales

Ciberseguridad
UV-CSIRT

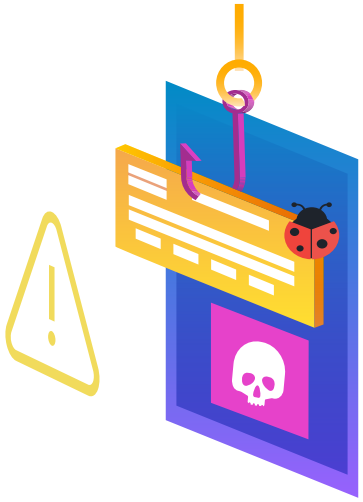
Información segura... ¡es cultura!®

Seguridad en redes sociales

El uso de las redes sociales se ha incrementado cada vez más a nivel internacional convirtiéndose en una herramienta de marketing indispensable en las empresas o instituciones públicas, ya que permite tener mayor visibilidad de lo que hace u ofrece la organización, sin embargo existen riesgos que pueden afectar la seguridad y privacidad de la información que se publica y comparte en dichas redes sociales.

Conoce los riesgos en el uso de las redes sociales

- **Exposición de información personal.** Las redes sociales al ser de uso masivo son un buen medio para acceder a gran cantidad de información personal que los usuarios publican en sus redes sociales y que llaman la atención de los cibercriminales para usarla con malos propósitos.
- **Problemas por realizar una configuración de privacidad débil o nula.** Los usuarios frecuentemente no realizan una configuración de privacidad y seguridad adecuada, no hacen ningún tipo de restricción en la información que publican o de permisos que dan a las aplicaciones que no son necesarios.
- **Ciberacoso o cyberbullying.** La información que una persona puede obtener de los datos del perfil de las redes sociales de la víctima, puede usarla para acosar psicológicamente, incluso a menores de edad.
- **Posible aplicación de sanciones.** Al compartir información sensible que pertenece a otras personas o al difundir, difamar, insultar o hacer rumores falsos podría ser sujeto de sanciones conforme a la ley aplicable.



- **Fraudes por suplantación de identidad.** Aprovechan la información difundida por los usuarios en las redes sociales para robar la identidad.
- **Distribución de malware.** Las redes sociales son un medio de distribución de código malicioso, en el que los medios más comunes que se usan para ese fin son phishing, enlaces maliciosos, videos o publicidad falsa.
- **Ser víctima de delitos físicos.** Al publicar información sensible, los ciberdelincuentes pueden aprovecharlo y usar su ubicación actual u otro tipo de información para cometer robos, estafas u otros delitos.

Seguridad en redes sociales

¿Cómo protegerte en las redes sociales?

- **Protege tu imagen e identidad.** El nombre de usuario y el icono en el perfil pueden ser visibles al público aún cuando se configure la privacidad, por lo que al usar el nombre completo de una persona en las redes sociales o usar el mismo alias que el correo electrónico es mayor el riesgo de que sea utilizada la información de forma ilícita.

Respecto al **icono del perfil** se debe pensar bien qué se quiere transmitir y considerar que una vez que se sube a la red social se pierde el control de la misma ya que pueden ser descargadas, manipuladas y circuladas por otras personas con intenciones desconocidas.

- **Contraseñas robustas.** Una contraseña fuerte debe ser larga, combinando números, letras y caracteres especiales en la que no se tenga un patrón. Es preferible usar un gestor de contraseñas para guardarla, al que también se tendrá acceso mediante otra contraseña robusta. Se recomienda no usar datos personales en las contraseñas como fechas de nacimiento.

- **Localización.** Una buena práctica es no difundir tu domicilio en la información de tu perfil o publicar tu ubicación actual o futura ya que pueden exponerse a riesgos de ser víctima de algún delito.

- **Leer las condiciones de prestación de servicios de la red social.** En la mayoría de los casos el correo electrónico y teléfono no son visibles de forma pública aunque se brinden, permanecen privados solo para el usuario, sin embargo se deben leer las condiciones para saber a qué empresas serán o no compartidos los datos y bajo qué condiciones.

Seguridad en redes sociales

- **No utilizar la misma contraseña para varias redes sociales.** Esta es una buena práctica ya que en caso de que la contraseña de una red social quedara comprometida, las demás redes no serían comprometidas.

- **Utilizar autenticación en dos pasos.** Para asegurar más el acceso a una red social, se puede agregar la opción de verificación en dos pasos.

- **Precaución al aceptar solicitudes.** En algunas ocasiones se suelen aceptar solicitudes incluso de desconocidos, por lo que es más probable de presentarse algún riesgo, por ello es importante que se acepten solicitudes sólo de personas conocidas.

- **Configuración de privacidad.** En esta configuración se define lo que el usuario muestra y oculta públicamente en las redes sociales. Se puede proteger contenidos a todos o de forma individual para que sean visibles solo por el usuario y/o por sus contactos o amigos.

  Los permisos para acceder a los contactos de un usuario, es otro aspecto importante a considerar en el uso de las redes sociales.

- **Usa el sentido común al publicar.** Al subir contenido en redes sociales es fundamental usar el sentido común, es decir, si de forma habitual por seguridad no damos datos personales, en el ciberespacio debemos hacer lo mismo. Por ello debemos **pensar en los riesgos, antes de publicar una foto, información personal del usuario, de amigos, conocidos o noticias.**

Seguridad en redes sociales

“El usuario es la primer línea de defensa para protegernos en el ciberespacio.”

#InformaciónSeguraEsCultura

Referencias

https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3009-ccn-cert-bp-08-redes-sociales/file.html

https://www.incibe.es/protege-tu-empresa/blog/buenas-practicas-redes-sociales-aumenta-tu-popularidad-sacrificar-seguridad