



DGTIC UNAM

DIRECCIÓN GENERAL DE CÓMPUTO Y
DE TECNOLOGÍAS DE INFORMACIÓN
Y COMUNICACIÓN



Seguridad en las Redes Sociales

CURSOS EN LÍNEA



Seguridad en las Redes Sociales

La evolución de las tecnologías e infraestructuras de comunicación, así como el crecimiento exponencial en el uso de dispositivos electrónicos conectados a internet, han facilitado la adopción y proliferación de las redes sociales.

Las redes sociales se han convertido en una de las principales formas de interacción de las sociedades modernas. En estos espacios, las personas comparten sus intereses sociales, culturales, actividades de entretenimiento y su forma de vida. De esta manera, las redes sociales complementan las relaciones interpersonales, y favorecen la creación de sistemas complejos de comunicación. Sin embargo, dado su alcance y la inmensa cantidad de información que se puede obtener de ellas, las redes sociales representan un riesgo a la seguridad de las personas si no se toman las medidas adecuadas. Por lo tanto, en los siguientes materiales estudiaremos cómo protegernos ante posibles situaciones que afecten la seguridad de nuestra información en estos medios.

Redes sociales

Como se ha mencionado, las redes sociales han cambiado la forma en la que la sociedad interactúa, pues en estos medios los usuarios son tanto consumidores como productores de datos en la forma de texto, imágenes, videos, mensajería, video llamadas, entre otros tantos diferentes formatos de interacción. Es tal su impacto en nuestra sociedad que se han llegado a utilizar para crear mensajes destinados a influir en los resultados de elecciones presidenciales en diferentes países, formar opiniones, así como para actividades tan diversas como la búsqueda de empleos, encontrar una pareja sentimental, o incluso, para realizar transacciones comerciales. Es por esto que las redes sociales se convierten en un medio relevante que debe ser tomado con seriedad y prudencia.



Figura 1. Desde hace años las redes sociales juegan un papel central en la interacción de las personas.

Existen una gran variedad de redes sociales entre las que destacan: FACEBOOK, X (ANTES TWITTER), TIKTOK, INSTAGRAM, YOUTUBE, LINKEDIN, etc. Incluso aplicaciones como TINDER y WHATSAPP también se pueden considerar como una red social.

Es innegable que las redes sociales han permitido adoptar el espacio digital como un medio de convivencia e información. Sin embargo, a pesar de los aspectos positivos destacables, es importante establecer los riesgos inherentes en el uso de estos medios de comunicación.

Existen personas malintencionadas que utilizan las redes sociales como un medio para recabar información sobre las personas y para preparar ataques especializados en su contra. Es por esta razón que los usuarios deben ser conscientes del tipo de información que comparten en estos espacios.



Figura 2. Existen diferentes tipos de riesgos tanto a nuestra información como a nuestra integridad al hacer uso de redes sociales.

Información de alto riesgo

En este apartado se revisará el tipo de información que se comparte en las redes sociales y se intentará concientizar al lector sobre los peligros de publicar información sensible.

La información que se comparte en redes sociales debe revisarse con lupa, pues de manera inconsciente puede revelarse información que podría traer consecuencias adversas para los usuarios que la publican.

Información	
Información general	+ Agrega un lugar de trabajo + Agrega una escuela secundaria + Agrega una universidad
Empleo y formación	
Lugares de residencia	+ Agrega tu ciudad actual + Agrega tu ciudad de origen
Información básica y de contacto	
Familia y relaciones	
Información sobre ti	+ Agrega tu situación sentimental
Acontecimientos importantes	

Figura 3. Ejemplo de información que se solicita para un perfil en la red social Facebook.

Reflexione por un momento sobre la información que comparten las personas en redes sociales, todos aquellos mensajes, fotografías, videos, pensamientos y vivencias. Ahora, medite ¿qué información podría utilizar un atacante para hacer daño? Esta reflexión es importante porque las publicaciones pueden llegar a un gran número de personas, incluso personas que usted nunca pensaría (¿realmente los usuarios de redes sociales conocen a todos y a todas las personas que han agregado como amigos?).



Figura 4. Recuerde que existen personas dedicadas a la recopilación de información para realizar un ataque.

Además, al momento de compartir datos tendrá que asimilar que, una vez que la información se ha compartido en internet, se pierde la posibilidad de su control. Por lo tanto, es necesario limitar la información que se comparte para evitar ser víctima de algún ataque.

Información personal

En ocasiones, los usuarios de redes sociales llegan a publicar información personal en sus redes sociales. Información como la fecha de nacimiento, información financiera, fotografías, videos, datos profesionales, así como cualquier información que permita su ubicación geográfica como su domicilio o lugares que frecuenta deben ser analizadas antes de compartirse por estos medios.

El siguiente video muestra la cantidad de información que se pueden encontrar de las personas en redes sociales: <https://www.youtube.com/watch?v=k046eLzdU1o>

Principales riesgos en redes sociales

Existe una gran cantidad de riesgos al utilizar redes sociales que los usuarios deberían conocer. En este apartado se listan los principales.

Robo de identidad

El robo de identidad ocurre cuando una persona malintencionada roba la información personal de alguien más y la utiliza para realizar diversas actividades maliciosas. Por ejemplo, se puede llegar a usar para fraudes financieros o actividades ilegales.

Para esto, los atacantes buscarán robar de los usuarios de redes sociales información como sus fotografías, datos de nacimiento, u otra información para hacerse pasar y suplantar la identidad de las víctimas. Por esta razón, es importante limitar tanto los contactos con los que se comparte la información, así como el tipo de información que se publica, en especial si se trata de datos sensibles.



Es justamente la inmensa cantidad de información que se comparte en las redes sociales lo que provoca que los atacantes tengan acceso a la materia prima necesaria para preparar un ataque. Un ejemplo común que un atacante realiza es el de utilizar la información que comparten los usuarios para intentar descifrar las respuestas a preguntas de seguridad de las cuentas. Por ejemplo, ¿cuál es el nombre de su mascota?, ¿cuál es su fecha de nacimiento?, etc. Tenga cuidado con revelar inconscientemente esta información.

Otro vector de peligro potencial que puede derivar en el robo de identidad es que, en algunos casos, se puede acceder a otros servicios (cuentas de correo, otras redes sociales, otras aplicaciones web) utilizando las mismas credenciales de autenticación que se usan para redes sociales. Si bien esto puede resultar conveniente en algunas ocasiones, el uso de esta verificación no es recomendable, pues supone un mayor riesgo ya que no solo su cuenta de la red social se vería comprometida, sino que también afectaría su cuenta en múltiples servicios. Por esta razón, se sugiere no utilizar la misma contraseña para todos los servicios y aplicaciones, así como evitar la autenticación por medio de cuentas de redes sociales.



Figura 5. Cada pieza de información es importante para las personas maliciosas que intentan robar su identidad.

Por otro lado, el atacante puede crear nuevas cuentas en la red social y copiar la información para suplantar la identidad de una persona y hacerse pasar por esta ante otros usuarios o contactos originales de la víctima. Es decir, cuando se roba la identidad de las personas pueden surgir diferentes tipos de ataques más elaborados. El atacante puede fingir ser la persona a la que le ha robado la cuenta para solicitar información a otras personas. En este caso, la víctima podría resultar ser no solo aquella a la que le han robado la cuenta original, sino también todos aquellos contactos que confían en que se trata de la persona conocida. Existen muchos ejemplos: un contacto que ofrece (con urgencia) algún aparato electrónico en un precio increíble, o que le solicita dinero, o información porque enfrenta una necesidad grave. Por lo tanto, resulta importante también estar atento al tipo de mensajes que se reciben en redes sociales, incluso de aquellas personas que consideramos son de confianza. Cuando note algo fuera de lo normal con un contacto, no actúe con precipitación, piense por un momento e intente contactar a la persona por otro medio para comprobar que realmente se trata de quien usted piensa.

Fraudes y estafas

Los fraudes en internet no son nuevos, pero se han modificado para aprovecharse del ambiente de las redes sociales. Estos fraudes ahora se realizan de manera personalizada gracias a la gran cantidad de información que los usuarios colocan de sí mismos en estos medios.

Los fraudes pueden ser diversos y pueden llegar a utilizar enlaces maliciosos. Por ejemplo, los enlaces con una supuesta oferta de descuento de un producto o servicio que se anuncia como exclusivo, o por un periodo de tiempo limitado, y que guían al usuario a un sitio web que contiene malware o en el que se solicita, por medio de engaños, información adicional al usuario que pudiera comprometer su seguridad.

Las estafas en redes sociales son tan variadas que resultaría imposible abarcarlas todas, pues, además, muchas de ellas están diseñadas para contextos específicos. Sin embargo, por regla general: **si algo parece demasiado bueno para ser verdad, es muy probable que se trate de una estafa.**

En México algunas de las principales estafas en la red están relacionadas con descuentos y préstamos económicos, ofertas de empleos, automóviles y departamentos en oferta, e incluso, las estafas relacionadas con supuestas parejas sentimentales. Existen noticias muy desagradables sobre alguna de estas estafas que han llevado a consecuencias irreversibles en la vida de las personas.

Malware

El malware es todo software malicioso. Los atacantes utilizan este tipo de programas para afectar los equipos de las víctimas, y comprometer su seguridad. Pero ¿cómo es que se puede descargar malware de una red social? Por medio de engaños y redirecciones. Por esta razón, deberá prestar especial atención a todos aquellos enlaces que recibe. Existen muchas personas que envían mensajes anónimos a otras para intentar que hagan clic en enlaces, accedan a páginas web o descarguen un archivo. Los atacantes utilizarán diferentes tipos de técnicas para hacer un enlace atractivo para la persona, este enlace podría comenzar la descarga de software malicioso o enviar al usuario hacia un sitio web diseñado para esto.



Figura 6. Las redes sociales no están exentas del riesgo de descarga de malware en nuestros equipos.

Información y noticias falsas

Si bien las redes sociales son una poderosa fuente de información, es posible que esta se vea alterada o que no sea verdadera. Existen perfiles, usuarios, y organizaciones dedicadas a la producción de información falsa. Es la falta de verificación de la información que se comparte en algunas redes sociales lo que permite la proliferación de mensajes falsos.

Las noticias falsas son utilizadas frecuentemente en campañas que intentan influir en la opinión general. Las campañas de influencia intentan cambiar la opinión, acciones o comportamiento del público al que van dirigido por medio de una serie de acciones coordinadas. Si bien este tipo de campañas han existido por siglos, la tecnología de comunicación y la evolución de los dispositivos informáticos, así como el surgimiento de redes sociales, han permitido que la información se pueda compartir y divulgar a un ritmo nunca antes visto.

Este tipo de mensajes también puede ser utilizado en combinación con otros ataques. Por ejemplo, esta información se puede usar para crear un miedo innecesario y provocar conductas irracionales.

Imagine una falsa campaña donde se alerta a los usuarios de un virus informático destructivo que puede afectar sus equipos sino descargan cierto programa o que elimine ciertos archivos de su computadora. Puede adivinar que el malware es justamente lo que el usuario descargará en caso de seguir esta noticia falsa o que sería el mismo usuario el que afectaría su sistema por eliminar posibles archivos clave. Nuevamente, en este apartado resulta imposible imaginar todos los escenarios posibles. Por lo tanto, se recomienda prudencia y la verificación de información en fuentes oficiales y acreditadas.

Ciberacoso

El ciberacoso implica el uso indebido de tecnologías digitales para acechar, intimidar o acosar a individuos. Pero es realizado, principalmente, a través de plataformas de redes sociales. Los *stalkers* (acosadores) pueden recopilar información personal de perfiles en línea, como nombres, direcciones, números de teléfono y ubicaciones, para rastrear los movimientos de sus víctimas. Este comportamiento intrusivo viola la privacidad de las personas y puede dejarlas vulnerables a la vigilancia no deseada.

El ciberacoso no solo infringe la privacidad de los usuarios de redes sociales, sino que también puede tener graves consecuencias emocionales y psicológicas. Por ejemplo, en una variante como el cyberbullying donde se realiza la burla, ofensa o exclusión, las víctimas de este tipo de acoso pueden experimentar miedo, ansiedad, depresión y estrés postraumático debido a la constante sensación de ser observadas y perseguidas en línea. Este impacto negativo en la salud mental puede afectar la calidad de vida de las personas y socavar su bienestar general.

Las políticas de privacidad y seguridad de las redes sociales a menudo no son lo suficientemente robustas como para proteger adecuadamente a los usuarios contra este tipo de abuso en línea. Por lo tanto, es fundamental que los usuarios sean prudentes en la información que comparten.

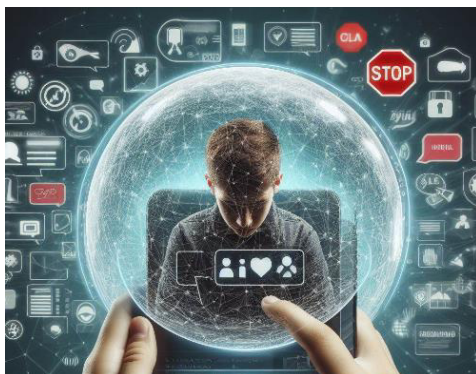


Figura 7. El ciberacoso es un problema serio que afecta emocionalmente a las víctimas.

Daño a la reputación personal

Antes de realizar alguna publicación usted tiene que meditar si el contenido pueda afectar su reputación o la de los demás. ¿Su jefe o su familia encontrarían apropiada su publicación?, ¿realmente es necesario publicar esta información? Incluso si no tiene como contactos a las personas, recuerde que, una vez en internet, usted pierde el control de lo publicado. Algún contacto en común puede mostrar la información a otras personas a las que usted no ha concedido

el permiso. Esto es importante a considerar puesto que, hoy en día, cuando las organizaciones ofertan un empleo realizan una revisión de las cuentas de redes sociales de los candidatos en busca de información sobre ellos. Incluso para obtener la visa americana se realiza un estudio de las redes sociales de las personas¹. Por lo tanto, resulta necesario cuidar nuestra identidad digital tanto como nuestra identidad personal y limitar nuestra exposición, sobre todo si se trata de información que puede traer un daño a nuestra reputación.



Figura 8. Recuerde la importancia de su reputación cada vez que realiza una publicación en una red social.

Geolocalización

Agregar información geográfica de su localización o de los sitios que frecuenta es un peligro, mucho más cuando esto se realiza en tiempo real. Una persona malintencionada puede abusar de esta información para cometer un crimen en su contra o de sus seres queridos.

La característica de geolocalización se utiliza en algunas redes sociales que permiten adjuntar esta información en fotografías, videos, o mensajes, para señalar el punto de ubicación, o bien, desde dónde se ha realizado la publicación de un mensaje.

También es común que las personas publiquen de manera voluntaria dónde han estado o dónde se encuentran. Esto es una actividad no recomendable. La dirección de su domicilio y los sitios que frecuenta, su localización, cuándo y dónde toma sus vacaciones, deberían considerarse como información confidencial y no se debería compartir con cualquier persona.

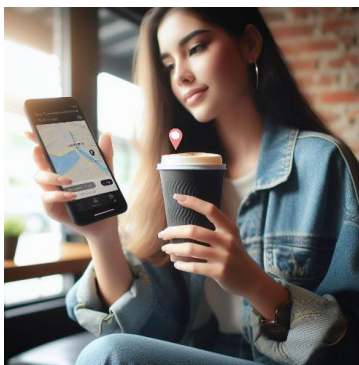


Figura 9. La información de nuestra geolocalización puede utilizarse para atacarnos.

¹ El financiero. (26 de marzo de 2023). Visa 2023: ¿Revisan tus redes sociales para darte el documento estadounidense? <https://www.elfinanciero.com.mx/mis-finanzas/2023/03/26/visa-2023-revisan-tus-redes-sociales-para-darte-el-documento-en-estados-unidos/>

Sexting

Una práctica que pone en un mayor riesgo aún a las personas en las redes sociales es el sexting. Se trata del envío de mensajes de texto, audio, fotografías y videos íntimos o con connotaciones sexuales que se comparten con otra persona utilizando este medio. Obviamente, la utilización de redes sociales para compartir este tipo de mensajes esta desaconsejada, justamente, porque **una vez que se publica información en internet, se pierde su control**. Pero el sexting es una práctica que muchas personas llevan a cabo. De hecho, existen diferentes casos documentados de robo de esta información que han llegado a crear incluso leyes especializadas como lo es la LEY OLIMPIA que prohíbe compartir este tipo de material sin consentimiento de las personas que aparecen en ellas, justamente, porque este tipo de material puede ser robado y distribuido rápidamente por medio de las mismas redes sociales.

No se puede enfatizar lo suficiente que **esta práctica no debería ser realizada** porque se pierde el poder sobre la confidencialidad una vez que se utiliza un medio inseguro como internet para compartir este tipo de información.



Figura 10. El sexting es una práctica que conlleva un riesgo significativo en la vida de las personas.

Otros riesgos

Desgraciadamente, la información de las redes sociales puede servir para que personas malintencionadas lleguen a cometer delitos graves:

- Secuestros. Se han documentado casos en los que personas llegan a citarse con algún contacto que conocieron por medio de redes sociales y que terminan secuestradas, violentadas, o, incluso, sin vida.
- Amenazas para menores de edad. Las redes sociales representan un riesgo considerable para las personas más vulnerables. Los menores de edad son el blanco de depredadores sexuales y pedófilos. Estas personas aprovechan las posibilidades de las redes sociales y pueden llegar a hacerse pasar por menores de edad para entrar en contacto y engañarlos.

Aunque la mayoría de redes sociales solicitan información para prevenir que menores de edad utilicen el servicio (incluso hay países donde se prohíbe explícitamente el uso de redes sociales a menores), es muy común que estos se encuentren enganchados con alguna red social y que no tengan la conciencia suficiente para identificar los riesgos que representa su exposición a este medio.



Figura 11. Los menores de edad son el sector más vulnerable en redes sociales.

MEDIDAS DE PROTECCIÓN

Existen diferentes medidas de protección que conviene adoptar para nuestra protección en el uso de redes sociales:

Contraseñas

- Utilice contraseñas complejas y robustas en las cuentas de redes sociales.
- No usar o reusar contraseñas en redes sociales que se han utilizado en otros sitios. Si las cuentas de redes sociales han sido comprometidas, es posible que un actor malicioso pueda intentar acceder a otros sitios con las mismas credenciales.

Enlaces

- Tener extremo cuidado de los enlaces y archivos adjuntos de los mensajes que se reciben, así como de aplicaciones que se descargan. De manera general, se recomienda NO abrir cualquier tipo de enlace a menos de que se confíe totalmente de la persona que envía el mensaje.

Configuración de privacidad

- Configurar la privacidad en el perfil. El usuario debería investigar las configuraciones de privacidad de la red social y ajustar los parámetros según sus necesidades. Sin embargo, de manera general se debería:
 - Definir alertas de acceso a cuenta.
 - Desactivar la geolocalización automática y nunca publicarla de manera voluntaria.
 - Limitar la audiencia. Identificar y seleccionar, cuidadosamente, los contactos que pueden observar su información.
 - Limitar quién puede contactarlo. En la mayoría de redes sociales existen configuraciones para bloquear cualquier tipo de mensajes que vengan de usuarios a los que no se han aceptado como contactos.
 - Limitar quién puede buscarlo. Definir parámetros que limiten su aparición en los sistemas de búsqueda de las redes sociales.
 - Bloquear usuarios. Establezca los controles necesarios para bloquear a otros usuarios que usted considere como un riesgo y bloquear los mensajes no solicitados o de remitentes desconocidos.
- Prestar atención a las solicitudes de amistad que recibe. Se recomienda aceptar en su red solamente a aquellas personas que realmente conozca.
- Nunca publicar información sensible que pudiera ser utilizada para el robo de información. Meditar sobre la necesidad de hacer una publicación y considerar que la información podría colocarlo en una situación vulnerable si expone información considerada de riesgo.
- No compartir información personal, embarazosa de usted ni de sus conocidos y familiares. Mantenga su trabajo y su vida personal separada de sus redes sociales. Se recomienda que use redes separadas, una para el ámbito profesional y una para el ámbito personal si lo considera necesario.
- Revisión y auditoría de las amistades. ¿Realmente conoce a esta persona? Es posible que entre sus contactos haya alguien que pudiera estar planeando un ataque en su contra. Valore la eliminación de los contactos desconocidos.
- Mantener activadas las preferencias seguras del navegador. Revise siempre las URLs que aparecen en la barra de navegación, estas podrían indicarle información importante sobre los sitios que está utilizando y prevenir posibles ataques.
- Reportar abusos en caso de acoso. Las autoridades podrían llegar a intervenir en casos severos, pero necesitan ser reportados.
- Mantenga su sistema operativo y una solución antimalware actualizados. En caso de algún ataque, es posible que su sistema se encuentre mejor preparado si cuenta con las últimas actualizaciones y parches de seguridad.



Copyright© 2024

Todos los derechos reservados, incluyendo el derecho de reproducción en su totalidad o en parte, bajo cualquier forma.

Universidad Nacional Autónoma de México

AUTOR

ELIER EMANUEL LÓPEZ BASILIO