Redes sociales

Las redes sociales nos permiten comunicarnos con otras personas y compartir nuestras opiniones, gustos personales, fotografías, etc.

De esta forma, se convierten en un almacén de información personal. Además, mediante ellas, podemos ampliar nuestras relaciones profesionales, personales o, simplemente, compartir aficiones.

Pero es fundamental que consideremos algunos consejos y los posibles riesgos para disfrutar de ellas de una forma segura.

Cuidado con lo que publicas

Cada vez que publicamos algo en una red social perdemos el control sobre ese contenido. Aunque lo borremos, quedará como mínimo registrado en los servidores de la red social y cualquiera que lo haya visto puede haber hecho uso de esa información, ya sea difundiéndola o copiándola.

Debemos valorar qué queremos publicar, especialmente teniendo en cuenta nuestra configuración de la privacidad y en consecuencia quién podrá ver toda esa información.

Cuida tu privacidad

Todas las redes sociales disponen de diferentes controles para proteger nuestra privacidad.

Debemos aprender a utilizar y configurar adecuadamente las opciones de privacidad de nuestro perfil. De esta forma sólo tendrán acceso a nuestros datos las personas que establezcamos y reduciremos el riesgo de que pudiera ser utilizada con fines malintencionados.

Cuidado con los permisos de las aplicaciones

Existen multitud de juegos y aplicaciones disponibles en las redes sociales, algunos de ellos muy populares: Candy Crush Saga, Instagram, Farmville, etc. La mayoría están desarrollados por terceras empresas.

Para poder utilizarlos, debemos aceptar ciertas condiciones y permisos de acceso a nuestro perfil que, en ocasiones, se activan simplemente pulsando el botón de “Jugar”, como en la imagen que vemos a continuación:

Debemos ser muy precavidos con los permisos que damos a las aplicaciones y evitar aquellas que requieren autorizaciones que no son necesarias (acceso al correo electrónico, fotografías, información de nuestros contactos, etc.) dado que algunas aplicaciones son desarrolladas para obtener información de nuestro perfil y de nuestros contactos con fines que no son los previsibles para el propio funcionamiento del juego, generalmente para fines publicitarios, pero en algunas ocasiones, con fines maliciosos.

Cuidado con los virus

Las redes sociales se han convertido en un foco importante de distribución de virus con el fin principal de robar información. Existen muchas formas de distribuir virus, pero el objetivo del delincuente es siempre el mismo: conseguir que pinchemos en un enlace que nos descargará un virus o nos llevará a una página web fraudulenta donde se nos solicitará que introduzcamos nuestro usuario y contraseña.

Para ello, los delincuentes utilizan vídeos o artículos "gancho", y falsas publicaciones que prometen informarnos de quién ha visitado nuestro perfil o ha dejado de ser nuestro "amigo".

Para no caer en la trampa, debemos desconfiar de cualquier enlace sospechoso, provenga o no de un conocido, ya que éstos también pueden haberse infectado y estar distribuyendo este tipo de mensajes sin ser conscientes de ello. Por tanto, debemos ignorar aquellas noticias, vídeos o imágenes morbosas que nos invitan a salir de la red para poder verlos, a instalar algún plugin o reproductor, etc.

Como siempre, debemos disponer de un antivirus actualizado y estar prevenidos ante cualquier comportamiento sospechoso. En caso de duda, es útil realizar una pequeña búsqueda sobre el contenido en Internet. Si se trata de un virus, no tardaremos en averiguarlo.

Cuida tu identidad digital

En las redes sociales tenemos mucha información personal, fotografías nuestras y de nuestros familiares, información sobre nuestros gustos... por lo que resulta un campo interesante para personas malintencionadas.

Con tanta información al alcance, se pueden producir situaciones como el robo de identidad o la suplantación de identidad.

- **Robo de identidad:** Alguien se ha hecho con nuestra cuenta y se hace pasar por nosotros publicando o enviando mensajes en nuestro nombre. Ha accedido a través de nuestra contraseña.
- **Suplantación de identidad:** Alguien ha creado un perfil con nuestros datos y fotografías para que la gente piense que somos nosotros.

Tanto en un caso como en otro, el delincuente puede utilizar nuestra imagen y nuestros datos para realizar acciones delictivas.

Para evitar este problema, debemos tener mucho cuidado en entornos no seguros: equipos compartidos o públicos y redes WiFi no confiables. Si es posible, lo más prudente es no acceder desde estos sitios. Si lo hacemos, debemos recordar cerrar siempre la sesión al terminar, y no permitir recordar la contraseña.

También debemos denunciar al centro de seguridad de la red social cualquier sospecha de suplantación, tanto si somos nosotros las víctimas como si sospechamos que pueden estar suplantando a otra persona.

Si pensamos que la suplantación de identidad puede haber ido más lejos y que se han realizado actos delictivos con nuestra identidad, debemos denunciarlo ante las Fuerzas y Cuerpos de Seguridad del Estado.

Suplantación de identidad, robo de identidad y ciberacoso son algunos de los delitos más frecuentes en redes sociales.

Actúa frente a los acosadores

Algunas personas utilizan las redes sociales para intimidar a otros usuarios mediante insultos, amenazas, fotos comprometidas o difusión de rumores falsos. También podemos ser víctimas de ciberacoso.

Al ciberacoso están expuestos tanto los menores como los adultos, pudiendo generar situaciones verdaderamente dramáticas y complicadas. Si en una red social sufrimos algún tipo de acoso, tenemos que ignorar y bloquear al acosador y guardar las pruebas del acoso: sacar pantallazos y no borrar los mensajes, por ejemplo. Además, debemos informar de la situación al centro de seguridad de la red social y denunciar el acoso a las Fuerzas y Cuerpos de Seguridad del Estado.

Consejos finales

Las redes sociales son estupendas herramientas de comunicación con otras personas, pero debemos utilizarlas de forma segura. Para ello:

- Configura adecuadamente la privacidad de tu perfil.
- Filtra la información que subes a Internet. Ten en cuenta que una vez subida pierdes el control de la misma.
- Piensa antes de publicar algo, ya que una vez publicado no sabes si saldrá de la red social. Podrán utilizar esa información en tu contra.
- Revisa las aplicaciones instaladas y ten cuidado con publicaciones sospechosas, aunque provengan de contactos conocidos.
- Las principales redes sociales se toman muy en serio los problemas de seguridad de sus usuarios. Si tienes problemas, contacta con ellos a través de los mecanismos de contacto o de denuncia que facilitan.

- Asegúrate de que tus contactos en las redes sociales son realmente quienes crees que son. No nos conformemos con ver la foto, el nombre o que es amigo de nuestros amigos.
- Al igual que en la vida real, en las redes sociales también debemos ser respetuosos y tratar con educación a nuestros contactos. No envíes mensajes ofensivos a ningún contacto. Debes ser respetuoso y tratar con educación a tus contactos.
- No compartas fotos ni vídeos en los que aparezcas en situaciones comprometidas (sexting).
- No te olvides de leer la política de privacidad y las condiciones del servicio antes de usarlo.