feuso Federación de Enseñanza
www.feuso.es
SALUD LABORAL
nº 383

TU SEGURIDAD EN LA RED

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. Al ciberacoso o ciberbullying 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.

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 posibles riesgos para disfrutar de ellas de una forma segura.

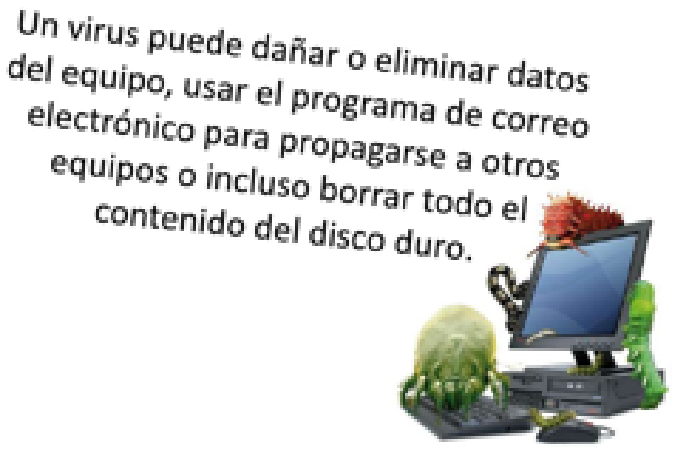
UN POCO DE VOCABULARIO

- **Ciberbullying:** Amenazas, hostigamiento, humillación u otro tipo de molestias realizadas por un adulto contra otro por medio de tecnologías telemáticas de comunicación, es decir: Internet, telefonía móvil, videoconsolas online, etc.
- **Grooming:** Es un nuevo tipo de problema relativo a la seguridad de los menores en Internet consistente en acciones deliberadas por parte de un adulto de cara a establecer lazos de amistad con un niño o niña en Internet, con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual.
- **Sexting:** Consiste en el envío de contenidos de tipo sexual (principalmente fotografías y/o vídeos) producidos generalmente por el propio remitente, a otras personas por medio de teléfonos móviles.
- **Netiqueta:** La *netiqueta* es un conjunto de normas de comportamiento que hacen de Internet y las TIC sitios más agradables, en donde la convivencia y el respeto mutuo son primordiales. Aunque representan un código de conducta, la *netiqueta* fue ideada para indicar la mejor manera de comportarse usando las TIC. Gracias a ella podemos comunicarnos adecuadamente, mientras disfrutamos y aprovechamos de mejor manera las redes sociales, chats, videojuegos, foros y las TIC en general.

CUIDADO CON LO QUE PUBLICAS

Cada vez que publicamos 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 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 condiciones y permisos de acceso a nuestro perfil que, en ocasiones, se activan simplemente pulsando el botón de "Jugar".

Debemos ser muy precavidos con los permisos que damos a las aplicaciones y evitar las 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 se han convertido en un foco importante de distribución de virus con el fin principal de robar información. Existen 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, 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 (FCSE).

Fuente: www.osi.es/es/redes-sociales

Más información para docentes:
www.tudecideseninternet.es/educadores/lexicon/glosario
www.tudecideseninternet.es/menores/

Imma Badia Camprubí
Secretaria de Salud Laboral
FEUSO