LA SOCIEDAD DE LA INFORMACIÓN

Riesgos de las Redes Sociales

Hoy en día todos utilizamos las redes sociales, y por lo tanto, estamos expuestos a riesgos que, algunas veces, minusvaloramos.

Para un adolescente, pertenecer a una red social tiene como objetivo acaparar el mayor número de amigos. Estos amigos pueden ser amigos personales que conocemos, o amigos de amigos o incluso, personas que nos han solicitado "amistad" pero que no conocemos.

El "AMIGO" en las redes sociales, tiene un significado diferente al tradicional que recibe en la vida real. En la red "AMIGO" es todo aquél que ha sido aceptado en nuestro sitio, blog, etc.

Lo que más valoran los adolescentes es la POPULARIDAD, es decir, tener muchos amigos. Y para tener amigos y ser popular necesitamos "humor" y "espontaneidad". Los jóvenes quieren aumentar su lista de amigos compartiendo información personal perdiendo el anonimato y la intimidad.

Cuando compartimos nuestra información en la red, CUAQUIERA puede verla.

RIESGOS:

1. Abrir sitios para que cualquiera los pueda ver.
2. Dar información personal.
3. Subir fotografías, propias o ajenas, que reflejen situaciones de intimidad.
4. Hacerse amigos de gente que no conocen.
5. Encontrarse en persona con "amigos" que sólo conoce en la red.

Un estudio de la Unión Europea determinó que el 50% de los adolescentes suele dar información personal en Internet y casi un 10% se encuentra personalmente con gente que conoció en la web.

80% menciona su ciudad
60% sube sus propias fotos
30% da el nombre de su escuela
10% usa su nombre completo

PREVENCIÓN

Qué podemos hacer ante los riesgos que hay en la Red.

Lo ideal sería que el adolescente confiara en el asesoramiento de los padres, y pedir ayuda ante cualquier duda.

Podemos también tomar ciertas precauciones en las redes sociales:

1. **Ordenar los contactos en GRUPOS:** Podemos separarlos por familia, amigos, escuela, etc. Así cuando los grupos estén formados podremos decidir que publicación pueden ver.

2. **Decidir qué se permite ver.** Podemos configurar qué parte de nuestro portal se ve y quiénes acceden a él.

3. **Dirección y teléfono:** Es mejor no subirlo nunca, pero si decidimos hacerlo, configurar el sitio para que solo lo vean aquéllas personas que nosotros decidamos.

4. **No habilitar siempre el acceso:** A veces es conveniente configurar nuestra página para que solo la puedan ver los amigos o solo familiares, y así no te encuentran los desconocidos.

TECNOADICIONES

Los adolescentes pasan demasiado tiempo en el ordenador, concretamente en las redes sociales, buscando mejorar las relaciones con sus amigos y conocidos. Sin embargo, actualmente, se está sustituyendo el ordenador por el teléfono móvil, pues nos permite acceder a todos los contenidos de la red en cualquier lugar que nos encontremos. A las redes sociales clásicas como FACEBOOK, TWITER, MYSPACE, etc podemos añadir otras nuevas que han ganado mucha popularidad como WHASTAPP, e INSTAGRAM.

EL SEXTING

El 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.

No lo produzcas:

Si te sacas una fotografía erótica y se la envías a alguien mediante un móvil o Internet, pierdes inmediatamente el control sobre dónde podrá acabar algún día. Y si se la sacas a alguien, asegúrate de tener su permiso y de las implicaciones que podría tener perderla o que te la robasen. Y, por supuesto, tener permiso para sacar una foto a alguien para uso privado ¡no significa que tengas permiso para difundirla!

No lo transmitas:

Si te llega una foto o vídeo de algún/a conocido/a, no colabores en su expansión pues podría tener consecuencias graves tanto para él/ella como para ti.

No lo provoques:

No le solicites a nadie ese tipo de fotografías puesto que aunque tú no tengas malas

intenciones, alguna tercera persona podría hacerse con ellas y haceros mal a ti o a tu novio o novia.

GROOMING

Podemos definir Grooming de manera sencilla como el conjunto de estrategias que una persona adulta desarrolla para ganarse la confianza del menor a través de Internet con el fin último de obtener concesiones de índole sexual. Hablamos entonces de acoso sexual a menores en la Red y el término completo sería child grooming o internet grooming. Desde un acercamiento lleno de empatía y/o engaños se pasa al chantaje más cruento para obtener imágenes comprometidas del menor y, en casos extremos, pretender un encuentro en persona. El daño psicológico que sufren niños, niñas y adolescentes atrapados en estas circunstancias es enorme.

PHISING

El "phishing" consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la **realización de algún tipo de fraude**.
Para ello, suelen incluir un enlace que, al ser pulsado, lleva a **páginas web falsificadas**. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar **a manos del estafador**.

SPAM

Se llama **spam** o **correo basura** a los mensajes no solicitados, no deseados o de remitente desconocido y que son sumamente molestosos.

Por lo general, las direcciones son robadas, compradas, recolectadas en la web o tomadas de cadenas de mail. Aunque hay algunos **spammers** que envían solamente un mensaje, también hay muchos que bombardean todas las semanas con el mismo mensaje que nadie lee.

La mayoría de las veces si uno contesta el mail pidiendo ser removido de la lista, lo único que hace es confirmar que su dirección existe. Por lo tanto, es conveniente **no responder nunca a un mensaje no solicitado**, únicamente borrarlo y añadirlo a la lista de correo no deseado (spam).

MALWARE

Malware es la abreviatura de **“*Malicious software”,*** término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como**: Virus, Adware, Troyanos**, etc.

Los Virus Informáticos son sencillamente programas maliciosos que “infectan” a otros archivos del sistema con la intención de modificarlo o dañarlo.

El adware es un software que despliega publicidad de distintos productos o servicios y que incluyen código adicional que muestra la publicidad en ventanas emergentes, o a través de una barra.

Un troyano es un pequeño programa generalmente alojado dentro de otra aplicación para pasar inadvertido al usuario e instalarse en el sistema para realizar diferentes tareas sin que el usuario se dé cuenta, como por ejemplo conectar la webcam. Por ejemplo, cuanto te bajas un programa de Softonic, el archivo lleva incluido un troyano que se instala en nuestro ordenador y realiza tareas sin nuestro permiso (publicidad, cambios en el navegador, acceso remoto a nuestra webcam, etc.)

Principales vías de infección:

- Redes Sociales.
- Sitios webs fraudulentos.
- Programas “gratuitos” (pero con regalo)
- Dispositivos USB/CDs/DVDs infectados.
- Sitios webs legítimos previamente infectados.
- Adjuntos en Correos no solicitados (Spam)

¿Cómo protegernos del Malwares?

La prevención consiste en un punto vital a la hora de proteger nuestros equipos ante la posible infección de algún tipo de malware y para esto hay algunos puntos vitales que son:

- Un **Antivirus** actualizado
- Un “poco” de **sentido común.**
- **Todo siempre actualizado** (Win, Java, Flash, etc)
- **Mantenerse medianamente informado**s sobre las nuevas amenazas.