

¿Qué te acecha?



Cada vez que te metes en Internet, puedes ser víctima de múltiples amenazas, muchas de ellas con consecuencias muy serias y graves. ¡Estate alerta! En esta sección, te enseñamos los principales usos que se hacen de Internet y los riesgos que implican:

La mensajería instantánea

La mensajería instantánea (a través de programas como MSN Messenger, Yahoo! Messenger, Google Talk, etc.) es una gran herramienta para hablar con amigos y familiares a distancia, pero siempre tienes que andarte con mucho ojo.

1. **Uno de los riesgos es la suplantación de identidad.** Un contacto se hace pasar por alguien que tú conoces para acercarse a ti. Es el caso de pervertidos que se hacen pasar por personas jóvenes o fotógrafos de moda y se inventan cualquier excusa para citarse con niños como tú. No te creas nada de lo que te cuente por este medio alguien que no conoces bien, porque perfectamente puede estar mintiendote sin que lo sepas.
2. **La entrada de virus o código malicioso es otro riesgo.** Muchos virus están preparados para propagarse a través de programas de mensajería y así infectar a más gente.

Para evitar estos riesgos, lo mejor es no tratar con desconocidos y en caso de dudas o temor, hablar abiertamente con tus padres u otro adulto. Además, para evitar virus e infecciones no ejecutes ningún

archivo ni sigas ningún link que te llegue por este medio.

El correo electrónico

El correo electrónico, siendo algo habitual y extendido supone también múltiples riesgos que debemos tener en cuenta.

1. **El spam.** En muchas ocasiones, llegan a tu correo e-mails que anuncian todo tipo de cosas, desde casinos on-line hasta medicinas. Estos correos, no siempre dicen la verdad, sólo quieren engañarte. Bórralos sin remordimientos.
2. **Infección con virus u otro malware.** Son e-mails que te incitan a seguir un vínculo o descargar y ejecutar un archivo (lo que provocará la infección por un virus o código malicioso en tu computador) mediante el uso de un tema sugerente.

Para protegerte ante estas amenazas, lo mejor es desconfiar de los e-mails que proceden de gente que no conozcas. No todo lo que se cuenta en los e-mails es verdad y no debes ejecutar ningún archivo, ni hacer click sobre ningún link que proceda de este tipo de fuentes.

Las redes de Intercambio de archivos

El intercambio de archivos a través de programas como Emule o Kazaa es otra forma de que los ordenadores se infecten con virus. Muchos virus y códigos maliciosos se disfrazan con títulos de películas, programas, etc. para animar a ser descargados y abiertos.

Debes vigilar qué archivos puedes bajarte y cuáles no de estas redes. Además, conviene que analices el archivo con una solución de seguridad antes de ejecutarlo por primera vez.

Las redes sociales y blogs

Las llamadas redes sociales (portales como MySpace o Facebook) que sirven para compartir fotos y vídeos, conocer gente o chatear junto con los blogs o bitácoras, que son a menudo usados como diarios on-line, son algunos de los sitios web más visitados.

En ambos tipos de portales se da en muchas ocasiones más información de lo aconsejable. Por eso,

debes tener cuidado y no dar datos que puedan servir para identificarte como un menor, o para conocer dónde vives, dónde estudias, etc. Además es recomendable no dar tu verdadero nombre en Internet sino un pseudónimo o “nick”.

Móviles con Internet: nueva fuente de riesgo

El teléfono móvil es otro de los grandes complementos de hoy en día. Los riesgos del móvil son parecidos a los que hemos comentado para los ordenadores.

Servicios de mensajería instantánea para móviles es algo ya habitual. Puedes chatear en cualquier sitio y los riesgos son los mismos que ya se han comentado más arriba: robo de identidad, malos encuentros, infección del teléfono, etc.

1. **Spam.** Para el móvil también es algo que está a la orden del día. A menudo llega publicidad indiscriminada por medio de mensajes SMS y lo mejor es no hacerle caso.

Debes informarte sobre el uso adecuado de los móviles. Evita dar demasiada información o tratar con desconocidos. Sobre todo no contestes a mensajes de procedencia sospechosa.

Fuente: www.pandasecurity.com