INTERNET EN BUENAS MANOS

PROTEGIENDO LA SEGURIDAD DE LOS MAYORES EN INTERNET

PANDA SECURITY

PROTEGIENDO LA SEGURIDAD DE LOS MAYORES EN INTERNET

La proliferación del uso de Internet y de las nuevas tecnologías ha hecho que el acceso a la Red esté al alcance de todos. Sin embargo, **es necesario tomar algunas precauciones ya que esta accesibilidad no está exenta de algunos peligros.**

El objetivo de esta guía es **informar sobre las amenazas que tenemos que tener en cuenta** a la hora de navegar por Internet, así como ofrecer algunos consejos de prevención básicos para poder utilizar **Internet de forma segura.**

Cuando hablamos de los riesgos de Internet, hay que entender que hay un verdadero negocio mediante el cual, los ciberdelincuentes o hackers, generan mucho dinero mediante el engaño y técnicas fraudulentas. Estas son cada vez más imaginativas, para conseguir que un mayor número de personas sean víctimas. Por eso siempre decimos que cada vez hay más amenazas informáticas que utilizan los principales puntos de encuentro de la red para distribuirse, a la vez que pueden llegar también por correo electrónico, simplemente por la navegación web, etc.

A día de hoy, **nuestro laboratorio antimalware, PandaLabs, tiene analizadas y clasificadas más de 60 millones de ejemplares de malware,** y seguimos recibiendo una media de 63.000 nuevas muestras cada día. Este simple dato puede dar una idea de la necesidad de tomar precauciones cada vez que se accede a Internet. No obstante, salvaguardar la seguridad es más fácil de lo que se puede llegar a pensar.

DATOS SIGNIFICATIVOS: MAYORES DE 60 EN INTERNET

Internet ha pasado a formar parte de nuestra vida diaria. Los mayores, que tienen más tiempo libre a su disposición, han descubierto **una nueva forma de estar en contacto con amigos o familiares,** ya sea por correo electrónico o utilizando las redes sociales, de realizar compras o de informarse. Por eso es tan **importante ser consciente de sus riesgos y saber cómo mitigarlos.**

Los mayores, que tienen más tiempo libre a su disposición, han descubierto ***una nueva forma de estar en contacto con amigos o familiares,*** *ya sea por correo electrónico o utilizando las redes sociales, de realizar compras o de informarse gracias a Internet.*

PRINCIPALES AMENAZAS

Los mayores están expuestos a una gran cantidad de amenazas en Internet, que pueden llegarnos e infectarnos haciendo cualquier cosa: utilizando aplicaciones de comunicación como mensajería instantánea, chat o correo electrónico; navegando por la web, etc… Estas son **las principales vías de infección:**

Mensajería instantánea y correo electrónico

La mensajería instantánea (a través de programas tales como MSN Messenger, Yahoo! Messenger, Google Talk…) se ha convertido en un **canal de comunicación ampliamente utilizado tanto por los jóvenes como por los mayores.** Este fenómeno no ha pasado desapercibido para los ciber-delincuentes, que rápidamente lo han adoptado como uno de los nuevos canales para realizar sus actividades.

- **Una de las mayores amenazas** a las que se enfrentan las personas que utilizan estas herramientas **es el robo de identidad** (alguien que intenta fingir que es otra persona para engañar a las víctimas potenciales). En los programas de correo y mensajería instantánea los usuarios se identifican a través de una dirección de correo electrónico vinculada a una contraseña. Así que, si alguien consigue acceder a la cuenta de uno de sus contactos, no habrá nada que advierta al usuario atacado de que la persona con la que está hablando no es quien dice ser. Y, lo que es aún peor: en caso de tener archivos compartidos con dicha persona, el atacante podrá acceder a ellos libremente. Por eso es tan importante no compartir información confidencial (datos personales, fotografías, números identificativos, etc.) a través de canales inseguros como la mensajería instantánea.

*Según una encuesta realizada por Panda Security, **nuestros mayores,** es decir, **usuarios de más de 60 años**, pasan más de cinco horas a la semana conectados a Internet.*

- Otro riesgo potencial de la mensajería instantánea son las **infecciones por virus y códigos maliciosos.** En la mayoría de las ocasiones nos llegan a través de un link en el que nos invitan a ver un vídeo, o abrir un archivo: cuando lo hacemos, probablemente estaremos ya infectados sin saberlo.

Hay sencillas medidas que se pueden adoptar para impedir que llegue código malicioso a los ordenadores a través de la mensajería instantánea. La principal consiste en **no ejecutar ningún archivo ni hacer clic en ningún enlace que nos llegue.** Al menos, no sin antes comprobar que la persona que lo ha enviado es realmente quien dice ser. Y tener instalada una buena protección, por si acaso somos víctimas de un engaño. Si es un link que tiene malware, el propio antivirus lo detectará y evitará que nos infectemos.

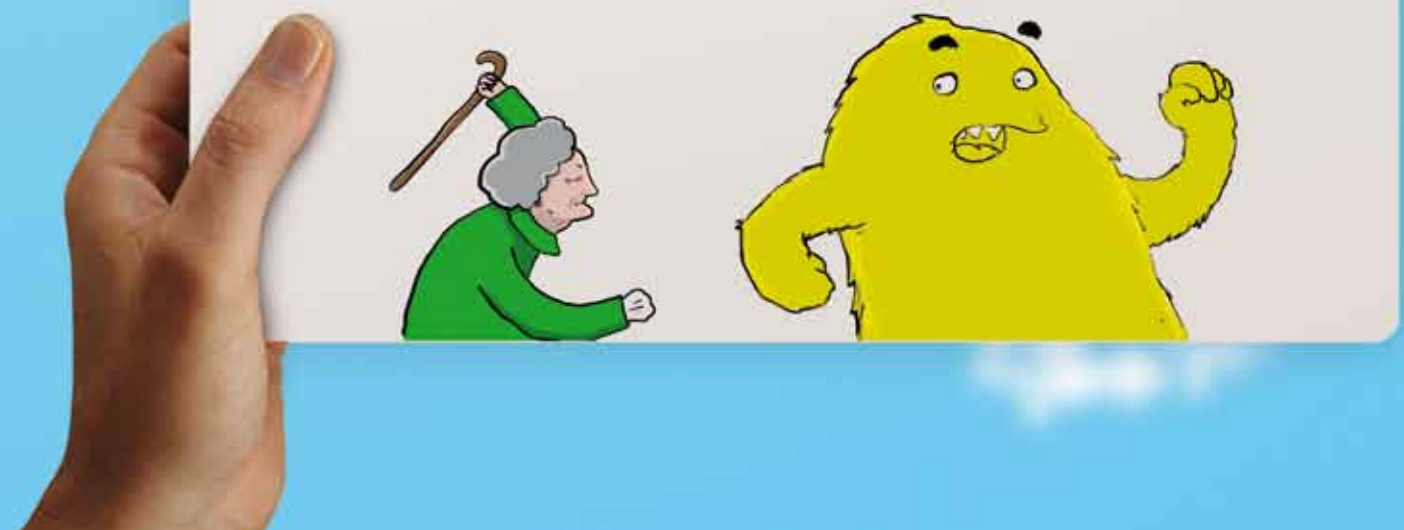
El correo electrónico es otra fuente de peligro para los mayores. Son varias las amenazas que llegan a través de este medio:

- En primer lugar está el **spam** (correo basura). A menudo, este tipo de correo basura se utiliza para publicitar cualquier cosa, desde casinos online hasta productos farmacéuticos. Los mayores son uno de los grupos más propensos a creer en los mensajes incluidos en estos correos, con los peligros que esto conlleva: pueden acceder a casinos online y engancharse al juego, o comprar productos farmacéuticos con riesgos graves para su salud.

- Además, también podemos encontrar el problema de las **falsas ofertas de trabajo.** Estos mensajes ofrecen grandes salarios a cambio de prácticamente ningún esfuerzo. Parece demasiado bueno para ser verdad, y cualquier adulto sensato desconfiaría. Sin embargo, un ciudadano mayor que busque dinero extra podría caer fácilmente en la trampa. En ese caso, se convertirían sin quererlo en cómplices de un delito, ya que el objetivo de los ciber-delincuentes es el de blanquear dinero procedente de actividades criminales.

- Otra amenaza es la de los **virus y malware que entran en el ordenador.** A menudo, el código malicioso distribuido en estos mensajes de correo intenta engañar a los usuarios para que pulsen ciertos enlaces o descarguen un archivo (lo que desencadena la infección) utilizando una gran variedad de asuntos llamativos: trailers de películas, fotografías eróticas, descargas de juegos, etc. Esta técnica se conoce como “ingeniería social”.

La mejor forma de protegerse de estas amenazas es **desconfiar de los correos electrónicos recibidos de fuentes desconocidas.** Hay que ser consciente de que muchos de los contenidos escritos en estos mensajes son falsos y de que **nunca se deben de ejecutar archivos o hacer clic en enlaces incluidos en este tipo de correos.** Una buena protección nos ayudará en la labor de saber identificar cuáles son verdaderos y cuáles pueden contener amenazas.



INGENIERÍA SOCIAL, REDES SOCIALES Y WEB 2.0

Durante años, la ingeniería social ha sido la técnica preferida por los ciber-delincuentes para infectar a los usuarios. Y el año 2010 no ha sido distinto a este respecto; de hecho, **la popularidad de las redes sociales ha causado un resurgir de los ataques** que emplean este tipo de técnica. No olvidemos la escala de estas redes sociales: **Facebook tiene más de 500 millones de usuarios a nivel mundial, y Twitter sigue creciendo, con más de 15 millones de usuarios solo en los Estados Unidos.**

Cada vez es más común que los usuarios empleen estas redes para comunicarse con sus amistades en lugar de, por ejemplo, mediante correo electrónico. Y la verdad es que los ciber-delincuentes son muy conscientes de ello.

Además de la potencial distribución de amenazas a través de estas redes, otro punto de riesgo es el facilitar más información personal de la necesaria, de forma que delincuentes al acecho pudieran tener datos específicos de nuestra vida y utilizarlos para robar en nuestro hogar cuando no estamos, por ejemplo.

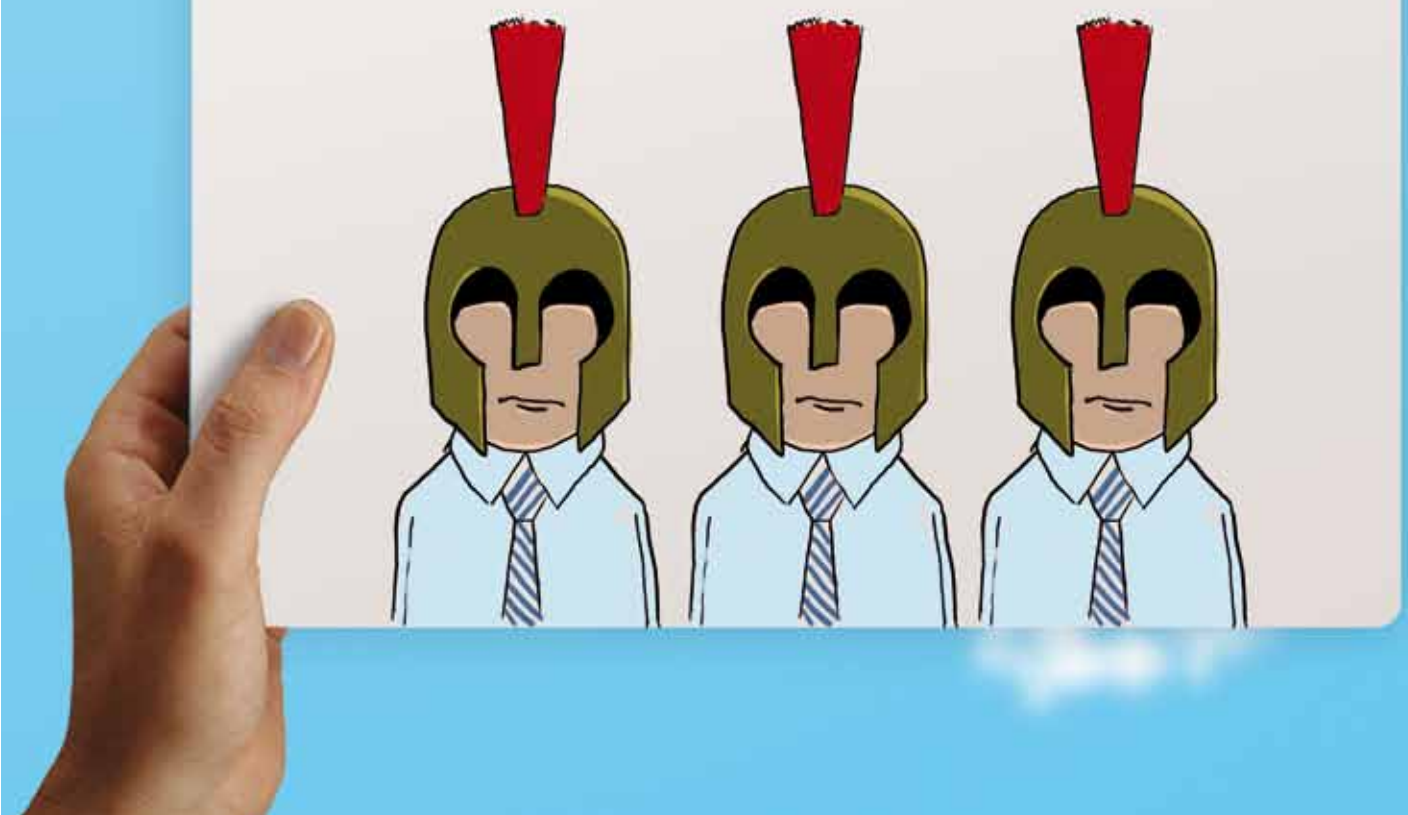
Del mismo modo, algunas redes sociales, como MySpace, permiten compartir archivos con otros usuarios. Hay que prestar especial atención a lo que se comparte y a quién se le da permiso para ver dicha información. No hay ningún problema en, por ejemplo, publicar fotografías protegidas por una contraseña que solo se distribuya a los amigos y familiares. Los mayores y los niños deberían conocer estos servicios, así como su funcionamiento y los riesgos que plantean.

EL PELIGRO DE LOS PROGRAMAS DE INTERCAMBIO DE FICHEROS (EMULE, KAZAA, ETC.)

El intercambio de ficheros a través de redes P2P es otra fuente importante de infecciones. Un gran número de códigos maliciosos son copiados a las carpetas de estos programas con nombres atractivos (nombres de películas, programas informáticos, etc.) en un intento de animar a otros usuarios a descargarse los archivos y ejecutarlos en su ordenador. Esto supone - a todos los efectos - otra variedad de ingeniería social: los nombres de estos ficheros podrían estar dirigidos de forma deliberada a la gente mayor, que no sabrían que al ejecutar dichos archivos estarían introduciendo software malicioso en su ordenador.

Por eso es tan **importante saber qué archivos puede uno bajarse y cuáles no.** También resulta recomendable analizar dichos archivos con una solución de seguridad antes de abrirlos por primera vez. **Si aparece un mensaje de error** o un cuadro de diálogo solicitando la descarga de una licencia o de un codec, **hay que empezar a sospechar ya que casi seguro que dicho archivo contiene un virus o malware.**

Resulta recomendable analizar estos archivos con una solución de seguridad antes de abrirlos por primera vez.



MÓVILES CON INTERNET: UN NUEVO RIESGO

Según un informe de **Frost & Sullivan *,** la creciente sofisticación de los teléfonos móviles los convertirá en uno de los objetivos principales de los ciber-delincuentes durante los próximos años. El estudio revela que tecnologías como el Bluetooth (que permite el intercambio de archivos entre dispositivos mediante una tecnología sin cables) y el acceso rápido a Internet hacen que estos dispositivos sean vulnerables a los ataques.

Los móviles son dispositivos cada vez más utilizados por las personas mayores. Y los riesgos a los que se enfrentan a este respecto son similares a los que hemos comentando en el caso de los PCs:

- En primer lugar, los servicios de mensajería instantánea para los dispositivos móviles son ya una cosa habitual hoy en día. Resulta sencillo entrar en un chat desde cualquier sitio, y los riesgos son los mismos que se han detallado anteriormente: robo de identidad, infecciones de malware, etc.

- El spam también ha empezado a afectar a los teléfonos móviles: los mensajes SMS que anuncian todo tipo de productos y servicios llevan años entre nosotros, y muchos de estos anuncios están relacionados con la pornografía. Es decir, los usuarios ya no solo se ven expuestos a este tipo de contenido a través de sus ordenadores, sino también de sus teléfonos móviles.

Los servicios de mensajería instantánea para los dispositivos móviles son algo habitual hoy en día. ***El spam está empezando a afectar a los teléfonos móviles****. Los mensajes SMS que anuncian todo tipo de productos y servicios llevan años entre nosotros.*

* Frost and Sullivan, 9 de septiembre de 2010. “World Vulnerability Research Tracker Q2 2010”. http://www.frost.com/prod/servlet/report-brochure.pag?id=N862-01-00-00-00#report-overview.

CONSEJOS PRÁCTICOS PARA LOS MAYORES

1. **No pulses enlaces incluidos en correos electrónicos o mensajes si no confías en el remitente.**

   Incluso si un enlace proviene de alguien que conoces, es mucho más seguro teclear la dirección manualmente en el navegador. Si no estás seguro de dónde proviene un mensaje de correo electrónico, ignóralo.

2. **No descargues o ejecutes archivos que provengan de fuentes dudosas.**

   Seguro que a menudo recibes mensajes instantáneos invitándote a descargar una foto, una canción o un vídeo. Sin embargo, puede que a veces dicho archivo no haya sido enviado por el contacto del que parece proceder, sino por un programa malicioso que haya infectado tu ordenador y esté intentando propagarse a otros usuarios. Por si acaso, lo mejor que puedes hacer es preguntarle a tu contacto si realmente te ha enviado algo. Si no lo ha hecho, hazle saber que está infectado para que pueda borrar el archivo y advertir a sus demás contactos.

3. **No reveles información confidencial en Internet**.

   Nunca envíes información privada (datos personales, tu dirección, etc.) a través del correo electrónico o mensajería instantánea, y nunca publiques dicha información en un blog o en un foro. Ten cuidado con la información que facilitas al crear perfiles en servicios como FaceBook o MySpace.

4. **Mantente alerta ante cualquier signo sospechoso.**

   Si un programa que no recuerdas haber instalado comienza a decirte que tu PC está infectado o aparecen mensajes emergentes invitándote a comprar algún tipo de antivirus, puede que se haya instalado un programa malicioso en tu ordenador.

5. **No ejecutes archivos sospechosos.**

   Si tu solución de seguridad te dice que un archivo contiene o podría contener malware, no lo abras. Bórralo.

6. **Instala una solución de seguridad efectiva.**

   La mejor forma de protegerte contra los códigos maliciosos es disponer de una solución actualizada y efectiva. Panda ofrece soluciones para usuarios domésticos que no solo eliminan el malware, sino que también bloquean páginas Web que podrían infectar ordenadores y filtran el spam.

www.protegetumundoonline.es