BOLETÍN DE NOTICIAS n. 2

¿Cuáles son los peligros de Internet que hay que conocer y con los que hay que tener cuidado?

Los peligros de Internet que hay que conocer, con los que hay que tener cuidado y a los que hay que hacer frente cuando sea necesario se pueden resumir en 9 grandes categorías.

1) Sitios con malware y virus listos para infectar su ordenador.

Al navegar por Internet, es muy fácil hacer clic en el enlace equivocado y abrir un sitio que cargue malware en su ordenador. Afortunadamente, si tienes un antivirus actualizado instalado en tu PC, este virus casi siempre se detendrá antes de que pueda causar algún daño. El mayor peligro, además del de un antivirus que deje pasar el virus por error, es no darse cuenta de que se ha arriesgado a sufrir una infección que podría comprometer el funcionamiento de su PC o la integridad de sus datos. Precisamente por la falta de atención de muchas personas, en el último año se han extendido los virus ransomware como Cryptlocker, que cifran los archivos personales y piden un rescate.

Sabemos qué sitios son peligrosos, generalmente los que tienen que ver con la piratería, los sitios de streaming, los contenidos para adultos, las citas y el material ilegal. Si no puedes evitar visitar este tipo de sitios, ten mucho cuidado con dónde haces clic porque el virus puede esconderse en cualquier lugar. Basta con hacer clic en el botón de "Descarga" equivocado para acabar instalando un malware. Y no olvides esos banners publicitarios que te dicen que tu PC está infectado, cuando en realidad no lo está.

En caso de tener dudas, existen herramientas para reconocer y evitar los enlaces peligrosos y los sitios sospechosos. Un factor clave para reconocer y evitar los sitios con virus es utilizar un navegador actualizado y protegido contra todos los fallos descubiertos hasta la fecha.

Entre los sitios más peligrosos que pueden contener malware están, sin duda, los sitios para adultos, los de piratería de cualquier tipo, casi todos los sitios de torrents (también con piratería), los de descargas ilegales (como películas y música) y los de crack.

Lo ideal es que, si necesariamente tienes que visitar un sitio de este tipo, lo mejor sea navegar usando un sandbox. Tanto en Windows 10 como en Windows 11 se puede utilizar una función de escritorio virtual que, además de ser una herramienta de seguridad, es una forma estupenda de hacer cosas en el ordenador sin que queden registradas o sean recordadas, un poco como el modo incógnito de los navegadores web. Esta herramienta se llama Sandbox y está pensada como una zona del ordenador en la que todo lo que se hace no influye en el sistema y se borra inmediatamente después de cerrarlo. El SandBox funciona como una máquina virtual desechable en la que se puede ejecutar con seguridad todo lo que se quiera; incluso se puede abrir un virus o malware sin preocuparse de que dañe el PC o robe datos del equipo.

2) La privacidad online siempre en peligro

Es bastante obvio que si uno quiere utilizar Internet de forma participativa, es decir, entrando en foros, redes sociales y chats, tiene que sacrificar parte de su privacidad. En sitios como Facebook, uno está obligado a dar su nombre real, mientras que en otros sitios sigue siendo necesario dejar una dirección de correo electrónico a través de la cual se puede, si se desea, rastrear al propietario. Básicamente, en el uso normal de Internet, el anonimato no puede existir, y si alguien estuviera interesado en saber quiénes somos y tuviera las habilidades y el talento adecuados para hackear, podría teóricamente saber todo sobre nosotros.

Proteger la privacidad en línea, sin embargo, no significa impedir que un hacker espíe nuestras vidas porque, a menos que estemos siendo acosados por un acosador o haciendo cosas que son ilegales y necesitan ser ocultadas, digamos que es probable que nadie pierda su tiempo hackeando nuestras vidas. La privacidad en línea, en cambio, significa mantener en privado cierta información sensible, como los números de nuestras tarjetas de crédito, nuestras contraseñas, dónde estamos en cada momento, qué buscamos en Internet, etc.

3) Páginas no protegidas

Este es un factor de peligro que la mayoría de la gente sigue ignorando.

Los sitios web no son todos iguales y se dividen en sitios seguros, donde la información que se transmite está encriptada y no puede ser interceptada desde el exterior, y sitios normales que transmiten en claro. Navigaweb.net es actualmente un sitio no encriptado, lo que no significa que no sea seguro, sino que al no requerir una contraseña para entrar, no necesita proteger la información. Todos los sitios en los que hay que introducir una contraseña deben estar encriptados, y esta protección es reconocible por el candado en la dirección de Internet y el prefijo https en lugar de http. Cuando un sitio está en HTTPS y no tiene errores de certificado, entonces toda la información que enviamos, incluidas las contraseñas de acceso, los números de tarjetas de crédito o de cuentas bancarias, no es visible en Internet para nadie, ni siquiera para el operador del sitio al que enviamos esta información. Ni que decir tiene que en todos los sitios con http y sin https no se debe compartir información personal.

Si todavía está utilizando un servicio de correo electrónico sin https o un servicio de banca en línea tan superficial, absolutamente cambiar de inmediato.

4) Phishing

Entre los sitios peligrosos en general, una categoría particular es la de los sitios de estafa, como los sitios de compras desconocidos y no recomendados o, peor aún, los sitios falsos que parecen idénticos a los sitios famosos y que se crean para robar las contraseñas de las cuentas.

Hacer copias de sitios bancarios o de compras es una de las técnicas más comunes utilizadas por los hackers para robar contraseñas de cuentas web y se llama Phishing. El phishing siempre funciona enviando un mensaje por correo electrónico, Facebook, SMS, Whatsapp, etc. La mejor manera de no caer en esta técnica es utilizarla como excusa para robar contraseñas. La mejor manera de evitar caer en este tipo de trampas es no escribir nunca las contraseñas y datos importantes (ni siquiera por correo electrónico), salvo

en las webs oficiales de las cuentas, reconocibles por la dirección escrita en la parte superior del navegador y el HTTPS con candado verde.

Lo ideal sería utilizar un cliente de correo electrónico como Microsoft Outlook y utilizar un filtro de spam para bloquear estos mensajes.

5) Spam

El peligro del spam es mucho menor hoy que hace unos años.

El spam sería toda la categoría de mensajes basura, publicidad, phishing y virus o comunicaciones inútiles. Afortunadamente, los principales servicios de correo electrónico actuales, como Gmail y Outlook.com, disponen de un eficaz filtro de spam que regula la recepción de correos electrónicos.

6) Desinformacion

Aunque puede formar parte de la categoría de Spam, la desinformación en Internet se ha convertido en un peligro real en el último año debido a la difusión de noticias falsas de sitios de bulos que debemos aprender a reconocer para no quedar como imbéciles que se creen cualquier cosa que leen en Internet o Facebook.

7) Citas online

Este es uno de los peligros más graves de Internet para los jóvenes.

Suena mal decirlo, pero un padre responsable debe comprobar si sus hijos chatean con extraños a través de Internet, sean cuales sean las circunstancias. Se puede chatear con un desconocido en un juego online, en un sitio de citas casuales, en una red social, en un foro y en cualquier otra sala de chat. Ya sea por motivos sexuales, de citas o puramente recreativos, es importante no dar demasiada información personal: no digas tu edad real, no digas dónde vives, no digas a qué colegio vas, no des nombres reales de familiares o amigos y no des tu número de teléfono. Los depredadores online son muy buenos haciéndose pasar por chicos normales y saben explotar las debilidades de los adolescentes como ni siquiera los mejores psicólogos, movidos, en los casos más graves, por esa terrible enfermedad que es la pedofilia.

8) Cyberbullying

Chatear con extraños puede ser peligroso porque nunca se sabe quién está detrás del teclado, pero chatear o enviar mensajes con personas conocidas también puede ser peligroso. El ciberacoso funciona más o menos así: si se burlan de ti en la escuela o de tus amigos, uno de ellos puede publicar un vídeo o una foto en Facebook u otras redes sociales que puede avergonzar a la víctima.

Otro caso de ciberacoso puede provenir de mensajes anónimos que insultan mucho a la víctima, incluso con amenazas.

En comparación con el acoso real, el ciberacoso tiene la ventaja de que no hay control y de que puede decir lo que quiera sin mirar a su víctima a la cara, o incluso de forma anónima, escondiéndose detrás del

teclado. En cualquiera de los dos casos, no sería tan difícil, al menos a nivel técnico. Sin embargo, es mucho más complicado defenderse a nivel psicológico, lo que puede requerir la ayuda de un padre o un experto.

Para empezar, sin embargo, sería un excelente paso adelante borrar la cuenta en Ask.fm, uno de los sitios que más se presta al ciberacoso online.

9) Desconocimiento total de la seguridad informática

Desconocimiento total de la seguridad informática

Se trata de un peligro evidente, tan extendido que uno se sorprende.

¿Es posible que aún hoy la contraseña más común en el mundo sea 123456?

¿Piensa la gente que, por no tener nada que ocultar, ningún hacker va a robar su cuenta?

¿Cómo es posible que la gente siga utilizando la misma contraseña para todos los sitios web?

¿Y aún hay quien escribe sus contraseñas, quizá todas diferentes y difíciles de recordar, en un papel que puede leer cualquiera?

Este proyecto ha sido financiado con el apoyo de la Comisión Europea. Este documento refleja únicamente las opiniones de los socios del proyecto, y la Comisión no se hace responsable del uso que pueda hacerse de la información contenida en el mismo.