10 reglas esenciales de seguridad en Internet

Desde el año 1988, el 30 de noviembre se celebra el Día Internacional de la Seguridad Informática. El objetivo de esta fecha es concientizar a los usuarios sobre la importancia y necesidad de tomar medidas de protección en el ámbito digital.

Es por esto que ESET comparte 10 consejos básicos que todo usuario digital debería incorporar como parte de sus hábitos para disfrutar de la tecnología e Internet de forma segura y minimizar considerablemente los riesgos de ser víctima de las amenazas informáticas más comunes.

Como se observa en la imagen previa, es posible dividir los consejos en tres niveles: básico, intermedio o avanzado. Y si bien se podrían nombrar más recomendaciones, lo más importante es tomar verdadera conciencia de los riesgos que existen en el mundo virtual actualmente y de lo vital que es y seguirá siendo aprender a gestionar la seguridad digital.

10 reglas de seguridad en Internet para todos los usuarios

1. **Utilizar contraseñas largas y complejas**

Evitar las contraseñas simples y fáciles de adivinar, como fechas, nombres o cualquiera de las que año tras año se ven en la lista de las peores contraseñas. Otro aspecto fundamental: no utilizar la misma contraseña para más de una cuenta. La reutilización de claves es una de las peores prácticas en seguridad.

A la hora de crear una contraseña segura lo ideal es que tengan entre 15 y 20 caracteres, que incluyan letras, números, mayúsculas, minúsculas y caracteres especiales. Una buena idea también es utilizar un administrador de contraseñas, ya que estas herramientas no solo permiten almacenar de forma ordenada las credenciales de acceso para todas las cuentas del usuario, sino que en general ofrecen la posibilidad de confeccionar contraseñas realmente seguras y únicas.

2. **Utilizar la autenticación en dos pasos en todas las cuentas**

El paso siguiente a la buena gestión de las contraseñas es implementar la autenticación en dos pasos, también conocido como doble factor de autenticación, en cada una de las cuentas y servicios que utilices. Activar esta opción brinda una capa de seguridad adicional muy importante que dificultará a un atacante lograr acceder a las cuentas por más que tenga el usuario y contraseña. Para más información, se puede leer el siguiente artículo que explica todo sobre la autenticación en dos pasos y cómo activarla en algunas de las plataformas y herramientas más populares.

3. **Utilizar una conexión a Internet segura**

En el caso de los dispositivos móviles como el smartphone, utilizar los datos para navegar por Internet y evitar —o utilizar con precaución y siempre a través de una VPN— las redes Wi-Fi públicas, sobre todo si se van a ingresar credenciales de acceso o información sensible. En el hogar, asegurarse de que la conexión a la red Wi-Fi cuente con una contraseña segura y corroborar que la configuración del router sea la adecuada.

4. **Configurar correctamente la privacidad de todas las cuentas**

Son muchas las buenas razones para gestionar correctamente la privacidad de la información en cada una de las plataformas y servicios que se utilizan, ya que el uso indebido de los datos personales, incluso los que parecen más inofensivos, pueden representar un riesgo al que la mayoría está expuesto. Más aún si no se toma ningún recaudo para evitarlo.

Datos como la fecha de nacimiento, lugar de trabajo, profesión, lugar de residencia, entre otros, pueden ser utilizados por estafadores para robar identidades o realizar engaños con una historia bien elaborada a partir de información publicada. Limitar la información accesible de forma pública y mantener el mayor control posible sobre quiénes pueden ver lo que se publica puede hacer la diferencia. Si se piensa publicar en Internet algo que es preferible que no lo vean todos, quizás sea mejor no publicarlo.

Más allá de la información publicada y cómo los cibercriminales pueden aprovecharla e incluso recolectarla para venderla, la configuración de la privacidad también implica estar atentos a los permisos que se otorga a las aplicaciones instaladas o a los servicios en los que se crea una cuenta.

5. **Realizar backup de la información de valor**

Se debe ser consciente de que, por más cuidadoso que uno sea, a cualquiera le puede ocurrir que extravíe o le roben su computadora o teléfono. También puede ocurrir que se baje la guardia un instante y se infecte con malware por descargar un archivo o una aplicación indebida, o que por alguna otra razón se pierda el acceso a información preciada. En estos casos, contar con una copia de seguridad de la información más importante se convierte, sin lugar a duda, en el bien más preciado. Por eso, no se debe postergar la tarea de organizar el backup como corresponde para asegurar fotos, videos, documentos y archivos más importantes.

6. **Mantener los dispositivos y aplicaciones actualizadas**

Diariamente se ven noticias sobre el descubrimiento de nuevas vulnerabilidades en Sistemas Operativos, herramientas de uso diario y el lanzamiento de actualizaciones para corregir esos fallos. Muchas veces incluso se conocen nuevas vulnerabilidades que, previo a su descubrimiento, ya están siendo explotadas por atacantes de manera activa.

Lamentablemente, la mala costumbre de muchos usuarios de no mantener la tecnología que utilizan con las últimas actualizaciones instaladas los expone, ya que los atacantes aprovechan estos fallos para lanzar sus ataques. De hecho, muchas de las vulnerabilidades más explotadas en la actualidad fueron parcheadas hace ya varios años pero siguen siendo efectivas para los atacantes por la falta de instalación de actualizaciones.

7. **Únicamente descargar aplicaciones de tiendas oficiales**

A la hora de instalar una aplicación en el teléfono, asegurarse de descargarla de tiendas oficiales como Google Play o App Store y evitar fuentes desconocidas. Los cibercriminales suelen crear aplicaciones maliciosas que intentan engañar a los usuarios haciéndoles creer que son apps oficiales de bancos, juegos, billeteras virtuales, etc.

Incluso en las tiendas oficiales se debe tener cuidado porque como se ha visto en reiteradas oportunidades, pese a los controles de seguridad que aplican estas tiendas los cibercriminales muchas veces encuentran la forma de sortear los mecanismos de seguridad y logran publicar falsas apps. Por lo que es importante también leer los comentarios y las calificaciones de otros usuarios ya que ahí podemos encontrar señales en caso de que se trate de algo sospechoso. Además de las aplicaciones, se debe tener cuidado con las descargas que se realizan en general. Los atacantes también buscan distribuir malware a través de cracks de programas o juegos. Por lo tanto, a la hora de descargar solo se debe confiar en fuentes oficiales.

8. **Desconfiar de las personas que se conocen en Internet**

Las plataformas sociales abundan en la actualidad y los usuarios cada vez más, y a menor edad, pasan más tiempo interactuando con amigos y también con desconocidos. Sin embargo, las plataformas sociales también tienen un lado oscuro y la violencia digital está presente en diversas formas, afectando a grandes y chicos. Los fraudes o el acoso en sus diversas formas son moneda corriente en las redes sociales tradicionales, en apps y plataformas de citas online, foros, etc. Por lo tanto, tener cierto grado de desconfianza y cautela en Internet puede ayudar a evitar varios malos momentos.

9. **Instalar una solución antimalware en la computadora y teléfono**

Tener los dispositivos asegurados con una solución de seguridad confiable que proteja contra el phishing, malware, archivos adjuntos en correos o sitios sospechosos será un gran aliado para proteger no sólo los dispositivos, sino la información en ellos. Las soluciones de seguridad en la actualidad cuentan con muchas funcionalidades que contemplan las necesidades actuales, como la posibilidad de realizar acciones de manera remota a un equipo en caso de robo o extravío, como bloquearlo y enviar un SMS de alerta a usuarios previamente seleccionados o eliminar los datos del dispositivo.

10. **Mantener la guardia alta con los correos, mensajes y al momento de realizar búsquedas**

Más allá de las consideraciones técnicas mencionadas hasta ahora, se debe recordar que el factor humano es el eslabón más débil de la cadena. Por eso, siempre se debe estar atento y nunca bajar la guardia. Tener presente que en cualquier momento se puede recibir un correo inesperado solicitando descargar algo, hacer clic en un enlace o enviar información personal y sensible. También al momento de realizar compras online se deben realizar las debidas diligencias y chequear la reputación del vendedor, los comentarios de otros compradores y no dejarse llevar

por ofertas demasiado buenas para ser verdad.

Por último, al momento de buscar información tener cuidado con los sitios que aparecen en buscadores como Google, ya que los atacantes pueden alterar los resultados que ofrecen los motores de búsqueda o incluso usar anuncios falsos para posicionar falsos sitios que suplantan la identidad de bancos, aplicaciones, juegos, tiendas, etc.

“Los consejos podrían continuar, podríamos mencionar otras recomendaciones más específicas, pero lo más importante es tener presente que las modalidades delictivas van cambiando y los cibercriminales siempre prueban distintas estrategias para agarrar desprevenido a los usuarios. Tener conocimiento de cuáles son los riesgos y tomar las medidas de seguridad necesarias para reducirlos, van a hacer que podamos disfrutar de los beneficios que nos brinda internet de una forma más segura” concluye Cecilia Pastorino, especialista en Seguridad Informática del Laboratorio de Investigación de ESET Latinoamérica.