CÓMO CUIDAR LA SEGURIDAD DE NUESTROS DISPOSITIVOS

Con la llegada de la globalización, se generaron nuevas posibilidades, nuevas formas y nuevas herramientas de trabajo, además de mayor entretenimiento e interacción. Las personas y los dispositivos convivimos día a día rodeados de datos que se intercambian con otras personas y otros dispositivos a través de diferentes redes digitales. Aquí presentamos una serie de consejos y sugerencias para estar más atentos en el cuidado de nuestra valiosa información, la base de nuestro trabajo.

| Por la **Comisión de Recursos Tecnológicos**

Es obvio que, si sabemos usar la tecnología a nuestro favor, esto nos beneficia. Podemos contactarnos con más clientes sin movernos de casa, podemos contestar correos electrónicos desde nuestro teléfono o nuestra tableta, descargar herramientas gratuitas o pagas de internet, trabajar en línea, subir datos a la nube y un sinfín de actividades más.

A esta interacción se la conoce como internet de las cosas. Este concepto supone que todos los objetos y dispositivos que nos rodean estarán conectados a la red de manera que se puedan comunicar entre sí y transmitir información en tiempo real. Se espera que para el año 2020 haya veinticinco mil millones de dispositivos conectados a la red de redes.

Sin embargo, no todo es una ventaja, también debemos pensar en las consecuencias para la seguridad. Al estar todo conectado con todo, los riesgos de perder información personal, bancaria, etcétera, siempre están presentes; y, conforme aumente la cantidad de dispositivos conectados a internet, seremos más vulnerables a posibles ataques cibernéticos.

Según los expertos de Intel, Microsoft y Eset, el promedio diario de ataques cibernéticos fue de quinientos cincuenta mil el año pasado en todo el mundo y se crean aproximadamente ciento sesenta mil nuevos tipos de *software* malicioso al día. Estos ataques no se dirigen únicamente a las PC o computadoras personales, los dispositivos móviles, como los teléfonos o las tabletas, también se ven afectados.

El objetivo principal de estos ataques es obtener datos personales y valiosos para nosotros, que luego se utilizan para beneficio de quienes los robaron o se venden en el mercado negro de datos. También existen ataques menores que simplemente interfieren con el funcionamiento de nuestras herramientas de trabajo.

Amenazas de seguridad informática más comunes

***Malware*:** surgió como un experimento o broma. Con el paso de los años, se comenzó a utilizar para causar daños o pérdida de datos o sabotear sitios web. A medida que aumentaron los usuarios en internet, se desarrollaron virus y gusanos con la finalidad de controlar las computadoras. Se pueden instalar en la máquina en forma de *backdoor, drive-by downloads, rootkits* y troyanos sin que el usuario los note. Otros ejemplos de *malware* son el *spyware, adware* y *hijacker*, que generalmente se usan para mostrar publicidad que uno no desea; o los *keyloggers* y *stealers*, que se usan para robar información personal.

***Eavesdropping* (intercepción pasiva):** se usa para interceptar el tráfico en una red, mediante programas (*sniffers*) que recogen datos a medida que estos se mueven de un lado a otro. Se usa generalmente para obtener números de tarjetas de crédito, contraseñas o direcciones de correo electrónico.

***Snooping* (espionaje de información):** su objetivo principal es obtener información privada. Permite acceder a la mayoría de los datos en el equipo.

***Tampering* (modificación de la información):** su objetivo principal es modificar o borrar datos de un equipo, ya sea *software*, archivos o cualquier otro tipo de información. Los programas troyanos son ejemplos claros de esta práctica.

Saturación de servidores web: se envían cantidades masivas de datos a un servidor para saturar los recursos del sistema y dejarlo fuera de línea.

***Spoofing*:** se usa la identidad de otro usuario y se actúa en su nombre. Se accede al equipo porque conocen nuestra IP o nuestras contraseñas.

***Ransomware*:** mediante un código malicioso que llega al dispositivo, los archivos quedan cifrados o encriptados y el usuario no puede acceder a estos. Luego se pide un rescate para devolverle la información.

***Botnet*:** *software* que convierte al dispositivo en un equipo zombi. El atacante controla el equipo y puede robar información o espiar para qué se utiliza.

Soluciones de seguridad

Es imprescindible contar con un paquete antivirus o *software* especializado. Sin embargo, la mejor defensa es saber qué hacemos con nuestras máquinas, qué descargamos, a quién le enviamos información y cómo lo hacemos, cómo generamos nuestras contraseñas, etcétera.

Recomendamos:

— Contar con un antivirus o *firewall* actualizado que permita reconocer todo tipo de virus al analizar las descargas, adjuntos, etcétera.

— Realizar un análisis del sistema del equipo con frecuencia.

— Instalar las actualizaciones automáticas de sistema operativo y del navegador para subsanar las fallas de la versión anterior.

— Tener cuidado con la generación y escritura de las contraseñas. No debemos usar datos personales o fáciles de obtener y sí incluir mayúsculas, minúsculas, números y signos. Tener cuidado con respecto a dónde escribimos la contraseña, usar el teclado virtual, no activar la opción «recordarme». No tener la misma contraseña en todos lados.

— No hacer clic en cualquier lado. ¿La plataforma, el sitio web, los adjuntos del correo electrónico entrante, la mensajería instantánea o la solicitud de personas en una red social son legítimos? Debemos estar seguros de la veracidad de los datos antes de obtener información de estos sitios o personas y conocer bien a quién le vamos a suministrar nuestros datos.

— No descargar sin mirar. Solo debemos descargar archivos de fuentes seguras y confiables o *software* de los sitios oficiales. No se recomienda usar sitios web intermediarios.

En los tiempos que corren, mantener la seguridad implica un gran desafío. Depende de nosotros y de nuestras decisiones saber cuál es el camino correcto.

Si tienen dudas o inquietudes sobre este tema u otro relacionado con la informática y la tecnología, pueden escribirnos a recursostecnologicos@traductores.org.ar. También pueden visitar el Cartapacio del Traductor Tecnológico en http://www.traductores.org.ar/cartapacio, donde encontrarán notas de interés. Si desean formar parte de la Comisión, los esperamos a partir del miércoles 22 de marzo a las 18.30.■