Publicado en Madrid el 23/11/2018

8 errores comunes que ponen al usuario en el punto de mira de los hackers, según IMF Business School

Al menos el 33% de los españoles ha sido víctima de un cibercrimen, según cifras de Norton. España es el tercer país que más ciberataques, después de Estados Unidos y Reino Unido. Pinchar en cualquier enlace, conectarnos a redes wifi-públicas o utilizar la misma contraseña para todo son algunos de los errores informáticos que benefician a los hackers, señala IMF Business School

Sufrir un ciberataque es más común de lo que se piensa. Al menos el 33% de los españoles ha sido víctima del cibercrimen, dato que sitúa a España como el tercer país que más ataques sufre después de EEUU y Reino Unido, según el estudio Norton Cyber Security Insights Report 2018. Las cifras son reveladoras, pero son aún más alarmantes al compararlas con el riesgo de padecer una alergia, el 25% de los españoles, según informa la Sociedad Española de Alergología e Inmunología Clínica (SEAIC). Así, hay más probabilidades de sufrir un ciberataque que una alergia.

Con este contexto se celebra el Black Friday, un día en el que se disparan las ventas online en todo el mundo, pero también este tipo de ataques. Según un estudio realizado por RiskIQ, más de un 5% de las 4.331 apps móvil que se encuentra al buscar “Black Friday” en las app store globales están marcadas como maliciosas. Ante esta situación, IMF Business School, escuela con una amplia experiencia en la formación en ciberseguridad, ha detectado 8 errores informáticos que facilitan el hackeo de los equipos y que podrían contribuir a que tener un ”viernes negro”:

Huir de las actualizaciones. Las prisas y los problemas de memoria en el dispositivo son responsables de que se pospongan las actualizaciones del sistema operativo, software de las apps o el antivirus. Sin embargo, la actualización constante es una buena barrera para frenar a los hackers, por lo que hay que asegurarse de que todos los datos están seguros y protegidos.

Descargas o instalaciones no oficiales. Al descargar aplicaciones o programas de páginas de dudosa credibilidad, aumenta el riesgo de sufrir un ciberataque.

Uso de redes wifi públicas. Si se puede acceder a ellas fácilmente, ¿por qué no lo harán también los hackers? Desde IMF Business School recomiendan leer atentamente las condiciones de uso, además de no realizar operaciones delicadas como consultar la cuenta bancaria o contratar nuevos servicios.

Pinchar en cualquier enlace o publicidad. Hay que revisar su origen siempre. Durante estos días aparecen cientos de anuncios con ofertas poco creíbles y, aunque los ecommerces se vuelven locos por bajar los precios, no se debe hacer clic sin más, sino dirigirse directamente a la página oficial para comprobar que el precio es real.

Una contraseña para todo. Cada vez se necesitan más contraseñas y acordarse de todas puede ser un

caos. Sin embargo, tener una sola hace que la vulnerabilidad a posibles ciberataques aumente. ¿Cómo generar contraseñas seguras? Desde la escuela hacen hincapié en la importancia no solo de que sean únicas, sino también cambiarlas con frecuencia.

Restar importancia a las copias de seguridad. Procrastinar no está permitido en este caso. Es una tarea fácil de realizar y que garantiza la conservación de todos los archivos.

Pagar con tarjeta en webs desconocidas. Desconocidas o no, lo mejor es utilizar pagos online seguros. Un buen ejemplo de ello es PayPal, donde se paga online desde la cuenta de email mientras los datos bancarios estarán totalmente protegidos. Además, avisan por email cada vez que se produce un cobro.

No usar la autenticación de dos pasos. Muchas de las plataformas online ya incluyen la opción de autentificación en dos pasos, es decir, además de la contraseña se genera un código numérico aleatorio que envían por SMS y que funciona como un doble control.

Datos de contacto:
Redacción

Nota de prensa publicada en: Madrid

Categorías: Sociedad Innovación Tecnológica