Prepárate ante un ciberataque

La tecnología y su adopción facilitan las relaciones y la vida de los individuos, pero también las de las empresas. Sin embargo, la digitalización conlleva una responsabilidad, si lo que se busca es **evitar ser víctima de un ciberataque**.

Lucas Paus, investigador de ciberseguridad de ESET, asegura que **hay formas de evitar un ciberataque**, y sobre todo arruinar al delincuente al frustrarle sus intentos de vulnerar la seguridad cibernética de una compañía.

Recomienda siempre actualizar la solución de seguridad, aplicaciones y sistema operativo. “Las actualizaciones no sólo arreglan errores, si no también fallos y brechas de seguridad. Estar al día con estos aspectos evitan que los atacantes exploten las vulnerabilidades conocidas en dichos sistemas.

“Hay que instalar soluciones de seguridad en todos los dispositivos. Esto sirve para proteger desde la computadora, smartphone, tablets y demás dispositivos que se usan en el día a día. Un firewall y antivirus detectará múltiples amenazas como troyanos u otro tipo de malware, evitando fugas o robos de información.

“Además, hay que realizar una copia de seguridad periódicamente de toda la información. Un disco externo puede servir, pero se debe asegurar de no mantenerlo conectado todo el tiempo, ya que si se es víctima de ransomware, la información de este dispositivo también puede verse comprometida y cifrada. Contar con un respaldo es un as bajo la manga para no pagar por un rescate de la información”, explica Paus.

Otra de las maneras para frenar los ataques informáticos son la pronta denuncia de los correos con phishing. “Está práctica es la favorita de los cibercriminales, ya que las personas son el factor más vulnerable en la cadena de seguridad. Para frenar esta amenaza, es muy importante denunciar los sitios de phishing desde los navegadores utilizados, e inclusive reportarlos al programa de antivirus en caso de que no los reconozca”.

Paus señala que es importante actualizar las contraseñas y asegurarse de que siempre sean más fuertes y complejas de descifrar. “Debe de contar con mayúsculas, números y signos y, mientras más larga, es mejor.”

Muchos especialistas consideran necesario en estos días activar siempre el segundo factor de autentificación.

“Los servicios en línea cuentan con esta medida extra de seguridad que frecuentemente requiere de un código obtenido a partir de una aplicación, o un mensaje SMS, además de una contraseña para acceder al servicios. A ello hay que sumarle checar la privacidad en las redes sociales, y evitar siempre subir información sensible a plataformas como Facebook”, agrega Paus

Finalmente, el especialista de ESET comenta que hay que verificar los estados de cuenta del banco, y poner atención a anomalías o transacciones desconocidas.