Con el avance de la tecnología y el uso masivo de Internet por parte de la población mundial, los actos delictivos cibernéticos aumentan considerablemente cada año. Debido a esto, es necesario conocer algunas acciones que te pueden ayudar a evitar ser una víctima de los hackers.

Los hackers se encuentran al asecho todos los días, a cualquier hora, en busca de víctimas potenciales, ya sean empresas o personas, con técnicas de hacking para cualquier servicio, desde redes sociales, hasta robo de información corporativa, ataques de ransomware, robo de criptomonedas o dinero de cuentas bancarias, entre muchos otros.

Para el caso de redes sociales, siempre es necesario ser cuidadosos con los datos personales, pues los ciberdelincuentes tienen métodos para Hackear Facebook, algunos de estos, pueden ir desde la ingeniería social, que mediante contacto con la víctima, ponen trampas para obtener las credenciales de inicio de sesión. Otras tácticas pueden ser sitios de scam, donde colocan una página idéntica a Facebook o Twitter para que el usuario ingrese sus datos de inicio de sesión.

Para evitar esto, es necesario comprobar que el dominio web sea el correcto, es decir, la dirección URL, por ejemplo: www.twitter.com es el dominio verdadero, que puede ser suplantado por un hacker por un dominio como twiitter.com, al que un usuario desprevenido puede acceder confiando en que se parece al original.

Otra opción para protegerse ante esto es el uso de la autenticación multifactor, para que en caso de que un hacker logre obtener una contraseña, no pueda acceder al servicio porque se le pedirá un segundo código de acceso, que por lo general llega al teléfono del usuario como mensaje de texto o por medio de alguna aplicación de autenticación como Google Authenticator.

Los hackers también intentan constantemente el robo del acceso a aplicaciones bancarias de los teléfonos inteligentes, por lo que siempre es necesario instalar únicamente aplicaciones de las tiendas oficiales y evitar la instalación de aplicaciones de fuentes desconocidas, incluso cuando se encuentren en las tiendas de Google o Apple. Aplicaciones que parezcan

confiables como juegos, podrían intentar robar los datos de acceso a aplicaciones bancarias en segundo plano.

Esto no solo afecta a los dispositivos móviles. También pasa en computadoras, mediante software que promete ser para cierta utilidad, y en realidad se trata de algún tipo de malware. Incluso, los hackers pueden distribuir software legítimo pero adicionado con malware, con el fin de instalar algún troyano de conexión remota con el que podrían robar información de la computadora.

Para evitar lo anterior y proteger tu información, es recomendable contar con un software antivirus actualizado, que podrá detectar archivos maliciosos, sitios web maliciosos y escanear todo el dispositivo en busca de virus.

Además, siempre se debe ser cauto al navegar en Internet, evitando visitar sitios web desconocidos, descargar archivos de fuentes desconocidas, abrir correos electrónicos de remitentes desconocidos, instalar aplicaciones de desarrolladores no conocidos, entre otros. Protege tus cuentas de cualquier servicio con dos métodos de autenticación y evita ingresar tus datos personales en sitios web que no conoces.

Si tienes alguna duda o comentario, déjalo aquí abajo.