Los hackers han estado apuntando cada vez más al robo de cuentas de redes sociales, con el fin de cometer diversos delitos cibernéticos que van desde la suplantación de identidad, hasta extorsión. Debido a esto, es necesario conocer los diferentes métodos que emplean los piratas informáticos y cómo evitar ser una víctima más.

Los métodos que utilizan los hackers para Hackear Facebook o cualquier otra red social son diversos, siendo uno de los más comunes y sencillos el uso de keyloggers, ya sea como software o hardware. Un keylogger es un programa que almacena lo que se pulsa en el teclado, incluyendo correos electrónicos, números de tarjetas y contraseñas. De este modo, un ciberdelincuente puede instalar el software o hardware para posteriormente obtener los datos almacenados.

Para evitar ser víctima de esto, al utilizar una computadora de otra persona o en un lugar público, es recomendable revisar que el CPU no tenga ningún dispositivo conectado en los puertos USB. Si existe algún aparato conectado, aparte del teclado, mouse y otros periféricos de uso, podría tratarse de un keylogger y lo más recomendable es no utilizar ese equipo.

De igual forma, es necesario comprobar que no exista este programa espía en modo de software, revisando el administrador de tareas para ver qué procesos se están ejecutando.

Otro método común entre los ciberdelincuentes para robar cuentas de redes sociales el uso de scams, que son clones de las páginas web legítimas, pero con dominio distinto. Por ejemplo, facebook.com puede tener el dominio facebok.com y el mismo diseño web, si el usuario no pone atención a la URL, ingresa sus datos de inicio de sesión y se envían automáticamente al hacker.

Por esto es necesario siempre revisar que la dirección URL sea la correcta y que el certificado de seguridad SSL sea válido.

Existen otros métodos mucho más complejos que requieren conocimientos de programación, redes y demás. Si te interesa conocer todo esto e incluso aprender, puedes tomar algún curso. La Academia de Hacking de Citeia ofrece cursos de ciberseguridad y hacking ético de

forma gratuita, por lo que puede ser una muy buena opción para aprender.

Los hackers se van actualizando y siempre existen nuevas metodologías y herramientas para realizar actos cibernéticos delictivos, por lo que aprender sobre esto no está por demás.

Por ejemplo, hackers más avanzados pueden emplear troyanos de acceso remoto para acceder a las computadoras de las víctimas y obtener información personal. Pueden utilizar esta metodología utilizando archivos de uso común como imágenes o videos, o en plugins de navegadores web, etcétera.

Siempre es bueno ser precavidos para evitar ser víctimas de hackers, utilizando un software antivirus actualizado, evitando abrir correos electrónicos de remitentes desconocidos, evitar abrir archivos adjuntos de fuentes desconocidas, revisar siempre las URL de los sitios web que se visitan, no instalar software pirateado o de desarrolladores poco confiables, entre otros.

Todas estas medidas de seguridad también son aplicables a dispositivos móviles, ya que actualmente, los hackers han apuntado cada vez más a sistemas operativos como Android y Apple, mediante aplicaciones maliciosas que roban datos sensibles de los smartphones.

Algunas de las opciones para proteger tus redes sociales de los hackers incluyen el uso de una contraseña segura, autenticación multifactor, no dejar sesiones abiertas si el dispositivo que usas es compartido y no utilizar sitios web que pidan credenciales de inicio de sesión de redes sociales.

Si tienes alguna duda o comentario al respecto, déjala aquí abajo!