Hoy en día existe una gran cantidad de fraudes electrónicos que son aprovechados por delincuentes para robar datos personales y dinero de los usuarios que día a día utilizan Internet. Aunque existen muchas formas de prevenir esto, desde el sentido común hasta el uso de software antivirus, los ciberdelincuentes siempre encuentran nuevas formas para realizar sus fechorías.

Muchos de los fraudes electrónicos se basan en el phishing, que es una forma de suplantación de identidad para suplantar la identidad de una entidad y robar información sensible. Por lo general, los delincuentes que utilizan el phishing para robar información, llevan a cabo técnicas de ingeniería social, habitualmente, haciéndose pasar por algún agente bancario, empresa o incluso familiares y amigos, con el fin de obtener la información requerida.

Los ataques de phishing se pueden clasificar según el objetivo contra el que se dirige el ataque, el fin o medio que se utiliza, o según el modo de operación. Si una persona es víctima de un ataque de phishing, es necesario reportarlo a las autoridades y, dependiendo de la información robada, podría ser buena idea realizar un peritaje informático para poder dar con los responsables y hacer que puedan enfrentarse a la ley, o solicitar, en su caso, el resarcimiento de la cantidad robada a la entidad que no había puesto todos los medios de seguridad en sus sistemas.

Qué es el Spyware

Otra técnica de robo de datos es el spyware, que se basa en el uso de software malicioso que recopila información del dispositivo, incluyendo datos bancarios, datos personales, contraseñas, ficheros de audio y video, etc.

Este tipo de malware puede ser utilizado en computadoras, tabletas o smartphones. Debido a esto, es muy recomendable evitar instalar programas o aplicaciones de fuentes desconocidas que tengan mala reputación o que se alojen en sitios web sin buenas reseñas.

En qué consiste el Pharming

Este tipo de ataque cibernético o estafa cibernética se desarrolla a partir del phishing. En este caso, el atacante intenta redirigir el tráfico web, especialmente los datos de solicitud, a un sitio web fraudulento. Esto se hace mediante la explotación de vulnerabilidades de seguridad en los sistemas de nombre de dominio (DNS), o en los equipos de los mismos usuarios, que permiten a los piratas redirigir un nombre de dominio a otra máquina distinta.

De este modo, un usuario que introduce un determinado nombre de dominio que haya sido redirigido, accede desde su explorador de Internet a la página web que el atacante haya especificado.

Es necesario tener mucha precaución cuando se navega en Internet, pues siempre se puede ser víctima de los criminales informáticos, instalando aplicaciones en el equipo, que podrían contener malware, ransomware u otro tipo de virus que pueden dañar el equipo y robar información sensible.

Siempre es necesario procurar tener un antivirus actualizado y sistemas de seguridad para navegar en Internet, estas herramientas ya son ofrecidas por la mayoría de los sistemas antivirus.

De igual modo, si se ha sido víctima de una estafa informática, es prudente consultar con un perito informático colegiado para obtener una valoración del problema y un presupuesto si se requiere conocer más al respecto e incluso poder saber quién fue el atacante o recuperar lo sustraído.