reclamador.es

Situaciones que ponen en peligro la seguridad en Internet: scam, phishing, keylogger, pharming

Madrid, 19 de mayo de 2021. Muy diversas son las situaciones de peligro a las que nos enfrentamos día a día todos los que accedemos a Internet, independientemente del dispositivo utilizado.

Internet permite ahora hacer casi cualquier trámite sin necesidad de desplazamiento, por ejemplo, contratar viajes, hablar con un abogado a través de videollamada, poner reclamaciones a empresas, presentar la Declaración de la Renta o realizar trámites bancarios como transferencias. La pandemia ha provocado que el acceso a la red para realizar cosas tan habituales como realizar la compra se haya generalizado. Pero usar Internet puede derivar en importantes problemas de seguridad, como son el robo de los datos bancarios y personales. Por ello, para intentar evitar esos intentos de fraude y que todos podamos usar Internet de forma segura disfrutando de sus incalculables ventajas, reclamador.es ha recopilado los principales peligros de la red para poder detectarlos y evitar ser víctimas de estas técnicas maliciosas.

Keylogger

El Keylogger es un malware que, al ser descargado o instalado en el dispositivo, registra las pulsaciones que se realizan en el teclado, guardando toda la información que se escribe.

Para evitar este malware, reclamador.es recomienda no descargar contenidos, ni software, películas o series de webs que no sean habituales. También se debe prestar especial atención a los correos que se reciben simulando ser enviados desde direcciones de empresas, ya que muchas veces contienen software dañino. Por supuesto, nada de descargar archivos adjuntos de estos emails. Si hay que instalar una aplicación, lo ideal es que se haga desde un repositorio oficial, como Google Play o Apple Store.

Phishing

Este es uno de los términos que más suena desde hace unos años. Se trata de correos electrónicos que se hacen pasar por reconocidas empresas y que piden

descargar un archivo o acceder a través de un enlace a una página web donde incluir todos los datos bancarios y personales. En definitiva, señala reclamador.es, el phishing es la técnica que, suplantando la identidad de cualquier entidad, busca estafar o robar los datos de carácter personal de los receptores mediante el engaño.

Los casos de phishing más conocidos se dan con entidades bancarias. En correos electrónicos, haciéndose pasar por un banco, piden al receptor que acceda a un enlace donde le piden que meta todos sus datos. Para evitar caer en las redes phishing, reclamador.es recuerda que **los bancos no solicitan incluir todos los datos a través de un correo electrónico**. Hay que desconfiar si piden facilitar número de cuenta y PIN, y más si no se dispone cuenta en esa entidad.

Lo mismo ocurre con Hacienda, ahora que estamos en plena campaña de la renta, pues este organismo en alguna ocasión ha sido suplantado para robar información personal de los usuarios. En su página web, la Agencia Tributaria aconseja *"desconfiar de cualquier comunicación que incluya la petición de información confidencial, económica o personal o incluya cualquier enlace que no remita a su página web o a su Sede electrónica".*

Pharming

El pharming supone "clonar" una página web, desde la que el usuario, confiado en que se encuentra en la oficial de la empresa que se trate, introduce sus datos y lógicamente son recogidos por los ciberdelincuentes. Lo cierto es que la clonación es prácticamente perfecta, y para evitar caer en sus redes hay que ser especialmente observador en la URL que se muestra en la barra del buscador. A la más mínima diferencia que se observe con la habitual de nuestro banco, seguro, o cualquier prestador del servicio que queremos obtener de la que ya seamos clientes, lo mejor es abandonarla inmediatamente. Y si hemos llegado a ella por primera vez, hay que fijarse que en la dirección de la página aparezca el protoco https.

Scam

Otra técnica maliciosa que intenta engañar al usuario que recibe el mensaje para que este termine pagando una determinada cantidad económica. Cuando las comunicaciones se hacían por carta, este timo recibía el nombre de "carta nigeriana" por la habitualidad con se remitían por parte de un supuesto "heredero" o "ganador de lotería" de dicha nacionalidad que requería ayuda al destinatario. Aunque pudiera resultar poco creíble, aún se envían correos electrónicos o mensajes con el mismo contenido.

Se trata de sutiles técnicas de engaño en las que los ciberdelincuentes intentan hacer creer al usuario de Internet que podrá conseguir una importante cantidad económica

si antes les envía a ellos una determinada cantidad. Una vez el usuario remite el dinero, los ciberdelincuentes desaparecen y no vuelven a tener contacto.

También, mediante este término, se hace referencia a esos engaños amorosos que pretenden que la víctima caiga en las redes de la persona que está detrás del engaño para que le envíe dinero. Una vez recibida esa partida económica, la otra persona desaparece.

¿Qué hacer si se es víctima de uno de estos peligros?

En caso de ser víctima de una de estas técnicas que tienen como fin conseguir dinero, datos bancarios y personales, reclamador.es recomienda denunciar en cuanto la víctima sea consciente de que ha sido víctima de phishing, pharming, scam o keylogger. Con la denuncia, señala la compañía online de servicios legales, es aconsejable acudir a la entidad bancaria para poner en su conocimiento la situación, en el caso de haber ofrecido datos bancarios. Estas dos acciones facilitarán la posterior reclamación si terceras personas hacen un uso indebido de los datos personales.

En los casos de phising y pharming en que se haya sacado dinero de nuestras cuentas, hay que saber además que el banco está obligado a devolverlo con una franquicia de 150 €, puesto que la Ley de Servicios de Pago impone a las entidades bancarias la responsabilidad de estos hechos por no haber puesto todas las medidas necesarias para evitar el engaño

El afectado, también puede comunicar la situación a la Oficina de Seguridad del Internauta (OSI). Este organismo depende del Ministerio de Energía, Industria y Turismo.

Y, además de todo lo anterior, si se han facilitado claves, PIN o contraseñas, lo más recomendable es cambiar todas ellas lo antes posible.

derechos de los pasajeros aéreos APRA (Association of Passenger Rights Advocates) y de la sección española de ELTA (Asociación Europea de LegalTech) en la que se encarga de los servicios legales digitales. reclamador.es se proclamó ganadora en South Summit 2017 como mejor servicio de la categoría B2C entre miles de startups europeas, y se encuentra entre las 250 compañías que más rápido crecen en Europa, según el ranking FT1000 (2019) elaborado para el periodo 2013-2018, del diario Financial Times y Statista. Durante los años 2018 y 2019, reclamador.es se ha posicionado como marca líder en España en reputación digital en el sector legal según el ranking de Law & Trends.

Con 100.000 casos resueltos y 50 millones de euros de indemnizaciones conseguidos hasta el momento, trabaja con una tasa de éxito del 95% y bajo un modelo No Win, No Fee, es decir, solo cobra si gana. La plataforma ofrece todos sus servicios online y cuenta con más de 300.000 usuarios registrados y 170 millones de euros reclamados. reclamador.es ha conseguido que se eleven tres cuestiones prejudiciales al Tribunal Europeo de Justicia Europea (TJUE) para proteger los derechos de los consumidores, entre ellas la restitución total de los gastos de hipoteca pagados por el consumidor, cambiando la doctrina del Tribunal Supremo español.

Tiene en su accionariado, a Martin Varsavsky (VAS Ventures), al fondo Cabiedes & Partners, a la red de inversores Faraday, y relevantes inversores del mundo online como Francois Derbaix (fundador de Toprural), Yago Arbeloa (presidente de la AIEI), Carlos Blanco (ITnet) o Making Ideas Business (xISDI Venture Club), entre otros. Cuenta con financiación de ENISA y EMPRENDETUR (Ministerio de Economía, Industria y Competitividad) y CDTI.

Para más información:

Cristina Naveda / Alicia Riaño

comunicacion@reclamador.es

https://www.reclamador.es/prensa/

633 120 224 / 635 87 35 74