Asociación de Internautas

Timos y estafas, una constante en Internet

Internet es un amplio y extenso espacio virtual en el que los **cibercriminales** difunden de manera continuada sus ataques en busca de posibles víctimas. Una actuación bastante común es la relacionada con las estafas, un tipo de **engaño** que no para de crecer y que persigue un propósito principal, obtener información personal de los internautas para suplantar su identidad y lograr un beneficio económico a su costa.

Martín Castro en Computer Hoy.com.- En este sentido, son llamativos los últimos timos aparecidos como consecuencia de la proliferación de aplicaciones de mensajería instantánea y redes sociales, que aprovechan los envíos de **mensajes en cadena** para la mayor difusión posible.

Alimentación y salud (59%), tecnología (8%) y economía (7%) son los ganchos principales de estas estafas según el ?III Estudio sobre bulos y fraudes en Internet?. Lo realizó la **Asociación de Internautas** hace algunos años y los datos recogidos en él son extrapolables a la actualidad.

Ya entonces, un 88% de los encuestados afirmó haber recibido un correo electrónico felicitándole por un premio de lotería que había ganado ?cuando en realidad no era verdad?, y un 68% un mensaje del servicio de Correos en el que se le decía que un paquete le estaba esperando. Asimismo, este documento señalaba que un 75% de los españoles se había encontrado una **oferta falsa** de trabajo vía email.

Parece ser que un 48% de los usuarios ha vivido un intento de **fraude online** según ?El Estudio sobre la Ciberseguridad y confianza en los hogares españoles?, y el Cuerpo Nacional de Policía informa que el 80% de los delitos cometidos en la web son estafas. ?Cada vez recibimos más casos de personas que han sido víctimas de una estafa en Internet. Cualquier precaución en la Red es poca, hay que ir con cuidado y evitar reenviar información falsa y no facilitar **datos personales** y bancarios en páginas que no cuenten con un mínimo de garantía?, explica Ofelia Tejerina, responsable del departamento legal de la Asociación de Internautas.

Cuidado con WhatsApp

Uno de los últimos timos puestos en circulación y del que se ha hecho eco la Oficina de Seguridad del Internauta, es el relacionado con una promoción que a través de WhatsApp prometía a los clientes de la popular aplicación Internet gratis sin WiFi, algo totalmente falso por que desde el punto de vista técnico no resulta posible.

¿Cómo era y cuáles son las características que tenía este fraude? El mensaje de los usurpadores era sencillo a la vez que llamativo y en él se pedía a la víctima que lo **compartiera** con 13 amigos o 5

grupos de la app para intentar llegar al mayor número de personas.

Si este mensaje se enviaba y pulsabas el botón ?Continuar? eras redirigido a diferentes páginas en las que, por ejemplo, te notificaban que tu teléfono móvil estaba **infectado** y que necesitabas bajarte una determinada herramienta; otras, en cambio, te pedían contestar a una encuesta para recibir un premio y lo único que debías hacer era responder a una batería de preguntas personales. Podía darse el caso, por otro lado, que el propio navegador de tu smartphone identificase un sitio como potencialmente peligroso y lo bloquease al instante.

Coincidiendo con el inicio de 2017, **Legalitas**, empresa dedicada al asesoramiento jurídico a particulares, alertó de un nuevo fraude relacionado con WhatsApp y que ya había afectado a más de 260.000 personas. El cebo, que prometía conseguir videollamadas o nuevos emoticonos,en realidad era una aplicación maliciosa encargada de acceder a los datos almacenados en el teléfono del usuario.

Ofertas fraudulentas

La popularidad alcanzada por ciertas aplicaciones para dispositivos móviles ?como las de búsqueda de empleo o pareja? se está convirtiendo en caldo de cultivo de los estafadores en sus ataques. ¿Recuerdas las cartas nigerianas? Es un clásico entre los timos y quienes lo ponen en práctica ya se han actualizado y adaptado a los nuevos tiempos.

Foto: ?Estudio sobre la Ciberseguridad y confianza de los hog res españoles?, de ONTSI.

Así, en diciembre de 2016 se conocía la noticia de la detención de 31 personas de una organización criminal ?por parte de la Policía Nacional? acusadas de un fraude de cinco millones de euros. Para recabar información de sus posibles víctimas recurrían a las **redes sociales en Internet** en busca de patrones o características comunes.

Las plataformas de compra y venta online entre particulares también están siendo utilizada de forma habitual por algunos estafadores, como ocurre con las dedicadas a los automóviles de segunda mano. A este respecto, Legalitas recuerda que cualquier usuario puede convertirse en víctima de esta clase de estafa y sugiere varias recomendaciones que, aunque sencillas, no hay que olvidar nunca.

Es el caso del medio de pago: si el desembolso económico no puede efectuarse en persona, siempre es preferible optar por plataformas seguras como PayPal. Indica, de igual forma, que consultemos el perfil del vendedor para analizar las valoraciones y los comentarios que realizan otros usuarios de la página en la que te encuentres.

Los falsos cupones descuento y tarjetas regalo son otras tácticas que vienen empleándose desde hace algunos meses. H&M, Lidl, Burguer King, Ikea, El Corte Inglés o Zara son algunas de las grandes firmas que han visto suplantada su identidad a consecuencia del **phishing**.

En este caso, los ciberatacantes se valen de la confianza que generan para atraer la atención del consumidor, engañarle y hacerse con sus datos confidenciales. Los clientes de la cadena de supermercados Carrefour también se han visto afectados y, en su caso, recibían un correo electrónico (siempre falso) en el que se les notificaba que su cuenta estaba bloqueada y que era preciso que realizaran una verificación y corroboración de datos de la misma.

La banca siempre está en el punto de mira

Los sistemas de monitorización de la Oficina de Seguridad del Internauta se hicieron eco de diversos correos fraudulentos que **suplantaban** la identidad de La Caixa y Abanca, con el objetivo de sustraer información de las tarjetas de sus clientes de banca electrónica, siempre a través de ataques phishing.

En el caso de La Caixa, los ciberdelincuentes informaban al usuario de que el banco estaba actualizando la normativa de seguridad para realizar operaciones desde el teléfono móvil a petición del Banco Central Europeo, y que era necesaria la sincronización de su tarjeta (MasterCard o Visa) a través del enlace que aparecía en pantalla. Para Abanca, los estafadores idearon un mensaje de correo que decía en el asunto ?Estado de cuenta inactivo?; en teoría, y para volver a activarla, había que introducir la información referida a la tarjeta de coordenadas del usuario.

Obtención de datos

Los ciberatacantes, incluso, lo han intentado con emails engañosos en los que se hacen pasar por el popular servicio de entretenimiento **Netflix** para robar los datos bancarios y las contraseñas de las personas que tienen contratados los servicios de esta plataforma. La Policía Nacional alertó de ello a finales del pasado mes de enero a través de su Twitter, explicando que la estafa en cuestión consistía en actualizar los datos de la cuenta de los clientes de Netflix.

En concreto, el último párrafo del citado email indicaba: ?Este mensaje fue enviado por correo automáticamente por Netflix en los controles de seguridad de rutina. No estamos completamente satisfechos con la información de su cuenta y obligados a actualizar su cuenta para continuar utilizando nuestros servicios sin interrupción?.

Estafas en empresas

Algunos estafadores centran su interés en el ámbito de la empresa. Lo hacen a través de un delito que se conoce como ?fraude al CEO? y que consiste en recopilar información de los **responsables financieros** de las compañías a los que envían falsos emails en los que suplantan la identidad de un cargo o directivo importante para que realicen determinadas transferencias económicas. Detrás de este engaño hay una labor meticulosa de seguimiento de estos responsables a los que **espían** su teléfono móvil o recaban datos personales a través de distintas fuentes como redes sociales o páginas de contactos.

En definitiva, hay que ser precavidos y estar atentos a cualquier mensaje que se reciba a través de Internet, sobre todo si la **fuente** es desconocida o su propuesta nos resulta demasiado atractiva para ser cierta.

Mantenerse al día respecto a las nuevas artimañas de los ciberdelincuentes es una buena ayuda pero, en general, un poco de precaución y desconfianza junto con una buena dosis de **sentido común** serán suficientes para evitar este tipo de engaños.

Reconoce una estafa

- La situación. Cuando recibes un mensaje de un remitente que es desconocido proponiéndote, por ejemplo, una oferta de trabajo tentadora a nivel económico o que le ayudes a completar una tarea, hay que sospechar y reflexionar sobre el mismo.
- La redacción del mensaje. El estilo también te puede proporcionar una pista importante para su identificación. Son frecuentes las faltas de ortografía, la mala redacción y la poca o nula

concordancia gramatical.
- Hay tendencia a aprovecharse de marcas y nombres populares con cierto gancho.
- Apelar a las emociones. Algunos ciberestafadores optan por apelar a los sentimientos para conmoverte y que así caigas en su trampa.
- Solicitud de información o ayuda. Por ejemplo, las entidades bancarías jamás pedirán a sus clientes sus contraseñas para poder operar.
