PERE CERVANTES y OLIVER TAUSTE

INTERNET NEGRO

EL LADO OSCURO DE LA RED

Pere Cervantes
Oliver Tauste

Internet negro

El papel utilizado para la impresión de este libro
es cien por cien libre de cloro
y está calificado como papel ecológico

Ediciones Temas de Hoy, sello editorial de Editorial Planeta, S. A.
Avda. Diagonal, 662-664, 08034 Barcelona
www.temasdehoy.es
www.planetadelibros.com
ISBN: 978-84-9998-518-3
Depósito legal: B. 23.972-2015
Preimpresión: Safekat, S. L.
Impresión: Huertas, S. A.

Printed in Spain - *Impreso en España*

Índice

Si Internet fuera un iceberg, solo la parte visible que emerge por encima de la superficie del mar sería «lo que Google ve», es decir, esa área a la que accedemos, o podemos acceder, la mayoría de usuarios. Sin embargo, el gran cuerpo del iceberg, el que puede causar el hundimiento del trasatlántico más potente del mundo, es lo que hemos denominado «lo que Google no ve».

En el índice verás que hemos estructrado el libro a partir de esas dos realidades. La primera la encontramos gracias a buscadores como Google, referencia principal para todos a la hora de buscar información y también donde acontecen los delitos más comunes que vamos a tratar, como los fraudes *on line* en la compra-venta de objetos, los delitos que afectan a menores, mayores, empresas, etc., o las nuevas formas de ejercer la violencia de género. Se trata de una delincuencia al alcance de cualquiera, porque tan solo se necesitan dos requisitos: un dispositivo con conexión a Internet y ganas de hacer el mal.

Pero detrás de esta faceta visible de Internet se esconde la cara oculta y, por tanto, más peligrosa, formada por todo aquello que Google no ve. Hablamos de la *Deep Web*, o Internet profunda, un territorio al que no se puede acceder tan fácilmente y donde se desarrolla el crimen organizado virtual a gran escala. Esta cara suele ser invisible incluso para las Fuerzas y Cuerpos de Seguridad del Estado, incapaces de seguir el vertiginoso desarrollo de una delincuencia que se aprovecha de los avances tecnológicos —y de los retrasos de nuestro ordenamiento jurídico— para lucrarse sin escrúpulos.

Así pues, en la primera parte expondremos las modalidades delictivas más actuales y frecuentes que tienen lugar en la red. Aunque sea únicamente la punta del iceberg, vale la pena que el barco en el que navegamos —el ciudadano digital— esté preparado para percibir el peligro que entraña una gran masa de hielo y poder así sortearla. Además de explicarte las características de los principales delitos, te proporcionaremos algunas medidas básicas de seguridad. Sabemos que la mayoría de los ciudadanos se encuentran bastante perdidos en lo referente a acciones preventivas, y ese vacío es el que deseamos llenar.

1
No caigas en la red de los fraudes: que no te vendan la moto

> «Nadie tiene más posibilidades de caer en el engaño que aquel para quien la mentira se ajusta a sus deseos».
>
> Jorge Bucay

Has encontrado una oferta irresistible: el coche que estabas buscando se anuncia en una página web a un precio increíble. Es un verdadero chollo y no quieres que nadie se te adelante. Pese a que por un momento has pensado que es demasiado bueno para ser verdad, decides interesarte por el anuncio y enviarle un mensaje al vendedor a través de la web. Al momento recibes la contestación con unas condiciones inmejorables: a cambio de un pago a modo de señal, una empresa de transporte internacional te llevará el coche a tu casa para que lo pruebes. De hecho, si no quedas convencido, tú le devuelves el coche y él te devuelve el dinero. Así de sencillo. El vendedor te explica que le urge vender el vehículo porque está viviendo en Reino Unido y no le resulta práctico un modelo español

con el volante a la izquierda. Todo te parece lógico y, sin sopesar riesgos —ni siquiera lo has consultado con tu pareja—, realizas el pago a modo de señal: un chollo hay que cazarlo en pleno vuelo. La forma de pago es a través de una agencia de envío de dinero (MoneyGram, Western Union, etc.) con destino a la persona y el lugar que te han indicado en el último *e-mail:* un agente financiero que resulta ser un intermediario en otro país. Esto no te acaba de convencer, pero las ganas pueden ante cualquier duda. Ya te imaginas conduciendo tu coche y piensas: «¿Qué puede salir mal si cada día se hacen millones de operaciones como esta por todo el mundo?». Pero pasan los días y el coche no llega… Intentas contactar con el vendedor, que ha dejado de responder a los *e-mails,* y descubres que el teléfono que te dio no está operativo. Comienzas a preocuparte porque está claro que algo no va bien. Enviaste el dinero al agente financiero y ahora todo el mundo ha desaparecido del mapa. Te pones en contacto con la empresa de transportes que te traería el coche desde Reino Unido y tienes la suerte de que es una empresa real, aunque te aseguran que no tienen ninguna entrega pendiente a tu nombre ni en tu domicilio. Entonces empiezas a atar cabos y caes en la cuenta: «Me han estafado. ¿Cómo he podido picar?… El coche estaba en Reino Unido, lo vendía un español que escribía un castellano con errores, como si usara un traductor *on line* para escribir, y, sobre todo, ¿cómo podía ser tan barato?».

Quizá te ha ocurrido algo parecido, o conoces a alguien a quien hayan estafado de este modo. Si es así, no

te tortures, se trata de un tipo de delincuencia internacional muy especializada y sus artífices no dudan en usar cualquier argucia para enriquecerse en tiempo récord. Detrás de esta estafa hay toda una estrategia, basada en técnicas de ingeniería social —de las que hablaremos a continuación—, que consiste en publicar en Internet ofertas de coches, o de lo que sea, a un precio muy por debajo del normal. Ese es el cebo, el bajo precio, que se apoya en las ganas de comprar y en la costumbre, cada vez más extendida, de adquirir objetos a través de la red. El caso de los coches tiene su propio nombre, *phishing car,* un fraude que sigue funcionando pese a su antigüedad y a las miles de víctimas que ya ha cosechado.

Las estafas por Internet tienen siempre la misma base: un cebo. Coches, ordenadores, *tablets,* relojes inteligentes, incluso mascotas…, cualquier cosa que alguien dice vender a un precio increíblemente bajo para ser cierto. Y, en efecto, no lo es.

¿Qué es la ingeniería social?

Mediante técnicas de ingeniería social los cibercriminales consiguen engañar a personas a lo largo y ancho del planeta. Son técnicas de manipulación psicológica y sociológica dirigidas a ganarse la confianza de sus víctimas para que estas hagan algo que normalmente no harían, como enviar dinero a desconocidos o proporcionar contraseñas y todo tipo de datos personales y bancarios. Pueden tener

varios formatos, aunque lo habitual es que estos «ingenieros» diseñen una historia, una artimaña o una situación ficticia que la víctima se cree sin excesiva dificultad.

Un clásico de las técnicas de ingeniería social es recibir un *e-mail,* con el asunto «URGENTE», en el que un banco te informa de que alguien ha intentado acceder a tus cuentas bancarias *on line* sin tu permiso, por lo que están realizando una auditoría de seguridad interna para solucionar el problema. A continuación te piden que pinches en el enlace que aparece en el propio *e-mail* y que verifiques tus claves de acceso; de lo contrario, te dicen, el banco se verá obligado a cancelar tus cuentas. Se trata de una situación urgente y repentina que puede solucionarse con un simple clic. La ingeniería social lo tiene todo calculado al milímetro y basa su éxito en el hecho de que las personas somos predecibles y solemos reaccionar de un modo parecido ante una determinada situación. Así, el mismo correo electrónico que está generando el problema ofrece la solución, que pasa por verificar tus claves. Seguro que ya habrás intuido que la página web que se abrirá tras pinchar en el enlace es falsa, ubicada en algún servidor extranjero y gestionada de forma anónima por ciberdelincuentes. De este modo obtienen multitud de claves y contraseñas que podrán utilizar para realizar futuras transferencias fraudulentas y saquear cuentas bancarias. Este es el fraude denominado *phishing,* del que hablaremos en el siguiente apartado.

Pero la ingeniería social es mucho más que un simple *e-mail.* Los ciberdelincuentes también emplean técnicas

como la suplantación de identidad de personas conocidas, de altos cargos de organismos oficiales, o bien se sirven de nombres de empresas de prestigio que prestan servicios o venden algún producto y, haciéndose pasar por ellas, publican falsas ofertas de trabajo para obtener datos reales de personas que posteriormente utilizarán para el blanqueo de capitales. Igualmente se sirven de la cobertura y la credibilidad que proporcionan los cambios y acontecimientos sociales, como los conflictos internacionales, las catástrofes naturales, la crisis económica o el paro. Cualquier circunstancia puede servir para diseñar nuevas estrategias de manipulación y así captar más víctimas.

Personas muy avispadas acaban mordiendo el anzuelo, pero estamos seguros de que, con los conocimientos adecuados, los miles de fraudes que circulan por Internet se pueden evitar. Todos estos engaños tienen en común el querer aprovecharse de las debilidades humanas, y sabemos que, para sentirse protegido, un primer paso es familiarizarse con los fraudes más habituales, que veremos a continuación.

Los fraudes más habituales

Junto a los griegos, los españoles somos los ciudadanos europeos que más tememos ser engañados en Internet y, sin embargo, los que menos precauciones tomamos. Así, por ejemplo, la instalación de antivirus en nuestros dispositivos (ordenadores, *smartphones, tablets*, relojes inteli-

gentes, etc.) es muy inferior a la del resto de países de nuestro entorno.

Para romper las estadísticas es necesario saber de qué estamos hablando. Por eso ahondaremos en los fraudes más frecuentes y en cómo prevenirlos. Por supuesto, estas modalidades de fraude *on line* evolucionan con el tiempo, pero hay una serie de características que se mantienen y que en ningún caso debemos olvidar.

Phishing: *pescando incautos en Internet*

El *phishing* es un tipo de estafa informática que se desarrolla en varias etapas, apenas deja rastro y proporciona enormes beneficios. Básicamente consiste en obtener las claves de acceso a la banca *on line* de la víctima, por lo general empleando alguno de los procedimientos de ingeniería social a los que nos hemos referido. Esto permite a los ciberdelincuentes ordenar tantas transferencias como saldo disponga la cuenta de la víctima, o vender en el mercado negro las contraseñas para que otros las utilicen. También pueden realizarse otras acciones, como solicitar préstamos *on line,* hacer recargas telefónicas o pagar facturas de terceros. Los titulares de las cuentas bancarias beneficiarias son colaboradores captados previamente y conocidos en la jerga policial como «muleros». Tras haber pactado el cobro de una comisión, calculada sobre el total del importe de la transferencia, los muleros se encargan de retirar las cantidades en efectivo de sus cuentas y de enviar-

las, a través de alguna agencia de envío el dinero, a otra persona, que suele estar en un país distinto al de la víctima.

A raíz de las numerosas investigaciones en las que hemos participado relacionadas con el *phishing* (del inglés *fishing*, «ir de pesca»), sabemos que cada una de estas fases tiene su particular desarrollo, y es fundamental conocerlas con detalle para estar prevenidos. No podemos olvidar que estamos ante grupos organizados de carácter internacional, cuyos miembros —los *phishers*— se reparten las diferentes tareas, especializándose cada uno en un «trabajo» concreto que va dirigido a «pescar» peces en el océano de Internet para obtener sus datos confidenciales y saquear cuentas bancarias. A continuación explicaremos con detalle en qué consisten esas fases, no sin antes advertir al lector de que está a punto de entrar en un asunto complejo y muy bien calculado por estas mentes tóxicas. Como ocurre cuando nos introducimos en una habitación en penumbra, se necesitarán unos cuantos segundos para apreciar las sombras, después una relativa claridad y finalmente la luz.

1. *Primera fase:* contraseñas al descubierto: estamos ante el *phishing* propiamente dicho, que consiste en obtener información confidencial de las víctimas, principalmente sus contraseñas de acceso a la banca *on line* o a otros sitios web que exigen verificación mediante usuario y contraseña.

El método más extendido es el envío masivo de correos electrónicos a modo de *spam* —correos comerciales no

deseados que llegan a miles de usuarios— que parecen proceder de un banco, una entidad financiera o un organismo oficial. En ese *e-mail* se explica que, por motivos de seguridad, mantenimiento, mejora en el servicio, confirmación de identidad o cualquier otra causa (el pago de un premio inexistente), el destinatario debe actualizar los datos de su cuenta bancaria. El mensaje imita el diseño —formato, logotipo y firma— de la entidad para comunicarse con sus clientes. Si el usuario que recibe el *spam* es cliente de esa entidad bancaria, dispone de acceso a la banca *on line* y carece de unos mínimos conocimientos sobre cómo funcionan los fraudes en Internet, es fácil que muerda el anzuelo. En el mismo correo aparece un enlace a una página web a la que puede acceder directamente para verificar sus credenciales y solucionar el problema. Esta página es prácticamente igual que la de la entidad bancaria, lo que se ha conseguido copiando el código fuente[1] de la web original. La dirección URL[2] también será similar —e incluso

[1] Conjunto de líneas de texto que continen las instrucciones necesarias para que se ejecute y funcione un programa o una página web. En el caso de las páginas web, esas instrucciones se escriben con algún lenguaje de programación, como HTML o Javascript, para luego ser ejecutadas por el navegador web que permite la visualización de la página visitada.

[2] Siglas del inglés de Uniform Resource Locator, o localizador de recursos uniforme. Es la cadena de caracteres que se corresponde con un lugar específico de Internet, como una página web, un blog o un chat. Ejemplo de URL del blog de *Tranki pap@s:* http://trankipapas.blogspot.com.es/.

idéntica—, pues los ciberdelincuentes se han aprovechado de los fallos de algunos navegadores o bien han realizado técnicas como el *homograph attack* —también llamado *IDN spoofing—,* que es la utilización de caracteres de otro idioma con una misma apariencia. Por ejemplo, la letra «o» latina se escribe igual que la griega o la cirílica, pero representan sonidos diferentes.

La mayor parte de los ataques de *phishing* van dirigidos contra las entidades bancarias, aunque pueden utilizar cualquier otra web como gancho para robar datos personales: Twitter, ebay, Facebook, PayPal, etc.

El proceso de captación de contraseñas puede iniciarse también con técnicas de *hacking*, para lo que utilizarán aplicaciones o programas informáticos diseñados para infectar nuestros dispositivos con conexión a Internet y espiar toda la información que por ellos circula. El fin es la captación ilegal de datos confidenciales de las víctimas para tener el control, especialmente de sus claves y contraseñas de acceso a la banca *on line*. Asimismo existen técnicas capaces de interceptar los datos que se introducen en la banca *on line* real, como el llamado *Man in the middle,* que consiste en insertar una especie de «intermediario» que puede leer y modificar las comunicaciones que se realizan entre la entidad financiera y el usuario sin que ni una ni otro lo sepan. O programas tipo *keyloggers*, que capturan las pulsaciones del teclado y se apoderan del contenido que escribimos y, cómo no, de nuestras claves de acceso a la banca *on line* o a cualquier otro sitio web en el que debamos verificarnos.

Detengámonos un momento en el *spoofing*, que, aunque lo parezca, no es un personaje de *Star Trek*, sino un conjunto de técnicas de suplantación de identidad. El atacante crea un contexto falso para engañar a la víctima con el objetivo de que facilite información confidencial, como nombres de usuario y contraseñas. El engaño se consigue de distintas formas, por ejemplo, suplantando páginas web de entidades bancarias o direcciones de correo electrónico de otras personas o entidades. Para que la suplantación surta efecto, se realizará el envío masivo de correos electrónicos *(spam)*, en los que puede aparecer el enlace a la web falsa. Lo que se pretende es que los usuarios faciliten información confidencial bajo cualquier pretexto. Los ataques de *spoofing* (contexto falso) son posibles tanto en el ciberespacio —creando una web falsa— como en el mundo físico, consiguiendo claves y contraseñas mediante llamadas telefónicas a empresas y particulares. El delincuente dice que llama desde el banco de la víctima y, con cualquier pretexto, pide la verificación de sus credenciales de acceso a la banca *on line*, a pesar de que los propios bancos avisan de que nunca solicitarán al cliente sus claves de acceso.

Los troyanos son otro tipo de *malware* (*software* malicioso instalado en contra de la voluntad o sin el conocimiento del usuario del ordenador dañado) que permite la monitorización y el control remoto de otro ordenador infectado, llamado ordenador «zombi». Así, se construye toda una red de ordenadores zombis —*botnets*— para realizar actividades ilícitas. Los troyanos se difunden a través

de páginas web, programas de intercambio de archivos, mensajería instantánea o correos electrónicos, y modifican la configuración del dispositivo electrónico de la victima para captar la información tecleada (como operaciones bancarias *on line).* Los troyanos residen de forma oculta y silenciosa en los ordenadores que logran infectar y se activan cuando el usuario visita determinadas páginas web, capturando las claves de acceso e incluso pantallas con el estado de las cuentas corrientes.

2. *Segunda fase:* captación de muleros. Una vez que disponen de las claves y contraseñas de acceso a las cuentas *on line* de las víctimas, los miembros de la organización necesitan colaboradores que abran cuentas bancarias en el mismo país en el que van a desarrollar la operativa de traspaso, antes de proceder a su extracción y envío por agencias de envío de dinero. Es habitual que los muleros sean ciudadanos residentes en el país en el que se encuentran las cuentas bancarias que van a ser saqueadas y que sean captados mediante técnicas de *scam,* que suelen consistir en supuestas ofertas de trabajo enviadas a través del correo electrónico o de mensajería instantánea desde números desconocidos (mediante Whatsapp*,* Telegram, etc.). Así, el mulero recibe un anuncio de trabajo en el que se ofrece una forma fácil y rápida de ganar dinero, pues solo debe disponer de acceso a Internet y tener conocimientos básicos sobre la utilización del correo electrónico y de espacios web (los correos enviados al intermediario, o mulero, suelen estar escritos en un castellano con bastantes errores gramaticales y ortográficos). En ocasiones, en el propio

mensaje aparece un enlace a una página web de la presunta sociedad o empresa que ofrece el puesto de trabajo con el fin de proporcionar mayor credibilidad.

Si el receptor del mensaje responde al correo electrónico interesándose por la oferta de trabajo, se establece una comunicación entre ambas partes mediante correspondencia electrónica, y en ella se definirán aspectos tales como el tipo de contrato y la operativa mercantil a desarrollar, que será la siguiente: cuando la supuesta empresa le avise, deberá abrir una cuenta bancaria en la entidad que le indiquen —si aún no la tiene abierta—. Como norma general, será en la misma entidad bancaria de la que han conseguido claves y contraseñas de acceso de diferentes usuarios. El motivo de esto es porque las transferencias se hacen efectivas en menos tiempo cuando se trata de cuentas de una misma entidad, y en esto del ciberdelito el tiempo siempre es dinero. Posteriormente, el mulero deberá facilitar su número de cuenta, el código IBAN[3] y sus propios códigos de acceso a la banca *on line.* Gracias a estos datos, los ciberdelincuentes dispondrán del medio necesario —una cuenta bancaria— para poder transferir el dinero desde la cuenta de la víctima a la del mulero. Después le comunicarán (generalmente por la tarde-noche o a primera hora de la mañana) que ya puede dirigirse a su

[3] International Bank Account Number, o código internacional de cuenta bancaria. Identifica una cuenta bancaria en concreto dentro del sistema financiero internacional (país, entidad, oficina y número de cuenta).

banco a retirar el dinero de la transferencia que ha recibido; el titular de la cuenta beneficiaria se quedará con el tanto por ciento estipulado (entre un 5 y un 10 %) y enviará el resto al país —normalmente, del este de Europa— y a la persona que le indiquen mediante una agencia de envío de dinero.

De este modo, los muleros suelen recibir en las cuentas que han abierto grandes sumas de dinero en muy poco tiempo. Como decimos, por lo general, se quedan con una cantidad en concepto de comisión, que variará en función de la cantidad transferida. En un día los muleros pueden ganar miles de euros sin tener que hacer prácticamente nada y sin, por supuesto, estar dados de alta en la Seguridad Social, lo que debería llevar a cualquiera a sospechar de la legalidad de esa actividad y, por tanto, a ponerlo en conocimiento de las autoridades.

Las épocas de crisis son las más favorables para que este tipo de fraudes se desarrollen en mayor medida. Incluso cuando se tiene un trabajo más o menos estable, ¿quién no desea obtener unos ingresos extra? Los «ingenieros» del fraude que trabajan para el *phishing* conocen bien estas circunstancias y el deseo de cualquiera de tener un mayor poder adquisitivo, por lo que siempre consiguen captar personas que, aunque sospechen, aceptan estos dudosos trabajos sin pensar en sus consecuencias.

La investigación se centrará principalmente en el seguimiento del dinero, por lo que el mulero tiene mucho más que perder que cualquier otro, ya que las transferencias ilícitas dirigidas a su cuenta bancaria dejarán un rastro

que la Policía podrá seguir: nombre, apellidos, dirección, teléfono y el número de la cuenta beneficiaria de un fraude. El mulero puede estar cometiendo un delito de estafa —además de otro de blanqueo de capitales—, y todo está a su nombre y queda bajo su responsabilidad.

3. *Tercera fase:* acceder a las cuentas sin dejar rastro. Pero el *phishing* sigue su camino. Una vez conseguidas las claves de acceso a la banca *on line* de la víctima y hallado un mulero que abra una cuenta en esa entidad con sus datos personales, el siguiente paso será ordenar las transferencias del primero al segundo dejando el menor rastro posible. Para ello es necesario una conexión a Internet para acceder a los servidores de las entidades bancarias. Obviamente, las organizaciones delictivas que se esconden detrás del *phishing* cuentan con personas que poseen conocimientos avanzados de Internet y logran que la navegación sea anónima. Para no ser identificados emplean diversos métodos, como el uso de máquinas comprometidas —los citados ordenadores zombis infectados por algún *malware* que permite un uso remoto—, servidores proxy —ordenadores que se conectan a Internet y abastecen de direcciones IP enmascaradas a los usuarios, lo que favorece el anonimato— o conexiones desde lugares públicos con acceso a Internet (cibercafés, bibliotecas, etc.), generalmente ajenos al grupo organizador del fraude y de la víctima.

4. *Cuarta fase:* disponibilidad del dinero. El titular de la cuenta bancaria de destino de las transferencias deberá dirigirse a su banco y extraer el dinero. Es posible que, debido a la cantidad transferida, deba hacer el reintegro

en ventanilla, pero en ocasiones lo obtienen a través de un cajero automático. Cuando ya tiene el dinero en la mano, el mulero lo enviará, mediante alguna agencia de envío de dinero (MoneyGram, Wester Union, etc.), al lugar y a la persona que la organización haya facilitado previamente por correo electrónico o por teléfono. El mulero se quedará con el tanto por ciento acordado y enviará un último correo informando de que el importe restante ha sido enviado, junto con el código identificador de la transferencia, necesario para hacerla efectiva. En el último paso, otro colaborador de la organización se dirigirá a la agencia de envío de dinero de la ciudad y país de destino, y, tras identificarse como el titular de la transferencia y proporcionar el código identificador, la hará efectiva.

Vacunas disponibles contra el phishing

Ya sabemos qué es el *phishing,* pero, por muy bien organizado que te parezca, no dudes de que dispones de herramientas para no convertirte ni en víctima ni en mulero. La prevención es la mejor estrategia para evitar riesgos, así que te pedimos que tomes nota de las siguientes vacunas:

- Identifica y verifica el origen de las direcciones de correo electrónico y mensajes (Whatsapp, Telegram, etc.) que recibas y que te parezcan sospechosas, especialmente si solicitan datos personales, contraseñas, u ofrecen supuestos trabajos.