LA DEFENSA FRENTE AL *PHISHING*

PASO A PASO

Guía práctica sobre el *phishing* y la defensa que frente al mismo ofrece nuestro ordenamiento jurídico

EDICIÓN 2023

Incluye formularios

LA DEFENSA FRENTE AL *PHISHING*

Guía práctica sobre el *phishing* y la defensa que frente al mismo ofrece nuestro ordenamiento jurídico

EDICIÓN 2023

Obra realizada por el Departamento de Documentación de Iberley

COLEX 2023

© Editorial Colex, S.L.
Calle Costa Rica, número 5, 3.º B (local comercial)
A Coruña, 15004, A Coruña (Galicia)
info@colex.es
www.colex.es

I.S.B.N.: 978-84-1359-843-7
Depósito legal: C 427-2023

SUMARIO

1.
EL *PHISHING:* ¿QUÉ ES?

El concepto de *phishing*

El *phishing* es una técnica empleada por ciberdelincuentes con la finalidad de engañar a las personas para que faciliten información personal confidencial. El término hace alusión a la pesca, entendiéndose como una «pesca de datos protegidos».

Existen muchas modalidades de *phishing* pero la más habitual es aquella en la que los ciberdelincuentes «suplantan la identidad» de una persona o entidad (por ejemplo, un banco), enviando un correo electrónico o un mensaje de texto haciéndose pasar por el suplantado. La víctima, en la creencia de estar recibiendo información de una entidad legítima, accede al enlace facilitado y revela datos protegidos.

Habitualmente el correo electrónico o el SMS busca asustar a la víctima, exigiéndole que acceda a algún enlace a fin de solucionar la situación. Una vez ha hecho clic en el enlace se le redirecciona a una página web que imita y simula a la de la entidad suplantada, en la que se le pide que se registre con sus datos y contraseñas, lo que es aprovechado por los ciberdelincuentes para quedarse con la información de inicio de sesión y poder robar su identidad.

A TENER EN CUENTA. La RAE para evitar el anglicismo «phishing», recomienda emplear en su lugar expresiones como «fraude informático», «ciberestafa», «suplantación de identidad», etcétera.

CUESTIÓN

¿En qué se diferencia el *phishing* del *spam*?

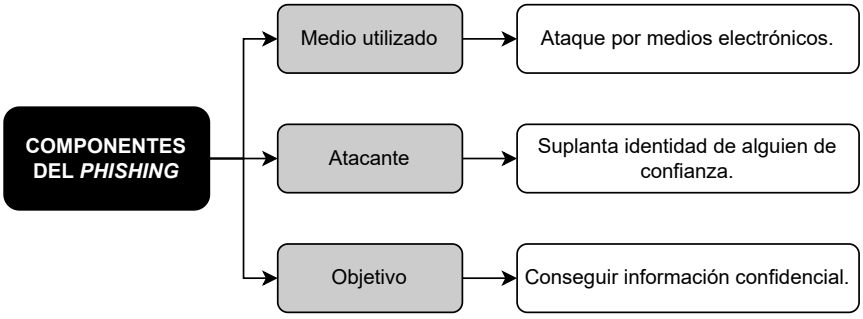
El *spam* no intenta obtener datos del destinatario, si no únicamente incluyen anuncios no deseados.

La Oficina de Seguridad del Internauta (OSI) recoge en su página web distintos avisos sobre campañas de *phishing* que se están utilizando en 2023, pudiendo citar, por ejemplo, correos suplantando la identidad de BBVA o Banco Santander y hablando de avisos de pagos o facturas pagadas al vencimiento, correos suplantando a la DGT comunicando una multa impagada, también suplantando a las Fuerzas y Cuerpos de Seguridad del

Estado acusando a las víctimas de haber cometido un delito, SMS suplantando la identidad de Abanca comunicando un cargo en cuenta o un acceso no autorizado a la cuenta, o también correos fraudulentos suplantando a la Seguridad Social.

Por su parte el Código Penal, tras la reforma realizada por la Ley Orgánica 14/2022, de 22 de diciembre, de transposición de directivas europeas y otras disposiciones para la adaptación de la legislación penal al ordenamiento de la Unión Europea, y reforma de los delitos contra la integridad moral, desórdenes públicos y contrabando de armas de doble uso, en vigor desde el 12 de enero de 2023, da cabida al *phishing* en el **art. 249.1.a)**, que dispone:

> «1. También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años:
>
> a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro».



Por lo tanto, el *phishing* se encuentra cada vez más extendido, ya que, al no atacar al sistema informático propiamente dicho, si no basándose en el engaño a la persona, no requiere unos conocimientos técnicos especialmente sofisticados.

A TENER EN CUENTA. Según el informe de verizon.com, el 82 % de las infracciones de violación de datos involucraron el elemento humano, incluidos los ataques sociales, los errores y el uso indebido.

|| El concepto de *phishing* en nuestra jurisprudencia

Nuestros tribunales no nos facilitan una definición de *phishing* común, pero podemos citar distintas sentencias que sí nos ofrecen una aproximación al concepto.

Si acudimos al **Tribunal Supremo** podemos citar, por ejemplo, las siguientes:

STS n.º 834/2012, de 25 de octubre, ECLI:ES:TS:2012:8284

«Estamos, por tanto, en presencia de una **actuación fraudulenta que toma como punto de partida el envío masivo de mensajes de correo electrónico desde diversos sitios en la web**, que tiene como destinatarios a usuarios de la banca informática —banca on line— a quienes **se les redirecciona a una página web que es una réplica casi perfecta del original** y en la que se les requiere, normalmente con el aviso amenazante de perder el depósito y la disponibilidad de las tarjetas de crédito, a que entreguen sus claves personales de acceso con el fin de verificar su operatividad. De forma gráfica se dice que el autor " **pesca los datos protegidos**" —de ahí la denominación phishing—, que permiten el libre acceso a las cuentas del particulares y, a partir de ahí, el desapoderamiento».

STS n.º 506/2015, de 27 de julio, ECLI:ES:TS:2015:3520

«Como señala la STS 834/2012, de 25 de octubre, esta doble secuencia forma parte de una estrategia delictiva única. Se trata de obtener dinero mediante el **fraudulento acceso a las claves bancarias de confiados usuarios de Internet** y, a partir de ahí, buscar una fórmula que permita colocar esos remanentes dinerarios en un país seguro, a nombre de personas de difícil identificación por los agentes de policía del Estado en cuyo territorio se efectúa el acceso inconsentido a las cuentas de la víctima y las transferencias a terceros países. **Es una actuación fraudulenta que tiene como destinatarios a usuarios de la banca informática cuyas claves personales se obtienen engañosamente, técnica denominada 'phishing', porque parte de una acción de pesca de las claves que permiten el libre acceso a las cuentas del perjudicado**».

STS n.º 291/2021, de 7 de abril, ECLI:ES:TS:2021:1601

«(...) Con los particulares, los acusados se relacionaban a través de Internet utilizando diversas modalidades como el phishing bancario, engaños en la venta de bienes y prestación de servicios por internet, sobre todo, engaños en arrendamientos temporales o turísticos por internet y recibían de las víctimas el precio de estos servicios o arrendamientos que no prestaban, en cuentas bancarias abiertas al efecto con documentación no verdadera. **El Phishing bancario consiste en el envío de un enlace, normalmente de una entidad bancaria, al correo electrónico o al teléfono móvil de la víctima, de manera que cuando el receptor pincha sobre el mismo, cree estar en la página oficial correspondiente y al poner las claves personales de acceso, las mismas son extraídas y utilizadas con posterioridad por terceros**, en éste caso los acusados, para realizar transferencias no queridas por la víctima (...)».

Si nos centramos en la jurisprudencia menor de las **audiencias provinciales** también podemos encontrar distintas aproximaciones al concepto de *phishing*:

Sentencia de la Audiencia Provincial de Zaragoza n.º 804/2022, de 1 de julio, ECLI:ES:APZ:2022:1482

«De acuerdo con la Agencia Española de Protección de Datos (Resolución del Expediente Nº: NUM000, DE 24 DE MAYO DE 2006): "**el objetivo de los**

ataques de 'phishing' es la obtención de forma engañosa y fraudulenta de los códigos de usuarios y contraseñas de clientes de Banca Electrónica, al objeto de realizar transferencias no autorizadas...Su operatoria comienza con la adquisición en internet de un 'paquete de herramientas', que incluyen programas informáticos e información necesaria para realizar los ataques. Esta información incluye 'listas de equipos comprometidos' que pueden ser utilizados bien para mandar correos electrónicos, bien para alojar páginas web falsificadas. Incluyen además 'bases de datos de direcciones de correo electrónico'. Una vez en posesión del paquete, se remiten los correos electrónicos con carácter indiscriminado (buscando contactar con clientes de la entidad financiera) informando de la necesidad de conectarse a una página web que parece pertenecer a la citada entidad y portar los códigos de acceso y contraseñas de clientes. Dicha página web se suele alojar en un equipo conectado a Internet cuya seguridad se haya [visto] 'comprometida', sin conocimiento de su usuario, y que se encuentra normalmente en un país distinto al de los destinatarios del ataque. De esta forma se constituye un 'fichero de datos personales con códigos de usuarios y contraseñas de clientes' recabados de forma engañosa y fraudulenta, que se ubica normalmente en el mismo 'equipo remoto comprometido' en el que se aloja la página web falsificada. Con los datos obtenidos se realizan transferencias a cuentas de colaboradores situados en España los cuales a su vez retiran el dinero en efectivo y tras descontar una comisión realizan transferencias monetarias internacionales mediante entidades especializadas"».

Sentencia de la Audiencia Provincial de Valencia n.º 254/2022, de 13 de junio, ECLI:ES:APV:2022:2622

«Entiende la demandada que la actora fue víctima de un caso de "phishing" que, en esencia, consiste en una **actividad delictiva cuyo objeto es dar la apariencia frente a la víctima de ser un tercero,** valiéndose incluso de emblemas y/o marcas comerciales similares, **con** ánimo **de obtener datos personales y de seguridad provocando en la víctima un perjuicio patrimonial**».

Sentencia de la Audiencia Provincial de Las Palmas n.º 44/2019, de 19 de febrero, ECLI:ES:APGC:2019:248

«Y es que en la estafa informática conocida como —phising—, **mediante un artificio informático se logra acceder a las cuentas y claves de terceros para con las mismas engañar a la entidad bancaria, al sistema, haciéndole ver que quién realiza una transferencia desde esa cuenta es el titular cuando en realidad es el hacker** —quién ha efectuado la manipulación informática—. Normalmente los idearios del engaño y de ese artificio informático defraudatorio se valen de terminales situados en el extranjero, usualmente países con los que resulta difícil la colaboración trasfronteriza policial para atajar las redes de fraude por internet, más como levantarían sospechas a los sistemas de seguridad bancario que las transferencias se realizasen directamente a cuentas en el extranjero y con órdenes emanadas desde esos terceros países, se cuenta con la —colaboración— de personas del país de origen que prestan un número de cuenta propio, normalmente a cambio de un porcentaje, para luego realizar una

conducta activa de transferir el grueso de la transferencia recibida a las cuentas de los autores del engaño en el extranjero, quedándose con un porcentaje a modo de comisión, haciendo residenciar la responsabilidad penal en esos colaboradores que en la inmensa mayoría de los casos son reclutados también a través de ofertas de trabajo ficticias en las redes».

Sentencia de la Audiencia Provincial de Madrid n.º 412/2020, de 28 de septiembre, ECLI:ES:APM:2020:11402

«Parte del tribunal para el análisis del recurso de apelación interpuesto del delito objeto de acusación " estafa informática mediante artificios semejantes". Conocido vulgarmente como "phishing" concepto informático que denomina el **uso de un tipo de fraude caracterizado por intentar adquirir información confidencial de forma fraudulenta** (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

El estafador, conocido como **"phisher",** envía a numerosas personas correos electrónicos masivos en los que se hace pasar por una empresa de confianza (por ejemplo, una entidad bancaria, o una compañía telefónica, etc.); otras veces lo hace mediante la creación de páginas "web" que imitan la página original de esa entidad bancaria o empresa de reconocido prestigio en el mercado; en ocasiones también se realiza por medio de llamadas telefónicas masivas realizadas a numerosos usuarios en las que se simula ser un empleado u operador de esa empresa de confianza. En todo caso, siempre se trata de **una aparente comunicación "oficial" que pretende engañar al receptor o destinatario a fin de que** éste **le facilite datos bancarios o de tarjeta de crédito,** en la creencia de que es a su entidad bancaria o a otra empresa igualmente solvente y conocida a quien está suministrando dichos datos. Finalmente, en otras ocasiones el sistema consiste simplemente en remitir correos electrónicos que inducen a confianza (simulando ser de entidades bancarias, etc.) que cuando son abiertos introducen "troyanos" en el ordenador del usuario, susceptibles de captar datos bancarios cuando este realiza pagos en línea. En todo caso, fuere cual fuere el "modus operandi" elegido, el objetivo son clientes de banco y servicios de pago en línea».

Otros conceptos relacionados con el *phishing* y los ciberataques

A la hora de analizar el *phishing* nos encontramos con distintos conceptos cuyo significado conviene conocer para poder comprender el alcance del mismo.

El *spoofing*

El *spoofing* es un ciberataque, una técnica o método utilizado por el ciberdelincuente que consiste en suplantar la identidad de una fuente conocida haciéndose pasar por ella. El fin es la obtención de información sensible de la víctima, como por ejemplo datos de usuario, contraseña, datos de la tarjeta de crédito... El *spoofing* se usa habitualmente en los ataques de *phishing.*

La **Audiencia Provincial de Valladolid, en su sentencia n.º 205/2016, de 29 de junio, ECLI:ES:APVA:2016:636**, nos da una definición del *spoofing* en los siguientes términos:

> «El "Spoofing", en términos de seguridad de redes, hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación. Entre ellos, el más conocido es el IP spoofing, que es la suplantación de la IP».

Por su parte, la **Audiencia Provincial de Burgos en sentencia n.º 64/2016, de 3 de marzo, ECLI:ES:APBU:2016:168**, profundiza más en este concepto y en sus posibilidades tanto en el mundo físico como en el electrónico:

> «En los ataques de Spoofing, el atacante crea un contexto engañoso para así engañar a la víctima de forma que haga una decisión relacionada con la seguridad inapropiada. Un ataque de Spoofing es como una estafa: el atacante monta un mundo falso pero convincente alrededor de la victima, actuando esta de forma que pasa inadvertida su situación de peligro. Los ataques de Spoofing son posibles tanto en el mundo físico como en el electrónico.
>
> Por ejemplo, ha habido varios incidentes en los que los criminales ponen máquinas expendedoras falsas, normalmente en áreas públicas de grandes almacenes, éstas aceptan el dinero plástico y piden a la persona que meta sus códigos secretos. Una vez que la máquina tiene los códigos de la victima, puede o bien tragarse la tarjeta o dar un error y devolver la tarjeta. En cualquiera de los casos, los autores tienen la suficiente información para copiar la tarjeta de la victima y realizar un duplicado operativo con las contraseñas captadas. En estos ataques, la gente era engañada por el contexto que veían: la localización de las maquinas, su tamaño y peso, la forma en que estaban decoradas, y la apariencia de sus pantallas electrónicas. La gente que usa sistemas informáticos, a menudo, toma decisiones relacionadas con la seguridad, basadas en indicaciones contextuales que ven. Por ejemplo, puedes decidir teclear tu número de cuenta bancario por que crees que estas visitando la página de tu banco. Esta creencia puede surgir por que la página tiene un aspecto familiar, por que el URL del banco aparece en la línea de localización del navegador, o por otras razones».

|| El *phisher*

Phisher es el nombre con el que se conoce al ciberdelincuente que utiliza el engaño para conseguir que las víctimas le faciliten información personal confidencial, es decir, utiliza el *phishing* para conseguir datos personales de terceros.

|| El *malware*

Cuando empleamos el término *malware* nos referimos a un programa informático o software malicioso que se ejecuta sin el conocimiento ni con-

sentimiento del usuario del equipo infectado. La finalidad del *malware* es instalar en los equipos un tipo de software que realiza algún tipo de daño en el dispositivo. Como ejemplos podemos citar los virus informáticos, los troyanos, el spyware...

CUESTIÓN

¿En qué se diferencia el *malware* del *phishing*?

Cuando hablamos de *malware* nos referimos a programas informáticos con intenciones maliciosas, mientras que el *phishing* es una técnica utilizada empleando el engaño o fraude para manipular a la víctima y conseguir información confidencial.

El *spyware*

El *spyware* es un software malicioso que se instala en el dispositivo sin conocimiento de la víctima, cuya finalidad es recabar todo tipo de datos personales e información privada para facilitársela al ciberdelincuente.

Los *keyloggers* y los *screenloggers*

Los *keyloggers* son un tipo de *malware* en el que sin que el usuario se percate se registran las teclas pulsadas en el ordenador o dispositivo móvil recopilando, por tanto, información de los afectados. Los *screenloggers* son similares, pero capturan imágenes de pantalla.

¿Cómo puedo identificar un ataque de *phishing*?

Actualmente nadie está a salvo de sufrir un ataque de *phishing* y estos cada día son más elaborados, por lo que es importante intentar prevenirlo y estar atento a las distintas señales que pueden ayudarnos a identificarlos.

La Organización de Consumidores y Usuarios (OCU) destaca 4 puntos a tener en cuenta para distinguir estos ataques:

- Comprobar si el nombre del remitente es conocido y, en su caso, si su dirección de correo electrónico es legítima. En este aspecto es importante comprobar que el dominio de la dirección de correo electrónico se corresponde con la entidad de la que dice provenir.
- Como los *phisher* suelen utilizar traductores automáticos, también resulta importante prestar atención a las faltas ortográficas y a los errores de concordancia o de redacción.
- Otra recomendación de la OCU consiste en pasar el ratón por encima de cualquier enlace o link que contenga el correo. Al hacerlo suele mostrarse la dirección URL a la que dirige el link que, si no coincide con la que figura en el link, o con la del sitio que en teoría representa, probablemente estemos ante un supuesto de *phishing.*
- Atender al contenido de los mensajes, ya que cuando se refieren a premios en los que no se participó, ofertas de trabajo a las que uno no se apuntó, multas que no constan, avisos amenazantes de bloqueos de cuentas... suele tratarse de este tipo de ciberataques.

LA DEFENSA FRENTE AL *PHISHING* PASO A PASO

En esta guía analizamos el concepto de *phishing*, sus tipos y las distintas opciones de defensa que encontramos en nuestro ordenamiento jurídico tanto en vía civil, como en vía penal, centrándonos en el análisis de la responsabilidad de las entidades bancarias cuando se ven implicadas en estos casos.

El lector encontrará todas las herramientas necesarias para tramitar reclamaciones de afectados por este delito, y exigir las responsabilidades correspondientes.

Para dotar a la obra de un contenido práctico se incluyen esquemas, resolución directa a preguntas frecuentes, análisis jurisprudenciales y formularios de interés.

COLEX

www.colex.es

COLEX READER

PVP 16,00 €

ISBN: 978-84-1359-843-7

9 788413 598437