INTERBEL
Email & Ciberseguridad

Colaboración de:
ASOBAN

Guía sobre el phishing bancario en 2025

Claves sobre la responsabilidad ante este fraude online

+34 123 456 789
contacto@interbel.es
www.interbel.es

ÍNDICE

INTRODUCCIÓN

El fraude online, especialmente a través de técnicas como el **phishing**, está en constante aumento. De hecho, el 85% de los correos electrónicos que recibimos son **spam**, y el 95% del malware se distribuye mediante correo electrónico para **introducir virus, suplantar identidades o robar contraseñas.**

Ante esta realidad, es crucial comprender quién es responsable ante un ataque de phishing. No solo se trata de proteger los sistemas y datos, sino también de asignar correctamente la **responsabilidad en caso de incidentes**.

En esta Guía (“White Paper”), en conjunto con la colaboración de Asoban Abogados, exploraremos en detalle quién es responsable ante un ataque de phishing y cómo se pueden tomar **medidas legales y de ciberseguridad** para mitigar los riesgos asociados y posibles consecuencias legales.

¿Qué es el Phishing? ¿Cómo funciona el engaño?

El Phishing es una técnica que utilizan los ciberdelincuentes **para robar información personal y confidencial** a través del engaño. En otras palabras, es "pescar" información importante usando un anzuelo (el engaño).

Las estafas de phishing representan casi el 36% de todas las violaciones de datos y el 71% de las empresas experimentaron un ataque de phishing con éxito en 2023.[1]

¿Cómo funciona el Engaño?

Suplantación de identidad: También conocida como spoofing. Los cibercriminales envían correos electrónicos, sms o te llaman haciéndose pasar por empresas, personas o instituciones de confianza (bancos, redes sociales, tiendas online, personas de tu entorno, empresas que son clientes, etc.).

Infección: Estos mensajes suelen contener enlaces a páginas web falsas o archivos adjuntos infectados.

***Robo de información*:** Al hacer clic en el enlace o abrir el archivo, podrías ser dirigido a una página falsa que solicita tus datos personales (como contraseñas o números de tarjetas) o te induce a realizar acciones como transferencias o compartir claves, comprometiendo tus credenciales.

Aspectos legales en Casos de Phishing

Principales Modalidades de Phishing

MAN IN THE MIDDLE El ataque de “Man in The Middle”, (en español, “Hombre del medio”), consiste en que **un cibercriminal intercepta una comunicación** entre un emisor y un receptor, pudiendo **espiar o modificar** la información contenida en dicha comunicación, con fines maliciosos.

Este tipo de ataque es difícil de detectar, ya que la comunicación parece legítima. Los atacantes suelen emplear esta técnica para interceptar correos entre empresas.

Por ejemplo, al estudiar las relaciones comerciales entre la empresa 'A' (proveedora de bienes y servicios) y la empresa 'B' (compradora), pueden interceptar un correo con una factura enviada por la empresa 'A'. La empresa 'B', confiando en la legitimidad del correo recibido, realiza el pago, pero los fondos son desviados a la cuenta del atacante, quien únicamente modifica la cuenta de destino en la factura.

El phishing se disfraza en diversas modalidades. No importa el método, el objetivo es siempre el mismo: **tu información.**

FRAUDE DEL CEO

El atacante **suplanta la identidad del CEO** para engañar a empleados con acceso financiero, pidiéndoles realizar pagos urgentes a cuentas designadas por él. Este fraude afecta principalmente a quienes tienen autorización **para hacer transferencias o gestionar recursos económicos.**

SMISHING Consiste en el **envío de mensajes de texto** (SMS) a las víctimas, haciéndose pasar por todo tipo de entidades de confianza. El objetivo es obtener información personal y bancaria para llevar a cabo nuevos fraudes o hacerse con nuestro dinero.

VISHING Se realiza a través de **llamadas telefónicas,** donde el atacante **suplanta la identidad** de una empresa, organización o incluso de una persona de confianza, con el fin de obtener información personal de sus víctimas.

Leyes que aplican

Normativa	Artículos Aplicables
Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (Actual Ley de Servicios de Pago)	36, 38, 39, 41, 42, 43, 44, 45, 46, 56, 59
Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal	247, 248
Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (Reglamento General de Protección de Datos - RGPD)	5 a 11, 24 a 26, 32, 33, 34, 35, 82, 83, 84
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales	70 a 78
Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil	1902, 1903
Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal (LECrim)	264
Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información	2
Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018	2

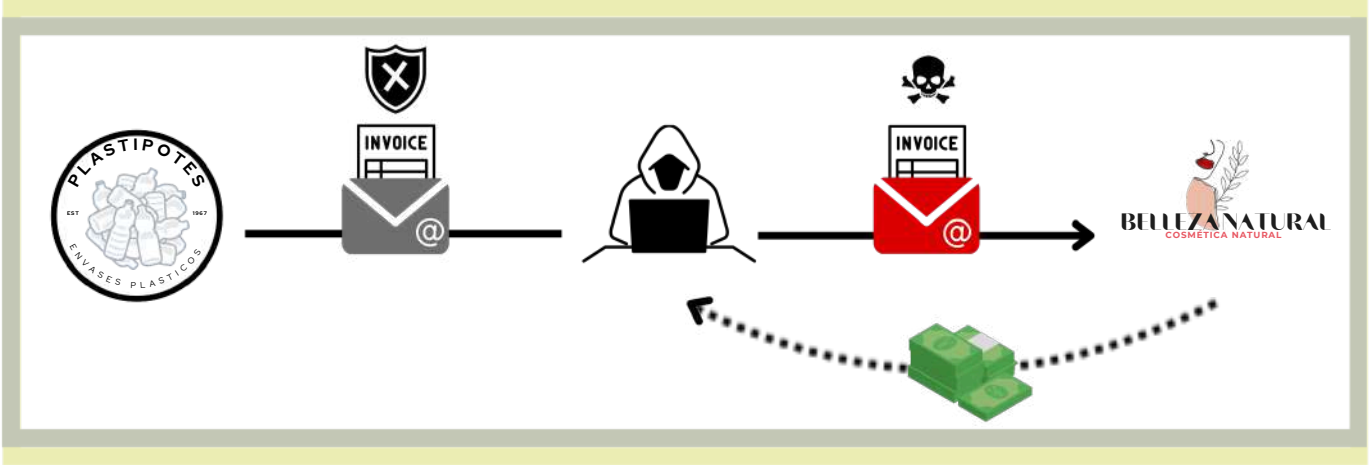
Un ejemplo de caso de Phishing

A continuación, presentamos un caso como ejemplo que ilustra cómo un ataque de phishing tipo **Man in The Middle** puede tener consecuencias legales graves para las empresas involucradas.

En 2023, PlastiPotes S.A., fabricante de envases plásticos, y Belleza Natural S.L., una empresa de cosméticos, mantenían una relación comercial basada en facturas electrónicas y transferencias bancarias. Aprovechando esta dinámica, los cibercriminales interceptaron una factura legítima enviada por PlastiPotes a Belleza Natural y modificaron la cuenta bancaria del destino. Reenviaron el correo a Belleza Natural con su apariencia original. Belleza Natural, confiando en su autenticidad, transfirió 160.000 euros a la cuenta del cibercriminal (creyendo que lo estaba enviando a la cuenta de PlastiPotes.

El fraude se descubrió cuando PlastiPotes reclamó la factura como impagada, y Belleza Natural les demandó alegando negligencia en la seguridad del email.

El tribunal falló a favor de Belleza Natural, concluyendo que PlastiPotes, aunque tenía un antivirus y un cortafuegos (firewall), no implementó otras medidas de ciberseguridad adecuadas como detección de intrusiones con DNS, protocolos seguros como DMARC en su dominio de email, formación y contraseñas seguras en sus usuarios y otras medidas que hubieran prevenido el fraude. La sentencia obligó a PlastiPotes a indemnizar el importe perdido y asumir los costes legales.



¿Qué hay que hacer ante un caso de Phishing?

Desde que se tiene conocimiento de la existencia de un caso de phishing, se deben tomar las siguientes acciones de manera cronológica desde una perspectiva legal:

1- En primer lugar, se debe **notificar inmediatamente el ciberataque a las autoridades policiales o la Guardia Civil**, para intentar localizar al responsable y cumplir con lo establecido por la Ley de Enjuiciamiento Criminal (LECrim), que regula el procedimiento penal ante delitos. Cuanto más rápida sea la actuación, más diligente se valorará la conducta del "estafado", tanto frente a la Agencia Española de Protección de Datos (AEPD) como en el ámbito civil, para intentar recuperar las cantidades defraudadas, como se verá en el punto 3.

2- En segundo lugar, **se debe analizar con el equipo de IT** propio o externalizado —incluso con peritos forenses— si el atacante ha tenido acceso a datos personales de la empresa. El responsable del tratamiento debe tener un **protocolo de actuación eficaz para gestionar la brecha de seguridad,** y tomar todas las nuevas medidas de ciberseguridad necesarias para evitar que se repita. En otras palabras, **incurrir en el análisis y la inversión que hubiera evitado el fraude.**

Una vez realizado, hay dos opciones a seguir según los resultados del análisis:

a) Si se confirma que el ciberatacante ha tenido acceso a datos personales, la empresa, como responsable del tratamiento, debe valorar si corresponde **aplicar el artículo 33 del RGPD*** notificando la brecha a la AEPD dentro de las 72 horas**. Y si implicara un alto riesgo para los derechos y libertades de los usuarios, también notificarlo a los afectados, según el artículo 34 del RGPD.

b) Si no hay evidencias de acceso a datos personales, la empresa **debe documentar la violación de seguridad**, las evidencias recogidas y las medidas adoptadas, conforme al artículo 33.5 del RGPD.

Ante un ataque de Phishing, es esencial notificar a las autoridades, realizar un análisis de la brecha y proceder con la recuperación de pérdidas económicas conforme a la normativa aplicable.

3- En caso de **perjuicio económico**, se deben llevar a cabo las siguientes acciones:

a) Notificar al **seguro de ciberseguridad** (si se tiene) para analizar la cobertura de la pérdida financiera derivada del phishing. b) Informar al banco para **bloquear fondos o intentar recuperar los importes** (conforme al artículo 44 y 59.2 del Real Decreto-ley 19/2018). c) Contactar con la empresa proveedora desde donde quizás se generó el email del fraude para verificar si hubo falta de medidas de ciberseguridad o anti-spoofing. d) Si no se recuperan los fondos, presentar **una reclamación extrajudicial** ante el banco y, si es necesario, recurrira la vía judicial con asesoramiento legal, dado que el banco podría no haber cumplido con sus obligaciones de seguridad.

*Artículo 33 RGPD: Establece la obligación por parte del responsable del tratamiento de datos de notificar a la autoridad de control (AEPD en España) en caso de violación de seguridad de datos personales. 4 Artículo 83 RGPD: Contiene los criterios para la imposición de sanciones
**Art 264 LECrim: establece la obligación de denunciar la perpetración de algún delito de los que deben perseguirse de oficio al Ministerio Fiscal, al Tribunal competente o al Juez de instrucción o municipal, o funcionario de policía.

¿Quienes son los responsables?

Tipo de Responsabilidad	Referencia Legal	Descripción
Responsabilidad del Banco Ordenante	Artículo 44 Ley de Servicios de Pago	El banco debe demostrar que la operación fue autenticada, registrada con exactitud y contabilizada.
Responsabilidad del Banco Receptor	Artículo 59.2 Ley de Servicios de Pago	El banco debe cooperar en recuperar los fondos del ordenante, detraídos fraudulentamente.
Responsabilidad de la Aseguradora	Basado en la póliza de ciberseguridad	La aseguradora debe cubrir los daños por brechas de seguridad en sistemas informáticos.
Responsabilidad de la Empresa atacada	Artículos 1.101 y 1.902 del Código Civil, Artículo 19 LOPD	Responsabilidad civil por daños a terceros y cumplimiento de obligaciones de seguridad y prevención.

En casos como **"Man in the Middle"** o Fraude del CEO, la responsabilidad puede recaer en varias partes. Por un lado, las empresas deben proteger la información que gestionan, sus dominios y sus infraestructuras tecnológicas mediante medidas de ciberseguridad adecuadas.

Por un lado, **las empresas deben tomar las medidas de ciberseguridad** adecuadas para proteger la información que gestionan, sus dominios y sus infraestructuras tecnológicas.

Por otro lado, **los bancos también tienen obligaciones clave**. Si bien el banco emisor de la transferencia debe verificar que el destinatario coincida con el habitual, el banco debe evitar abrir cuentas a ciberdelincuentes, cumpliendo la **Ley de Prevención de Blanqueo de Capitales.**

Aunque las entidades bancarias también deben asumir su papel como intermediarios, las empresas tienen una responsabilidad preventiva contra el fraude. **La responsabilidad es compartida** y debe analizarse según cada caso.

Jurisprudencia en España y Europa

Aplicable a perjuicios económicos ocasionados a empresas por la falta de implementación de medidas de seguridad :

A)Jurisprudencia Española:

La sentencia nº 106/2024, de 29 de julio de 2024, del Juzgado de Primera Instancia e Instrucción nº5 de Getxo, resuelve un caso de estafa conocida como "Man in the Middle". La empresa compradora del vehículo recibió un correo electrónico con la factura pendiente de pago, pero el número de cuenta había sido modificado por el estafador. Como resultado, la transferencia fue dirigida a la cuenta del delincuente. Al no poder acreditar que su correo electrónico no había sido hackeado (no pudo demostrar tener las medidas de ciberseguridad adecuadas), se condena a la empresa compradora a abonar nuevamente la cantidad acordada en el contrato, ya que la vendedora nunca recibió el dinero. **Aplicable a perjuicios económicos causados mediando la intervención de entidades bancarias:**

A) Jurisprudencia Española:

- Sentencia AP Sevilla. Sección 6ª. Sentencia nº 289/2021. Rec. 8540/2019, de 30 de julio de 2021. “Fraude del CEO”. Establece que la responsabilidad del proveedor de servicios **sólo cesa en caso de fraude** o culpa grave; supuestos que no concurren en este caso.
- Sentencia AP Madrid, Sección 9ª. Sentencia nº 244/2020. Rec. 80/2020, de 8 de junio de 2020. “Fraude del CEO”. Se constata la grave negligencia de la entidad bancaria a la hora de no comprobar las firmas de los ordenantes de las transferencias.
- Sentencia AP Ciudad Real. Sección 1ª. Sentencia nº 169/2021. Rec. 528/2019, de 20 de mayo de 2021. “Man in The Middle”. La sentencia confirma que el hecho de que la estafa se haya cometido a través de una operación fraudulenta de piratería no minimiza ni anula la obligación del banco de responder por su responsabilidad.

B)Jurisprudencia Europea:

- STJUE (Sala 5ª) de 16 de marzo de 2023, en el asunto C-351/21: Establece la obligación del proveedor de servicios de pago (La entidad bancaria), de identificar al beneficiario de los movimientos bancarios sin excepción alguna.

Aplicable a filtración de datos por brechas de seguridad:

- STS 188/2022 de 15 de febrero de 2022. El recurso de casación interpuesto por la empresa sancionada por la AEPD se desestima: **incumple con su obligación de adoptar medidas efectivas** para impedir el acceso de terceros a datos personales de los usuarios. Se filtran 14 contratos de financiación por un error cometido por una trabajadora. Se le imputa a la persona jurídica el resultado lesivo producido.

La negligencia en la protección de datos personales no solo compromete la confianza de los clientes, sino que también acarrea severas sanciones legales.

- Resolución de AEPD: EXP202304633. **Impone una multa** de 600.000 euros a una empresa por no garantizar la confidencialidad de los datos de 9497 clientes, tras ser víctima de una suplantación de identidad y spoofing y usar fraudulentamente esos datos. Vulneración de los artículos 5.1 y 32 del RGPD.

- STJUE (Sala 3ª), de 14 de diciembre de 2023, en el caso C-340/21 (Natsionalna agentsia za prihodite, NAP) refuerza la importancia para las empresas de adoptar medidas proporcionadas y adecuadas para proteger la información personal de los usuarios en el entorno digital.

Ciberseguridad Básica de Protección AntiPhishing

El phishing continúa siendo una de las **amenazas más graves** con importantes implicaciones legales y operativas. Ante su constante evolución, **un antivirus y un firewall ya no son suficientes**. Adoptar una **protección multicapa es esencial** para mitigar estos ataques de forma efectiva. A continuación, se presentan las capas de protección básicas e imprescindibles para cualquier organización.

PROTECCIÓN MULTICAPA

Protocolos de Seguridad del Email DKIM, SPF y DMARC	Validan la autenticidad de los remitentes y previenen la suplantación de identidad en los emails
Filtrado del Email	Detecta y bloquea correos maliciosos y aquellos con archivos adjuntos peligrosos, antes de que lleguen al usuario
Detección de Fraude	Solución que detecta si un archivo (como una factura) ha sido modificado
Protección DNS/WEB	Impide el acceso a sitios fraudulentos al bloquear dominios y páginas web peligrosas durante la navegación
Concienciación y Formación a Usuarios	La formación y educación constante a todos los usuarios reduce el riesgo de clics en enlaces maliciosos.
Antivirus/EDR	Protege los dispositivos frente a amenazas avanzadas detectando y respondiendo a intentos de intrusión

Es importante destacar que cada capa por sí sola no es suficiente; la combinación de todas es esencial para **reducir la superficie de ataque al máximo y el acceso a los hackers**. Además, en caso de que un ataque de phishing sea efectivo, se recomienda complementar con medidas de ciberresiliencia, como **protección anti- ransomware, copias de seguridad y soporte SOC.**

Conclusiones y Recomendaciones

Conclusiones Legales

Frente a un ataque de phishing, se deben cumplir normativas como el **RGPD y el Real Decreto-ley 19/2018**, notificando brechas de seguridad y gestionando transacciones fraudulentas. Además, la **contratación de seguros y la adopción de medidas preventivas** son esenciales para mitigar riesgos legales y económicos. La responsabilidad **puede recaer en la empresa con menores medidas de ciberesegurIdad**, o entidades bancarias o aseguradoras, según las circunstancias y el cumplimiento de las medidas de protección. También es crucial cumplir con **normativas (como NIS2), evaluar regularmente los riesgos y responder con rapidez** para minimizar el impacto de los incidentes.

Conclusiones Técnicas

Una **Protección Multicapa** es la estrategia de ciberseguridad más efectiva: **protocolos de seguridad del email, filtrado email, detección de fraude, protección DNS/WEB, formación a usuarios y un antivirus/EDR.** También se recomienda adoptar una política de ciberresiliencia para mitigar los riesgos en caso de sufrir un ataque de phishing que acabe en un ataque ransomware. En Interbel recomendamos las siguientes soluciones:

Protocolos de Seguridad del Email DKIM, SPF y DMARC	Validan la autenticidad de los remitentes y previenen la suplantación de identidad en los emails	SPOOFPROTECT
Filtrado del Email	Detecta y bloquea correos maliciosos y aquellos con archivos adjuntos peligrosos, antes de que lleguen al usuario	Heimdal, Protect BY MAILINBLACK
Detección de Fraude	Solución que detecta si un archivo (como una factura) ha sido modificado	Heimdal
Protección DNS/WEB	Impide el acceso a sitios fraudulentos al bloquear dominios y páginas web peligrosas durante la navegación	Heimdal
Concienciación y Formación a Usuarios	La formación y educación constante a todos los usuarios reduce el riesgo de clics en enlaces maliciosos	Cyber Academy BY MAILINBLACK, usecure
Antivirus/EDR	Protege los dispositivos frente a amenazas avanzadas, detectando y respondiendo a intentos de intrusión	Heimdal

CONTACTO

INTERBEL

Con más de 27 años de experiencia, Interbel es un referente en soluciones de email y ciberseguridad en España y Latam, trabajando con más de 2.000 distribuidores y 18.000 clientes finales.

Nuestro objetivo es ofrecer una protección completa mediante un enfoque multicapa que abarca desde la **Ciberprotección hasta la Ciberresiliencia**, utilizando tecnologías avanzadas, inteligencia artificial y ciencias cognitivas para ofrecer una excelente gama de productos. También brindamos servicios de **soporte técnico y formación especializada**, ayudando a nuestros Partners y clientes en España, Portugal y países de Latinoamérica como México, Colombia, Panamá, Chile, Perú y Argentina.

+34 93 184 53 53

interbel@interbel.es

www.interbel.es

INTERBEL
Email & Ciberseguridad

Colaboró en la parte legal de esta Guía:

ASOBAN ABOGADOS

ASOBAN ABOGADOS es un despacho especializado en derecho bancario, procesal civil y estafas cibernéticas. En el área de estafas cibernéticas, ASOBAN ABOGADOS asesora a sus clientes en materias relacionadas con protección de datos, brechas de seguridad y todo tipo de reclamaciones y solicitudes de indemnización por ciberataques de toda índole.

+34 91 186 34 53

info@asobanabogados.com

www.asobanabogados.com

ASOBAN
ABOGADOS