Phishing

Nociones básicas y consejos.

Guía para combatirlo.

[ÍNDICE]

Contenidos

1 ¿QUÉ ES EL *PHISHING*?

El *phishing*, en castellano deberíamos decir pesca (aunque está muy aceptado el término en inglés) es un fraude de suplantación de identidad que suele hacerse por correo electrónico, aunque también por mensajería instantánea e incluso por teléfono, con el fin de obtener datos de tarjetas de crédito, datos bancarios u otros tipos de información de interés.

En estos mensajes los ciberdelincuentes se hacen pasar por una persona o empresa conocida y de confianza y con todo tipo de argumentos normalmente relacionados con la seguridad - nuestra seguridad sobretodo - quieren hacernos "morder el anzuelo" para que introduzcamos nuestros datos en una página web que ellos nos indican y así poder hacerse con ellos.

Y ¿para qué los quieren?

Para robarnos, ya sea dinero de nuestras cuentas bancarias y tarjetas o realizando compras a nuestro cargo, para cometer estafas y otros delitos suplantando nuestra identidad, para venderlos a terceros que podrán cometer delitos también... Vamos, para nada bueno. :-(

[ÍNDICE]

2 TIPOS DE *PHISHING*

Existen muchos tipos de ataques de *phishing* pero todos tienen en común el uso de un pretexto fraudulento (problemas de carácter técnico, recientes detecciones de fraudes, nuevas recomendaciones de seguridad, cambios en la política de seguridad de la entidad...) para adquirir datos valiosos (datos personales, bancarios, credenciales de acceso a servicios de correo, a comercios online, etc.).

La mayoría de los métodos de *phishing* utilizan la manipulación en el diseño del correo electrónico para conseguir hacerse pasar por un tercero (organización, empresa, banco...) y normalmente que un enlace parezca una ruta legítima de esta organización por la que se hace pasar al impostor, para que confiemos e introduzcamos los datos que nos solicitan.

Las **URLs manipuladas, o el uso de subdominios**, son trucos comúnmente usados; por ejemplo en esta URL: http://www.nombredetubanco.com/ejemplo, en la que el texto mostrado en la pantalla no corresponde con la dirección real a la que conduce.

O a veces el atacante utiliza contra la víctima **el propio código de programa del banco o servicio por el que se hace pasar**. Este tipo de ataque resulta particularmente problemático, puesto que dirige al usuario a iniciar sesión en la propia página del banco o

servicio, donde la URL y los certificados de seguridad parecen correctos. En este método de ataque (conocido como **Cross Site Scripting**) los usuarios reciben un mensaje diciendo que deben "verificar" sus cuentas, seguido por un enlace que parece ser la página web auténtica; en realidad, el enlace está modificado para realizar este ataque, además es muy difícil detectar si no se tienen los conocimientos necesarios.

También tenemos lo que se conoce como **"Spear *phishing*", que son ataques dirigidos a objetivos concretos.** En general la mayoría de las campañas de *phishing* envían correos electrónicos masivos al mayor número posible de personas, en cambio este tipo de *phishing* va dirigido a una persona u organización específica, a menudo con contenido personalizado para la víctima o víctimas. Esto implica que los ciberdelincuentes necesitan un reconocimiento previo para descubrir nombres, cargos, direcciones de correo electrónico y similares. Los ciberdelincuentes buscan en Internet toda esta información para crear un correo electrónico creíble. Por eso hay que ir con cuidado con la información que hacemos pública en Internet (redes sociales, webs...).

En el llamado **"*phishing* de clonación"** lo que hacen es **una copia de un correo electrónico legítimo** enviado anteriormente que contiene un enlace o un archivo adjunto, y el ciberdelincuente sustituye los enlaces o archivos adjuntos con contenido malicioso disfrazado para hacerse pasar por el auténtico. Los usuarios desprevenidos hacen clic en el enlace o abren el adjunto, porque creen que es de confianza y con esto pueden tomar el control de sus sistemas, robar datos, etc, que luego les servirán para falsificar la identidad

de la víctima para hacerse pasar por un remitente de confianza ante otras víctimas de la misma organización.

Y no podemos dejar de comentar las curiosas y famosas estafas conocidas como **"Estafas nigerianas".** Quien no ha recibido alguna vez un correo electrónico de alguien que afirma ser un príncipe nigeriano, o empresario de algún país africano, que dispone de mucho dinero pero necesita ayuda para poder transferirlo desde el país en cuestión a otro país más seguro, y pide una cuenta bancaria donde transferir este dinero a cambio de una importante comisión. A lo largo de los años han aparecido multitud de variantes de la estafa original, y aunque parezca increíble, hay personas que aun hoy siguen cayendo en la trampa.

Comentar también que lamentablemente el *phishing* abarca más que solo Internet, **hay *phishing* telefónico,** a veces llamados *phishing* de voz o "vishing,". Es esto caso el *phisher* llama afirmando representar a su banco local, la policía o incluso la Agencia Tributaria. A continuación, le asustan con algún tipo de problema e insisten en que lo solucione inmediatamente facilitando su información de cuenta o pagando una multa. Normalmente le piden que pague con una transferencia bancaria o con tarjetas prepago, porque son imposibles de rastrear. El *phishing* telefónico también tiene su variante vía SMS, el **"smishing",** que realiza el mismo tipo de estafa (algunas veces con un enlace malicioso incorporado en el que hacer clic) por medio de un mensaje de texto SMS.

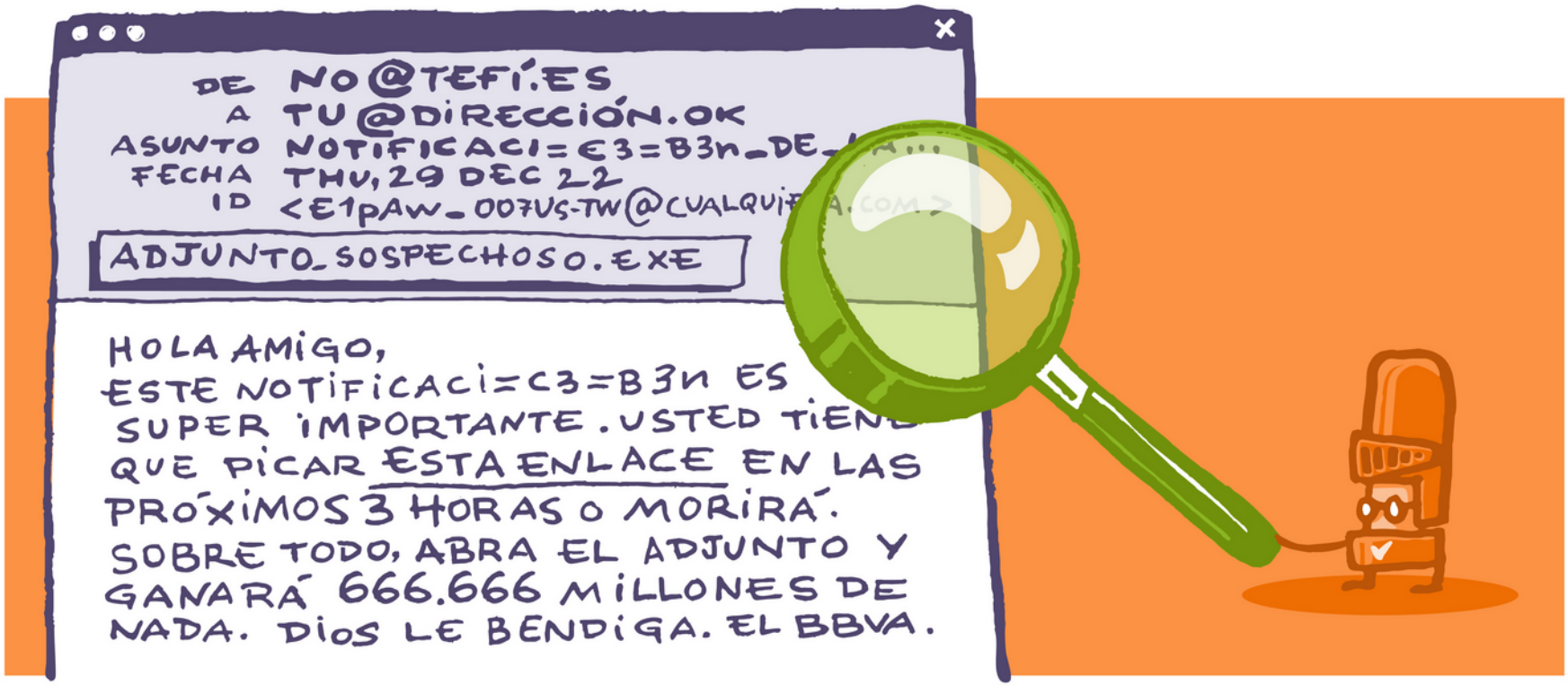
[ÍNDICE]

3 HAY QUE ESTAR ALERTA. ¿CÓMO DETECTAR/RECONOCER UN MENSAJE DE *PHISHING*?

Como decíamos la mayoría utilizan la manipulación en el diseño del correo electrónico para conseguir hacerse pasar por un tercero que es conocido o de nuestra confianza. Algunas veces los mensajes no son muy buenos, salta a a vista que son un fraude, pero otras veces están tan bien hechos que no es sencillo reconocerlos.

A continuación os daremos algunos **consejos que pueden ayudaros a identificarlos** junto con un poco de disciplina y una pizca de sentido común. Hay que buscar los detalles raros o inusuales y pensar antes de actuar. Muchos mensajes de *phishing* buscan meternos miedo (por ejemplo: tu cuenta de correo va a ser eliminada, tu cuenta bancaria bloqueada....) para que reaccionemos rápido y sin pensar.

[ÍNDICE]


DE NO@TEFÍ.ES
A TU@DIRECCIÓN.OK
ASUNTO NOTIFICACI=C3=B3N_DE_...
FECHA THU, 29 DEC 22
ID <E1pAW_007US-TW@CUALQUI...A.COM>
ADJUNTO_SOSPECHOSO.EXE
HOLA AMIGO,
ESTE NOTIFICACI=C3=B3N ES
SUPER IMPORTANTE. USTED TIEN
QUE PICAR ESTA ENLACE EN LAS
PRÓXIMOS 3 HORAS O MORIRÁ.
SOBRE TODO, ABRA EL ADJUNTO Y
GANARÁ 666.666 MILLONES DE
NADA. DIOS LE BENDIGA. EL BBVA.

[ÍNDICE]

Señales que podemos buscar:

- **¿El contenido es sospechoso?**

El primer paso para identificar un *phishing* es valorar el contenido del mensaje o correo electrónico. El intento de suplantación puede ser a un banco, una plataforma de pago, una red social, un servicio público, etc.

El objetivo es intentar asustar al usuario e instarle a actuar según las indicaciones del mensaje. Siempre añaden una excusa, ejemplo "problemas técnicos o de seguridad", y proporcionan una solución sencilla del tipo "acceda a su banco utilizando este enlace". Además, es muy habitual que soliciten nombre de usuario, claves y otros datos de acceso a las cuentas, **práctica que las entidades legítimas nunca llevarían a cabo**.

Por ejemplo, si no somos clientes de un banco que nos escribe para decirnos que nos va a bloquear nuestra cuenta si no hacemos cierta operativa para solucionarlo, debemos sospechar y no caer en el trampa. Y si por casualidad somos clientes de ese banco, lo mejor es que vayamos directamente por nuestra cuenta a la web del banco y veamos si realmente pasa algo con nuestra cuenta o, si aun tenemos dudas, podemos contactar por otra vía (teléfono, en persona...) con nuestro banco y aclararlo, **pero nunca hacer clic en los enlaces que nos ofrece ese correo electrónico.**

O si el correo electrónico hace una oferta que parece demasiado buena para ser verdad. Podría decir que ha ganado la lotería, un premio caro, o alguna otra cosa de valor muy elevado, pues de entrada es para sospechar. Y la ecuación: solicitud de datos bancarios + datos personales = fraude, no suele fallar.

[ÍNDICE]

- **¿La escritura es correcta?**

A menudo en estos mensajes podemos ver que no se han utilizado tildes, que hay errores gramaticales como ene en lugar de eñe, errores de puntuación... Es extraño que una entidad envíe una comunicación a sus clientes con una redacción y ortografía descuidadas, esto nos tiene que hacer sospechar.

Muchas veces estas campañas de estafa las realizan extranjeros que traducen los mensajes al español con traductores que generan errores, como por ejemplo:

- Fallos semánticos: artículos “el” o “la” intercambiados.
- Palabras con símbolos extraños: donde deberían haber palabras acentuadas, por ejemplo: “DescripciÃ?n”.
- Frases mal construidas.

Si detectamos que el correo tiene una ortografía pobre y su escritura es informal, debemos estar alerta.

Sabemos cómo nos escriben y qué tipos de mensajes nos envían las entidades con las que nos relacionamos. Por ejemplo, desde Pangea os enviamos mensajes informativos y avisos siempre en catalán y castellano y nunca os pedimos vuestros datos, ya que los que necesitamos ya nos los habéis facilitado al haceros socios/as, así que si recibís un mensaje nuestro en inglés o pidiendo según qué datos, ¡sospechad !

- **¿A quién va dirigido el correo?**

[ÍNDICE]

Si un delincuente quiere estafar a cientos de miles de personas, es muy complicado saber el nombre de todas esas personas. Por ello, utilizan fórmulas genéricas como “Estimado cliente", “Hola", “Hola amigo", etc. para evitar decir un nombre.

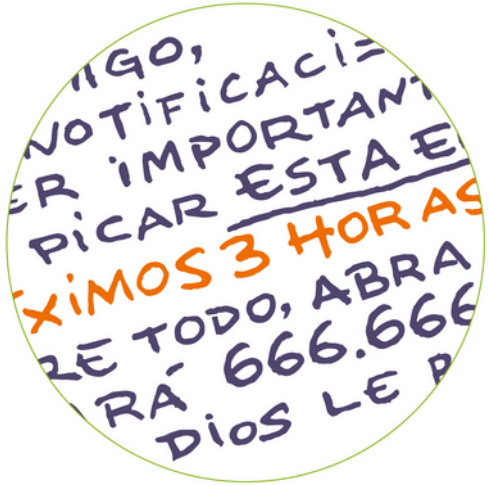
Cuando una entidad tiene que dirigirse por correo a un usuario o cliente, suele hacerlo enviando correos electrónicos personalizados, donde utilizará el nombre de la persona e incluso en algunas ocasiones, parte de su DNI. Si recibimos un correo no personalizado debemos estar alerta y mirarlo bien antes de responder o hacer lo que nos pide.

- **¿Pide hacer algo de manera urgente?**

Otra técnica utilizada por los delincuentes es la de pedir la realización de una acción en un período de tiempo muy corto: “Una vez emitido este correo electrónico, tendrá un plazo de 8 horas para llevar a cabo dicha acción, de lo contrario…":

Con esta urgencia, los delincuentes intentan que su víctima tome una decisión precipitada y caiga en la trampa, que incluye visitar un enlace e indicar datos personales y/o contraseñas.

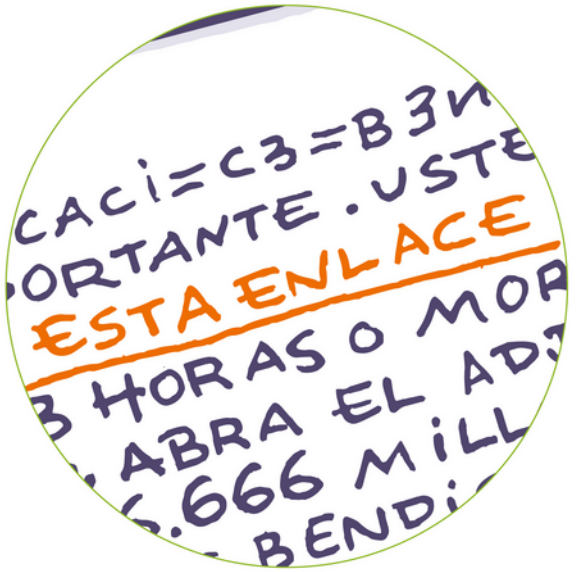
Si el mensaje suena aterrador, tiene un lenguaje alarmista para crear un sentido de urgencia, instando a hacer clic y “actuar rápido" antes de que se elimine la cuenta, o se bloquee... es otro síntoma que nos hace sospechar que el mensaje recibido ha sido enviado por un delincuente.



- **¿El enlace es fiable? ¿y los adjuntos?**

[ÍNDICE]

La intención de los delincuentes es que pinchemos en un enlace para llevarnos a un sitio web fraudulento. En el texto del mensaje hay un enlace que en lugar de llevarte a la web oficial, página legítima, te lleva a otra fraudulenta que estéticamente es igual o muy parecida.



¿Cómo podemos saber la verdadera dirección a la que apunta un enlace? Muy fácil: situando el puntero encima del enlace y observando la verdadera dirección que se muestra en la parte inferior izquierda del navegador o del cliente de correo.

Una recomendación a seguir es la de no acceder a una web a través de un enlace en el correo electrónico. Si deseamos acceder a la web legítima, la mejor práctica es escribir directamente en la barra de direcciones del navegador la dirección deseada (si se conoce previamente).

Si el mensaje contiene archivos adjuntos inesperados o extraños, hay que ir con cuidado, estos adjuntos pueden contener malware, ransomware o alguna otra amenaza online. Es importante tener un antivirus o aplicación que nos permita revisarlos antes de abrirlos.

- **¿Quién envía el correo?**

Comprobar la identidad del remitente es importante y complicado a la vez, ya que no ofrece garantías para saber a ciencia cierta si un correo es fiable o no.

Debemos sospechar si el remitente es una dirección de correo que no pertenece a la entidad a la que el mensaje hace referencia y el correo electrónico del remitente no hace ninguna alusión a dicho servicio. Por ejemplo si recibimos un correo de Pangea pero la dirección no es @pangea.org ya es para empezar a sospechar.

[ÍNDICE]

Pero el hecho de que el correo provenga de un correo aparentemente correcto no es indicio concluyente de la legitimidad del mismo. El remitente de un correo electrónico puede estar manipulado, como explicamos en otra de nuestras guías sobre correo. Los ciberdelincuentes son capaces de enviar correos con el remitente falsificado.

Si reconoces al remitente, pero es alguien con quién no tratas o que no te comunicas normalmente, o aunque lo sea, pero el contenido del correo electrónico no tiene nada que ver con sus correos habituales o son de un tema totalmente ajeno a esa persona, o no es algo que esperes... lo mejor es sospechar.

[ÍNDICE]

4 ¿QUÉ HACER SI DETECTAS UN MENSAJE DE *PHISHING*?

Lo básico es lo siguiente:

- **No respondas** el mensaje.
- **No facilites la información** que te solicitan. Si tienes dudas puedes consultarnos o puedes ponerte en contacto con la empresa o servicio que se supone que representan a través de los canales oficiales.
- **No accedas a los enlaces** facilitados en el mensaje ni descargues ningún documento adjunto, podría tratarse de malware.
- **Elimínalo** y si puedes, **alerta a tus contactos** sobre este fraude para que no caigan tampoco en la trampa.

Si quieres puedes avisarnos para ver si podemos establecer nuevas reglas en nuestro filtro antispam que puedan ayudar a detectarlo y filtrarlo.

[ÍNDICE]

5 ¿QUÉ HACER SI SOMOS VICTIMAS DE UN *PHISHING*?

Lo primero, si creemos estar ante un correo fraudulento, como hemos dicho, es ignorar el mensaje y eliminarlo, y por supuesto, no hacer clic en ningún enlace ni descargar ningún archivo adjunto del correo.

Si tenemos la sospecha de haber sido víctima de uno de estos correos, debemos **recopilar toda la información** que sea posible: correos, capturas de conversaciones mediante mensajería electrónica, documentación enviada, etc.

1. Escanear nuestro dispositivo con un **antivirus** actualizado.
2. **Eliminar cualquier archivo** que hayamos descargado del correo.
3. **Cambiar nuestras contraseñas** de las cuentas implicadas.
4. Activar la **verificación en dos pasos** en las cuentas que lo permitan para evitar la suplantación de identidad.
5. Para los casos de *phishing* bancario, **contactar con vuestra oficina bancaria** para informarles de lo sucedido con tu cuenta online.

NOTA

Es muy recomendable no usar la misma contraseña en diferentes cuentas y servicios. Y las contraseñas debe cumplir un mínimo de requisitos para ser seguras.

/ No utilizar información personal en la contraseña (tu nombre, fecha de nacimiento, etc.)

/ No utilizar patrones de teclado (qwerty) ni números en secuencia (1234).

/ No utilizar únicamente números, mayúsculas o minúsculas en tu contraseña.

/ No repetir caracteres (1111111).

/ Que tenga al menos 8 caracteres – cuantos más caracteres, mejor.

/ Que sea una mezcla de letras mayúsculas y minúsculas.

/ Que sea una mezcla de letras y números.

/ Que incluya al menos un carácter especial, por ejemplo: #!@] *($

[ÍNDICE]

6. Por último **presentar una denuncia** ante la autoridad pertinente.
    - En algunos casos puede bastar con contactar con el servicio o empresa implicada para reportar el problema. Muchas empresas ofrecen secciones de ayuda y soporte donde podemos denunciar el caso que nos haya podido afectar. Por ejemplo:
        - Una red social permite denunciar un perfil falso o una suplantación de identidad.
        - Los servicios de correo electrónico cuentan con métodos de recuperación de cuenta en caso de que haya sido "hackeada".
    - Para eliminar comentarios de un foro que atentan contra el honor y la intimidad de una persona, se puede contactar con el administrador del sitio para solicitar su retirada.
    - En la OSI - Oficina de seguridad del Internauta - del INCIBE (Instituto Nacional de ciberseguridad) encontraréis donde reportar un incidente de ciberseguridad: https://www.osi.es/es/reporte-de-fraude
    - Denuncia ante las Fuerzas de Seguridad correspondientes.
        - Si estás en Cataluña debes dirigirte a la Unidad Central de Delitos Informáticos de los Mossos d'Esquadra.(https://mossos.gencat.cat/ca/inici/)
        - Brigada de Investigación Tecnológica de la Unidad de Investigación Tecnológica (UIT) de la Policía. (https://www.policia.es/_es/denuncias.php#)

NOTA

La OSI, canal especializado en ciudadanos de INCIBE, "ayuda a todos los usuarios elaborando recursos de concienciación, como los que se pueden encontrar en su campaña 'Experiencia sénior', con los que fomentan buenas prácticas en ciberseguridad. Además, el INCIBE, pone a disposición de la ciudadanía la Línea de Ayuda en Ciberseguridad, 017, teléfono gratuito y confidencial desde el que resolver dudas".

6 BIBLIOGRAFÍA

- https://ca.wikipedia.org/wiki/Pesca_(inform%C3%A0tica)
- https://www.osi.es/es/banca-electronica
- https://www.osi.es/sites/default/files/docs/phishing.pdf
- https://www.osi.es/es/guia-fraudes-online
- https://www.osi.es/es/como-identificar-un-correo-electronico-malicioso

  https://es.malwarebytes.com/phishing/

[ÍNDICE]

www.pangea.org
Plaça Eusebi Güell 6-7
Edifici Vertex, planta 0
08034 Barcelona
Tel: +34 934015664
Correu: suport@pangea.org

CON EL SOPORTE DE:

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Pangea.org
< INTERNET
ÈTIC I SOLIDARI >

[ÍNDICE]