Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.
CONSEJERÍA DE ECONOMÍA, INNOVACIÓN, CIENCIA Y EMPLEO

AndalucíaCERT
CENTRO DE SEGURIDAD TIC

Informe de divulgación

Amenazas en la Red Corporativa de la JdA II
Suplantación de identidad o phishing

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-5781-140617*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*14/06/2014*
N° de Páginas	*1 de 16*

1 TABLA DE CONTENIDOS

2 OBJETIVO Y ALCANCE

El objetivo de este documento es aportar información que les permita conocer las principales técnicas usadas en los ataques de phishing y cómo protegerse de ellas.

Este documento va destinado al personal de la Junta de Andalucía y al público en general. Se dará una visión de los riesgos que los ataques de phishing pueden conllevar para los usuarios, sistemas y organismos de la Junta de Andalucía, así como proporcionar una serie de recomendaciones para detectar y actuar ante esta amenaza.

3 INTRODUCCIÓN

Gracias a la facilidad que ofrecen los sistemas informáticos para realizar multitud de trámites en la vida diaria, el uso de las computadoras en redes telemáticas se ha introducido en nuestro día a día (PCs, notebooks, smartphones, etc). Cada vez más usamos estos sistemas en trámites donde se maneja información sensible. Este hecho no ha pasado inadvertido para las empresas, gobiernos y otros. Muchos de ellos usan este creciente uso en nuestro beneficio y en el suyo, en general de forma benévola. Sin embargo hay otros actores que también han encontrado una forma de beneficiarse, pero de forma malintencionada.

La mayoría de las personas, bien por trabajo, por necesidad administrativa o simplemente por mantener comunicación con amigos o familiares, **nos hemos visto obligados a poseer una cuenta de correo** (llegando a ser, hoy en día, algo indispensable). El correo es un método de intercambio de información, o simplemente una vía de comunicación. También es el medio por el que las compañías ofrecen productos y servicios. **Para los ciberdelincuentes, esto representa una puerta virtual** para acceder a sus víctimas, que además tiene la ventaja de que permite el anonimato del remitente, una de las bases de la delincuencia online.

Los delincuentes no pueden acceder a nuestra casa mediante el correo electrónico, pero sí a la información que almacenamos en nuestras computadoras, teléfonos, etc. Es muy habitual que entre la información que almacenamos en nuestros sistemas haya suficiente para suplantar nuestra identidad, datos bancarios, datos médicos, credenciales de acceso a servicios, información personal de familiares, preferencias de navegación, aficiones, fotografías, vídeos y un largo etc.

Normalmente no somos conscientes de la cuánta información almacenamos. La gran mayoría se sorprendería si revisara un dispositivo personal y comprobara archivo por archivo la información contenida. Los ciberdelincuentes son conscientes de esto, y para conseguir esta información

hacen gala de una gran cantidad de técnicas. Una de las más usadas y más efectivas es el phishing, y la vía más usada es el correo electrónico.

4 PHISHING O SUPLANTACIÓN DE IDENTIDAD

> *"**Phishing** o suplantación de identidad, es un término informático que denomina un tipo de abuso informático y que se comete mediante el uso de un tipo de **ingeniería social** caracterizado por intentar adquirir información confidencial de forma fraudulenta. El cibercriminal se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas."*

El termino phishing proviene de la palabra inglesa "fishing" (pesca), haciendo alusión al intento de hacer que los usuarios "muerdan el anzuelo".

Aunque el termino phishing puede ser aplicado a casi cualquier intento de suplantación de identidad mediante el uso de sistemas telemáticos, **su forma más común y la que se sigue en este documento, se refiere al envío de correos electrónicos malintencionados** que mediante el engaño, pretenden conseguir algo del destinatario.

Los correos de tipo phishing pueden usar nombres de compañías u organizaciones existentes para aparentar venir de fuentes fiables. Suelen adoptar su imagen corporativa para aumentar la confianza del destinatario en que el mensaje es auténtico. En muchos casos contienen enlaces a páginas falsas que suplantan la identidad de empresas o servicios y en las que, si introducimos nuestros datos, éstos podrían pasar directamente a manos del estafador. Usar el miedo es muy común para provocar rápidamente la acción deseada en el usuario, ya que los atacantes cuentan con una ventana de tiempo muy breve de oportunidad. Por ejemplo:

Asunto: Urgente verificar su cuenta

Estimado Cliente:

Recientemente, hemos determinado que una persona puede usar su tarjeta sin su autorización, y no los pagos de varios intentos. Ahora tenemos que confirmar la información de tu tarjeta de crédito.

(...)

Se utilizan multitud de argumentos para justificar la necesidad de que el usuario facilite sus datos personales. Algunos muy frecuentes son:

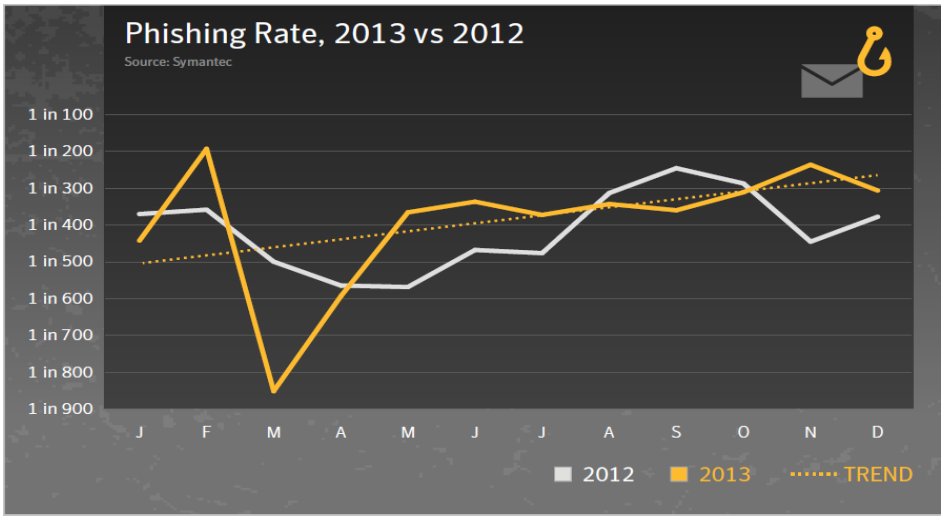
- Problemas técnicos.
- Cambios en la política de seguridad de la organización.
- Premios, regalos o ingresos económicos inesperados.
- Accesos o usos anómalos a tu cuenta.
- Inminente desactivación del servicio.
- Falsas ofertas de empleo.

5 TENDENCIAS

Desde mediados del 2000, la mayoría de la los intentos de phishing han sido realizados a través de correo electrónico, y han tenido como objetivo la obtención de ganancias financieras. Este tipo de ataques, que en principio tenían como objetivo entidades bancarias, se han ido expandiendo a otros ámbitos como cooperativas de créditos, plataformas de pago y otras instituciones financieras.

Las técnicas de ingeniería social involucradas se han vuelto cada vez más sofisticadas. Ejemplos recientes incluyen phishing para acceder a cuentas online de los clientes de las empresas de energía. Esto tiene como objetivo recopilar información de facturas y compras que permitan, por ejemplo, la creación de cuentas bancarias en nombre de otra persona para su utilización en el lavado de dinero negro.

El phishing ha experimentado un auge importante, llegando a incrementarse de manera que 1 de cada 193 correos enviados en el mundo fuera un correo de phishing.



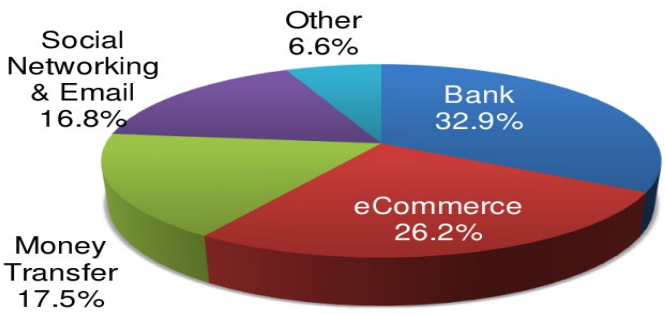
Phishing Rate 2013 vs 2014. Fuente: Internet Security Threat Report 2014 – Symantec.

El hecho de que sea posible el acceso a una gran variedad de servicios mediante el uso de una única cuenta de usuario (Single Sing On) como la de Facebook o Google, unido al interés por obtener información sensible, ha hecho que este tipo de cuentas sean un objetivo prioritario para los atacantes. Es muy común encontrarse con páginas de inicio falsas que intentan suplantar las de las redes sociales más famosas u otros servicios muy extendidos.

Para la captura de credenciales de ciertas organizaciones, es muy común el uso de campañas de correos electrónico fraudulentos indicando que el buzón de la cuenta de correo ha superado la cuota de espacio disponible y solicitando a continuación los credenciales de dicha cuenta.

Otra tendencia usada habitualmente es el uso de acortadores de URLs que permiten a los atacantes ocultar enlaces maliciosos detrás de ellos, habitualmente en servidores comprometidos, dominios sospechosos o servicios de alojamiento web ofrecidos por plataformas de servicios de hosting.

A continuación podemos ver una gráfica que nos indica cuáles han sido los principales tipos de servicios en la red objetivos de ataques de phishing en 2013.



Attacks by Industry, 2H2013. Fuente: Global Phishing Survey 2H2013 - APWG

De la gráfica anterior se puede deducir que el principal objetivo es el dinero a través de la suplantación a bancos, comercio electrónico y transferencias bancarias. También, presumiblemente para el mismo fin económico, se intentan conseguir credenciales de redes sociales y correo electrónico.

6 SPAM O CORREOS NO DESEADOS

Antes de proseguir indagando en los correos de phishing debemos aclarar el concepto de SPAM y diferenciarlo del phishing.

> *"Se llama spam, correo basura o mensaje basura a los* ***mensajes no solicitados, no deseados,*** *o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming."*

El phishing entraría en la categorización más amplia de spam o "correo no deseado", pero no son lo mismo. **El phishing siempre es malintencionado,** mientras que el spam está mas relacionado con campañas publicitarias, correos lúdicos, de carácter ideológico, etc, normalmente enviados de forma masiva o indiscriminada.

Al encontrarnos con un correo de spam, lo primero que habría que **comprobar es si es un correo legítimo de un servicio al que nos hemos suscrito**. Si fuera éste el caso, lo más recomendable sería **solicitar la baja del servicio** accediendo a algún enlace en el correo recibido, a la página web de la entidad remitente o enviando una solicitud de baja a la dirección de correo del remitente.

Si no es el caso, en el servicio de Correo Corporativo de la Junta de Andalucía el procedimiento más genérico para **marcar un correo como SPAM** sería **mover el correo a la carpeta "MarcaSPAM"**. Esta carpeta la crea automáticamente el sistema. El correo movido a la carpeta "MarcaSPAM" permanecerá 24 horas antes de ser eliminado automáticamente. Además, el sistema examinará el correo y aprenderá sus características, lo que le ayudará a identificar correos parecidos en el futuro y marcarlos correctamente como SPAM.

Cabe resaltar que los correos identificados por el sistema anti-SPAM como SPAM no son eliminados, sólo marcados. En caso de que no desee que estos correos le lleguen a su bandeja de entrada puede configurar un filtro en su cliente de correo que descarte o mande a la papelera todos los correos que empiecen por la cadena "-SPAM-".

Si desea acceder a **información más detallada** sobre el funcionamiento del tratamiento del correo SPAM por el correo corporativo de la Junta de Andalucía puede acceder a la sección "Ayuda" en **(**https://correo.juntadeandalucia.es/**)**.

7 IDENTIFICANDO CORREOS DE PHISHING

No existe un patrón definido que nos indique de forma inequívoca que un correo es malicioso. Por esta causa, aunque existen medidas electrónicas para la detección de correos fraudulentos, éstas no son infalibles al 100%. En muchos casos sucederá que un sistema antiphishing no detecte un correo fraudulento como tal, y en otros tantos casos sucede que correos legítimos pueden ser erróneamente identificado como sospechosos. Habitualmente se opta por el mal menor, evitando la eliminación preventiva de los correos y simplemente categorizándolos y marcándolos como maliciosos, con el objetivo de alertar al destinatario de su posible ilegitimidad y dejando en **nuestras manos la**

responsabilidad última de decidir si el correo es seguro o puede suponer un riesgo para nosotros y nuestra organización.

Para ayudarnos a tomar esta decisión vamos a dar una serie de puntos a tener en cuenta ante la recepción de un correo sospechoso:

1. ¿Conocemos al remitente del correo?¿Es de nuestra confianza?
2. ¿Esperábamos este correo o es inesperado?
3. ¿El asunto del correo nos indica alguna alerta o urgencia? Es muy común el uso del miedo o la urgencia para conseguir que el destinatario del correo crea que no tiene más remedio que atender a las demandas del correo.
4. ¿El correo pretende ser de un sitio oficial? Es habitual que estos correos suplanten a la Policía, bancos, distribuidores de tecnología, etc. Esto no significa que todos los correos de estos sitios sean maliciosos, sólo que **merecen que nos tomemos unos segundos para analizarlos**.
5. ¿Tiene faltas de ortografía o expresiones extrañas?. Éstas suelen deberse a una traducción literal de un correo en otro idioma, o de variantes del español. En general, estos pueden hacernos sospechar.
6. ¿El correo nos solicita información sensible como credenciales de servicios online, teléfonos, dirección, numero de cuenta bancaria o información corporativa? Como ya hemos visto uno de los usos más comunes del phishing es la recopilación de información. Debemos tener en cuenta que **ningún sitio oficial debería solicitarnos credenciales personales por correo electrónico**.
7. ¿El correo posee un formulario donde nos solicitan credenciales de algún tipo? Como ya hemos dicho, difícilmente se nos va a solicitar credenciales desde un servicio legitimo vía correo electrónico.
8. ¿Nos prometen ganancias económicas inesperadas, puestos de trabajo con condiciones extraordinariamente ventajosas o posibilidad de amor de personas desconocidas?
9. ¿El correo nos invita a pulsar un enlace? Muchas veces los correos de phishing enlazan a paginas fraudulentas o directamente a la descarga de malware. Tenga en cuenta que hay vulnerabilidades en los navegadores que pueden ser explotadas simplemente ejecutando un enlace. Puede analizar los enlaces copiando la dirección de estos y usando sistemas de reputación en internet como Virustotal.

10. ¿El correo adjunta un archivo (de cualquier tipo)? Es muy común la distribución de malware a través de ficheros adjuntos a los correos. Deberíamos analizar con un sistema antivirus estos adjuntos antes de abrirlos (de nuevo podríamos usar la herramienta Virustotal).

En cualquier caso de duda sobre la legitimidad del correo recibido, siempre podemos solicitar ayuda al personal informático de nuestra organización, o mediante un correo a "abuse@juntadeandalucia.es".

8 TIPOS DE PHISHING

Aunque hay multitud de tipos de phishing (la creatividad del ciberdelincuente juega un papel importante), con el tiempo se han organizado en varios conjuntos según su objetivo y el engaño que modelan. A continuación enumeraremos y explicaremos los tipos más comunes de correos engañosos:

- **Cartas nigerianas:** En este tipo de correos se nos comunica que hemos ganado un premio de lotería, que somos beneficiarios de una herencia, se hacen pasar por inversores extranjeros que buscan nuestra colaboración para realizar negocios en España, o se hacen pasar por alguien extranjero que está buscando "el amor". Estos correos solo tienen como objetivo obtener datos personales en primer lugar, y después, hacernos pagar alguna cantidad de dinero, impuestos, u otros conceptos para obtener algún beneficio.
- **Estafa Piramidal:** En este tipo de estafa se recibe una oferta de trabajo para la cual debe aportar una cantidad económica inicial. En muchos casos, este supuesto trabajo, consiste en la captación de otros "empleados", los cuales de nuevo deberán aportar una cantidad económica inicial. De esta forma repetitiva termina formándose la pirámide.
- **Mulas:** El concepto de mulero en este escenario, define a la persona que se usa como intermediario en actividades delictivas. Normalmente este tipo de phishing pretende convencer a la víctima para que realice transacciones económicas provenientes de delitos, usando cuentas bancarias propias a cambio de un porcentaje de beneficio. Este tipo de phishing es posiblemente de los mas peligrosos ya que criminaliza a la víctima y la convierte en un "cabeza de turco" de una actividad delictiva organizada.
- **Vishing:** Este tipo de phishing persuade al objetivo de la estafa a llamar a un número telefónico fraudulento. Este número al que llamaríamos puede ser de tarificación especial y tener un coste altísimo por minuto, o en otros casos nos puede atender un operador que mediante subterfugios intentará que le entreguemos información sensible cómo números de tarjetas, cuentas bancarias, usuarios, contraseñas de acceso, etc.
- **Spear phishing:** Este tipo de correo no cumple con muchos de los factores comunes del phishing. Su principal característica es que no se trata de un intento masivo e indiscriminado de conseguir víctimas. Éste **es un phishing dirigido**, y por tanto estará creado minuciosamente para evadir cualquier sospecha de la víctima. Normalmente el ciberdelincuente usará información previa recopilada para hacer que el engaño sea lo mas creíble posible.
- **SMShising**: Este tipo de estafa usa técnicas de ingeniería social empleando mensajes de texto dirigidos a usuarios de telefonía móvil.

9 TIPOS DE PHISHING MÁS COMUNES EN EL ENTORNO DE JUNTA DE ANDALUCÍA

Sin salirnos de la clasificación del phishing propuesta, a continuación vamos a exponer los tipos más comunes de phishing detectados en el entorno de la Junta de Andalucía, clasificados según el objetivo que persiguen.

Podemos dividirlos en dos categorías, los que pretenden el **robo de credenciales** corporativas y los que intentan comprometer los sistemas corporativos mediante la **descarga de software maliciosos**.

9.1 ROBO DE CREDENCIALES

9.1.1 FORMULARIO DE CORREO

Este tipo de correo se distingue porque solicita credenciales en un formulario embebido en el propio correo y para enviar estas credenciales es necesario responder al mismo. Habitualmente el correo pretende suplantar a algún servicio online, banco, administradores de correo, etc. Ejemplo:

Asunto: Administrador de sistemas
De: remitente@xxxx.xxx
Responder a: remitente@xxxx.xxx

Estimado usuario

Su correo electrónico ha superado 2 GB, que es creado por webmaster
ejecutan a las 2.30 GB, no puede enviar o recibir mensajes nuevos
hasta verificar su account.Complete el siguiente formulario para verificar su cuenta.

Por favor ingrese sus datos para verificar tu cuenta

(1) correo electrónico:
(2) Nombre:
(3) contraseña:
(4) confirme la contraseña:

Gracias
Administrador de sistemas

En ningún caso debemos dar nuestras credenciales personales de acceso a nadie, incluido los administradores del propio Servicio de Correo, entidad bancaria u otros servicios. Los verdaderos administradores de este tipo de servicios no necesitan conocer nuestras contraseñas para la administración de estos servicios en ningún caso. Suele ser habitual que el remitente del correo esté falseado. Podemos analizar las cabeceras del correo para intentar comprobar si el remitente ha sido falseado, o si el servidor de envío realmente se corresponde con el servicio que solicita nuestras credenciales.

9.1.2 FORMULARIO WEB

Este caso es similar al anterior, o al menos persigue también el robo de credenciales. La diferencia es que el formulario no se encontrará en el cuerpo del correo, sino que desde el correo nos enlazarán a una web fraudulenta que habitualmente tratará imitar el servicio oficial al que pretende suplantar. Ej:

Este tipo de phishing es un poco más difícil de discriminar ya que ciertos servicios sí nos pueden solicitar que ingresemos en los mismos. En cualquier caso, si aun siguiendo los pasos para la identificación de un correo fraudulento no somos capaces de discernir si el correo es malintencionado, lo que podríamos hacer es comprobar que la web es legitima mediante la revisión del certificado digital de la misma.

Deberíamos tener instalados en el navegador los certificados de la Autoridad Certificadora que ha emitido el certificado (CA, Certification Authority) para comprobar que el sitio es legítimo. En caso de que el sitio no sea legítimo el navegador nos alertaría inmediatamente indicando que el sitio no es confiable.

9.2 DESCARGA DE SOFTWARE MALICIOSO

9.2.1 ENLACE A FICHERO

Éste seguramente es el más común de los correos de phishing recibidos por los usuarios de la Junta de Andalucía. Se trata de un intento de distribución de malware. La técnica consiste en conseguir que el usuario se descargue el archivo enlazado desde el correo y lo abra. En el caso que vemos a continuación el atacante pretende hacer entender que nos manda unos documentos que previamente le hemos solicitado. Ej:

```
From: "Joao Paulo" <test@addurlfree.com>
To: xxxxx@juntadeandalucia.es
Content-Type: text/plain;
Reply-To: test@addurlfree.com

Bom dia,
estou te mandando as cópias dos contratos de aluguel,
de fevereiro e março que voçê me pediu,
qualquer dúvida me avisa, obrigada !!!!
imprimir:
http://ge.tt/api/1/files/42qpzqc1/0/blob?download
```

Obs: me liga se se não conseguir visualizar as planilhas, um ótimo dia !!!

Este caso es especialmente llamativo, ya que ni siquiera el correo se encuentra en español. Si consiguieran engañarnos, desde el enlace descargaríamos un archivo "Contratos.zip", que en realidad es un troyano bancario conocido como "Symmi". Este troyano intentará hacerse con nuestras credenciales bancarias y comunicarlas al atacante.

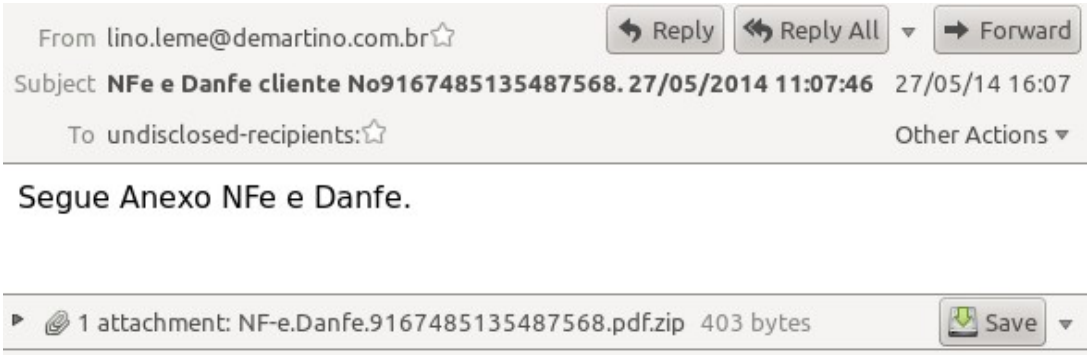
Una buena precaución contra este tipo de engaños sería realizar un análisis de la URL y del archivo que contiene. Para ello es muy común copiar la dirección del enlace desde el menú contextual e introducir dicho enlace en virustotal en la sección de análisis de URL.

De este modo podemos analizar la reputación de la misma y del archivo, sin necesidad de acceder a la página o descargar y ejecutar el fichero.

9.2.2 FICHERO ADJUNTO

Este tipo de phishing es muy parecido al anterior. Se diferencia en que el fichero sospechoso no se descarga desde un enlace, sino que viene adjunto en el mismo correo. Este método de distribución de malware, aunque casi tan habitual y numeroso como el método del enlace, es más fácil de prevenir por métodos automáticos, y por tanto es menos frecuente que estos correos lleguen al destinatario.

Los sistemas de correo suelen contar con antivirus que analizan todos los adjuntos de los correos. Los antivirus locales también suelen contar con funcionalidades de escaneo de correos y ficheros adjuntos. Pero ningún antivirus es infalible. Existen multitud de técnicas para evadir la detección por los antivirus. Ej:



En este tipo de correos se pretende hacer pasar un supuesto PDF que en realidad es un archivo malicioso, comprimido y posiblemente ofuscado. En caso de no tener claro si es un fichero malicioso o no, podemos analizarlo con nuestro antivirus o subir el fichero a Virustotal. Hay que prestar especial atención en no ejecutar el fichero hasta que no tengamos información de la muestra.

10 PRINCIPALES RIESGOS

A continuación se muestran algunos de los principales riesgos de seguridad a los que podemos estar expuestos a través del phishing.

- **Pérdida de información sensible**
  - Credenciales de usuario de algún servicio o aplicación sobre la que se esté llevando el engaño. Esto se vuelve especialmente grave si el usuario víctima tiene la mala práctica de usar la misma contraseña para diferentes servicios.
  - Información corporativa.
  - Información personal.
  - ...

- **Suplantación de identidad**. ¿Cuántos servicios, a día de hoy, pueden ser dados de alta o modificados simplemente con una llamada de teléfono y respondiendo a un formulario básico (nombre, DNI, numero de cuenta, etc)? La suplantación de identidad, además de poder causarnos daños económicos, puede desencadenar un daño severo en nuestra imagen o la de nuestra organización.

- **Propagación de infecciones**. Como ya hemos visto, uno de los objetivos más comunes del phishing es la infección del equipo de la víctima. Una vez infectados, la máquina podrá ser parcialmente o completamente controlada por el atacante. ¿Y qué podrá realizar con nuestra máquina? Pues prácticamente de todo. Propagar más malware por todas las redes internas, intentar pivotar hacia otros sistemas más críticos, usarnos para enviar más phishing a todos los contactos del usuario víctima, monitorizar todo lo que se realizar en el navegador, usar nuestros recursos para lanzar ataques a otras organizaciones, y un largo etcétera.

11 CONSEJOS PARA EVITAR SER VÍCTIMAS DEL PHISHING

Vamos a enumerar una serie de consejos que podrían ayudar a evitar que seamos víctimas de un ataque de phishing. Ya que se trata de una guía dirigida a cualquiera que posea una cuenta de correo, no vamos a entrar en recomendaciones para la protección de sistemas informáticos ni evitar la distribución de correos maliciosos con medios técnicos.

- A ser posible **no abra correos de remitentes desconocidos o que no haya solicitado**.
- Ante cualquier duda **intente aplicar los pasos para evaluar si se trata de un correo de phishing**. Cuanto más veces se moleste en seguir este pequeño procedimiento más difícil será ser víctima de este tipo de fraude.
    - En caso de duda, pida ayuda a los técnicos de informática de su organización, su experiencia puede darles una perspectiva más precisa de las pistas que deben tener en cuenta.
- **No conteste en ningún caso a estos correos.** Incluso si en su respuesta no aportara ninguna información solicitada, cuanto menos estaría confirmando que el phishing ha llegado a una cuenta activa y puede aumentar el interés de los atacantes contra usted.
- **Tenga precaución al seguir enlaces facilitados desde un correo** aunque sean de contactos conocidos. Si le es posible, analice los enlaces antes de seguirlos en webs de análisis de reputación.
- **Tenga precaución al descargar ficheros adjuntos de correos** aunque sean de contactos conocidos. Nunca abra directamente un adjunto, descárguelo y analícelo con los sistemas antivirus a su disposición.
- **Nunca facilite información personal sensible**. En caso de ser completamente necesario el envío de información sensible mediante el correo, hágalo bajo la mayor seguridad posible mediante el uso de cifrado y firmado electrónico, y sólo si el destinatario es absolutamente de su confianza.
- Asegúrese siempre que cuando **envía datos sensibles vía WEB es por una conexión segura HTTPS** mediante un certificado reconocido y de confianza.
- **Acceda regularmente a sus cuentas** y no las deje inactivas durante mucho tiempo. Aplique una política de contraseñas seguras y un rotado periódico de las mismas.
- **Reporte siempre los intentos de phishing** a la dirección de correo abuse@juntadeandalucia.es. Envíe el correo original recibido. Muy habitualmente los correos de phishing son enviados en campañas, de tal modo que al enviar lo antes posible el correo recibido, gracias a su ayuda, se podrá proteger al resto de usuarios corporativos estableciendo medidas de contención.

12 CONCLUSIONES

Los ataques de phishing no son nuevos. Los primeros ataques conocidos de phishing nos remontan a los años 90 y fueron llevados a cabo contra la compañía de servicios de Internet AOL. Pese a ello, en la actualidad aun siguen representando una de las amenazas más activas y persistentes.

El phishing no es más que una adaptación de las estafas tradicionales al mundo digital. Este es uno de los principales motivos que hacen que siga usándose. La base de estos ataques es el engaño y éste se dirige contra los usuarios finales. Otra razón de peso sobre por qué se sigue usando es que técnicamente son especialmente difíciles de detener.

Los riesgos que pueden tener lugar tras recibir un correo de phishing son elevados. Es muy recomendable por tanto que todos los usuarios sean capaces de detectar un correo de phishing, o al menos, tener la capacidad de dudar y saber a quién dirigirse para pedir ayuda ante un correo sospechoso o no controlado.

Pese a todo lo mencionado, siempre existe la posibilidad de que el ataque tenga éxito y la amenaza se materialice. Ante tal situación, entrarán en juego otros factores como el nivel de protección de nuestro equipo, las medidas de seguridad desplegadas en la organización o la capacidad de respuesta ante incidentes con la que cuente nuestro organismo. Cada capa de seguridad añadida será determinante en el daño que la amenaza llegue a causar.

13 REFERENCIAS

- Aprenciendo a identificar los 10 phishing más utilizados por los ciberdelincuentes - OSI
- Phishing por correo electrónico - SANS
- Como identificar phishing - CsirtCV
- Phishing: servicios más suplantados - ESET
- Internet Security Threat Report 2014 - Symantec
- RSA Online Fraud Report 2014 - EMC
- Global Phishing Survey: Trends and Domain Name Use in 2H2013 – APWG
- Firma y cifrado de correos electrónicos - Mozilla Hispano