GUIAS DE SEGURIDAD UJA

Phishing

Servicio de Informática
Vicerrectorado de Tecnologías de la Información
y la Comunicación y Universidad Digital
Universidad de Jaén

Edición: **enero 2018**

Contenidos

1. ¿Qué es el *phishing*?

Cada vez es más habitual recibir mensajes de correo electrónico que se hacen pasar por comunicados de bancos, tiendas de Internet u otros negocios y organizaciones reclamando la atención de los destinatarios para actualizar sus claves de acceso, confirmar su número de tarjeta de crédito o cualquier otra información personal especialmente sensible a través de un enlace que les conduce a páginas web falsas. En caso de caer en este fraude, nuestros datos son capturados y los delincuentes pueden suplantar nuestra identidad para realizar todo tipo de operaciones ilegales en Internet.

Este fraude se denomina *phishing* (que en castellano podríamos traducir como robo de identidad en Internet) y es posiblemente la modalidad de fraude digital más extendida, especialmente a través del correo electrónico.

El término *phishing* viene de la contracción del inglés *password harvesting fishing* (cosecha y pesca de contraseñas), y básicamente consiste en un fraude en el que el atacante duplica una página web válida (de un banco, de un operador de Internet…) y envía mensajes de correo electrónico de forma masiva incluyendo un enlace a la web falsa, haciendo creer a los destinatarios que se trata de la original.

La finalidad última de este engaño es la de dirigir al usuario a la web falsa donde, mediante el uso de formularios y haciendo uso de medidas de presión se le incita a que envíe credenciales e información personal: nombres de usuario, contraseñas, números de tarjeta de crédito, etc.

Los mensajes de correo enviados suelen intentar simular una apariencia seria y oficial, aunque en muchos casos las malas traducciones o diseños poco profesionales hacen que se detecten fácilmente como fraudulentos. Sin embargo, a veces las falsificaciones de las webs y los mensajes de correo son tan elaborados que parecen totalmente legítimos, lo que explica en parte el éxito que tienen estos fraudes y la cantidad de usuarios que caen en ellos.

Una vez que la víctima cae en el engaño y entrega su información personal, esta es usada para acceder a las cuentas de la víctima y usarla con diferentes propósitos (envío de spam, robo de dinero en el caso de banca on-line, etc).

Como se ha indicado, en el caso de la banca, este fraude suele ser muy común y periódicamente se detectan oleadas de envíos de este tipo de mensajes. Generalmente el mensaje suele hacer uso del miedo y la ignorancia, indicando al usuario que su cuenta está a punto de expirar y que debe cambiar la contraseña de acceso inmediatamente o mensajes similares.

Los daños causados por el *phishing* pueden ser múltiples, desde la denegación de acceso a la cuenta de correo electrónico hasta una pérdida económica que puede llegar a ser considerable.

2. Técnicas usadas en el *phishing*

El principal objetivo del *phishing* es el de conseguir el mayor número de credenciales de todo tipo de cuentas de usuario, que posteriormente son usadas de forma fraudulenta: para envío de SPAM desde cuentas comprometidas, robo de dinero mediante acceso a servicios de banca electrónica, uso de tarjetas de crédito de las víctimas, etc.

El procedimiento usado básicamente es el siguiente:

- El usuario recibe un e-mail de un banco, entidad financiera, tienda de Internet, Universidad o similar en el que se le explica que por motivos de seguridad, mantenimiento, mejora en el servicio, confirmación de identidad o cualquier otro, debe actualizar los datos de su cuenta. El mensaje imita exactamente el diseño (logotipo, firma, etc.) utilizado por la entidad para comunicarse con sus clientes.

- El mensaje puede incluir un formulario para enviar los datos solicitados, aunque lo más habitual es que incluya un enlace a una página donde actualizar la información personal.

- Esta página es exactamente igual que la legítima de la entidad (algo sencillo de falsificar) y su dirección (URL) es parecida e incluso puede ser idéntica, aprovechando fallos de algunos navegadores.

- Si se rellenan y se envían los datos de la página, estos caerán directamente en manos del estafador, quien puede utilizar la identidad de la víctima para operar en Internet, generalmente de manera fraudulenta.

La mayoría de los métodos de *phishing* utilizan alguna técnica de engaño consistente en incluir enlaces en un e-mail a un sitio web falso que simula un sitio real, pero que realmente conduce al sitio web fraudulento.

Otro truco común es hacer que el texto que se muestra en un enlace sugiera un destino confiable, cuando el enlace en realidad va dirigido al sitio fraudulento. Para comprobar esto, en la parte inferior de la mayoría de los navegadores se puede ver la dirección real a la que conduce cada enlace, simplemente situando el ratón sobre el mismo.

Otro ataque utilizado en el *phishing* consiste en remitir el cliente a la web legal del banco o la organización suplantada, después de colocar una ventana emergente solicitando las credenciales en la parte superior de la página web de una manera que parece que es la página oficial quien está solicitando esta información confidencial.

3. Consejos para evitar ser víctima de *phishing*

El consejo fundamental para no caer en este tipo de fraudes consiste en tener en cuenta que ningún banco lleva a cabo tareas de verificación de las cuentas usuario o de cualquier otro tipo de datos personales mediante el correo electrónico y que nunca nos solicitará de forma directa datos personales ni información sensible.

A partir de aquí, se indican algunas recomendaciones debemos tener en cuenta para evitar ser víctimas del *phishing* y otros fraudes informáticos:

- **Aprender a detectar un mensaje de *phishing*** es el primer paso fundamental para evitar caer en el engaño.
- **Nunca hacer caso a los mensajes de *phishing* y evitar enviar cualquier tipo de información confidencial que nos soliciten.**
- **Ser especialmente cautos al rellenar formularios en páginas web.** Muchos formularios solicitan a los usuarios su dirección de correo electrónico, además de muchos otros datos. Estos formularios son usados a menudo de forma ilegal para captar información sensible. **Esta recomendación es especialmente importante si nos solicitan contraseñas, números de tarjeta de crédito o cualquier otra información privada.**
- **No hacer caso de mensajes de correo electrónico que recibamos procedentes de remitentes desconocidos**, de entidades en las que no tenemos ningún tipo de cuenta o que están escritos en un idioma desconocido. En general, **nunca hacer caso a mensajes en los que se nos pida ningún tipo de dato personal.** Como norma general, ninguna entidad ni empresa solicita por correo electrónico datos personales. Ante la duda, jamás contestar ninguno de estos correos y contactar previamente con la entidad o empresa correspondiente vía telefónica o personalmente.

- **Si se sospecha del mensaje, no hace nunca clic en los enlaces que pueda incluir para acceder a una página web** (al colocar el ratón sobre el enlace se puede comprobar si la dirección a la que apunta es en realidad la que pretende ser o es sólo parecida).

- **Nunca contestar correos que informen de cancelación de cuentas y mensajes similares.** Contactar telefónica o personalmente con la entidad o empresa para contrastar la información. En la gran mayoría de los casos se tratará de un fraude. **La Universidad de Jaén y en general cualquier otra organización nunca le solicitará directamente por correo contraseñas ni ningún otro tipo de información sensible.**

- **Ante cualquier mensaje que solicite información financiera o datos personales:**
  - Tener en cuenta si tenemos alguna relación o no con la compañía de la que supuestamente procede el mensaje.
  - A no ser que vaya firmado digitalmente, no se puede estar seguro de que no sea falso.
  - Considerar si el asunto y la redacción del mensaje son propios de la entidad que pretende representar.
  - Los mensajes de *phishing* por lo general siempre incluyen mensajes alarmantes para hacer reaccionar al usuario, y requieren información como el nombre de usuario, contraseña o número de la tarjeta de crédito.
  - Normalmente no son personalizados, al contrario que los mensajes legítimos de cualquier compañía.

- **Considerar la instalación de una barra para el navegador que proteja de los sitios falsos.**

- **Si tenemos cuenta en algún banco en Internet, se aconseja entrar regularmente para comprobar el estado de nuestras cuentas.**

- **Instalar la última versión del navegador web que usemos habitualmente, así como las actualizaciones de seguridad.** Los usuarios de Internet Explorer deben aplicar regularmente las actualizaciones de Windows Update.

- **Siempre se recomienda acceder a las webs de entidades financieras o de otro tipo tecleando la dirección en el navegador.** Nunca haciendo clic en ningún enlace recibido por correo electrónico.

- **El acceso de todas las entidades financieras suele ser seguro (HTTPS).** Asegúrate de que la dirección web (URL) comienza por HTTPS (con la S al final) y el navegador web muestra un icono de un candado, asociado con las páginas web seguras.

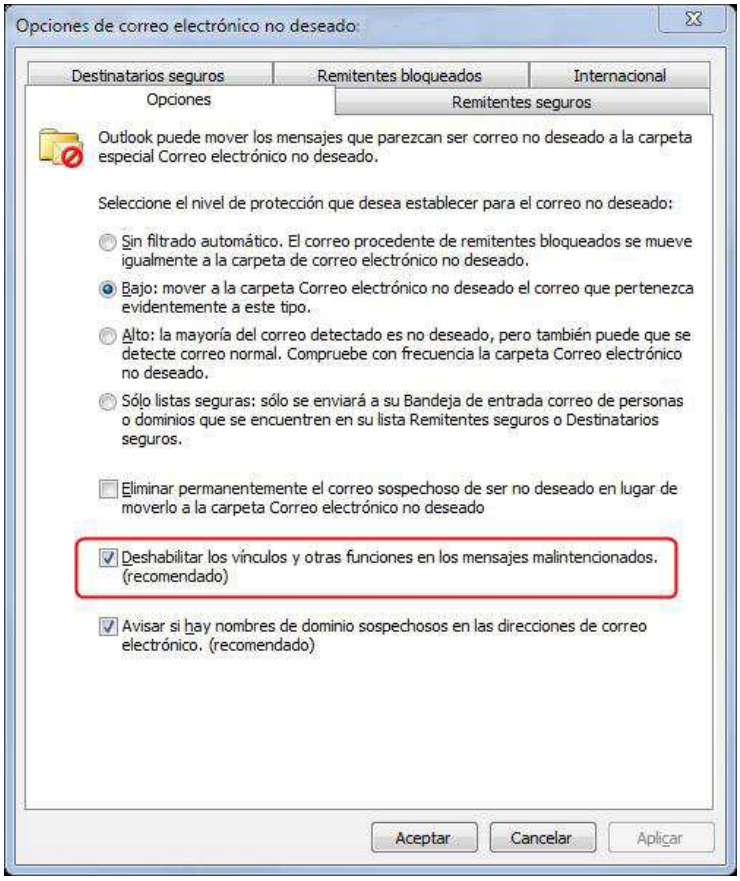
- Tener precaución con los **mecanismos de recuperación de contraseñas que ofrecen muchos sitios webs.** Generalmente proponen elegir una pregunta que le harán al usuario en caso de que solicite recuperar su contraseña. En estos casos, se recomienda utilizar una pregunta lo más compleja posible y cuya respuesta sólo conozcamos nosotros.

4. Medidas anti-phishing en el cliente de correo electrónico

4.1. Microsoft Outlook

Todas las versiones actuales de Microsoft Outlook ofrecen protección específica contra el *phishing* (Microsoft los denomina "mensajes malintencionados"), anulando el efecto de aquellos mensajes detectados y clasificados como tales. Para activar esta protección:

- Acceder al menú **Correo electrónico no deseado > Opciones de correo electrónico no deseado.**
- En la pestaña **Opciones** debe estar marcada la casilla **Deshabilitar los vínculos y otras funciones en los mensajes malintencionados (recomendado**).
- Aceptar todos los cambios.
- Es importante mantener actualizado los filtros de Microsoft Office usando **Office Update**.



4.2. Gmail (Google)

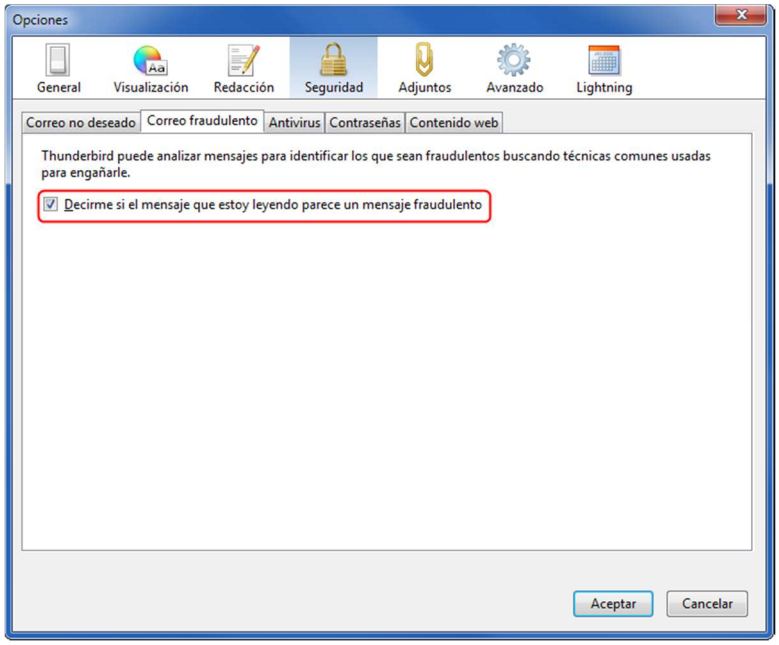
El correo de Google implementa desde hace un tiempo medidas específicas para prevenir y proteger contra el *phishing*. Se puede encontrar información detallada en el siguiente enlace:

https://support.google.com/mail/answer/8253?hl=es

4.3. Mozilla Thunderbird

El cliente de correo de la fundación Mozilla incluye filtros para la detección del correo fraudulento, marcándonos el correo que detecta como tal, y ofreciéndonos la posibilidad de marcarlo o no como fraudulento, de forma que el filtro aprenda para el futuro.

Podemos activar este filtro (por defecto ya viene activado), desde el menú **Herramientas > Opciones > Seguridad**. En la pestaña **"Correo fraudulento"** debemos marcar la casilla **"Decirme si el mensaje que estoy leyendo parece un mensaje fraudulento"**:


Opciones
General
Visualización
Redacción
Seguridad
Adjuntos
Avanzado
Lightning
Correo no deseado
Correo fraudulento
Antivirus
Contraseñas
Contenido web
Thunderbird puede analizar mensajes para identificar los que sean fraudulentos buscando técnicas comunes usadas para engañarle.
Decirme si el mensaje que estoy leyendo parece un mensaje fraudulento
Aceptar
Cancelar

5. Referencias en Internet

- Definición de phishing
  https://es.wikipedia.org/wiki/Phishing

- ¿Sabemos detectar el phishing? Test de detección:
  http://www.sonicwall.com/furl/phishing/

- Instituto Nacional de Ciberseguridad (INCIBE)
  http://www.incibe.es/

- Oficina de Seguridad del Internauta (OSI)
  http://www.osi.es/

- CCN-CERT
  https://www.ccn-cert.cni.es/

- Guardia Civil - Grupo de Delitos Telemáticos:
  https://www.gdt.guardiacivil.es

- Policía Nacional – Brigada de Investigación Tecnológica
  http://www.policia.es/org_central/judicial/udef/bit_alertas.html

- Seguridad en la Red:
  http://www.seguridadenlared.org/

- http://www.delitosinformaticos.com/