GUIAS DE SEGURIDAD UJA

Phishing

1. ¿Qué es el *phishing*?

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 o cualquier otra organización) 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 es la de dirigir al usuario a la web falsa donde se le incita a que envíe credenciales e información personal: nombres de usuario, contraseñas, números de tarjeta de crédito, etc.

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). 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 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 indica que 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.

- Generalmente se encamina al usuario a una página web exactamente igual que la legítima de la entidad y su dirección (URL) es parecida e incluso puede ser idéntica.

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

3. Consejos para evitar ser víctima de *phishing*

- **Aprender a detectar un mensaje de phishing** es fundamental para evitar caer en el engaño.

- **Nunca hagas caso a los mensajes de phishing y evita enviar cualquier tipo de información confidencial que te soliciten.**

- **Se cauto al rellenar formularios en páginas web.** 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 hagas caso de mensajes de correo electrónico que recibas de remitentes desconocidos**, de entidades en las que no tienes ningún tipo de cuenta o que están escritos en un idioma desconocido. En general, **nunca hagas caso a mensajes en los que te pidan algún tipo de dato personal.** Ante la duda, contacta previamente con la entidad o empresa correspondiente vía telefónica o personalmente.

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

- **Nunca contestes correos que informen de cancelación de cuentas y mensajes similares.** Contacta telefónica o personalmente con la entidad o empresa para contrastar la información. La Universidad de Jaén y en general cualquier otra organización nunca te solicitará directamente por correo contraseñas ni ningún otro tipo de información sensible.

- **Ante cualquier mensaje que solicite información financiera o datos personales:**
  - Ten en cuenta si tienes 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.
  - Considera 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.

- **Si tienes cuenta en algún banco en Internet, entra regularmente para comprobar el estado de tus cuentas.**

- **Instala la última versión del navegador web que uses habitualmente, así como las actualizaciones de seguridad.** Si eres usuario de Internet Explorer debes visitar regularmente Windows Update.

- **Accede a las webs de entidades financieras o de otro tipo siempre 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.** 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.

- Ten 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

Microsoft Outlook

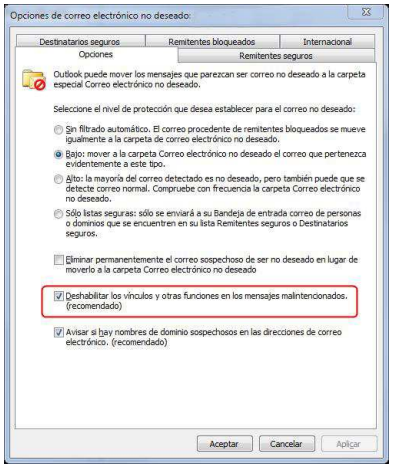
Todas las versiones actuales de Microsoft Outlook ofrecen protección específica contra el phishing (Microsoft los denomina "mensajes malintencionados"), anulando el efecto de aquellos mensajes detectados y clasificados como tales. Para activar esta protección:

- 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**.



Gmail (Google)

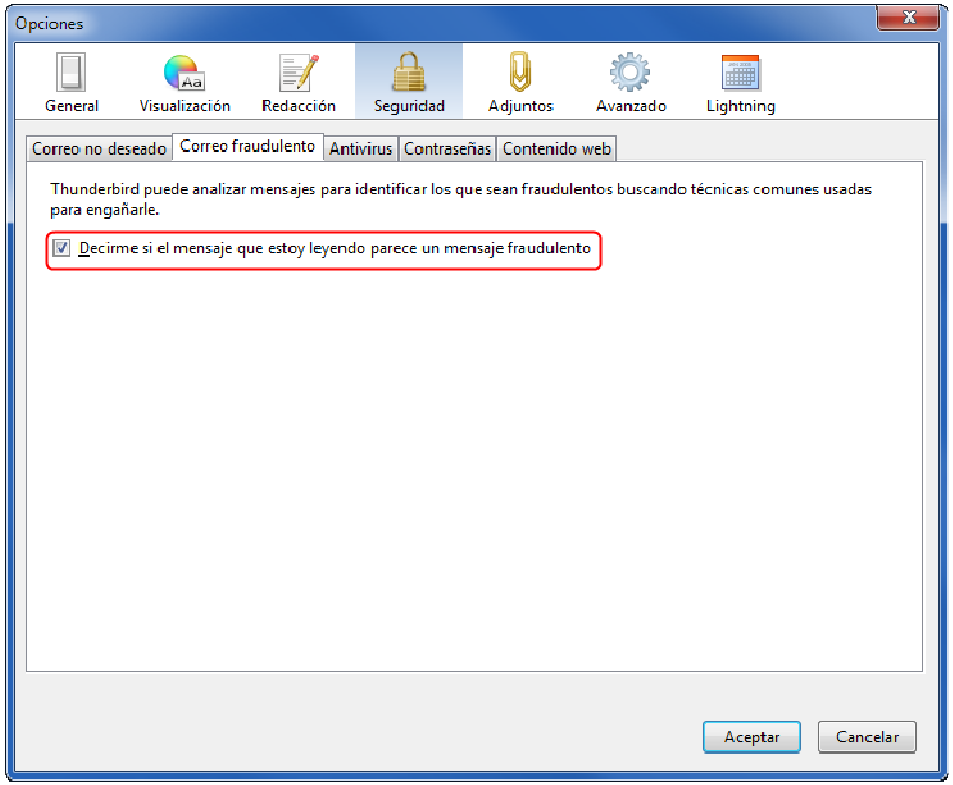
El correo de Google implementa desde hace un tiempo medidas específicas para prevenir y proteger contra el *phishing*. Se puede encontrar información detallada en el siguiente enlace:

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

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"**:



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/