

red.es

The logo for red.es features the text 'red.es' in a sans-serif font. The 'e' in 'red' is replaced by a stylized network diagram consisting of black nodes connected by lines, forming a grid-like structure.

FRAUDE EN INTERNET
Semana de la Ciencia
10 de Noviembre de 2005



red.es



1. Elementos básicos del Fraude
2. Tipos de Fraude
3. Actores implicados
4. ¿Qué ayuda puede proporcionar el CATA y Redlris para cada actor?
5. Recomendaciones al usuario
6. Enlaces



1.- ELEMENTOS BASICOS DEL FRAUDE

Cada vez es mayor el número de intentos de fraude registrados en Internet. Este tipo de amenaza trasciende el ámbito de los daños tecnológicos para atentar directamente contra el patrimonio, causando (o al menos intentándolo) daños económicos directos al usuario estafado. En ocasiones el fraude consiste en suplantación de entidades no financieras (bancos) sino proveedores de correo u otros relacionados con el comercio electrónico como subastas, etc.

El fraude en Internet se basa en tres herramientas básicas

- En primer lugar están los **malware**, virus, gusanos, troyanos, keyloggers, capturadores de pantalla, etc., diseñados específicamente para realizar tareas maliciosas,
- En segundo lugar se encuentra la **Ingeniería Social** como la mejor herramienta, basada en el engaño, para llevar a cabo toda clase de estafas, fraudes y timos sobre los usuarios más confiados.
- Por último el **correo masivo y no deseado (Spam)**, como el mejor y más barato mecanismo de difusión.

Estos tres elementos juegan papeles complementarios mas o menos relevantes en los distintos tipos de fraude existentes.



Los **troyanos** son un tipo de **malware** consistente en un pequeño programa alojado dentro de otra aplicación (imagen, archivo de música,...), que se instala en el sistema al ejecutar el archivo que lo contiene y que puede llegar a un ordenador por diversos medios (correo, redes P2P, paginas web, spyware, etc).

- El troyano realiza internamente algunas tareas de las que el usuario no es consciente, que básicamente consiste en:
 - Espiar las acciones del usuario legítimo de la computadora hace (**spyware**)
 - Instalar un software de acceso remoto a utilizando una puerta trasera (**back door**) que permite comunicarse con nuestra maquina
 - Capturar las pulsaciones del teclado (**key logger**) y capturar las pantallas con el fin de obtener contraseñas u otra información sensible.

El **Spam** consiste básicamente **en** el envío masivo de mensajes de correo no demandado ni deseado.

La gran popularidad del correo electrónico, su sencillez, su bajo coste, y su rapidez, han permitido que el spam sea una práctica cada vez mas difundida.

Los “**spammers**” se dedican a la recopilación de direcciones de correo electrónico para posteriormente utilizarlas en el envío de sus mensajes publicitarios.

Una de las técnicas mas utilizadas por los spammers se basa en la difusión de cierto tipo de **bulos o “hoax”**, que, bajo diversos pretextos, como puede ser apoyar a un niño enfermo, propician a que se envíen mensajes a una determinada dirección.

El spam no solo satura los buzones de nuestras cuentas, algunos datos recientes estiman en 20.000 los mensajes de spam recibidos diariamente por las compañías de todo el mundo, sino que se utiliza también como soporte para distintos tipos de fraude.



El **spim** es la versión del spam para mensajería instantánea, se presenta interrumpiendo conversaciones en MSN Messenger o AIM, en forma de información no solicitada o mensajes publicitarios..

La mayoría de los mensajes spim, son publicidad de sitios pornográficos, otros hacen publicidad de formulas para hacerse rico rápidamente, y el resto se refieren a productos o créditos financieros

Se considera que el spim **es más intrusivo que el spam** pues se abren en forma de pop up justo después de que el usuario se haya autenticado, por lo que, es imposible cerrarlos sin verlos

Las causas del crecimiento del SPIM son básicamente dos:

- La primera, el enorme crecimiento de la utilización de los sistemas de mensajería instantánea, que han pasado de 10 millones de usuarios en 2.002 a una estimación de 182 millones en 2.007.
- La segunda causa es la proliferación de filtros y sistemas antivirus se esta convirtiendo en un problema para los "spammers" profesionales, que tienen que buscar otros campos de actividad



Las Técnicas de ingeniería social consisten en utilizar un reclamo para atraer la atención del usuario y conseguir que actúe en la forma deseada por el autor del correo, por ejemplo que reenvíe un correo a su lista de direcciones, hoax, que abra un archivo que acaba de recibir que contiene un código malicioso, o que, como ocurre en el phishing, proporcione sus códigos y claves bancarias.

La ingeniería social utiliza multitud de técnicas para captar la atención de los receptores de sus correos:

- ❑ Incluir nombres o frases de temas de máxima actualidad, como el Prestige, el aniversario del 11 de septiembre de 2001 o el Mundial de Francia de 1998, o incluso las últimas catástrofes como el Katrina o el maremoto en Asia.
- ❑ Referencias a personajes famosos, como la tenista Ana Kournikova, cantantes como Shakira Jennifer López, o Thalía, personajes políticos como George Bush o Hugo Chávez .
- ❑ Fechas significativas como La Navidad (Happy Christmas)

2.- Tipos de Fraudes

Con los tres elementos básicos definidos se han diseñado distintos tipos de fraude, aunque en lo fundamental, pueden considerarse como ingredientes complementarios ó variantes de una misma actuación delictiva.

Los tipos de fraude mas frecuentes en la red se conocen por:

- ❑ PHISHING
- ❑ PHARMING
- ❑ SCAM

Cada una de estas técnicas tienen sus características específicas que se definirán a continuación



PHISHING

El Phishing es la suplantación de páginas y/o sitios de Internet, que permite al estafador, mediante el engaño, conocer los datos privados y personales que usted utiliza para la realización de operaciones económicas.

Habitualmente se utiliza el correo electrónico para enviar mensajes supuestamente originados en una entidad (Banco, Caja de ahorros...) de confianza, para con diversos pretextos, como:

- Problemas de carácter técnico.
- Nuevas recomendaciones de seguridad para prevención del fraude.
- Cambios en la política de seguridad de la entidad.,
- Promoción de nuevos productos de la entidad.

Pedir todos los datos necesarios para poder realizar operaciones en las cuentas de la entidad: Nombre de usuario, Clave de acceso, Clave Personal, Firma, etc.

El correo electrónico, junto a la Ingeniería Social y el Spam son los grandes aliados del “phishing”

PHISHING

El mensaje recibido responde a estas características:

Estimado cliente;

El departamento de seguridad del banco ha detectado en las últimas fechas diversos tipos de técnicas fraudulentas en Internet por medio de las cuales es posible que las claves de acceso de algunos de nuestros clientes hayan sido capturadas para, haciendo un uso ilegal de las mismas, acceder a su cuenta y operar en ella como si fuese usted mismo quien realice las operaciones.

Debido a ello, el banco ha decidido renovar las claves de acceso de todos los clientes como medida de protección que garantice la seguridad y evite el fraude.

El único lugar donde podrá realizar el cambio de claves se encuentra tras el siguiente enlace: <https://xxxxx.xx.xxxxx..> donde quedará disponible hasta el próximo día XX-XX-XXXX momento a partir del cual, se procederá a la cancelación de los accesos de todos aquellos usuarios que no hayan realizado el cambio de sus claves.

**Agradecemos su colaboración y la confianza depositada en nuestra entidad.
Retsam Sevalcabor
Departamento de seguridad BANCO DE INTERNET.**

PHISHING

En estos mensajes, la dirección del remitente estará falsificada aunque será muy parecida o incluso podrá coincidir con alguna cuenta legítima de la entidad en cuestión. **No importa.**

El objetivo es, que alguno de los millones de receptores de ese correo sea cliente de esa entidad y pulse sobre el enlace propuesto para realizar el cambio o confirmación de sus claves, o introduzca cualquier otro dato personal.

Obviamente, la página enlazada también será falsa y estará controlada por los estafadores quienes habrán cuidado hasta el más mínimo detalle, en replicar con toda fidelidad la imagen, logotipos, colores y formatos de las páginas legítimas de la entidad.

Otros phishing pueden ser mucho mas elaborados, como ejemplo la suplantación del INE u obtener el perfil del usuario a través del spyware para luego mandar phishing muy especializado.

PHARMING

El **pharming** es una modalidad de fraude en línea que consiste en suplantar , mediante la introducción de un troyano, el sistema de resolución de nombres de dominio (DNS) de la maquina infectada para conducir al usuario a una página web falsa.

Las direcciones reales de Internet son de tipo numérico pero llevan asociado un nombre que facilita la navegación.

Los nombres de los dominios se almacenan en distintos sitios, uno de ellos es una tabla de resolución que se incluye en un registro del ordenador (archivo hosts).

El troyano cambia el contenido de esta tabla de forma que asocia el nombre del banco o caja de ahorros a una dirección falsa, la del estafador, en vez de la dirección real.

De esta forma cuando uno teclea el nombre su banco y aparentemente le aparece la pagina del mismo, realmente esta viendo una página falsa y cualquier dato sensible que introduzca cae en manos del estafador.



SCAM

El '**Scam**' puede considerarse como la segunda parte del 'phishing' y se orienta a la captación de intermediarios, "mulas" en el argot, para blanquear el dinero obtenido con el phishing. La estafa se desarrolla en tres fases:

- En la primera fase diversas "empresas" ofertan, a través de chats, correos electrónicos o anuncios difundidos por Internet, trabajo fácil desde el domicilio con el que se pueden obtener grandes beneficios. Las condiciones para optar a este "trabajo" son: una conexión a Internet de 24 horas, una cuenta corriente propia y conocimiento de los sistemas internacionales de envío de dinero (Paypal, Western Union, etc.)
- La segunda fase es el phishing.
- En la tercera fase, después que la víctima facilita las claves de su cuenta online, los delincuentes efectúan transferencias de fondos de esas cuentas hacia las de los intermediarios. Efectuado el ingreso, contactan con ellos por correo electrónico indicándoles las directrices sobre cómo y dónde remitir el dinero que consistente en remitirlo a terceras personas mediante transferencias que efectúan por medio de los sistemas de envío rápido de dinero.

3.- Actores Implicados

Actores **directos** de los fraudes son

USUARIOS

- Son la “víctima” final del phishing.
- Disminuye su confianza en el uso de Internet.

Mulas

- Son los intermediarios mas o menos inocentes que facilitan el blanqueo de los fondos estafados. Si conocen cual es su papel están participando en un delito.

Bancos y/o Entidades suplantadas:

- Son el blanco de la suplantación de identidad o phishing.
- Pierden imagen y dinero.

ISP's:

- Son el “alojador” del phishing en un alto porcentaje de los casos



3.- Actores Implicados

Actores **relacionados** con los fraudes son:

- ❑ **Fuerzas y Cuerpos de Seguridad del Estado (FCSE):**
 - ❑ Reciben la denuncia y/o notificación del phishing
 - ❑ Investigan sobre:
 - ❑ Desde que servidor se aloja la suplantación.
 - ❑ Desde donde se envía el phishing por mail.
- ❑ **EI CENTRO DE ALERTA TEMPRANA ANTIVIRUS (CATA):**
 - ❑ Informa y ayuda al usuario
 - ❑ Colabora con Bancos y FCSE
- ❑ **Asociaciones de usuarios e internautas:**
 - ❑ Informa y ayuda al usuario
 - ❑ Colabora con Bancos y FCSE

4.- ¿Qué ayuda puede proporcionar el CATA/RedIris para cada actor? (I)

Para los Bancos y/o Entidades suplantadas podemos ser:

- Foco de **detección** a través de nuestros canales.
- Canal de **notificación temprana** sobre incidencias de phishing.
- Análisis** del phishing: de donde procede, como está montado, etc.
- Método de **inhabilitación** del phishing si la entidad afectada no dispone de recursos.
- Informe forense** del incidente.
- Asesores** de medidas de seguridad (SPF, firma de correos, etc.).
- Canal de **comunicación** para los usuarios.

4.- ¿Qué ayuda puede proporcionar el CATA/RedIris para cada actor? (II)

Para las FCSE e ISP's podemos ser:

- Foco de **detección** a través de nuestros canales.
- Canal de **notificación temprana** sobre incidencias de phishing.
- Ayuda al análisis** del phishing: de donde procede, como está montado, etc.
- Ayuda a la inhabilitación** del phishing.
- Canal de **envío de denuncias**.
- Canal de **comunicación** para los usuarios para elevar su cultura de seguridad.

4.- ¿Qué ayuda puede proporcionar el CATA/RedIris para cada actor? (III)

Para los USUARIOS podemos ser:

- Mecanismo de **alerta** sobre incidentes.
- Centro de **consulta**.
- Centro de **respuesta**:
 - Métodos para protegerse:
 - Antiphishing, Antipharming, Antispyware, Antispam.
 - Antivirus (troyanos, gusanos, keyloggers, etc).
 - Cortafuegos.
 - Escaneadores de puertos.
 - Test de velocidad.
 - Canalización de denuncias**.
 - Aumentar su **cultura de seguridad**.
- Generador de **confianza**.

5.- Recomendaciones al usuario (I)

- Detección/Reconocimiento de mensajes falsos.
- Uso de herramientas de detección de sitios fraudulentos.
- Uso de herramientas de antipharming.
- Sus claves y códigos son personales e intransferibles, por lo que no debe revelarlas a nadie.
- Cambie periódicamente sus claves de acceso y en especial cuando tenga la sospecha o duda sobre la confidencialidad de las mismas.
- No utilice las claves proporcionadas por defecto, cambiándolas por otras tan pronto como le sea posible.
- Procure, siempre que le sea posible, no utilizar las mismas claves y códigos en todas sus entidades financieras.

5.- Recomendaciones al usuario (II)

- La protección de su PC es clave, por lo que es necesario que disponga de un Sistema Operativo correctamente actualizado con los últimos parches y actualizaciones de seguridad proporcionados por el fabricante.
- Instale y mantenga permanentemente actualizado un software antivirus en su equipo.
- Instale y mantenga actualizado un software de protección personal “firewall” y revise con cierta periodicidad los registros “logs” de actividad que genera en busca de anomalías o eventos no comunes.
- Desactive las funciones de almacenamiento de claves en la “cache” del sistema.
- Evite la instalación de software de dudosa legitimidad.

5.- Recomendaciones al usuario (III)

- ❑ Procure no acceder a su entidad financiera a través de enlaces ubicados en email ni en webs de terceros, manualmente la dirección o utilice las opción de favoritos (usando un antipharming).
- ❑ Evite conectarse desde lugares públicos que no le ofrezcan suficientes garantías de seguridad en el equipo. Si es así limpie sus huellas.
- ❑ Compruebe que la conexión a su entidad de realiza a través de una conexión segura (HTTPS) y mediante un certificado de seguridad.
- ❑ Manténgase regularmente informado del estado de sus cuentas y de las últimas operaciones realizadas por el medio que habitualmente utilice su entidad
- ❑ Finalice todas sus conexiones con la entidad mediante la función “desconexión”, nunca cerrando directamente el navegador.
- ❑ En general lea y siga las recomendaciones de seguridad que su entidad le proporciona y recomienda.

5.- Otros servicios del Centro.

**Red de Sensores
RESCATA**

**Informes
Gratuitos**

**Información
detallada**

Útiles Gratuitos

Foros

**Buzones de
Consulta**

Teletexto

Chat IRC Hispano

**TV, Radio,
Prensa, Jornadas**

6.- Enlaces

alerta-antivirus.red.es

consultas@alerta-antivirus.es

sugerencias@alerta-antivirus.es

Visita nuestros foros en:

<http://alerta-antivirus.red.es/foros/index.php>



Gracias