Universidad Católica
"Nuestra Señora de la Asunción"

Facultad de Ciencias y Tecnología

Teoría y Aplicación de la Informática 2

Nuevas técnicas de *phishing*, robo de datos y falsificación de identidad

Ana María Azorero Velázquez
anama.azorero@gmail.com

Ingeniería Informática
10º Semestre

Prof. Ing. Juan E. de Urraza

2006

INTRODUCCIÓN

El robo de identidad es el delito de más rápido crecimiento en el mundo.

En el transcurso de un día normal, uno puede divulgar información al hacer transacciones en persona, por teléfono y *on-line* para efectuar la compra de productos y servicios. Si esta información confidencial cae en manos de un delincuente, podría utilizarse para robar la identidad financiera de la víctima y realizar muchas de las actividades en su nombre.

Nadie puede estar a salvo de estos fraudes ni puede tener la certeza de que nunca le robarán la identidad, pero lo importante es conocer los métodos existentes para reducir las probabilidades de convertirse en un blanco fácil de los delincuentes y qué medidas tomar si se llegara a caer en sus trampas.

Con este documento se intenta reunir las principales técnicas usadas actualmente para el robo de datos y todo lo referente en cuanto a modos de prevención y protección, regulaciones y campañas a favor de reducir la creciente oleada de ataques fraudulentos.

ROBO DE DATOS E IDENTIDAD

Las estafas conocidas como falsificación o robo de información para cometer un robo de identidad son cada vez más frecuentes.

El robo de identidad implica que una persona use información personal de otra (su nombre, número de seguro social, números de tarjeta de crédito o cuenta bancaria, número de licencia de conducir, fecha de nacimiento u otra información relacionada con su identidad) para cometer fraudes u otros delitos.

Con esos datos, el ladrón puede:

- Abrir nuevas cuentas bancarias y expedir cheques falsos.
- Establecer cuentas de tarjetas de crédito nuevas y no pagar las cuentas.
- Obtener préstamos personales o para vehículos.
- Obtener anticipos de dinero en efectivo.
- Obtener un teléfono celular o servicios públicos para que se generen facturas.
- Cambiar la dirección de correo de tu tarjeta de crédito y hacer cargos en tus cuentas existentes.
- Obtener empleo.
- Alquilar un apartamento, sin hacer los pagos del alquiler ni ser desalojado.

Las personas cuyas identidades han sido robadas pueden perder meses o años, y también miles de dólares, reparando los perjuicios que los ladrones han causado a sus registros de crédito y a su buen nombre. Pueden perder oportunidades de empleo, sus solicitudes de préstamo para estudios, vivienda o automóviles pueden ser rechazadas y hasta pueden ser arrestados por delitos que no cometieron. Todo esto sumado al daño emocional que produce el delito.

Por todo esto, proteger la información personal para evitar los robos de identidad se ha transformado en una tarea crucial, ya que existen diferentes maneras en las que personas inescrupulosas pueden acceder a esa información: desde hurgar en la basura o el robo de carteras hasta el robo *on-line* utilizando técnicas cada vez más sofisticadas.

TIPOS DE FRAUDES MÁS COMUNES

Como se mencionó anteriormente, las formas de cometer estos robos de información son cada vez más variadas, pero en este trabajo nos centraremos en resaltar aquellas que se realicen por medio de Internet, los llamados fraudes *on-line*.

Como principal técnica describimos a continuación el *phishing.*

PHISHING

Origen de la palabra

El término *phishing* viene de la palabra en inglés "fishing" (pesca) haciendo alusión al acto de pescar usuarios mediante señuelos y de este modo obtener información. Quien lo practica es conocido con el nombre de *phisher*. También se dice que el término "*phishing*" es la contracción de "*password harvesting fishing*" (cosecha y pesca de contraseñas).

Definiciones

Para empezar a hablar de *phishing* me parece conveniente proporcionar algunas definiciones encontradas en la Web:

"Término utilizado en informática con el cual se denomina el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria. El estafador (phisher) 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".
(Fuente: Wikipedia)

"Es una modalidad de estafa diseñada con la finalidad de robarle la identidad. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes".
(Fuente: Microsoft)

"No es más que la suplantación de sitios de Internet. Se tratan de correos electrónicos engañosos y páginas Web fraudulentas que aparentan proceder de instituciones de confianza (bancos, entidades financieras, etc.), pero que en realidad están diseñados para embaucar al destinatario y conseguir que divulgue información confidencial. Se vale de la ingeniería social, por lo que su éxito está limitado ya que no todos los usuarios caen en sus trucos".
(Fuente: Recovery Labs)

Como podemos ver, existen variadas descripciones de lo que significa hacer *phishing* que pueden abarcar diferentes situaciones o formas de cometer fraude. Pero en todas cabe destacar que un ataque *phishing* involucra dos cuestiones

importantes: primero, el robo de información y, luego, el robo o la falsificación de la identidad utilizando esos datos robados.

Podemos valernos de estas definiciones para resaltar las principales y más comunes características del *phishing*:

- Utiliza el correo electrónico para ponerse en contacto con los usuarios, enviando mensajes que imitan, casi a la perfección, el formato, lenguaje y logotipos de las entidades (bancos, financieras, tiendas de Internet) y que siempre incluyen una petición en la que se solicita la "confirmación" de determinados datos personales alegando distintos motivos: por seguridad, mantenimiento, problemas técnicos, posible fraude, etc.
- El mensaje puede incluir un formulario para enviar los datos requeridos, aunque lo más habitual es que incluya un enlace a una página donde introducir la información personal.
- La página Web "pirata" es exactamente igual que la legítima y su dirección URL es parecida y hasta incluso puede ser idéntica gracias a un fallo de algunos navegadores. Al completar los datos solicitados por la página pirata, la información cae en manos del *phisher*, quien puede utilizar la identidad de la víctima para operar en Internet.

A continuación se muestra uno de los mensajes tradicionales de *phishing* enviados por correo electrónico:

El siguiente gráfico es un esquema de un ataque *phishing* típico que nos describe sus partes principales:

Cuando el usuario accede al enlace ofrecido, se abre el navegador que le conduce a la página Web falsa con un formulario a llenar. Si el usuario mira en la barra de direcciones verá la dirección correcta del banco o entidad aunque, en realidad, está conectado a un sitio fraudulento. Esto se puede realizar por medio de un JavaScript que reemplaza la barra de direcciones en la parte superior del navegador y le permite al impostor mostrar una dirección URL falsa que no es a donde se está llevando a la víctima.

Una de las consecuencias más peligrosas de este fraude es que la barra falsa queda instalada aún después de que uno sale de esa página pudiendo el atacante hacer un seguimiento de todos los sitios que se visitan posteriormente y también observar todo lo que se envía y recibe a través del navegador hasta que éste sea cerrado.

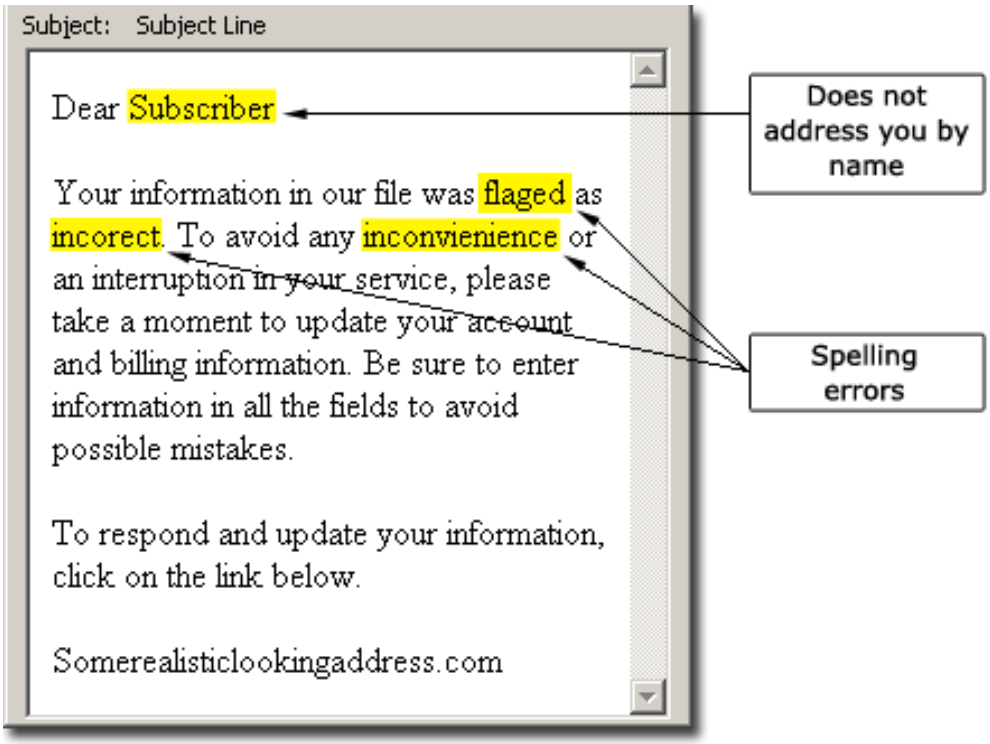
Anteriormente, una manera de descubrir el engaño era verificando que el candadito se encuentre en la parte inferior, lo que indicaba que la navegación era segura. Pero métodos más nuevos de *phishing* ya pueden superar esta dificultad.

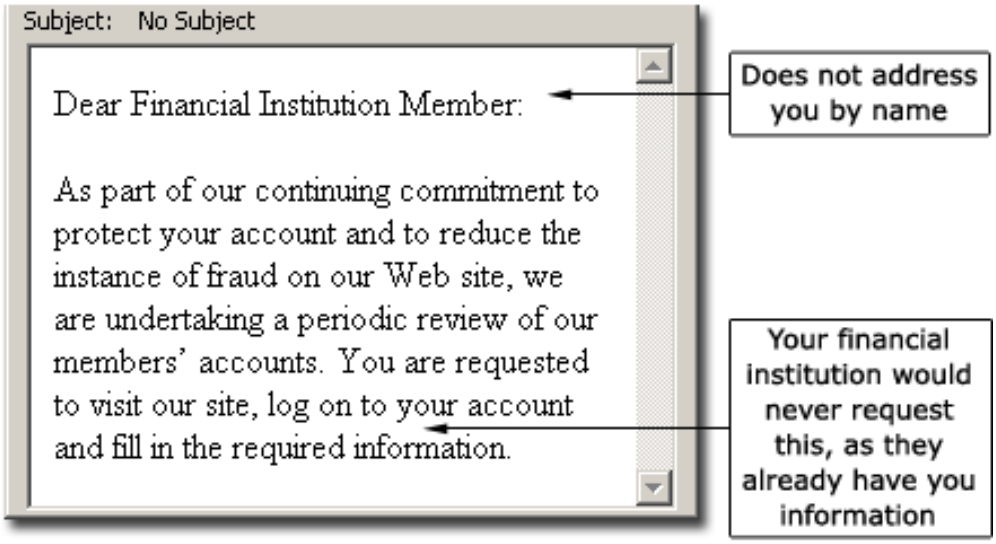
El mejor consejo que se puede dar es ignorar el enlace del e-mail y teclear a mano el URL en el navegador. Pero esto tampoco es seguro como veremos más adelante.

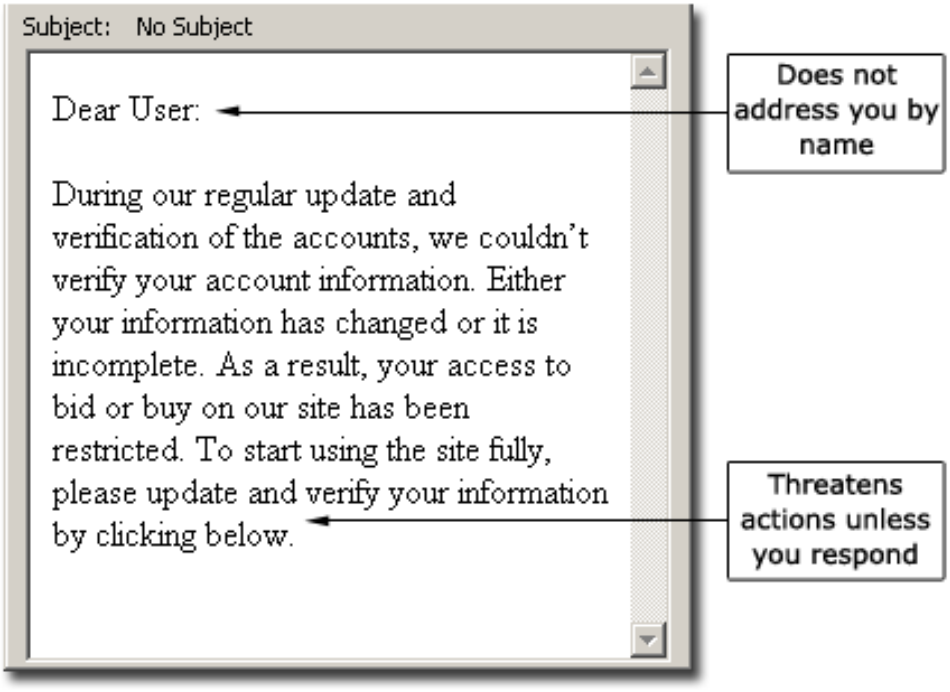
Es habitual que después de la introducción de los datos se muestre una página de error, para que la víctima piense que no se ha podido realizar la conexión y así no sospeche nada.

También es común que los datos robados sean vendidos en el mercado negro para que otras sean las personas que realicen los fraudes económicos con dichas cuentas.

Otras particularidades de los correos electrónicos de *phishing* se pueden observar en los siguientes ejemplos:




Subject: No Subject
Dear Financial Institution Member:
As part of our continuing commitment to protect your account and to reduce the instance of fraud on our Web site, we are undertaking a periodic review of our members' accounts. You are requested to visit our site, log on to your account and fill in the required information.
Does not address you by name
Your financial institution would never request this, as they already have you information


Subject: No Subject
Dear User:
During our regular update and verification of the accounts, we couldn't verify your account information. Either your information has changed or it is incomplete. As a result, your access to bid or buy on our site has been restricted. To start using the site fully, please update and verify your information by clicking below.
Does not address you by name
Threatens actions unless you respond

Scam

Una vez el *phisher* ha conseguido el dinero, se busca a una víctima que lo blanquee. Para ello, envía falsas ofertas de trabajo que prometen grandes ingresos en poco tiempo. En la mayoría de las ocasiones, dichas ofertas de trabajo consisten en recibir en sus cuentas bancarias grandes sumas de dinero y transferirlas a determinadas cuentas en otros países.

Así, la víctima o mulero, sin saberlo, está contribuyendo a cerrar el ciclo que el *phisher* comenzó cuando diseñó su e-mail con el que buscaba robar los datos personales o bancarios de usuarios.

Un ejemplo real de *scam* se muestra a continuación:

```
Asunto: Oferta de trabajo para usted

Hola!
Este correo electrónico le muestra una oferta de trabajo, que podrá ser
interesante a usted.
Gerente financiero situado en su país! Trabajo en Internet con buen sueldo!
GoldLeader Inc. busca a personas enérgicas y responsables para completar el
puesto de encargado de deudores de media jornada.
Como encargado de deudores, usted será el responsable de procesar y
facilitar las transferencias de fondos iniciadas por nuestros clientes bajo
la supervisión del gerente regional.

Ofrecemos:
- Ventajas buenas (más de 1000 $ por semana)
- Contrato legal

Se precisa puntualidad, capacidades directivas y responsabilidad. Usted
también recibirá instrucciones detalladas para acciones subsecuentes de
nuestro gerente, con información sobre como recibir/transferir el dinero.
1. Ser capaz de comprobar su correo electrónico varias veces por día
2. Ser capaz de responder a correos electrónicos inmediatamente
3. Ser capaz de trabajar horas extra si es necesario
4. Ser responsable y trabajador
5. Hablar inglés
6. Tener más de 21 años
7. Deberá tener una cuenta bancaria personal

Para informaciones adicionales y preguntas sobre el puesto de trabajo, por
favor envíe sus datos de contacto a career@goldleader.biz.
NO SON VENTAS!!! NO SON LLAMADAS!!!
USTED NO NECESITA DINERO PARA COMENZAR!!!
Gracias por su atención.
Con respeto, Departamento de personal Goldleader Inc.
http://www.goldleader.biz
```

PRINCIPALES TÉCNICAS UTILIZADAS

Dado que el fraude mediante *phishing* está siendo cada vez más comentado y los usuarios y empresas están ya alertas ante posibles ataques, los "cyber-delincuentes" van buscando nuevas alternativas para conseguir robar datos y cometer fraudes on-line.

Algunas de estas técnicas citadas a continuación pueden no ser tan novedosas en otros países, pero debido a que esta situación de fraudes y robos on-line prácticamente no nos afecta creo oportuno citarlas también.

KEYLOGGERS

Los *keyloggers* son un tipo de troyano capaz de registrar las pulsaciones del teclado al conectarse el usuario a determinadas páginas Web. Estos troyanos pueden estar escondidos en archivos adjuntos o descargarse de páginas falsas y se utilizan para robar datos bancarios o de otro tipo al introducirse en la computadora del usuario a espiar.

Cuando el troyano detecta que el usuario está visitando un URL que está en su lista, el *keylogger* se activa y recoge todas las pulsaciones del usuario, que, generalmente, introducirá contraseñas, números de cuentas y otros tipos de datos.

El registro de lo que se teclea puede hacerse también con medios de hardware. Los sistemas comerciales disponibles incluyen dispositivos que pueden conectarse al cable del teclado (lo que los hace inmediatamente disponibles pero visibles si un usuario lo revisa) y al teclado mismo (que no se ven pero que se necesita algún conocimiento de como soldarlos).

CROSS SITE SCRIPTING (XSS)

Hasta hace algún tiempo, las recomendaciones para acceder de forma segura a la banca electrónica hacían hincapié en comprobar que la URL del navegador comenzara por https:// seguido del nombre de la entidad, así como hacer doble click en el candado que aparece en la parte inferior del navegador para verificar el certificado, y así cerciorarse de que uno usuario estaba navegando en el servidor seguro de la entidad.

Debido al *Cross Site Scripting*, actualmente esto ya no es suficiente. Este tipo de ataque permite que el usuario compruebe el certificado de seguridad de la Web de la entidad que está visitando sin que en principio pueda observar nada irregular. Éste

era, hasta la fecha, uno de los métodos más seguros de los que el usuario disponía para cerciorarse de que no estaba siendo víctima de un ataque de *phishing* y que sus datos se transmitían de forma segura (cifrada) a su entidad financiera, de tal forma que sólo su banco o caja de ahorros pudiera descifrarlos.

El XSS, básicamente, se aprovecha de un tipo de vulnerabilidad muy común en aplicaciones Web que descuida el sistema de validación de HTML incrustado. El problema es que normalmente no se valida correctamente y se podría insertar código para que el formulario se envíe al sitio Web del *phisher*.

Si se produce este tipo de ataque la responsabilidad recaería en manos de la entidad financiera afectada, ya que es posible llevarlo a cabo aprovechando vulnerabilidades en la programación de su Web, y no se facilitan al usuario mecanismos adicionales para poder prevenir y detectar el fraude de forma sencilla.

SPEAR PHISHING

El *spear phishing* es una versión modificada del *phishing* habitual. Se trata de un ataque dirigido también por correo electrónico, pero con un objetivo específico.

Los *spears phishers* envían mensajes que parecen auténticos a todos los empleados o miembros de una determinada empresa, organismo, organización o grupo. El mensaje, con el remitente falsificado, puede aparentar proceder de un jefe o de un compañero que se dirige por correo electrónico a todo el personal, por ejemplo, el encargado de administrar los sistemas informáticos, solicitando los nombres de usuarios y contraseñas.

Mientras que el *phishing* típico está diseñado para robar datos personales, el objetivo del *spear phishing* está más bien dirigido a obtener acceso al sistema informático de una empresa.

Estas estafas de spear phishing también suelen enfocarse en personas que utilizan un determinado producto o sitio Web.

PHARMING

El *pharming* es una técnica aún más peligrosa y mucho más efectiva que el *phishing* tradicional, ya que no necesita utilizar técnicas de ingeniería social. Al igual que el *phishing* su objetivo es el robo de datos e información personal.

Consiste en manipular las direcciones DNS (Domain Name Server) que utiliza el usuario con el objetivo de engañarle y conseguir que las páginas que el usuario visite no sean realmente las originales, aunque su aspecto sea idéntico.

El *pharming* realiza su ataque sobre los servidores DNS y lo que hace es cambiar la correspondencia numérica (direcciones IP) a todos los usuarios que utilicen estos servidores.

Al cambiar esta correspondencia, el usuario escribe en su navegador la dirección correcta, pero el DNS le otorga una correspondencia numérica falsa distinta a la real, llevando al usuario a una página idéntica creada por los delincuentes. El usuario ve en su navegador que está en la dirección correcta y realiza sus operaciones con total tranquilidad y el delincuente tan sólo tiene que recoger la información que el usuario ingrese.

Otro tipo de pharming, aún más efectivo, es el que se realiza a nivel local, en cada equipo individualmente. En este tipo de pharming sólo es necesario modificar un archivo denominado "*hosts*" que cualquier ordenador que funcione bajo Windows y utilice Internet Explorer contiene.

Este archivo almacena una pequeña tabla con las direcciones de servidores y direcciones IP que más suele utilizar el usuario, por lo que no es necesario acceder al servidor DNS para acceder a alguna página deseada.

Al modificar este archivo con falsas direcciones, en el navegador se mostrará la dirección correcta, pero enviará al usuario a una página falsa.

Para realizar esta modificación, el delincuente podría acceder directamente a la computadora del usuario de forma remota a través de alguna vulnerabilidad del sistema, o bien mediante un virus o un troyano. Algunos ejemplos de troyanos reconocidos con la capacidad de realizar estos cambios en el archivo *hosts* son los de la familias *Bancos*, *Banker* o *Banbra*.

VISHING

Es un nuevo tipo de estafa por Internet que utiliza números de teléfono IP, muy baratos y fáciles de conseguir, como si fuesen los números de atención al cliente de tarjetas de crédito o de servicios financieros.

La estafa *vishing* sigue el mismo procedimiento que el *phishing*: el usuario recibe un falso e-mail en el que se le advierte de alguna circunstancia relacionada con su cuenta bancaria o tarjeta de crédito donde se incluye un teléfono -en lugar de una

dirección Web- al que puede llamar para aclarar dudas o resolver el problema. Este teléfono es en realidad un número asociado a una cuenta de voz sobre IP, que se puede obtener fácilmente en Internet a través de servicios como *Skype*.

También pueden usar un programa que llama a números de teléfono de una zona. Cuando descuelga un contestador automático, el programa deja un mensaje donde se pide a la víctima se comunique con un determinado número telefónico.

SMISHING

Otra modalidad de *phishing* es el llamado *smishing* que usa los mensajes SMS de los teléfonos móviles para realizar el ataque. Los mensajes intentan convencer para que se visite un enlace fraudulento, pero no llegan por correo electrónico sino por mensaje corto (SMS) al móvil. En otros casos, el mensaje suele incluir un teléfono al cual se debe llamar en lugar de un enlace.

El primer caso de *smishing* ocurrió en China donde algunas personas comenzaron a recibir un mensaje con el siguiente texto en su teléfono: "Estamos confirmando que se ha dado de alta para un servicio de citas. Se le cobrará 2 dólares al día a menos que cancele su petición. Los usuarios, temerosos de la amenaza de cobro (quizás pensaban que el cargo sería retirado del saldo de su tarjeta) acudían a obtener más información a la dirección indicada. En ella, si se visitaba usando Microsoft Windows (tal vez mediante alguna vulnerabilidad de Internet Explorer) y sin las medidas de seguridad necesarias, el incauto era infectado por un troyano.

PHISHING-CAR

Es la captación de compradores de coches a un coste muy bajo. La venta nunca se llega a efectuar y la víctima realiza un pago como seña, que siempre pierde y se queda sin dinero y sin coche.

Se producen por medio de llamativas ofertas que ofrecen vehículos lujosos que incluso tienen sitios Web falsos con nombre de dominios muy similares a empresas con mucho prestigio, que se dedican a la venta de vehículos de ocasión.

Todos los fraudes tienen algo en común:

- El pago se realiza por medio de empresas de envío de dinero a otros países (Tipo Western Union, Money Gram).
- El vendedor le oferta la entrega a domicilio a la víctima

- En un 90% de las ocasiones, el vehículo que venden está fuera de su país, de manera que la víctima sólo puede verlo en fotos.
- Piden primero a la víctima el 30% o el 40% del precio ofertado como primera señal.
- Muchas veces el vendedor dice que es un español que vive en Gran Bretaña y que por motivos laborales de estancia en el país inglés, tiene que cambiar de forma urgente de coche porque se conduce por la izquierda. Dice que su coche, al estar matriculado en España, el volante está al lado contrario y no se adapta, y que por este motivo vende el coche de forma muy económica.

LOTERÍAS FALSAS

La víctima recibe un correo electrónico donde le notifican que le ha correspondido un premio de lotería. Si el usuario contesta a este e-mail, a continuación le solicitan todos los datos bancarios para un falso ingreso del premio. En otras ocasiones, se le solicita que envíe una cantidad de dinero a otro país para poder cobrar todo el premio completo. Por supuesto, el premio es falso.

RANSOMWARE

El término *ransom* se define como la exigencia de pago por la restitución de la libertad de alguien o de un objeto, lo que en castellano se traduciría como "secuestro". Si a esto agregamos la palabra *software* obtenemos *RansomWare*, definido como el secuestro de archivos a cambio de un “rescate”.

RamsonWare, tipo de *malware* (*malicious* y *software*), se denomina a la técnica de “secuestro” de archivos a través de la compresión y encriptado de archivos, en donde los creadores buscan estafar a los usuarios con el pago de un rescate. Su modalidad de trabajo varía un poco con respecto a las demás, pero su objetivo es el mismo, robar información. Estos datos no se utilizan para provecho del ladrón sino sólo para pedir un rescate a la víctima a cambio de que ésta recupere sus archivos.

Un código malicioso infecta la computadora del usuario por los medios normalmente utilizados por cualquier *malware* y procede a cifrar los documentos que encuentre, eliminando la información original y dejando un archivo de texto con las instrucciones para recuperarlos.

Generalmente, el rescate se deposita en una cuenta bancaria determinada por el creador del código malicioso. Luego que el dinero es depositado, se le entrega al usuario la clave para descifrar los archivos.

SPLOGS

La palabra *splog* viene de la mezcla de *spam* y *blog* y se refiere a un *blog* ficticio creado por *spammers*. Un *splog* es un *blog* que no tiene contenido original; los *splogs* suelen ser *blogs* creados para llenarlos de muchos de enlaces. Como relleno se usa texto tomado de otros *blogs* o de otros medios sindicados.

Generalmente, la intención de estos es distraer los resultados en los motores de búsqueda y aumentar el tráfico en forma ficticia. Se considera que los *splogs* han existido al mismo tiempo que los *blogs*, en la medida que los *spammers* activos se dieron cuenta del nuevo potencial de explotación del medio. Se estima que de los 7000 *blogs* que se crean cada día, aproximadamente el 10% de ellos son *splogs*.

Objetivos y Propósitos

Tres son los objetivos que pueden perseguir los creadores de *splogs*:

- Promocionar sitios dedicados a la venta de productos determinados. El creador busca aumentar con el *weblog* falso recibir visitas atraídas por la temática del sitio para que puedan comprar sus productos.
- Enlaces patrocinados. Otra modalidad es lanzar miles de *weblogs* con palabras claves que se repiten hasta la saciedad y en los que se busca que el visitante pulse en alguno de los enlaces. En este caso, el creador del sitio recibe una cantidad (por visita o sobre venta) del tráfico inducido.
- Crear redes falsas de *weblogs*. Otra modalidad es establecer miles de *weblogs* que apuntan hacía un sitio concreto de la red. El objetivo es aumentar la popularidad del sitio y conseguir que este se muestre en los primeros lugares cuando un usuario acude a un buscador para hacer una consulta.

El trasfondo técnico detrás de los *splogs* se basa en contenido sacado de búsquedas en *blogs* automatizados en procesos programados y ejecutados periódicamente. La gran arma para que los *splogs* tengan éxito es un buen uso de los *pings* y en ocasiones de los *trackbacks*, dado que estos *splogs*, por su automatización, no tienen enlaces externos o al menos es una red básica. Existen algunas iniciativas para detectar *splogs* pero no son demasiado efectivas todavía.

El *splogger* gana dinero a partir de la publicidad colocada en el *splog* -muchas veces a través del servicio AdSense de Google- o dirigiendo visitantes a sitios de comercio

electrónico. Los temas varían desde cruceros y salud hasta pornografía y apuestas online.
El problema es que realizar *splog* sale tan barato como rentable: se trata de mezclar sistemas automatizados de recopilación de información con otros de publicación.

Los buscadores están empezando a detectarlos, pero al mismo tiempo, los *spammers* están empezando a crear *blogs* "menos detectables" mediante la inclusión de artículos que "parecen reales" y que en muchos casos son una mera copia de *posts* de otros *blogs*. Está claro que si al día de hoy el *spam* en el correo electrónico sigue siendo un grave problema para todos, los *splogs* y el *spam* en *blogs* no va a ser un problema de unos días.

Típico mensaje de *sploggers*:
"I thought your blog was cool and i think you may like this cool Website. Now just Click Here"

Típico caso:
Un grupo de estudiantes universitarios que habían creado recién su *blog* saltaron de alegría cuando se dieron cuenta de que ya tenían tres comentarios de usuarios externos en su primera publicación o *post*. Es más, eran del extranjero porque estaba en inglés. El remitente, luego de felicitarlos por su *blog*, los invitaba a entrar al suyo e incluía la dirección. Grande fue la desilusión al darse cuenta de que el comentario no era más que un engaño para que ingresaran a una página comercial. Fue ahí cuando conocieron cómo se llamaba esta técnica: *splog*.

TÉCNICAS Y SUGERENCIAS PARA COMBATIR FRAUDES

A continuación se resume una recopilación de técnicas para evitar caer en fraudes sugeridas por distintas organizaciones y entidades.

Testigos y contraseñas de un solo uso

Se trata del uso de testigos, con contraseñas válidas para un solo uso. El sistema se basa en un pequeño dispositivo, similar a una calculadora de bolsillo, que genera automáticamente contraseñas de un solo uso. El usuario introduce la contraseña facilitada por el testigo para acceder a su cuenta. Al otro lado de la conexión, el sitio Web del banco utiliza el mismo algoritmo para procesar la contraseña que se generará. Si las dos contraseñas coinciden, se autoriza el acceso. Las contraseñas generadas sólo pueden utilizarse una vez, lo que impide su robo y uso fraudulento.

Tarjetas con chip y llaves USB

A fin de mejorar la seguridad de las contraseñas, algunos bancos tienen previsto añadir un proceso de identificación adicional basado en tarjetas con chip y llaves USB. Los clientes que deseen acceder a sus cuentas *on-line*, además de introducir una contraseña, tendrán que introducir una tarjeta con chip en un lector especial, o bien una llave USB en el equipo. A menos que roben la tarjeta o la llave, los responsables de los fraudes de *phishing* no podrán acceder a la cuenta bancaria del usuario.

Resumen de las contraseñas para un sitio determinado

Es una de las medidas recomendadas por el *Anti-Phishing Working Group*. Dicha medida resulta eficaz frente al robo de identidad, ya que “recalcula” la contraseña y añade información específica del sitio en la que va a utilizarse. Desde el punto de vista del usuario, este sistema resulta totalmente transparente, ya que sólo tiene que introducir la contraseña en un formulario *on-line*. Acto seguido, el navegador convierte la contraseña y le añade más información. De este modo, la contraseña completa que el usuario ha introducido no resulta visible para el sitio Web al que va dirigida, que únicamente recibe la contraseña resumida y autoriza el acceso mediante el mismo algoritmo de resumen que ha empleado el usuario. En este caso, incluso si un usuario revela su contraseña en un sitio Web de *phishing*, los piratas informáticos no podrán utilizarla.

Seguridad a través de mensajes de texto

Este sistema se basa en la confirmación por parte de los usuarios de Internet de las solicitudes de transacciones y transferencias que deseen realizar, mediante el envío de mensajes de texto desde su teléfono móvil. La ventaja de este sistema radica en que las transacciones vinculadas a la cuenta online no se autorizan hasta que el banco recibe una respuesta al mensaje de texto. Por supuesto, para que este sistema funcione, los clientes deben facilitar al banco el número de teléfono

Barra anti-phishing

Internet y Firefox proveen actualmente barras *anti-phishing* que bloquean el acceso a aquellos lugares fraudulentos y también proveen más opciones para que los usuarios naveguen sabiendo si una página es segura o no, indicando el riesgo que hay en navegar por una determinada página, la popularidad de ésta y en qué país está alojada. Tampoco permite a los *popups* deshabilitar botones funcionales del navegador.

Direcciones de correo desechables

En este caso facilitamos nuestra dirección de correo electrónico real y disponemos de una dirección de correo que tiene un tiempo de vida límite que va desde media hora hasta un año. A partir de entonces, facilitaremos la nueva dirección a sitios de los que no queremos saber más de ellos más adelante, o sea, queremos que se nos facilite una información en concreto y luego que se olviden de nosotros. Los correos enviados a la cuenta temporal son reenviados a la dirección de correo electrónico que no les queremos facilitar.

Link Scanner

Es una utilidad *on-line* que nos permitirá identificar si el enlace que nos han enviado por correo electrónico o por mensajería electrónica se trata de un sitio Web inofensivo o por el contrario de un sitio Web malicioso.

Se trata de validar la fiabilidad de un sitio Web, de modo que es una opción a tener en cuenta antes de visitarlo, aunque no es un sistema 100% efectivo, con lo que la última decisión deberá de tomarla el propio usuario.

Sólo se debe introducir la URL del sitio Web y el sistema, perteneciente a *Exploit Prevention Labs*, verificará si está dentro de la lista de sitios Web conocidos como

potencialmente peligrosos, y nos devolverá un mensaje. En caso de ser un sitio Web que incluya *exploits* o instalen cualquier tipo de *malware* en el equipo del usuario, nos devolverá un mensaje de alerta.

Protection Manager

Es una herramienta de protección contra el *malware* que nos permite definir para cada ejecutable los privilegios que va a tener en el sistema. Mediante una lista, definiremos que permisos va a tener cada uno de ellos: permitir la ejecución, ejecutar con permisos de administrador, ejecutar como un usuario limitado o denegar la ejecución.

Por ejemplo, podríamos marcar el navegador para ejecución como usuario limitado de forma que, en caso de que algún tipo de *malware* intente colarse a través de este en nuestro ordenador, no tendría acceso a los ficheros de sistema y, por tanto, no podría llegar a instalarse.

Productos varios contra programas espías

- Spy Sweeper 5.0 (versión beta), de Webroot Software

Detección y desinfección. Protege contra *rootkits* y sitios de *phishing.* Ofrece la posibilidad de escoger entre un examen rápido del sistema que tiene prioridad sobre otros trabajos y un examen más lento pero menos agresivo.

- Spyware Doctor 3.8

Uno de los mejores en detección de *rootkits* activos. Su interfaz de exploración ofrece resultados fáciles de leer, de comprender y que ayudan a tomar decisiones.

- CounterSpy 2.0 (versión beta)

Sólida detección de programas maliciosos y protección en tiempo real, pero tiene problemas con la desinfección.

- Ad-Aware SE Personal 1.06

Gratuito. No ofrece protección en tiempo real.

- Spybot

Gratuito. Fue uno de los primeros de contraespionaje. Tiene profundidad y detalles en sus opciones, pero hoy en día simplemente no puede competir con las otras alternativas.

10 normas principales para defenderse contra el Phishing (recomendadas por McAfee)

1. Nunca deje de aplicar los parches necesarios en su sistema operativo, evitando, así, la explotación de las vulnerabilidades conocidas del software.
2. Descargue la versión más reciente de su navegador para asegurar que también esté totalmente actualizado y utilice las tecnologías más recientes.
3. El origen de un e-mail, la ubicación de una página y el uso del cifrado SSL se pueden falsificar.
4. Nunca haga clic en enlaces dentro de un e-mail y siempre ignore los e-mails que solicitan acciones.
5. Tenga mucho cuidado al descargar cualquier software de la Web.
6. Use programas que verifiquen automáticamente si una URL es legítima antes de que usted acceda al sitio.
7. Use un proveedor de acceso a Internet (ISP) que implemente tecnologías y políticas anti-spam y anti-phishing sólidas.
8. Examine sus estadios de cuenta bancarios y de tarjeta de crédito luego de recibirlos para verificar si hay algún débito no autorizado.
9. Sea uno de los primeros en adoptar nuevas tecnologías.
10. Proteja su computadora con un buen software de seguridad y no deje de mantenerlo actualizado.

Anti-Phishing Working Group (APWG)

La *Anti-Phishing Working Group* (APWG) es una organización con más de 600 miembros, creada en Estados Unidos, cuyo principal objetivo es acabar con el robo de identidad y fraudes resultantes del creciente problema del *phishing* y otros tipos de ataques.

Al inicio de su fundación sólo se ocupaba de los casos de *phishing* (de ahí su nombre), pero después de la aparición de nuevas técnicas de robo se vieron obligados a adaptarse e incluirlas dentro de su lucha.

Esta organización se dedica a ofrecer información sobre cómo prevenir el fraude y denunciarlo, al mismo tiempo que recopila datos y mantiene un archivo con todas las páginas y mensajes fraudulentos conocidos. Con esto realiza un informe mensual analizando todos los ataques de *phishing* denunciados a APWG.

Así como la APWG, existe una gran cantidad de organizaciones, entidades y fabricantes de software que se encuentran enfocados en concienciar y asesorar a los miles de millones de usuarios de Internet para que estén atentos a los posibles ataques de robos de información e identidad.

En España, el pasado mes de Julio, se lanzó la primera campaña contra el robo de identidad y el fraude *on-line*. Esta iniciativa pretende concienciar a los usuarios de Internet de la necesidad de protegerse ante los fraudes en la red, especialmente el *phishing*. Para ello, ofrece información dedicada a los usuarios con menos experiencia, para que estos sean conscientes de todos los riesgos que pueden sufrir durante la navegación por Internet. También permite descargar gratuitamente una gran cantidad de software para evitar virus y denunciar los intentos de fraudes que encontremos.

Iniciativas como estas van aumentando en los diferentes países donde víctimas de robos de datos e identidad se manifiestan en contra de los cyber-delincuentes que se encuentran al acecho ante cualquier oportunidad.

LEYES, JUICIOS Y REGULACIONES

Debido al aumento de los daños producidos por la gran cantidad de delitos on-line, en muchos países, a través de los últimos años, se han llevado a juicio a presuntos implicados en ataques de *phishing* y también se han dictado leyes que castigan a los autores de estos ataques.

A continuación se resumen los casos más destacados:

- El 26 de enero de 2004, la FTC (Federal Trade Commission) llevó a juicio el primer caso contra un *phisher* sospechoso, un adolescente de California que creó y utilizó una página Web con un diseño que aparentaba ser la página de American On Line, buscando con esto robar números de tarjetas de crédito.
- En Europa, a finales de marzo del 2005, un hombre estonio de 24 años fue arrestado utilizando un *backdoor*, a partir de que las víctimas visitaron su sitio Web falso, en el que incluía un *keylogger* que le permitía monitorizar lo que los usuarios tecleaban.
- En Brasil, las autoridades arrestaron al denominado *phisher kingpin* Valdir Paulo de Almeida, líder de una de las más grandes redes de *phishing* que en dos años había robado entre 18 y 37 millones de dólares.
- En el Reino Unido, dos hombres fueron arrestados por practicar el *phishing* en un caso conectado a la *Operation Firewall* del Servicio Secreto de Estados Unidos, que buscaba sitios Web que practicaran *phishing.*
- En Estados Unidos, el 1 de marzo de 2005, un senador introdujo el *Acta Anti-Phishing del 2005* que establecía que aquellos criminales que crearan páginas Web falsas o enviaran *spam* con la intención de estafar a los usuarios podrían recibir una multa de hasta 250.000 dólares y penas de cárcel de hasta cinco años.
- El 31 de marzo de 2005, Microsoft llevó a la Corte de Washington 117 pleitos federales. En uno de estos se acusó al *phisher* “John Doe” por utilizar varios métodos para obtener contraseñas e información confidencial.

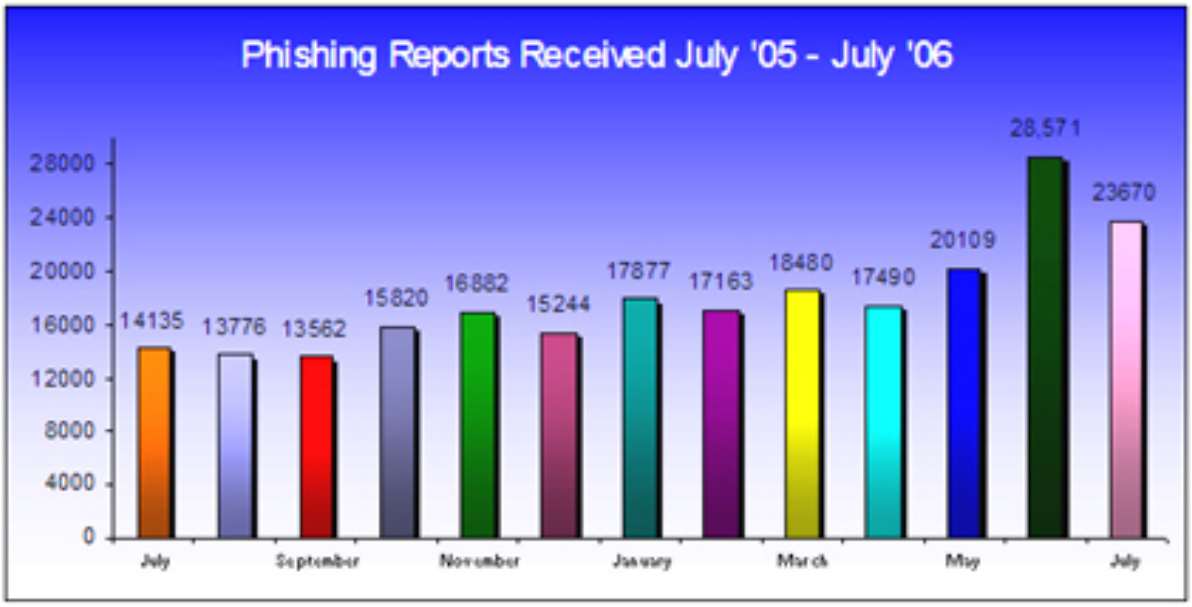
FRAUDES EN NÚMEROS

Para poder apreciar más significativamente la dimensión de todo lo expuesto anteriormente, se exponen a continuación algunos estudios estadísticos sobre cantidad de ataques, daños causados y organizaciones afectadas por los distintos tipos de fraudes llevados a cabo últimamente.

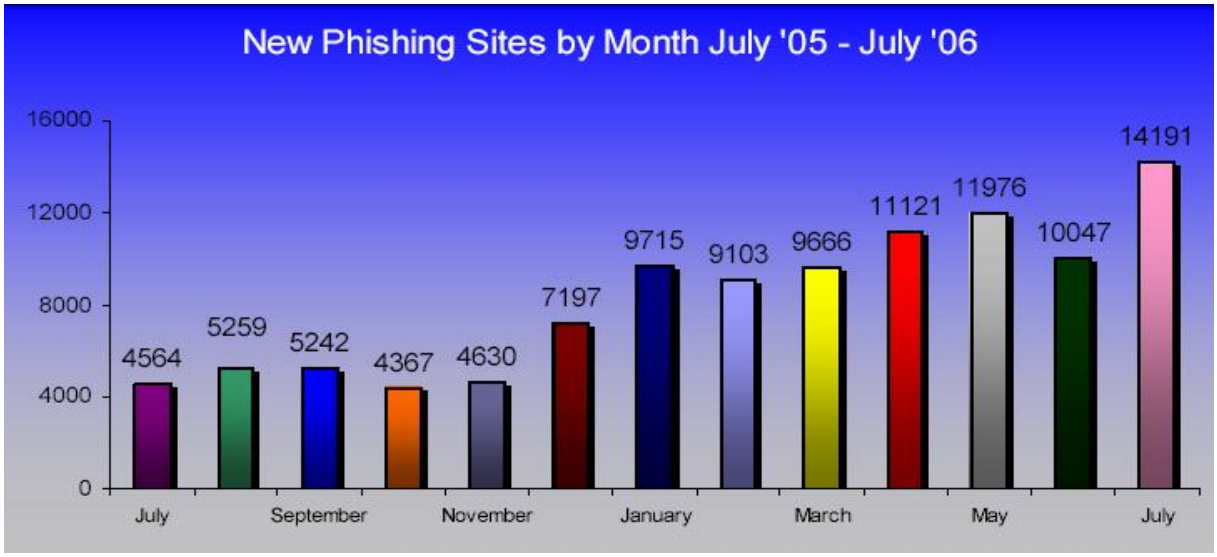
Según el último informe de la *Anti-Phishing Working Group* (Julio 2006), los datos más relevantes en cuanto a *phishing* son los siguientes:

- Número de ataques únicos de *phishing* reportados durante Julio: **23670**
  (Un ataque único de *phishing* se define como un solo envío masivo de correos electrónicos enviados de una vez)
- Número de sitios nuevos de *phishing* reportados durante Julio: **14191**
- Sectores más atacados: **Servicios financieros**
- País con mayor número de *websites* de *phishing*: **Estados Unidos**
- Tiempo promedio que permanece *on-line* un sitio de *phishing*: **4,8 días**

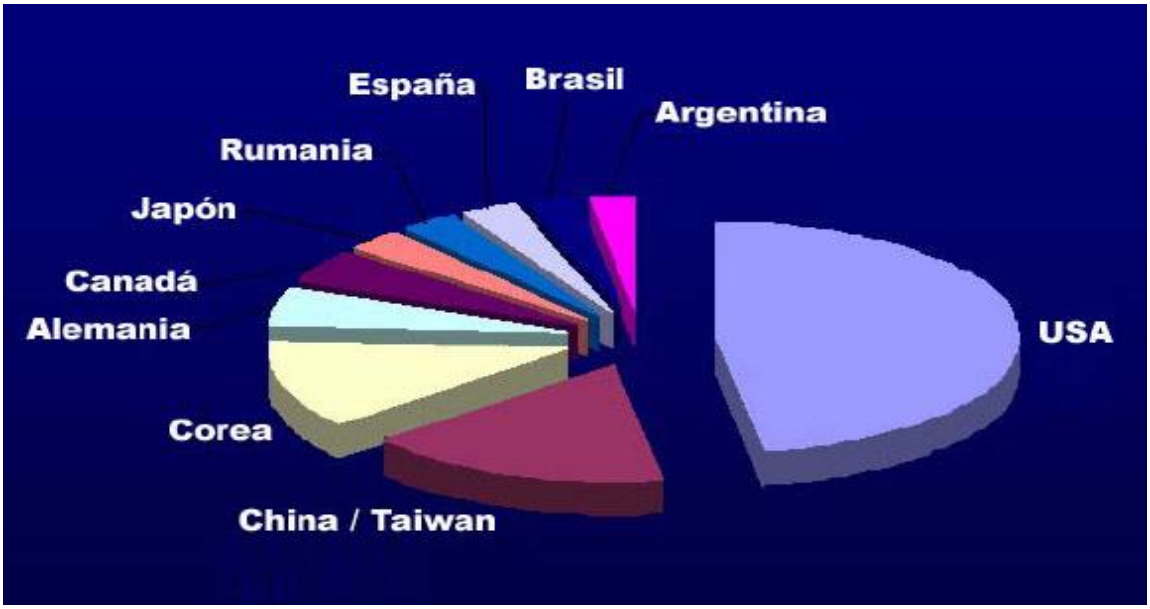
En este gráfico de barras podemos notar como fueron aumentando los ataques *phishing* reportados entre los meses de Julio 2005 y Julio 2006:



El número de *phishing websites* detectados por APWG en Julio del 2006 muestra un notable aumento sobre lo registrado en el mes anterior y es una medida record desde el inicio de la APWG:



Entre los países más afectados se encuentran Estados Unidos, Corea y China. En estos últimos estudios aparecen con una mediana participación países que hace dos años todavía ni figuraban. Esto se debe al idioma, ya que antes todos los ataques se lanzaban en inglés y ahora ya se extienden a otros idiomas como el español y el portugués.



Cabe destacar que los gráficos muestran los ataques (o sitios) *reportados* y no los *realizados* y también el hecho de que este estudio pertenece a una sola organización, habiendo en este momento un gran número de asociaciones y entidades luchando contra los robos de datos e identidad.

Según datos de la Comisión Federal de Comercio (FTC), en Estados Unidos el robo de identidad afecta a casi 10 millones de personas cada año y causa pérdidas por más de 50 mil millones de dólares.

En cuanto a los daños monetarios causados por *phishing*, estudios realizados durante el año 2005 estiman que entre mayo del 2004 y mayo del 2005, aproximadamente 1,2 millones de usuarios de computadoras en los Estados Unidos tuvieron pérdidas a causa del *phishing* por una suma de aproximadamente 929 millones de dólares. Los negocios en los Estados Unidos perdieron cerca de 2000 millones de dólares al año mientras sus clientes eran víctimas.

El Reino Unido también sufrió un alto incremento en la práctica del *phishing*. Para marzo del 2005, la cantidad de dinero que se perdió en este país era de aproximadamente 12 millones de libras esterlinas.

En España, investigadores de la campaña “No más fraude *on-line*” obtuvieron los siguientes datos interesantes:

- La media de dinero robado por fraude on-line a cada víctima ha aumentado desde 5.249 euros en 2003 hasta 6.383 en 2006.
- El fraude online en los primeros cuatro meses de 2006 creció un 50% más que en el año 2005.
- El 75% de los casos detectados de *phishing* en 2005 fueron a bancos, el 20% a empresas de subastas online y de intercambio de dinero, y el 5 % a paginas Web falsas de recargas de móviles.

CONCLUSIÓN

Cada vez son más las nuevas formas de estafas que utilizan como medio de transmisión Internet para llevar a cabo los delitos y robos descritos, usando técnicas existentes e innovando con características variadas, como son los casos expuestos en el presente trabajo.

Los daños causados por dichos robos pueden ir desde la pérdida de acceso al correo electrónico hasta pérdidas económicas sustanciales, sumando a esto el daño emocional que se causa a la víctima del fraude.

Afortunadamente, para nosotros que vivimos en esta parte del mundo, esta moda todavía no ha llegado con mucha fuerza. Esto se debe, principalmente, a que aún no estamos acostumbrados a realizar cierto tipo de transacciones comunes a través de Internet, como por ejemplo, comercio electrónico, por lo que menos aún estaremos preparados “sicológicamente” para realizar transacciones bancarias. Y digo sicológicamente porque en este país, declarado como uno de los más corruptos del mundo, la desconfianza y la suspicacia son parte de nuestra esencia.

GLOSARIO

Backdoor: Programa que se introduce en el ordenador y establece una puerta trasera a través de la cual es posible controlar el sistema afectado, sin conocimiento por parte del usuario.

Exploit: Software que ataca una vulnerabilidad particular de un sistema operativo. No son necesariamente maliciosos, son generalmente creados por investigadores de seguridad informática para demostrar que existe una vulnerabilidad. Y por esto son componentes comunes de los programas maliciosos como los gusanos informáticos.

Hoaxes: Son falsos mensajes de alarma que tratan de provocar cadenas de e-mails entre el mayor número posible de usuarios. El objetivo de estos mensajes suele ser el de ir recopilando direcciones a las que luego enviar *phishing* o incluso realizar ataques dirigidos.

Ingeniería Social: Consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían. En este caso, sería facilitar, por ejemplo, claves o datos personales.

Keylogger: Se trata de un tipo de troyano capaz de registrar las pulsaciones del teclado al conectarse el usuario a determinadas páginas Web.

Malware: *MALicious softWARE*, programa o archivo, que es dañino para el ordenador. Está diseñado para insertar virus, gusanos, troyanos, *spyware* o incluso los *bots*, intentando conseguir algún objetivo, como podría ser el de recoger información sobre el usuario o sobre el ordenador en sí.

Mulero: Nombre utilizado por los delincuentes de Internet para las personas que se dedican a blanquear el dinero obtenido a través del *cibercrimen*. Habitualmente, su función es abrir cuentas bancarias en las que debe recibir dinero que luego es transferido a otras cuentas a cambio de un porcentaje.

Scam: Es la captación de personas por medio de correos electrónicos, chats, IRC, etc., donde empresas ficticias le ofrecen trabajar cómodamente desde casa y cobrando unos beneficios muy altos. Sin saberlo, la víctima está blanqueando dinero obtenido por medio del *phishing* (procedente de estafas bancarias).

Spoofing: En términos de seguridad informática, hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación. También se refiere a las páginas falsas creadas por los *phishers* para realizar sus ataques (*spoofed Web sites*).

Troyano: También conocido como caballo de Troya. Es un programa que realiza algunas acciones inesperadas o no autorizadas, generalmente malignas, tales como desplegar mensajes, borrar archivos o formatear un disco. Un troyano no infecta otros archivos, por lo que no es necesario limpiar. Para deshacerse de él simplemente basta con borrar el programa.

REFERENCIAS BIBLIOGRÁFICAS

Sitios de Internet:

- http://www.antiphishing.org/
- http://en.wikipedia.org/
- http://www.navegaprotegido.org/
- http://www.phishinginfo.org/
- http://www.identidadrobada.com/
- http://www.pandasoftware.es/
- http://www.delitosinformaticos.com/
- http://www.recoverylabs.com/
- http://www.nomasfraude.es/

Artículos:

- http://seguridad.internautas.org/html/1/848.html
- http://catinello.webcindario.com/glosario/MN.html
- http://www.symantec.com/es/es/home_homeoffice/library/article.jsp?aid=article2_01_06
- http://www.genbeta.com/archivos/temas/seguridad.php
- http://www.microsoft.com/latam/athome/security/email/spear_phishing.mspx
- http://www.interbel.es/noticias/desglosarnoticia.cfm?id=125
- http://www.honeynet.org/papers/phishing/
- http://news.millersmiles.co.uk/article/0056
- http://www.ftc.gov/bcp/conline/spanish/credit/s-idtheft.htm
- http://bank.commerceonline.com/espanol/consumerAlert/avoidFraud.cfm
- http://www.consumer.gov/idtheft/ddd/espanol.html
- http://rootzero.wordpress.com/2006/07/28/ransomware-la-bolsa-o-la-vidapdf/

Ejemplos de *phishing:*

- http://www.shellsec.net/noticias.php?num=518
- http://www.auso.es/?q=node/2/03//pay%20pal
- http://www.hispasec.com/directorio/laboratorio/phishing/demo2/banesto_phishing.htm