Delitos informáticos: Pishing

Osvaldo Callegari
Analista de Sistemas
ocalle@ar.inter.net

El phishing es una técnica de captación ilícita de datos personales (principalmente relacionados con claves para el acceso a servicios bancarios y financieros) a través de correos electrónicos o páginas web que imitan/copian la imagen o apariencia de una entidad bancaria/financiera (o cualquier otro tipo de empresa de reconocido prestigio).

En términos más coloquiales, podemos entender el phishing como "pescando datos" o "pesca de datos", al asimilar la fonética de la palabra "phishing" con el gerundio "fishing" (pescando).

¿Cómo funciona el phishing?

La técnica del *phishing* utiliza el correo electrónico para ponerse en contacto con los usuarios, utilizando mensajes que imitan, casi a la perfección, el formato, lenguaje y la imagen de las entidades bancarias/financieras, y que siempre incluyen una petición final en la que solicita a los usuarios la "confirmación" de determinados datos personales alegando distintos motivos: problemas técnicos, cambio de política de seguridad, posible fraude, etc...

Estos mensajes de correo electrónico siempre incluyen enlaces que conducen "*aparentemente*" a las páginas web oficiales de las citadas entidades pero que, en realidad, remiten a "*páginas web piratas*" que imitan o copian casi a la perfección la página web de la entidad financiera, siendo su finalidad principal captar datos de los usuarios.

Dada la confianza que los usuarios tienen depositada en las entidades de las que son clientes, y por desconocimiento o simplemente ante la incertidumbre y temor creados, acceden a dichas páginas web piratas, donde el defraudador o delincuente informático, obtiene los datos personales o claves de acceso personales.

Es a partir de este momento donde empieza el fraude:

1. Utilización del **número de tarjeta** y fecha de caducidad para compras por internet (comercio electrónico).

2. Realización de **transferencias bancarias** no consentidas ni autorizadas.

3. Retiro de efectivo en cajeros con duplicados de las tarjetas.

Formas simples de proteger los documentos

1. Destruir las copias impresas. Si imprime documentos confidenciales para repartirlos en las reuniones, recopílelos después y destrúyalos o pida a los participantes que lo hagan.

2. Etiquetar los documentos. En ocasiones los empleados no saben que los documentos contienen información confidencial y, por lo tanto, no adoptan las precauciones que deberían. Indique a los creadores de los documentos que utilicen el encabezado o el pie de página para etiquetar el documento como "*confidencial*". También pueden agregar una marca de agua confidencial a un documento. En Word 2003, seleccione *Fondo* en el menú *Formato* y a continuación, seleccione *Marca de agua* impresa. Seleccione Marca de agua de texto en el cuadro de texto y elija "*confidencial*" en la lista desplegable.

3. Utilizar protección con contraseña. Puede restringir los usuarios que pueden ver un documento al requerir que cualquier usuario que abra el documento conozca e introduzca la contraseña que cree y comparta con ellos. Los documentos, las hojas de cálculo y las presentaciones creados con *Microsoft Office 2003* disponen de esta característica. Sólo tiene que abrir el archivo, seleccionar *Opciones* en el menú *Herramientas* y hacer clic en *Seguridad*. Puede configurar contraseñas para abrir y modificar un documento. Aunque los piratas informáticos disponen de herramientas para descubrir contraseñas, éstas, por lo general, dificultan la consulta de documentos.

4. Instalar un servidor de seguridad. Hay un sinfín de buenos motivos para instalar un servidor de seguridad y proteger los documentos. Los servidores pueden evitar que los intrusos de Internet tengan acceso a los archivos del equipo y consulten la información. *Windows XP Professional* incluye un servidor de seguridad de software que es fácil de configurar.

Protección avanzada

1. Codificar los archivos de documento. La codificación puede proteger los documentos si se roba un equipo de la empresa, lo que constituye una responsabilidad muy real para los que viajan con equipos portátiles y otros dispositivos móviles. La codificación deja ilegibles los datos excepto para los usuarios que tienen la "*clave*" necesaria instalada en su equipo.

Windows XP Professional incluye el sistema de archivos de cifrado (EFS), que permite cifrar archivos individuales, así como el contenido de toda una car-

Continúa en página 166

Viene de página 162

peta. Con EFS, sólo el usuario que codifica un archivo de documento puede abrirlo y trabajar con él. No obstante, la compatibilidad con la recuperación de datos integrada permite recuperar datos codificados por un empleado después de que el empleado deje la empresa o si se pierden las claves de codificación.

Aunque la codificación parece algo muy técnico, es posible que no necesite a un consultor externo para mostrarle su uso. La configuración predeterminada de EFS permite a los usuarios empezar a codificar archivos con muy poco esfuerzo y crea todas las claves necesarias que hay que tener.

2. Asignar permisos de archivo. Si su empresa utiliza un servidor, puede restringir los usuarios que pueden ver o cambiar un documento asignando permisos. Los permisos básicamente conceden o deniegan el acceso a un documento (o a cualquier recurso informático) según lo determinado por el propietario. Los derechos de acceso y los privilegios se pueden aplicar a personas así como a grupos de usuarios. Los permisos habituales permiten a un usuario ver o "leer" un archivo o todos los archivos de una carpeta y cambiar o "escribir" en un archivo o todos los archivos de una carpeta. *Windows Small Business Server 2003* y otros sistemas de servidor de Windows® permiten el uso de permisos mediante la "*lista de control de acceso*".

3. Utilizar Information Rights Management (IRM). Para un sistema de protección de documentos que se integre directamente con las versiones *Microsoft Office Professional 2003 de Word, Excel, PowerPoint y Outlook*, considere la posibilidad de utilizar la tecnología *Information Rights Management (IRM)* desarrollada por Microsoft.

Con IRM, puede establecer permisos de archivo en diferentes niveles y cambiar el nivel para determinados usuarios y grupos de usuarios.

• Restringir la impresión de archivos para reducir el número de copias impresas generadas

• Limitar el período de tiempo en el que se puede abrir un archivo

• Impedir que un usuario no autorizado abra archivos reenviados

IRM también concede control sobre los mensajes de correo electrónico y sus datos adjuntos incluso después de enviarlos. Puede impedir que los mensajes de correo electrónico se copien, reenvíen o impriman.

Information Rights Management requiere disponer de un servidor de empresa con *Windows Server 2003.*

Para tener en cuenta

- Sospeche de cualquier correo electrónico con solicitudes urgentes de información personal, que utilice argumentos como:
  - Problemas de carácter técnico.
  - Detecciones de posibles fraudes.
  - Cambio de política de seguridad.
  - Promoción de nuevos productos y/o servicios.
  - Premios, regalos, concursos, etc...

  Este tipo de correos suele incorporar advertencias tales como: "*si no realiza la confirmación/cambio solicitada, en el transcurso de --- horas/días se procederá al bloqueo/cancelación, de su cuenta bancaria/cuenta de cliente, etc...*"; de forma que se fuerza una respuesta casi inmediata del usuario.
- Sospeche de los correos electrónicos que le soliciten información como: nombre de usuario, password o clave de acceso, número de tarjeta de crédito, fecha de caducidad, número de la seguridad social, etc...
- Los mensajes de correo electrónico de phishing no suelen estar personalizados, mientras que los mensajes de las entidades de las que somos clientes suelen estar personalizados.
- Evite rellenar formularios en correos electrónicos que le soliciten información financiera personal.
- No utilice los enlaces incluidos en los correos electrónicos que conducen "aparentemente" a las entidades, especialmente si sospecha que el mensaje podría no ser auténtico. Diríjase directamente, a través de su navegador, a la página web de la entidad o empresa.
- Antes de facilitar cualquier dato sensible (datos bancarios, números de tarjetas de crédito, número de la seguridad social, etc...) asegúrese de que se encuentra en una web segura.

  Las páginas web que utilizan protocolos de seguridad, que impiden la captación de datos por parte de terceros no autorizados, se caracterizan porque la dirección web que aparece en la barra de navegación comienza con el protocolo "https" y en la parte inferior de la página aparece un candado.

  Igualmente podemos comprobar la veracidad del protocolo de seguridad; para ello, podemos clickear dos veces en el candado de la parte inferior de la página, y nos aparecerá una ventana en la que se identifica a la compañía de certificación y al titular del protocolo, así como su validez.
- Asegúrese de tener el navegador web actualizado y con los últimos parches de seguridad instalados.
- Si continua teniendo dudas acerca de la veracidad del correo electrónico, de su emisor o de su finalidad, no dude en ponerse en contacto con la entidad de la que es cliente.
- Compruebe regularmente sus cuentas bancarias para asegurarse que todos los movimientos o transacciones son legítimos. En caso de detectar algo sospechoso, no dude en ponerse en contacto con su entidad bancaria.