Protéjase del *Phishing*

Por Gustavo Ibáñez Padilla

Existe una modalidad de fraude denominada *phishing*, que consiste en “pescar” información de personas desprevenidas para luego emplearla a fin de robar su identidad y también sus fondos.

El *phishing* es una estafa diseñada con la finalidad de robarle su identidad. El delito se basa en obtener información personal tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos por medio de engaños. Este tipo de fraude se realiza habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.

En este sistema de fraude, el estafador envía millones de mensajes falsos que parecen provenir de sitios Web reconocidos o de su confianza, como su banco o la empresa de su tarjeta de crédito. Dado que los mensajes y los sitios Web que envían estos usuarios parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos. La gente confiada normalmente responde a estas solicitudes de correo electrónico con sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales.

Para que estos mensajes parezcan aun más reales, el embaucador suele incluir un vínculo falso que parece dirigir al sitio Web legítimo, pero en realidad lleva a un sitio falso o incluso a una ventana emergente que tiene exactamente el mismo aspecto que el sitio Web oficial. Estas copias se denominan "**sitios Web piratas**". Una vez que el usuario está en uno de estos sitios Web, introduce información personal sin saber que se transmitirá directamente al delincuente, que la utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad.

> El término *phishing* proviene de la palabra inglesa "*fishing*" (pesca), haciendo alusión al intento de hacer que los usuarios "piquen en el anzuelo". A quien lo practica se le llama *phisher*. También se dice que el término "*phishing*" es la contracción de "*password harvesting fishing*" (cosecha y pesca de contraseñas), aunque esto probablemente es un acrónimo retroactivo, dado que la escritura 'ph *es comúnmente utilizada por hackers para sustituir la* f*, como raíz de la antigua forma de hacking telefónico conocida como phreaking*.

Procedimientos para protegerse del *phishing*

Al igual que en el mundo físico, los estafadores continuamente desarrollan nuevas formas de engañar a través de Internet. Abajo se detallan cinco formas de protegerse y preservar la privacidad de su información.

1) Nunca responda a solicitudes de información personal a través de correo electrónico.

Las empresas de prestigio nunca solicitan contraseñas, números de tarjeta de crédito u otro tipo de información personal por correo electrónico. Si recibe un mensaje que le solicita este tipo de información, no responda. Si piensa que el mensaje es legítimo, comuníquese con la empresa por teléfono o a través de su sitio Web para confirmar la información recibida.

SUNTRUST

Ejemplos de mensajes fraudulentos

Dear SunTrust Bank client,

Recently there have been a large number of identity theft attempts targeting SunTrust customers. In order to safeguard your account, we require that you confirm your banking details (credit card information and login/password for online banking, if you have).

This process is mandatory, and if not completed within the nearest time your account or credit card may be subject to temporary suspension.

To securely confirm you SunTrust Bank details please follow the link:

http://www.suntrust.com/personal/Checking/OnlineBanking/Internet_Banking/security.asp

Thank you for your prompt attention to this matter and thank you for using SunTrust Bank!

Do not reply to this e-mail as it is an unmonitored alias

© 2004 SunTrust Banks, Inc. All rights reserved. Member FDIC

De: Visa Home
Para: suemail@servidor.com.ar
Enviado: Miércoles, 09 de Junio de 2010 05:25 p.m.
Asunto: Limitamos el acceso a su cuenta.

VISA HOME

VISA
Nº1 en el Mundo

Visa Home
para socios

- Estimado Cliente: Visa Home está constantemente trabajando para su seguridad, hemos notado una serie de irregularidades en su cuenta en los últimos días y tuvimos que suspender el acceso a su cuenta temporalmente, para reactivar su cuenta por favor diríjase a
https://inetserv.visa.com.ar/vhs/app/Login.po
Y llene los campos necesarios, esto hará que restablezcamos su cuenta lo antes posible.

Lamentamos las molestias.

Merlina Irigotia, Departamento Legales, Visa Argentina.

2) Para visitar sitios Web, introduzca la dirección URL en la barra de direcciones

Si sospecha de la legitimidad de un mensaje de correo electrónico de la empresa de su tarjeta de crédito, banco o servicio de pagos electrónicos, no siga los enlaces que lo llevarán al sitio Web desde el que se envió el mensaje. Estos enlaces pueden conducirlo a un sitio falso que enviará toda la información ingresada al estafador que lo ha creado.

Aunque la barra de direcciones muestre la dirección correcta, no se arriesgue a que lo engañen. Los piratas conocen muchas formas para mostrar una dirección URL falsa en la barra de direcciones del navegador. Las nuevas versiones de Internet Explorer hacen más difícil falsificar la barra de direcciones, por lo que es una conveniente visitar Windows Update regularmente y actualizar su software. Si cree que podría olvidarse o prefiere que la instalación se realice sin su intervención, puede configurar la computadora para que realice actualizaciones automáticas.

3) Asegúrese de que el sitio Web utiliza métodos de cifrado.

Si no se puede confiar en un sitio Web por su barra de direcciones, ¿cómo saber si es seguro? Existen varias formas: En primer lugar, antes de ingresar cualquier tipo de información personal, compruebe si el sitio Web utiliza cifrado para transmitir la información personal. En Internet Explorer puede comprobarlo con el icono de color amarillo situado en la barra de estado, tal como se muestra en la figura 1.

Icono de candado de sitio seguro

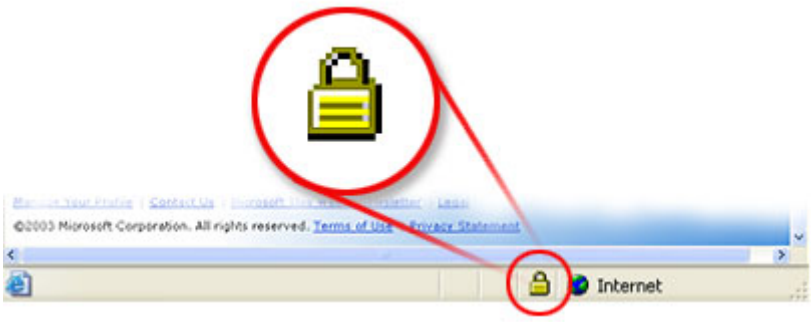


Figura1

Este símbolo significa que el sitio Web utiliza cifrado para proteger la información personal que introduzca: números de tarjetas de crédito, número de la seguridad social o detalles de pagos.

Haga doble clic sobre el icono del candado para ver el certificado de seguridad del sitio. El nombre que aparece a continuación de Enviado a debe coincidir con el del sitio en el que se encuentra. Si el nombre es diferente, puede que se encuentre en un sitio falso. Si no está seguro de la legitimidad de un certificado, no introduzca ninguna información personal. Sea prudente y abandone el sitio Web.

Para conocer otras formas de determinar si un sitio es seguro, consulte Seguridad de datos en Internet Explorer.

4) Consulte frecuentemente los saldos de sus Cuentas bancarias y de sus Tarjetas de crédito.


LOS ANGELES TIMES

JARTERLY MUTUAL FUNDS REPORT

r Stock Fund Leaders by Investment Category

Incluso si sigue los tres pasos anteriores, puede convertirse en víctima de las usurpaciones de identidad. Si consulta sus saldos bancarios y de sus tarjetas de crédito al menos una vez al mes, podrá sorprender al estafador y detenerlo antes de que provoque daños significativos.

5) Comunique los posibles delitos relacionados con su información personal a las autoridades competentes.

Si cree que ha sido víctima de *phishing*, proceda del siguiente modo:

• **Informe inmediatamente del fraude a la empresa afectada.** Si no está seguro de cómo comunicarse con la empresa, visite su sitio Web para obtener la información de contacto adecuada. Algunas empresas tienen una dirección de correo electrónico especial para informar de este tipo de delitos. Recuerde que no debe seguir ningún vínculo que se ofrezca en el correo electrónico recibido. Debe introducir la dirección del sitio Web conocida de la compañía directamente en la barra de direcciones del navegador de Internet.

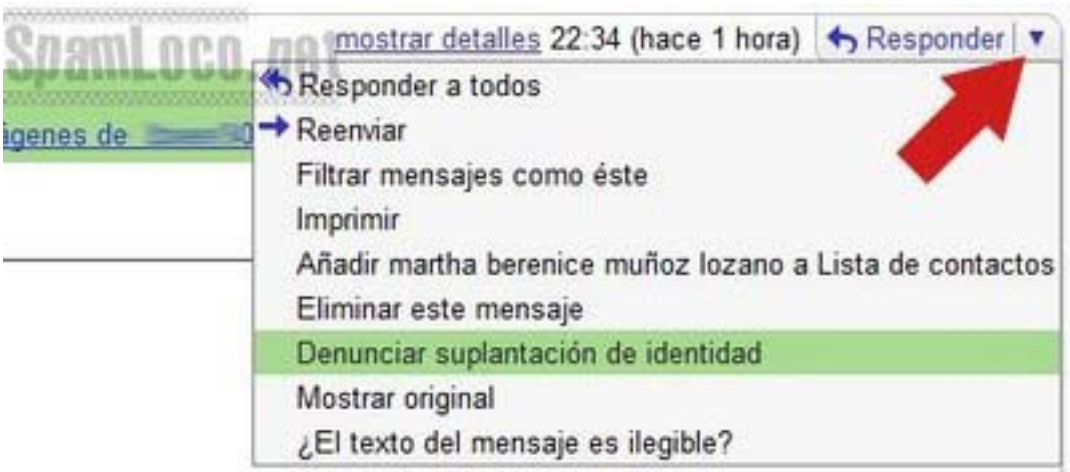
• **Proporcione los detalles del estafador, como los mensajes recibidos, a la autoridad competente** a través del Centro de denuncias de fraude en Internet. Este centro trabaja en todo el mundo en colaboración con las autoridades legales para clausurar con celeridad los sitios Web fraudulentos e identificar a los responsables del fraude.

Si cree que su información personal ha sido robada o puesta en peligro, también debe comunicarlo a la *Federal Trade Commission* (FTC) y visitar el sitio Web de robo de identidades de la http://www.ftc.gov/ para saber cómo minimizar los daños (válido para Estados Unidos, consulte a las autoridades de su país).

Cómo Denunciar casos de Phishing directamente desde Internet:

Denunciar Phishing en Gmail:

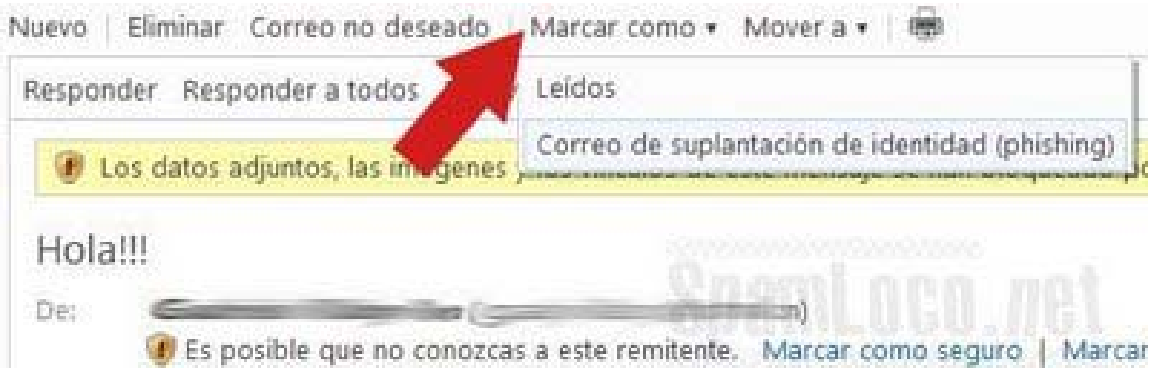
Con el correo abierto expandir las opciones del menú "Responder", ubicado a la derecha del mensaje. Luego seleccionar la opción "Denunciar suplantación de identidad":



En la nueva ventana hacer clic en el botón "Denunciar mensaje afectado por phishing":

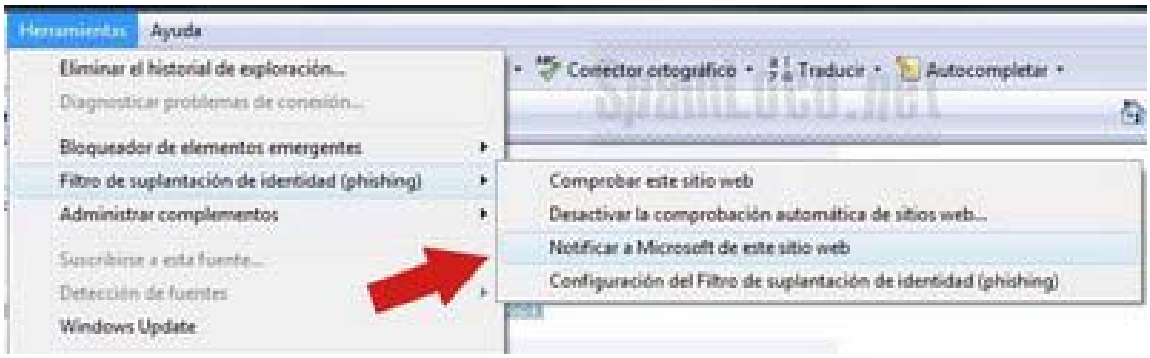
Denunciar Phishing en Hotmail:

Con el correo abierto debemos seleccionar en "Marcar como" la opción "Correo de suplantación de identidad (phishing)":



Denunciar Phishing en Internet Explorer:

En el menú "Herramientas" seleccionar "Filtro de suplantación de identidad (phishing)" y luego la opción "Notificar a Microsoft de este sitio web":



Finalmente, se accede a otra web donde se debe confirmar la denuncia:

- - - -

Colección Economía Personal

Gustavo Ibáñez Padilla es ingeniero civil, master en comunicación institucional, profesor universitario, consultor financiero, escritor y conferencista. Es miembro del Comité IRAM para la aplicación en Argentina de la Norma ISO 22.222 (Planificación Financiera Personal). Es autor del *Manual de Economía Personal*, el libro argentino de finanzas personales más vendido.