

Aviso de seguridad

Recuerde que el SAT:

- **NO** distribuye software,
- **NO** solicita ejecutar o guardar un archivo,
- **NI** requiere información personal, claves o contraseñas por correo electrónico.

En caso de que reciba algún correo de este tipo, no descargue ningún programa ni envíe información y por favor repórtelo a través de los Nuevos servicios por Internet.

Las cuentas de correos apócrifas son:

- **contacto@sat.com.mx,**
- **contacto@shcp.com ,**
- **contacto@shcp.gob.mx y**
- **sat@shcp.org.mx**

Por lo anterior, es importante conocer de los dos siguientes temas:

Todo lo que debe saber acerca del "phishing"



Si creía que su buzón estaba seguro, recuerde que hay una nueva forma de correo no deseado al acecho. Este tipo de correo basura no sólo es inesperado y molesto, sino que también facilita el robo de sus números de tarjetas de crédito, contraseñas, información de cuentas y

otra información personal. Continúe leyendo para obtener más información acerca de esta nueva modalidad de robo y saber cómo proteger su información personal.

¿Qué es el "phishing"?

El "phishing" 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.

Cómo funciona el "phishing"?

En esta modalidad de fraude, el usuario malintencionado envía millones de mensajes falsos que parecen provenir de sitios Web reconocidos o de su confianza,

Vínculos relacionados

- Proteja su información personal en línea
- Sugerencias de seguridad para las operaciones bancarias en línea

Cinco pasos que lo ayudarán a evitar el "phishing"

- Nunca responda a solicitudes de información personal a través de correo electrónico.
- Para visitar sitios Web, introduzca la dirección URL en la barra de direcciones.
- Asegúrese de que el sitio Web utiliza cifrado.
- Consulte frecuentemente los saldos bancarios y de sus tarjetas de crédito.
- Informe de los posibles abusos a las autoridades competentes.

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 estafador 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.

Procedimientos para protegerse del "phishing"

Al igual que en el mundo físico, los estafadores continúan desarrollando nuevas y más siniestras formas de engañar a través de Internet. Si sigue estos cinco sencillos pasos podrá protegerse y preservar la privacidad de su información.

1.	Nunca responda a solicitudes de información personal a través de correo electrónico. Si tiene alguna duda, póngase en contacto con la entidad que supuestamente le ha enviado el mensaje.
2.	Para visitar sitios Web, introduzca la dirección URL en la barra de direcciones.
3.	Asegúrese de que el sitio Web utiliza cifrado.
4.	Consulte frecuentemente los saldos bancarios y de sus tarjetas de crédito.
5.	Comunique los posibles delitos relacionados con su información personal a las autoridades competentes.

Paso 1: nunca responda a solicitudes de información personal a través de correo electrónico

Microsoft y 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. Consulte el Paso 2 para obtener información sobre las prácticas más adecuadas para acceder a un sitio Web si cree que ha sido víctima de una maniobra de "phishing".

Paso 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 buena idea 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.

Paso 3: asegúrese de que el sitio Web utiliza cifrado

Si no se puede confiar en un sitio Web por su barra de direcciones, ¿cómo se sabe que será 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.

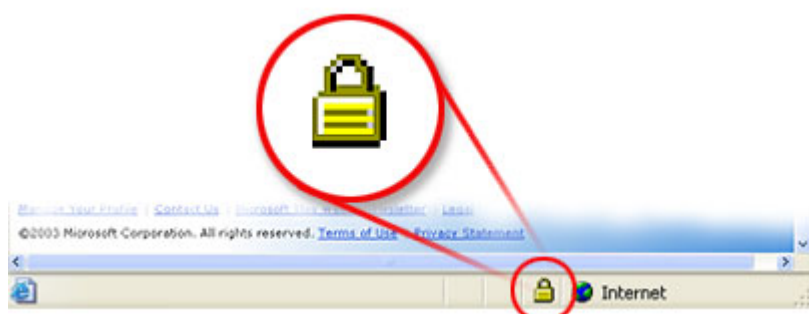


Figura 1. Icono de candado de sitio seguro. Si el candado está cerrado, el sitio utiliza cifrado.

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.

Paso 4: consulte frecuentemente los saldos bancarios y de sus tarjetas de crédito

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.

Paso 5: comunice 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 FTC y visitar el sitio Web de robo de identidades de la FTC para saber cómo minimizar los daños.

Fraude a través del "pharming": desvío del explorador a sitios Web falsos

¿Es su sitio Web de confianza... o una buena falsificación?



El "pharming" es una práctica delictiva en la que un pirata informático desvía el tráfico de Internet de un sitio Web hacia otro sitio de apariencia similar, con la finalidad de engañar a los usuarios para obtener sus nombres y contraseñas de acceso, que se registrarán en la base de datos del sitio falso. Con frecuencia, los sitios de banca en línea y otros similares se convierten en los principales objetivos de estos ataques, en los que los delincuentes intentan adquirir datos personales

con el fin de obtener acceso a cuentas bancarias, robar datos identificativos o cometer estafas suplantando a usuarios.

Las estafas de "pharming", basadas en el uso de sitios Web falsos pueden tener algunas similitudes con los timos de "phishing" que se llevan a cabo a través del correo electrónico, aunque las primeras resultan más insidiosas, dado que pueden desviar al usuario a un sitio falso sin que aquél participe o tenga conocimiento de ello.

Hasta la fecha se han registrado pocos ataques y hay que destacar que la integridad de los sitios Web es una de las máximas prioridades tanto de las empresas como de las administraciones. También es importante recordar que Internet es un recurso público y libre, similar a una biblioteca y a otros servicios públicos que pueda haber en una comunidad. Para la mayoría de las personas, las ventajas de poder comprar, hacer negocios, investigar y relacionarse, entre otras muchas, compensan los peligros y las condiciones imprevisibles de un espacio público.

A fondo: el "pharming"

P: ¿Cómo puede desviar un atacante mi explorador Web hacia otro sitio?

R: Mediante un proceso denominado envenenamiento de DNS (servidor de nombres de dominio), en el que el atacante obtiene acceso a alguna de las enormes bases de datos que utilizan los proveedores de Internet para enrutar el tráfico Web y realiza modificaciones para desviar a los usuarios hacia el sitio falso antes de que éstos tengan acceso a la página deseada.

P: Algunas compañías sostienen que su software de servidor de seguridad también sirve de protección contra el "pharming". ¿Es cierto?

R: Algunos proveedores de soluciones de privacidad para Web creen que los clientes que enrutan toda su actividad en Internet a través de los servidores seguros que ellos ofrecen están protegidos frente a los ataques de "pharming". La naturaleza del "pharming" parece indicar lo contrario. En cualquier caso, sean cuales sean las promesas del proveedor, siempre es recomendable estudiar

bien las ofertas de productos de seguridad y consultar análisis y comparativas a través de fuentes de prestigio, como CNET, antes de invertir y confiar en cualquier solución de software.

P: Para saber si un sitio Web es falso, ¿no basta con mover el puntero sobre los vínculos y observar si el código va a un número aparentemente aleatorio fuera del sitio?

R: No necesariamente. Los sitios Web falsos que se utilizan en las estafas de "pharming" suelen tener vínculos "usurpados" para que su apariencia sea verosímil, incluso en el código que se muestra cuando se pasa el puntero sobre los vínculos. Asimismo, es posible que en los sitios Web se cambie el código de los vínculos de vez en cuando por motivos internos; por ejemplo, tras una actualización de software o de la plataforma de servidores, o incluso por los métodos de análisis de tráfico de clientes.

P: ¿Por qué es "pharming" con "ph", y no con "f" (de "farming", cultivo)?

R: En este caso, parece seguir la tradición de una jerga que se inició con el término "phone phreaking" (en vez de "freaking"), consistente en el uso de sistemas electrónicos para realizar llamadas gratuitas utilizando teléfonos ajenos. Actualmente existe todo un argot de términos de Internet que evoluciona continuamente.

Fuente: www.sat.gob.mx