



- [Home](#)
- [English](#)
- [HSBC México](#)
- [Mapa del Sitio](#)
- [Bolsa de Trabajo](#)
- [Contacto](#)
- [HSBC en el Mundo](#)

Búsqueda



- [Banca Personal por Internet](#)

- [Personas](#)
- [HSBC Premier](#)
- [Banca Privada](#)
- [PYMES](#)
- [Empresas](#)
- [Banca Corporativa](#)
- [Banca de Gobierno](#)

- [Home](#)
- [Pie de página](#)
- [Seguridad](#)
- [Phishing](#)

- [Seguridad en Línea](#)
- [Las Cinco Reglas de Oro](#)
- [Tips de Seguridad](#)
- [El Idioma en Línea Descifrado](#)
- [Banca Segura por Internet](#)
- [Otros Fraudes en Línea](#)
- [Phishing](#)
- [Recursos Adicionales](#)
- [Preguntas Frecuentes](#)

Phishing

Engaños de Phishing.

Una estafa cada vez más frecuente que actualmente está siendo empleada por individuos sin escrúpulos, es el Phishing. El Phishing implica un mensaje electrónico que es enviado a tantas direcciones de correo electrónico de Internet como el defraudador puede obtener, presumiendo provenir de una organización legítima como un Banco, un servicio de pagos en línea, un minorista en línea, o similar.

El correo electrónico solicita que el destinatario ponga al día o verifique su información personal y financiera, incluyendo la fecha de nacimiento, la información de conexión, los detalles de cuentas, los números de la tarjeta de crédito, los números de identificación personal (NIP), etc. Algunos mensajes

electrónicos incluyen una amenaza de que si no se actualiza o se valida causará, por ejemplo, que la cuenta sea congelada. El objetivo es inducir a destinatarios confiados, que resultan ser los clientes de la organización legítima que ha sido imitada, a responder al correo electrónico y proporcionar la información solicitada.

El correo electrónico contendrá una liga que te llevará a un sitio web que imita y se aprecia idéntico, o al menos muy similar, al sitio genuino de la organización. En algunos casos, cuando la liga en el correo electrónico es pulsada, el sitio genuino es accedido, pero es cubierto con una ventana más pequeña con el sitio falso, haciéndolo más creíble. Pulsar sobre una liga también puede descargar en tu PC software malicioso, conocido como "spyware", que registrará tu uso del Internet y reenviará esta información, y posiblemente un registro de lo que hayas tecleado, al defraudador. El defraudador usará esta información financiera para comprometer cuentas bancarias, tarjetas de crédito, etc.

Para evitar que seas víctima del Phishing, nunca respondas a mensajes de correo electrónico que requieran información personal o financiera, y nunca pulses una liga en ese tipo de correos. Las organizaciones de buena reputación no envían mensajes de correo no solicitado pidiendo a sus clientes actualizar o verificar sus detalle personales y de seguridad. Si tienes duda respecto a la legitimidad del correo, o si crees que has sido víctima de un engaño de Phishing, debes contactar inmediatamente a la organización de la que se trate. Sin embargo, debes tener cuidado en utilizar el método acostumbrado con el que contactas a esta organización, en lugar de usar cualquiera sugerencia incluida en el correo o respondiendo a éste.



- [Regresar](#)

Mulas del Phishing.

Una vez que los defraudadores han recolectado la información financiera de individuos a través del Phishing, están en posición de abusar de esta información y de robar dinero de las cuentas comprometidas. Para cubrir sus pistas reclutan a individuos confiados para actuar como mediadores, que colocan una variedad de ofertas tentadoras de trabajo en el Internet, prometiendo la posibilidad ganar dinero rápidamente y sin mucho esfuerzo. A estos individuos se les conoce como mulas.

Las cuentas bancarias de las mulas son utilizadas para depositar las transferencias del dinero de las cuentas que han sido comprometidas. Entonces, los defraudadores de Phishing dan la instrucción a las mulas de retirar de sus cuentas el dinero en efectivo y reenviarlo, restando la comisión prometida, a través de agencias de transferencia de fondos internacionales. Por lo que los defraudadores pueden conservar su anonimato, aunque hay un rastro hacia las mulas, que puede ser seguido por las autoridades.

Ten mucho cuidado de las ofertas de trabajo que involucran aceptar y liberar fondos a una cuenta bancaria a cambio de una comisión. Las mulas reclutadas por los defraudadores de Phishing, lavan dinero, y es muy probable que tengan que enfrentar un proceso criminal.

- [Regresar](#)
-  [Imprimir página](#)
-  [Enviar a un amigo](#)

© Copyright HSBC México 2008. Todos los Derechos Reservados. [Tarifas y Comisiones](#) | [Seguridad](#) | [Legales](#) | [Quejas y Sugerencias](#) | [IPAB](#)



- [Home](#)
- [English](#)
- [HSBC México](#)
- [Mapa del Sitio](#)
- [Bolsa de Trabajo](#)
- [Contacto](#)
- [HSBC en el Mundo](#)

Búsqueda



- [Banca por Internet para Empresas](#)

- [Personas](#)
- [HSBC Premier](#)
- [Banca Privada](#)
- [PYMES](#)
- [Empresas](#)
- [Banca Corporativa](#)
- [Banca de Gobierno](#)

- [Home](#)
- [Pie de página](#)
- [Seguridad](#)
- Las Cinco Reglas de Oro

- [Seguridad en Línea](#)
- [Las Cinco Reglas de Oro](#)
- [Tips de Seguridad](#)
- [El Idioma en Línea Descifrado](#)
- [Banca Segura por Internet](#)
- [Otros Fraudes en Línea](#)
- [Phishing](#)
- [Recursos Adicionales](#)
- [Preguntas Frecuentes](#)

Las Cinco Reglas de Oro

Hay 5 reglas cuyo seguimiento derivará en una mejor protección de tu PC con un mínimo de esfuerzo. Al seguir las proteges tu información personal no sólo cuando ingresas a nuestros servicios bancarios sino en general mientras utilizas el Internet.

Dichas reglas no son todas las medidas de seguridad que puedes aplicar, pero son un excelente inicio. Se aplican por igual en equipos propiedad de entidades de negocio como de particulares.

1. Actualizaciones y Parches

Día a día se van descubriendo vulnerabilidades en los sistemas de cómputo. De la misma forma se realizan adecuaciones para corregirlas. Estas debilidades son explotadas regularmente por hackers para

tratar de acceder en equipos de cómputo de otros.

Los fabricantes de software ofrecen las correcciones a dichas vulnerabilidades bajo el nombre de parches y/o actualizaciones. Generalmente están disponibles en sus sitios Web y se pueden descargar de forma automática.

Ejemplo de ello es Microsoft, que en la página <http://windowsupdate.microsoft.com> valida en forma automática el nivel de parches de los equipos y ofrece el servicio de descarga.

2. Instalación de software Antivirus

Un virus informático se define como un programa malicioso que puede provocar daños en el software y/o hardware de tu PC. Posiblemente tu equipo tiene instalado un software Antivirus, sólo que para ser efectivo, este debe estar siempre actualizado. Si tienes dudas con respecto al manejo y actualización de este software consulta la función de Ayuda del mismo.

Existen diversos productos Antivirus entre los cuales puedes escoger, algunos ejemplos de ellos son McAfee, Symantec (Norton) y Sophos.

También es posible obtener una versión gratuita de software Antivirus. Puedes utilizar el criterio de “free anti-virus” desde el portal de Google para obtener una lista de los disponibles y seleccionar alguno de ellos.

3. Uso de Firewall Personal

El Firewall personal es un programa que ayuda a proteger tu equipo y su contenido contra accesos no autorizados de extraños en Internet.

Cuando se configura en forma apropiada, detiene todo el tráfico no autorizado hacia y desde tu PC.

Hay varias opciones de Firewall personal para escoger. Los más comerciales son:

- Zone Labs: www.zonelabs.com
- Symantec: www.symantec.com.mx
- McAfee: www.mcafee.com/mx
- Computer Associates: www.ca.com/mx

4. Uso adecuado de passwords o contraseñas

Las contraseñas son la llave a la información de tus cuentas en línea, a cuentas de tiendas en línea y a una multitud de otras actividades en línea. Tu contraseña de Internet de HSBC, junto con tu identificador de Internet, te permiten acceder a tus cuentas bancarias. Por esta razón, tu contraseña debe ser única y debe estar muy bien protegida.

- **Manténlas para ti mismo.**
No compartas tus contraseñas con nadie.
- **Ser diferentes.**
Evita utilizar la misma contraseña para distintos servicios.
- **No ser personal.**
No te veas atraído a utilizar contraseñas que sean adivinadas fácilmente, por ejemplo, tu nombre, tu fecha de nacimiento, números telefónicos, nombres de mascotas.
- **Nunca las escribas.**
Si realmente necesitas registrar tus contraseñas, entonces utiliza un sistema de codificación, por ejemplo invierte algunas de las letras.



5. Uso de programas Anti Spyware

Spyware es un término utilizado para los programas que pueden alojarse en tu PC a fin de monitorear y registrar las actividades que realizas mientras navegas por Internet. El resultado de este monitoreo puede utilizarse tanto para fines comerciales como con propósitos maliciosos, por ejemplo para extraer información personal que hayas ingresado como contraseñas, números telefónicos, números de tarjetas de crédito así como claves de tus cuentas bancarias.

El Spyware es comúnmente cargado en los equipos sin el consentimiento del usuario y puede formar parte de una descarga gratuita de otro servicio, por ejemplo en un servicio que presume mejorar el rendimiento de tu PC.

Para eliminar el software Spyware que pudiera estar instalado en tu equipo, te recomendamos la instalación de software Anti-Spyware.

Los programas de seguridad anti-spyware que se encuentran actualmente disponibles incluyen a McAfee, Spybot Search and Destroy, AdAware, Spyware Eliminator, Spyware Doctor y Microsoft Windows Defender. Recomendamos firmemente que instales y utilices un producto Anti-Spyware con buena reputación para protegerte a ti mismo contra el Spyware en tu PC.

-  [Imprimir página](#)
-  [Enviar a un amigo](#)

© Copyright HSBC México 2008. Todos los Derechos Reservados. [Tarifas y Comisiones](#) | [Seguridad](#) | [Legales](#) | [Quejas y Sugerencias](#) | [IPAB](#)



- [Home](#)
- [English](#)
- [HSBC México](#)
- [Mapa del Sitio](#)
- [Bolsa de Trabajo](#)
- [Contacto](#)
- [HSBC en el Mundo](#)

Búsqueda



- [Banca Personal por Internet](#)

- [Personas](#)
- [HSBC Premier](#)
- [Banca Privada](#)
- [PYMES](#)
- [Empresas](#)
- [Banca Corporativa](#)
- [Banca de Gobierno](#)

- [Home](#)
- [Pie de página](#)
- [Seguridad](#)
- [El Idioma en Línea Descifrado](#)

- [Seguridad en Línea](#)
- [Las Cinco Reglas de Oro](#)
- [Tips de Seguridad](#)
- [El Idioma en Línea Descifrado](#)
- [Banca Segura por Internet](#)
- [Otros Fraudes en Línea](#)
- [Phishing](#)
- [Recursos Adicionales](#)
- [Preguntas Frecuentes](#)

El Idioma en Línea Descifrado

A – C

Anti-Spyware Program (Programa Anti-Spyware). Los programas anti-spyware están diseñados para proteger tu computadora de spyware (ve la definición de éste en 'S') y son útiles en asegurar que tu computadora y detalles personales permanezcan seguros.

Antivirus Software (Programa Antivirus). Los programas antivirus están diseñados para detectar virus entrantes conocidos (típicamente por correo electrónico) y para prevenir que éstos infecten la PC. Los nuevos virus pueden distribirse muy rápidamente, por lo que debes asegurarte que tu programa

antivirus esté siempre ejecutándose y sea actualizado con regularidad – al menos semanalmente. Algunos recursos populares de programas de protección antivirus son McAfee, Symantec (Norton) y Sophos. Las personas privadas también pueden descargar versiones gratuitas de este tipo de programas desde Internet.

Broadband (Banda Ancha). Es un método de alta velocidad de conectarse al Internet, más rápido que un modem tradicional. Aunque el conservar la conexión a Internet no implica costos adicionales, una buena práctica es desconectarse de Internet cuando no se esté utilizando, ya que esto ayuda a reducir la exposición a riesgos.

Browsers (Explorador). Un browser (explorador) es un programa que provee una forma de ver páginas web. Los más populares son Microsoft® Internet Explorer , Netscape® Navigator y Mozilla Firefox®.

Cookies. Las Cookies son pequeños archivos guardados en el disco duro de una computadora. Las Cookies generalmente no hacen daño y son utilizadas para reconocer a un usuario de modo que pueda recibir una experiencia más consistente en un sitio web en particular. Las Cookies pueden contener información sobre tus preferencias, lo que permite la personalización de un sitio para su uso.

- [Regresar](#)

D – F

Digital Certificates (Certificados Digitales). Un certificado digital es una tarjeta electrónica de identificación que ayuda a establecer tu identidad cuando realizas negocios vía Internet. Dichos certificados pueden estar basados en un browser (“Soft Certificates”) o estar integrados en una smart card (“Hard token”) y ser utilizados con lectores especiales de tarjetas.

Encryption (Cifrado). El cifrado convierte tus datos a una forma codificada antes de que sean enviados a través de Internet, deteniendo a usuarios no autorizados de leer la información. En HSBC, utilizamos cifrado SSL a 128 bits, lo cual es aceptado como el nivel estándar de la industria. Tú sabes que tu sesión está en un ambiente ‘cifrado’ seguro cuando observas https:// en la dirección web, y/o cuando ves el símbolo de candado cerrado en la esquina inferior derecha de tu browser.

Filename extensions (Extensiones de nombres de archivos). Una extensión de nombre de archivo es simplemente las últimas tres letras (o números) del nombre completo del archivo. Normalmente son utilizadas por el sistema operativo para asociar un programa con un archivo particular.

Firewall. Un firewall es un pequeño programa que ayuda a proteger tu computadora y su contenido de invasores en Internet o en la red. Cuando se instala apropiadamente, previene tráfico no autorizado hacia y desde tu PC. Existen muchos programas efectivos de donde escoger. Algunos ejemplos comerciales comunes son de Zone Labs , Symantec (Norton), McAfee y Computer Associates. En muchos casos existe una versión gratuita del programa comercial, la cual es libre de cargo para el uso personal de los usuarios.

- [Regresar](#)

I – P

Identity Theft (Robo de Identidad). El robo de identidad es un crimen en el que un defraudador obtiene piezas clave de información personal, tal como la fecha de nacimiento, los detalles bancarios, o números de licencia de conducir, para hacerse pasar por alguien más. La información personal descubierta es entonces utilizada ilegalmente para solicitar créditos, comprar bienes y servicios, o acceder a cuentas bancarias. Los defraudadores comúnmente toman ventaja de la inclinación natural de las personas de escoger contraseñas que son significativas para ellas, y que son fácilmente adivinables (nombre de los hijos, nombres de mascotas, domicilios, o fechas de nacimiento).

Keystroke Capturing/Logging (Captura o Grabado de pulsaciones de teclado). Cualquier cosa que teclees en una computadora puede ser capturado y almacenado. Tal actividad encubierta puede llevarse a cabo a través de dispositivos de hardware conectados a tu computadora o por programas que se ejecutan casi de manera invisible en la máquina. El Keystroke logging es usado frecuentemente por

defraudadores para capturar detalles personales incluyendo contraseñas. Algunos virus recientes son capaces de instalar tal tipo de programas sin el conocimiento del usuario. El riesgo de encontrar tales keystroke loggings es mayor en las PCs que son compartidas por un número de usuarios, como aquellas de los Internet cafés. Ejecutar un programa anti-spyware podría revelar la presencia de tales programas en tu PC. Los usuarios pueden descargar programas anti-spyware gratuitos.

Plug-in. Un Plug-in es un modulo de un programa que adiciona funcionalidad específica al browser. Por ejemplo, los plug-ins para Netscape Navigator y para Internet Explorer permiten a los browsers ejecutar varios tipos de audio y mensajes en vídeo o ver archivos PDF del popular Adobe® Acrobat®.

Privacy Policies (Políticas de Privacidad). Actualmente, muchas compañías son obligadas a publicar una Política de Privacidad para proveer a los clientes los detalles de cómo la compañía conserva la información privada, cómo esta información es compartida y porqué es recolectada. Una buena práctica es leer la Política de Privacidad de la compañía con la que pudieras tener una cuenta o tratos financieros. La mayoría de las Políticas de Privacidad también explican cómo los clientes pueden solicitar que se remueva su nombre o datos particulares de una lista promocional de correo electrónico.

- [Regresar](#)

S

Secure Sessions (Sesiones Seguras). Cuando ingresas a la Banca por Internet, se dice que estás en una “sesión segura”. La tecnología SSL se utiliza en tu sesión de Banca por Internet para encriptar la información antes de que abandone tu computadora, a fin de asegurar que nadie más pueda leerla. Dependiendo de la configuración en tu browser, una ventana emergente puede mostrarse para notificarte que estarás ingresando a una página segura. Reconocerás una página ‘segura’ cuando veas ‘https://’ antepuesto a la dirección web. También verás un símbolo de candado cerrado en la esquina inferior derecha de tu browser.

SSL. El protocolo Secure Socket Layer (SSL) provee un alto nivel de seguridad para las comunicaciones de Internet. El SSL provee una sesión de comunicaciones cifrada entre tu browser y un servidor web. El SSL ayuda a asegurar que información sensitiva (e.g., números de tarjeta de crédito, estados de cuenta, y otros datos financieros y personales) que es enviada sobre el Internet entre tu browser y el servidor web, permanezca confidencial durante las transacciones en línea.

Security Vulnerabilities (Vulnerabilidades de Seguridad). Los hoyos/gusanos de seguridad, son fallas, defectos o errores de programación. Estos pueden ser explotados por usuarios no autorizados a acceder a redes de computadoras o a servidores web desde Internet. Conforme estas vulnerabilidades son conocidas, los fabricantes de programas desarrollan ‘parches’, ‘fixes’ o ‘actualizaciones’ que puedes descargar para arreglar los problemas.

Session Time-out. Esto es una desconexión automática, por motivos de seguridad, de cualquier sesión segura después de un periodo de inactividad del servidor. Esto puede ocurrir incluso si te encuentras tecleando algo en una página o en un campo de datos. El evento es provocado por no haber comunicación con nuestros servidores, mas no por la actividad del teclado o del Mouse. Todos nuestros servicios de Banca por Internet tienen esta protección.

Spam. A menudo, se llama Spam a los mensajes de correo electrónico no deseados que ofrecen productos y servicios con dudoso beneficio. Se encuentran disponibles varios tipos de programas anti-spam, aunque la primera línea de defensa pudiera ser tu propio proveedor de servicios de Internet, muchos de los cuales ofrecen servicios de filtrado de spam.

Spyware. Estos son programas/archivos que pueden residir ya en tu PC. Estos programas comúnmente llegan como componentes encubiertos de programas ‘gratuitos’. El spyware supervisa el uso de la web y lo reporta a compañías auténticas, que pueden después vender las estadísticas recopiladas. El spyware es relativamente benigno, aunque en su forma más extrema puede incluir programas que graben las pulsaciones del teclado y llevar a cabo espionaje virtual de toda la actividad en tu PC.

- [Regresar](#)



T – W

Trojan Horse (Caballo de Troya). Cualquier programa aparentemente legítimo que contiene la carga de otro destructivo no deseado. Típicamente el segundo es un virus utilizado por los hackers para obtener acceso no autorizado a los sistemas de computadoras.

Virus. Un programa de computadora diseñado para replicarse asimismo, copiándose en otros programas que se encuentran en una computadora. Pudiera ser benigno, pero usualmente tiene impactos negativos, tales como alentar una PC o corromper su memoria y archivos. Los virus hoy en día son esparcidos principalmente por correo electrónico, así como por los servicios para compartir archivos. Diariamente se descubren nuevos virus.

Virus Definition File. Este es un archivo utilizado por los programas antivirus para identificar virus específicos, gusanos y caballos de troya. Por esta razón, debes descargar regularmente la última versión de tu proveedor del software, o configurar tu programa para que lo realice automáticamente.

Worm (gusano). Es un programa malicioso que se replica asimismo hasta llenar todo el espacio de almacenamiento en un disco o en una red. Dichos gusanos pueden consumir el tiempo del computador, el espacio, y la velocidad cuando se replican con la intención maliciosa de alentar o tirar los servidores web, e interrumpir el uso de Internet.

- [Regresar](#)
-  [Imprimir página](#)
-  [Enviar a un amigo](#)

© Copyright HSBC México 2008. Todos los Derechos Reservados. [Tarifas y Comisiones](#) | [Seguridad](#) | [Legales](#) | [Quejas y Sugerencias](#) | [IPAB](#)