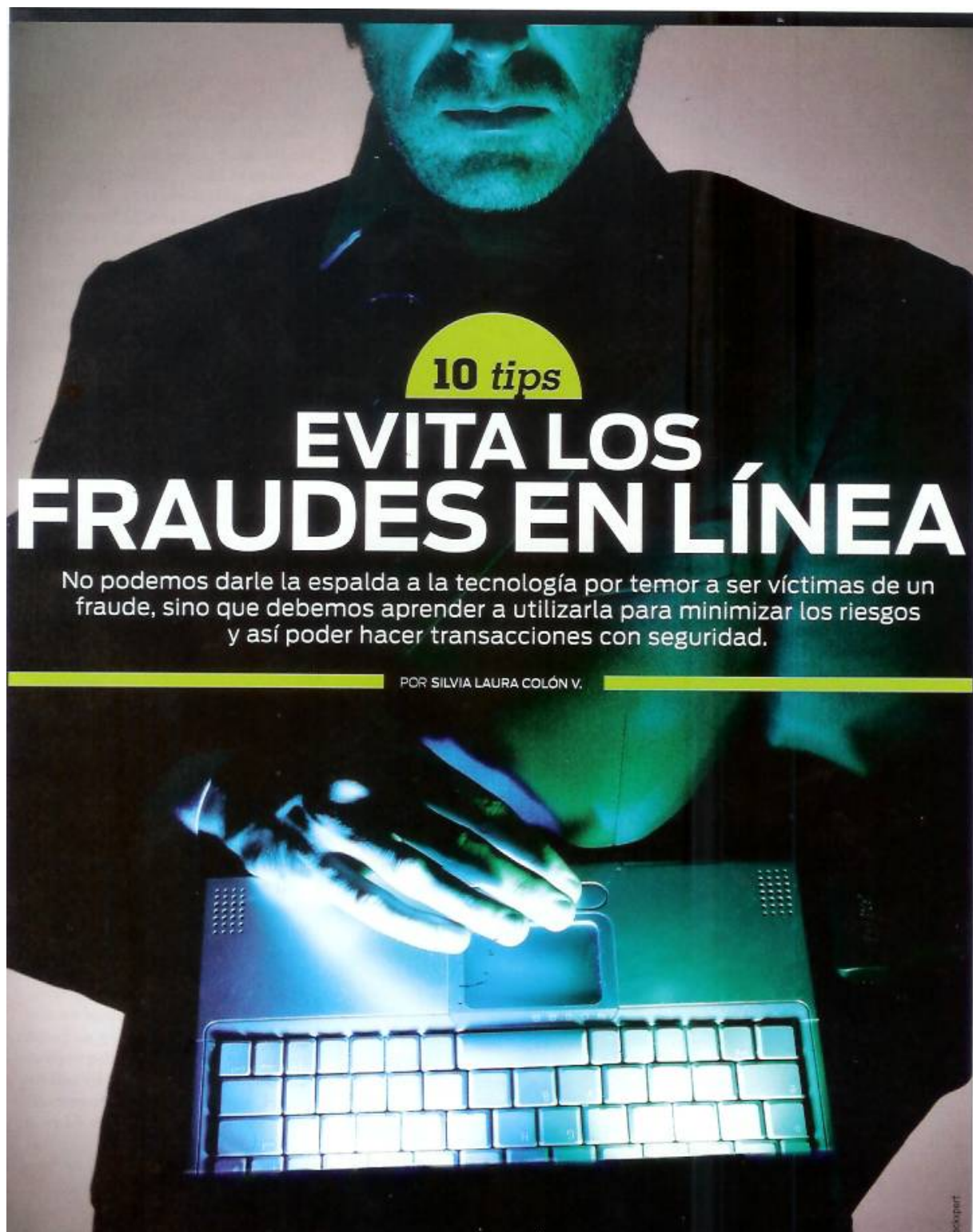


Fecha:	2009-03-04	Sección:	FINANZAS PERSONALES	Página:	22 A 25
Columnista:	SILVIA LAURA COLON		Cliente:	BURÓ DE CRÉDITO	

## INVERSIONISTA



**10 tips**

# EVITA LOS FRAUDES EN LÍNEA

No podemos darle la espalda a la tecnología por temor a ser víctimas de un fraude, sino que debemos aprender a utilizarla para minimizar los riesgos y así poder hacer transacciones con seguridad.

POR SILVIA LAURA COLÓN V.

© 2009 part



**L**A FORMA en que operan los estafadores en línea es engañando a los usuarios con ofertas en correos electrónicos y sitios fraudulentos, para que proporcionen información confidencial, como el número de tarjeta de crédito o débito y el de identificación personal (NIP). Este tipo de ataque es conocido como *phishing*. Asimismo, es común el robo de identidades para cometer todo tipo de ilícitos. Son ataques a gran escala, ya que se dirigen a miles de víctimas a la vez.

De acuerdo con la Asociación Mexicana de Internet (AMIPCI), en México hay más de 20 millones de internautas, y el comercio electrónico tiene un crecimiento promedio anual de 60%; en tanto que la banca en línea crece más rápido, con 70% al año, lo que significa que

hay más de 4 millones de usuarios en el país. Sin embargo, un estudio de la misma AMIPCI, revela que sólo 15.6% de las personas que cuentan con servicios bancarios utiliza algún servicio de banca en línea. Directivos de la asociación puntualizan que el bajo porcentaje se debe a la percepción de inseguridad que los usuarios tienen de este medio. De hecho, 43% de los encuestados creen que se requiere más seguridad para realizar transacciones en el ciberespacio.

Un informe de S21sec, compañía especializada en servicios de seguridad informática, revela que en América Latina sólo en el primer semestre de 2008 se registró un aumento de 135% de fraudes en línea respecto a todo 2007. Para evitar que seas víctima de algún fraude *online* te sugerimos seguir estas sencillas recomendaciones.

## 1 EVITA ENTRAR A LOTERÍAS Y COMPRAS DE "SÚPER OFERTAS"

El envío de millones de mensajes tiene un costo extremadamente bajo para un *spammer*, y si logra al menos que sólo una de 1 millón de personas compre algo, habrá logrado su objetivo de obtener ganancias. Por eso debes

tener presente que ellos se dedican a hacer dinero a través de la emisión de esos mensajes.

El *phishing* se puede presentar de diversas maneras. Una de ellas es a través de loterías que se presentan como ventanas emergentes (*pop-ups*) al visitar un *web-site*, donde te notifican que has ganado un premio por

ser el visitante 9,999,999 de ese sitio, por ejemplo. Al responder a este mensaje te solicitan tus datos bancarios diciéndote que es para depositarte el "premio".

Hay casos en los que incluso te solicitan que deposites dinero por concepto de gastos administrativos, a una cuenta para poder cobrar el premio completo.

## 2 EVITA HACER CLIC EN LOS CORREOS SPAM O LIGAS DESCONOCIDAS

No abras correos de procedencia dudosa, ni descargues archivos adjuntos de fuentes desconocidas. Debes tomar en cuenta que puedes recibir *links* en *e-mails*, mensajes instantáneos y archivos adjuntos (fotos, videos y de audio) que pueden ser maliciosos. Si una institución financiera te envía un correo electrónico relacionado con un supuesto problema urgente u otro problema relacionado con tu cuenta, es recomendable utilizar el número telefónico impreso en tu contrato para responderle y de esta manera comprobar su autenticidad.

Si respondes a un correo *spam*, incluso para solicitar que te eliminen de esa base de datos, confirmas al remitente que logró llegar a una dirección de correo válida y, por lo tanto, tu bandeja de entrada se convertirá en receptora de más correos de este tipo.

## 3 SUSCRÍBETE A UN SISTEMA DE PROTECCIÓN CONTRA ROBO DE IDENTIDAD

La mayoría de estos sistemas emiten reportes de crédito personales para que revises el historial de tus movimientos y verifiques si éstos son correctos.

Casi todos los servicios contra robo de identidad te permiten examinar tus operaciones crediticias a diario, y en caso de que exista alguna actividad sospechosa se te notifica de inmediato. También otorgan asistencia para corregir errores en tus registros, además de la cobertura contra fraudes.

El Buró de Crédito ofrece este servicio bajo el nombre BC Informa, que envía una notificación al usuario sobre cambios recientes en su expediente del historial crediticio. Este servicio tiene un costo de \$120 pesos anuales, más IVA. En caso de que no reconozcas alguno de estos movimientos, podrás tomar una acción inmediata para corregir la información. Si requieres contratarlo consulta:

[www.burodecredito.com.mx](http://www.burodecredito.com.mx)

**LOS SISTEMAS DE PROTECCIÓN TE NOTIFICAN SOBRE LOS MOVIMIENTOS QUE SE REALIZAN EN TUS CUENTAS**

### PROTECCIÓN INSUFICIENTE

Humberto Ayala Herrera, especialista en fraudes electrónicos y profesor de la Universidad Anáhuac del Sur, asegura que "ante la insuficiencia de la unidad especializada en delitos cometidos en internet, es prioritario contar con una legislación eficiente para combatir los delitos cibernéticos, donde se establezcan las diferentes conductas que se puedan desplegar para la realización de todo tipo de acceso no autorizado a sistemas o equipos informáticos, siendo urgente una clara definición de los conceptos que lo conforman para la oportuna prevención de este tipo de ilícitos".



>>>

## 4 NO CAIGAS EN TRAMPAS COMO EL SCAM

El *scam* es un fraude por medio de correos electrónicos de anuncios de trabajo en la *web*, *chats*, etcétera, donde empresas ficticias te ofrecen trabajar cómodamente desde casa y cobrando beneficios muy altos. Éstas son sus principales características:

- Siempre piden que tengas o abras una cuenta bancaria
- El trabajo consiste en recibir transferencias bancarias a tu cuenta bancaria y enviarlo a otros países por medio de empresas tipo Western Union o Money Gram

Las frases más comunes que usan para captar a víctimas son:

- ¿Quieres trabajar cómodamente desde casa?
- ¿Estás desempleado y con ganas de trabajar?
- ¿Quieres obtener ingresos extras?

Luogo, envían un contrato (falso) para hacer más creíble la oferta. Una vez obtenidos los datos de la víctima, si ésta no colabora, es amenazada.

## 5 UTILIZA TARJETAS DE CRÉDITO DE VIGENCIA LIMITADA O PARA CARGOS ÚNICOS EN LÍNEA

Siempre que tengas dudas respecto a algún sitio para realizar transacciones bancarias o compras *online*, utiliza una tarjeta de crédito secundaria, temporal o con vigencia de una sola transacción. De esta manera te expones menos a los abusos de los defraudadores en línea. La gran mayoría de las instituciones bancarias tienen estos productos disponibles.



### MERCADO NEGRO

- La identidad completa de un usuario puede valer entre \$1 y \$15 dólares
- Un correo electrónico relacionado con procesos para almacenar una página apócrifa se cotiza entre \$2.5 y \$50 dólares a la semana
- Las direcciones de correo electrónico pueden costar entre \$0.83 y \$10 dólares
- Una contraseña de e-mail puede cotizarse hasta en \$30 dólares

**SI UN WEBSITE TIENE NOTORIAS FALTAS DE ORTOGRAFÍA, ES PROBABLE QUE SEA FRAUDULENTO**

## 6 INSTALA ANTIVIRUS Y FIREWALLS PERSONALES

“Los códigos maliciosos (o virus) están siendo diseñados por personas que quieren obtener beneficios económicos directos con el manejo de sus conexiones en internet –señala Rafael García, gerente regional de productos para México y América Latina de Symantec-. De los principales códigos maliciosos diseñados, más del 20% están hechos para obtener información confidencial de los usuarios”.

De acuerdo con Trend Micro, compañía proveedora de soluciones de seguridad en aplicaciones *online*, las amenazas de internet aumentaron casi 2,000% desde 2005 a la fecha. Según los analistas de amenazas de esta empresa, más del 50% de los códigos maliciosos más peligrosos han sido

descargados accidentalmente por usuarios que navegan en sitios *web* desconocidos o peligrosos.

Los códigos maliciosos pueden tener múltiples objetivos como:

- **Extenderse por la computadora y otras computadoras en una red o por internet**
- **Robar información y claves de identificación personal**
- **Eliminar archivos e incluso formatear el disco duro**
- **Mostrar publicidad invasiva**

Estos ataques se pueden combatir con un *Firewall* personal, que bloquea la comunicación cuando se sale de los cauces normales establecidos por el usuario.

## 7 UTILIZA FILTROS ANTISPAM PARA FRENAR LOS VIRUS INFORMÁTICOS

Recuerda que tu proveedor de internet (ISP) debe contar con filtros *antispam*, *antivirus*, *antispyware* y *antimalware* para evitar que a tu computadora lleguen correos *spam*, ya que estos paquetes de datos, por lo general están relacionados con la transmisión de virus informáticos. Los correos *spam* pueden incluir vínculos a sitios de internet habilitados con algún *spyware*, que son programas que recopilan datos sobre tus hábitos de navegación, preferencias y gustos del usuario. También pueden incluir vínculos con *malware* (programas maliciosos), que son programas que pretenden dañar a tu computadora, porque tienen la capacidad de provocar la pérdida de datos o de productividad.

## 8 NO UTILICES LUGARES PÚBLICOS PARA HACER TRANSACCIONES EN LÍNEA

No ingreses tu información de contacto personal o de tu cuenta bancaria cuando te conectes en cafés, aeropuertos, etcétera. Utiliza estos lugares para buscar información, pero no para hacer compras o transacciones bancarias.

Pregunta por el proveedor de los servicios de acceso inalámbrico en los lugares públicos, ya que puede haber *evil twins* (mellizos maléficos) que son redes inalámbricas falsas configuradas por delincuentes informáticos, que piden información personal y de tarjeta de crédito con el supuesto propósito de registrar tu identificación para el acceso.

Estas redes también se conocen como *honey pots* (ollas de miel).

**EL 22% DE LOS ILÍCITOS ONLINE EN EL MUNDO SON EL ROBO DE INFORMACIÓN A CUENTAS BANCARIAS, CUYO COSTO VA DE \$10 A \$1.000 DÓLARES POR EVENTO**

## 9 ASEGÚRATE DE QUE ENTRAS A UN SITIO SEGURO

Cuando ingreses información confidencial, asegúrate de hacerlo en un sitio confiable. Las direcciones de los sitios seguros tienen "https" (fíjate en la "s") al principio; además, en la parte inferior derecha de tu explorador de internet podrás ver un candado de seguridad. Busca errores ortográficos obvios, pues los criminales son mejores programando computadoras que escribiendo.

También sospecha de todo correo que contenga pedidos urgentes de información personal. Los estafadores a menudo se valen de amenazas y de supuestas oportunidades para obtener información.

## 10 UTILIZA LAS REDES SOCIALES A TU FAVOR

La información que se encuentra en las redes sociales virtuales como MySpace, Facebook, Hi5 y Orkut, entre otras, constituye una fuente invaluable para las organizaciones de crimen cibernético. Por ello es de suma importancia mantener como confidencial tu perfil, es decir, que sólo tus contactos puedan acceder a él. También puedes recurrir a un *nick* o nombre clave que te identifique dentro de este espacio.

De acuerdo con Rafael García, de Symantec, los ataques generados a través de los conocidos que están en esas cuentas se dan en un marco de confianza en el que se obtiene información para robar la identidad. "Si una persona recibe un correo de alguien que pertenece a su red social, no va a dudar en hacer clic a la liga que se encuentra dentro su correo electrónico. Este *link* lleva a un sitio apócrifo, donde el generador de este código toma el control".



### ¿CÓMO HACER COMPRAS POR INTERNET?

Realiza tus compras con empresas conocidas o instituciones financieras de confianza, comprueba los datos que ellas mismas ofrecen en sus páginas y haz una búsqueda en internet sobre esa compañía.

• Bay porciona algunas sugerencias de seguridad:

• **No envíes transferencias a través de empresas como MoneyGram o Western Union. No se recomiendan los pagos por transferencia instantánea entre personas desconocidas.**

• **Contacta con el vendedor cuando se confirme la transacción. Una buena comunicación permite aclarar las condiciones de pago y de entrega.**

• **Utiliza las formas de pago que te ofrezcan mayores garantías.**

• **Si vas a comprar un artículo de gran valor, o si deseas inspeccionar el bien antes de realizar el pago, usa un servicio de depósito de garantía, el cual te protege en caso de que el artículo no llegue o no reúna las condiciones acordadas.**

Aquí hay algunas recomendaciones básicas para establecer tu identidad cibernética alejada de las tentaciones de *hackers* y delincuentes cibernéticos.

- 1 **Mantén tu información confidencial fuera de las comunidades de internet**
- 2 **Tu identidad dentro de una red social no debe ser asociada con tu correo electrónico personal o laboral**
- 3 **El error más común es llenar con precisión la información que nos piden al registrarnos. Sólo proporciona información general y que no se asocie directamente a ti**
- 4 **Lo primero que asocia un hacker con tus contraseñas personales es tu fecha de nacimiento o tu RFC, y posteriormente busca**

**información específica en las iniciales de tu nombre completo**

- 5 **Nunca proporciones información valiosa como tu número telefónico, correo electrónico o dirección física de donde vives. Cuando te des de alta en una red social piensa que estás publicando información que en la vida diaria nunca darías a un desconocido. Recuerda que en internet todos somos totalmente anónimos y no sabemos en realidad quien está al otro lado de la pantalla. De otra forma tu información será pública y de libre consulta, no sólo para los *hackers* profesionales sino personas que podrían aprovechar tu información para extorsionarte, molestarte o acosarte.**



