CONSEJOS PRÁCTICOS DE SEGURIDAD PARA PROTEGER LOS DATOS BANCARIOS AL COMPRAR EN LÍNEA

Israel Andrade Canales

ciberseguridad

numero-28

Uno de los atractivos más importantes de Internet es el comercio electrónico. En México, esta actividad aumentó su valor de mercado un 59% de 2014 a 2015, como lo demuestran estudios recientes sobre los hábitos de los usuarios de Internet en nuestro país (AMIPCI, 2016). Ya sea desde el celular o la PC, el internauta cuenta con una gran variedad de tiendas y métodos de pago, pero al mismo tiempo, de riesgos informáticos.

Lo anterior ha provocado que una de las resistencias más importantes al comercio electrónico esté relacionada con la seguridad informática (AMIPCI, 2016; Pagnotta 2016). Sin embargo, hoy el usuario tiene al alcance varios mecanismos que pueden ayudarle a tener más confianza en las tecnologías de comercio electrónico: desde buenas prácticas de seguridad hasta tecnologías que protegen sus datos bancarios.

En este artículo se presentan un conjunto de consejos, buenas prácticas y herramientas que reducen el riesgo de robo de información bancaria durante el pago de bienes y servicios en línea, y al mismo tiempo, se explica al usuario el porqué de dichos consejos.

Para lograr lo anterior, se describe de manera sencilla el proceso de compra en línea, y durante cada etapa se mencionan los principales riesgos de los datos bancarios y las mejores prácticas que puede emplear el usuario del comercio electrónico.

PROTECCIÓN DE LOS DATOS BANCARIOS

La información más importante durante la compra de productos y servicios por Internet son los datos

que hacen posible el pago en línea. En México, los métodos de pago más populares durante 2016 fueron Paypal y las tarjetas de crédito y débito (AMIPCI, 2016). Los datos bancarios de interés en estos tres métodos son (Ali, Arief, Emms, & van Moorsel, 2016):

- Las credenciales de acceso a las carteras digitales como Paypal.
- El número de tarjeta bancaria, el cual es una cifra única de 16 dígitos que vincula una tarjeta bancaria con el tarjetahabiente.
- El código verificador de tarjeta (CVV, por sus siglas en inglés), el cual es un número de tres dígitos impreso en el reverso de la tarjeta. Este dato se supone secreto y no debe ser almacenado por ningún sistema de compra en línea legítimo.
- La fecha de vencimiento de la tarjeta de crédito/débito.
- El código postal que registró el tarjetahabiente.

La información mencionada anteriormente es el objetivo principal que tiene un defraudador electrónico, el cual intentará obtenerla desde cualquier lugar donde se ingrese, almacene, procese y transfiera.

¿CÓMO PROTEGER LOS DATOS BANCARIOS MIENTRAS ESTÁN EN TU COMPUTADORA?

Al comprar productos o servicios por Internet requerimos varias tecnologías que se interconectan para realizar las mismas acciones que un cliente realizaría en una tienda física, esto es: solicitar el producto o servicio y realizar el pago.

De manera simplificada, para que un cliente indique a la tienda lo que desea comprar requerirá de un programa que será su interlocutor con la tienda: en los equipos de escritorio, el navegador web; y en los dispositivos móviles, la aplicación de la tienda.

Por lo anterior, el sistema operativo de tu dispositivo, el navegador web y las aplicaciones son herramientas clave para una compra menos riesgosa y su buen funcionamiento también es tu responsabilidad. Por ello:

1. **Nunca instales software pirata, de escasa reputación o de fuentes no confiables en los dispositivos donde realices las compras, ¡estos deben ser de tu absoluta confianza!** Tu navegador cuenta con mecanismos para identificar si los sitios que visitas son confiables y si modificas su configuración, podrías afectar esta protección.
2. Es muy importante actualizar el sistema operativo, tu navegador web y la aplicación de la tienda. De esta manera reparas las posibles debilidades de este software, además de agregarle nuevas funcionalidades que mejoren la experiencia de compra.

Adicionalmente, no debes realizar compras desde dispositivos en los cuales no tengas pleno control o que varios usuarios comparten. Existe software capaz de registrar lo que tecleas o envías por Internet.

En este sentido:

3. No utilices computadoras de sitios como salas de Internet públicas o de renta. Del mismo modo, no te conectes desde redes públicas o compartidas, ya que la red informática debe ser de plena confianza. Esto ayudará a reducir los riesgos asociados a la intercepción de los datos bancarios sobre la red.

Finalmente, si almacenas tus datos bancarios en tu computadora o dispositivo móvil, asegúrate de lo siguiente:

4. Utiliza llaveros[1] que cifren tus datos bancarios y evita que estos se encuentren almacenados en texto claro. Si los datos bancarios están en tu dispositivo portátil, asegura que tu dispositivo cuente con mecanismos de autenticación. **Debes estar consciente del lugar donde tienes almacenados tus datos bancarios y asegurarte de reducir estos sitios al mínimo necesario.**

¿CÓMO PROTEGER TUS DATOS BANCARIOS CUANDO ESTÁN EN LA TIENDA DIGITAL?

Hoy en día, la mayoría de los negocios apuestan al comercio electrónico (López, 2016) y por ello existe una gran variedad de tiendas en línea. No todas son confiables. Hay sitios creados intencionalmente para la obtención de los datos bancarios a través del engaño, y por tal motivo, la tienda donde realizas la compra debe tener una buena reputación; por lo anterior se recomienda hacer un poco de investigación sobre la tienda antes de comprar:

1. Verifica que la URL del comercio sea legítima. También revisa la fecha de creación del sitio web;

prefiere aquellos que tengan algún tiempo considerable en el mercado.

2. Una tienda electrónica de buena reputación invertirá en su plataforma de venta, por lo tanto, si el sitio que visitas es de poca calidad, con contenido desactualizado o generado automáticamente, evítalo.

Sin embargo, lo anterior no es suficiente. Los ataques informáticos ocurren en casi cualquier tipo de servicio electrónico (correo electrónico, almacenamiento en la nube, comercio electrónico, entre otros). Empresas importantes como Yahoo! y Dropbox han sufrido ataques informáticos escandalosos (puedes consultar aquí algunos casos). Por tal motivo, no podemos confiar en que los datos que almacenan serán resguardados de manera segura.

3. Preferentemente, elige comercios que no almacenen los datos de tu tarjeta de crédito o débito (lo anterior puedes consultarlo en las políticas de privacidad del sitio), o bien, prefiere las tiendas que cuenten con sistemas de pago administrado por terceros de confianza (como el caso de Paypal y otras carteras virtuales[2]).

Otra opción interesante es contar con una tarjeta virtual, la cual es una tarjeta de crédito o débito ofrecida por algunos bancos, cuyo CVV u otro dato bancario, cambia en cada transacción, haciéndola temporal y de un solo uso (Rubenking, 2014). De esta manera, si la tienda es comprometida, tus datos bancarios no pueden ser aprovechados por cibercriminales.

En un reciente estudio realizado por un grupo de investigadores de la Universidad de Newcastle se analizó la seguridad de los métodos y redes de pago. Se descubrió que es muy factible realizar un ataque coordinado en diversas tiendas electrónicas **para deducir el CVV de un número de tarjeta a través de técnicas de prueba y error** (Ali, Arief, Emms, & van Moorsel, 2016). Por lo tanto:

4. Las herramientas más útiles en la realización del pago son las que reducen el tiempo de validación, como la funcionalidad que ofrecen algunos bancos para activar y desactivar temporalmente las tarjetas de crédito; así como los mecanismos para variar dinámicamente los datos bancarios por medio de tarjetas virtuales.

CONCLUSIONES

De la misma manera que tomamos medidas de seguridad para comprar en una tienda física, es necesario hacerlo en línea. En este artículo se presentaron algunas recomendaciones que los usuarios pueden seguir al pagar productos o servicios por Internet. Estos consejos de seguridad van desde buenas prácticas en el uso de dispositivos electrónicos, hasta el manejo menos riesgoso de los datos bancarios durante el pago mediante tecnologías de seguridad bancaria.

La adopción de mejores prácticas durante la compra por Internet reducirá el riesgo de ser víctima de fraudes por esta vía , lo que favorecerá la confianza y el uso frecuente de las tecnologías de comercio

electrónico.

REFERENCIAS

- Ali, M. A., Arief, B., Emms, M., & van Moorsel, A. (2016). *Ne?.* IEEE Security & Privacy.
- Asociación Mexicana de Internet (AMIPCI). (2016). Estudio AMIPCI de Comercio Electrónico en México 2016, Asociación Mexicana de Internet. *Asociación de Internet*. Recuperado de https://www.asociaciondeInternet.mx/es/estudios
- López, J. (7 de abril de 2016). Sitios de e-commerce en México aumentan y abandonan tiendas físicas. *El Economista*. Recuperado de http://www.elfinanciero.com.mx/tech/aumentan-sitios-de-e-commerce-que-estan-dejando-el-mundo-offline.html
- Pagnota, S. (28 de diciembre de 2016). El 41,3% cree que las compras online son “altamente peligrosas”. *WeLiveSecurity en Español*. Recuperado de: http://www.welivesecurity.com/la-es/2016/12/28/compras-online-peligrosas/
- Rubenking, N. (17 de septiembre de 2014). 5 Things You Should Know About Virtual Credit Cards. *PC Magazine*. Recuperado de: http://www.pcmag.com/article2/0,2817,2468612,00.asp

MÁS INFORMACIÓN SOBRE LAS TARJETAS VIRTUALES

Algunos productos bancarios que ofrecen tarjetas virtuales son Pago móvil de Banorte, Bancomer Wallet de BBVA Bancomer y Entropay. Para mayor información se invita al lector a seguir los sitios electrónicos de dichos productos.

- https://www.banorte.com/cms/banorte/banortemovil/#!/pagomovil
- http://bancadigital.bancomer.com/wallet/
- https://www.entropay.com/

---

[1] Un llavero electrónico o gestor de contraseñas es un programa que almacena contraseñas u otros datos sensibles, los cuales protege con algoritmos criptográficos. Se recomienda la utilización de estas herramientas en lugar de almacenar los datos sensibles en archivos de texto plano. Algunos gestores de contraseñas populares son KeePass y LastPass, este último es un servicio ofrecido en línea y accesible desde dispositivos móviles.

[2] Las carteras virtuales son servicios electrónicos que concentran los datos de tarjetas de créditos o débito y realizan el cobro de productos o servicios evitando que los datos bancarios sean almacenados por tiendas en línea. Algunos ejemplos son Google Wallet, Apple Pay, Paypal, entre otros.
