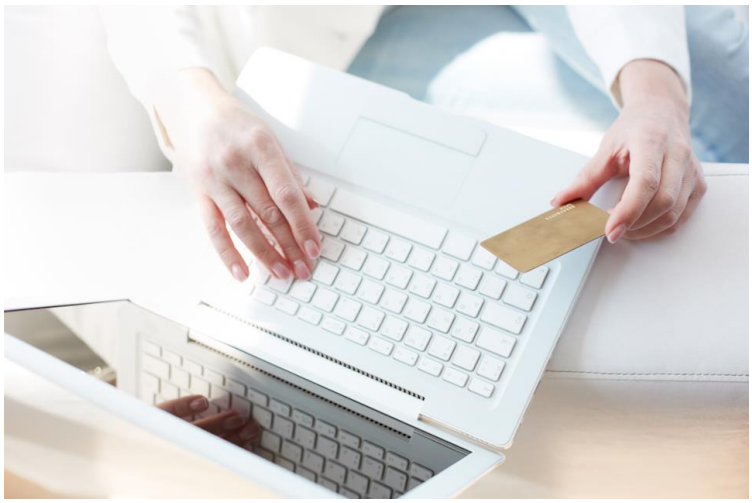
Reconozca el fraude en su tarjeta de crédito

Por: Yoivy Guerra
Analista Financiera de Servicio de Atención al Cliente Bancario de la Superintendencia de Bancos de Panamá

Seguramente, en algún momento, hemos escuchado sobre el fraude en las tarjetas, ya sea por las noticias o porque algún conocido o familiar haya sido víctima de él.



Por lo general, las tarjetas son vulneradas, con el propósito de crear tarjetas falsas con el número de cuenta de la víctima y efectuar cargos no autorizados a la tarjeta de crédito de la misma.

El fraude de tarjeta de crédito puede ocurrir cuando el consumidor revela el número de su tarjeta de crédito a un desconocido, la pierde o le roban las tarjetas, con el copiado de la banda magnética, cuando los empleados de una empresa hacen una reproducción de la tarjeta o del número de la tarjeta del cliente.

Cabe señalar que esta tarea era mucho más fácil, con el sistema de banda magnética, de allí que actualmente en nuestro país exista como regulación, el Acuerdo 6-2011 emitido por la Superintendencia de Bancos, por medio del cual se dictamina el cambio de este sistema en nuestro centro bancario por las tarjetas de chip, que proveen mayor seguridad a nuestros datos y, por consiguiente, a nuestras cuentas bancarias.

Por otra parte, debemos estar claros que también puede suscitarse el fraude en nuestras cuentas, entre otras formas delictivas, a través del *phishing* y robo de identidad, por lo que es importante que conozcamos un poco más sobre las modalidades utilizadas para el fraude en nuestras cuentas y herramientas bancarias, porque de esta forma podemos igualmente tomar las previsiones para evitar ser presa de malhechores.

A continuación, describimos un poco más, los tipos de fraudes más comunes.

Robo de identidad
Es el uso fraudulento de la información personal de alguien, como su número de

cédula, seguro social o fecha de nacimiento, etc., para cometer fraude financiero.

Los ladrones de identidad pueden dañar e incomodar a sus víctimas usando sus nombres y demás información personal para cometer delitos, abrir nuevas cuentas de crédito y obtener acceso a crédito y cuentas de banco existentes.

Aunque las víctimas del robo de identidad no son consideradas responsables de los delitos, les cuesta mucho trabajo probar el fraude y limpiar el caos financiero causado por los delitos.

Skimming o copiado de banda magnética
Consiste en hacer una copia ilegal de una tarjeta de crédito o bancaria, usando un dispositivo que lee y reproduce la información de la tarjeta original.

Los empleados deshonestos usan máquinas pequeñas llamadas *skimmers* para leer números y demás información de las tarjetas de crédito, capturarlas y revenderlas a delincuentes.

Los delincuentes por su parte, usan la información para crear tarjetas falsas o pagar artículos por teléfono o Internet.

Phishing
Modalidad delictiva que tiene como mecánica, enviar una cantidad enorme de mensajes por correo electrónico, haciéndole creer al consumidor que los mensajes vienen de su banco, tratando de conseguir que la víctima potencial revele la información personal, como los números de cuenta del banco.

El crimen tiene éxito porque los mensajes de correo electrónico parecen legítimos, con logotipos bancarios realistas y sitios web o URLs que son muy parecidos a los reales.

Cuando los titulares de cuenta responden, se les dirige a un sitio web falso donde se les pide que tecleen los números de cuenta, las contraseñas y demás información bancaria, personal o de la tarjeta de crédito. Entonces, en materia de horas, los delincuentes agotan o vacían las cuentas de banco de las víctimas, usando las contraseñas para autorizar el giro electrónico de fondos a otras cuentas.

Por ello, debemos tener presente que los bancos nunca piden información personal de esta manera. Por lo tanto, no responda a los mensajes de correo electrónico, ni a llamadas telefónicas en las que se le solicite proporcionar los números de su tarjeta de crédito, seguro social o demás datos personales.

Incluso cuando usted tiene una solicitud legítima, los bancos le piden que nunca envíe información detallada en un mensaje de correo electrónico, porque no son seguros y la información puede ser interceptada por los delincuentes. Es mucho más seguro y por consiguiente lo recomendable, ir en persona, usar el sitio web legítimo del banco, llamar por teléfono o escribir una carta, cuando requiera actualizar sus datos o arreglar una disputa con su banco.

Ahora que ya conocemos las modalidades más comunes de fraude bancario y sus características, pasemos a detallar algunos consejos de seguridad que le serán de mucha utilidad para protegerse de ser una víctima de la delincuencia.

Tarjetas nuevas

- Firme la parte de atrás de la tarjeta con una pluma de tinta negra indeleble en cuanto la reciba.
- Hay quienes sugieren escribir “pida IDENTIFICACIÓN" en el espacio de la firma. Esta no es buena idea. Muchos emisores de tarjetas de crédito aconsejan que los comerciantes no aprueben compras si la tarjeta no está firmada.
- Registre todos sus números de cuenta y la información de contacto de la compañía emisora y guarde el registro en un lugar seguro.

Proteja su cartera o bolsa

- Mantenga sus cosas bien vigiladas.
- Nunca lleve todas sus tarjetas; solo lleve una o dos que podría necesitar.
- Lleve sus tarjetas de crédito aparte de su billetera, en un estuche para tarjetas de crédito o en otro compartimiento de su bolsa.
- Si le roban su cartera o la bolsa, llame a los emisores de la tarjeta de crédito inmediatamente.

Protecciones en el Internet

- Si usted realiza operaciones bancarias en línea, no use “firmas automáticas" en sitios bancarios o de tarjeta de crédito.
- Algunos sitios web ofrecen “acceso libre" si proporciona su número de tarjeta de crédito. No lo haga, es probable que la compañía a la que le da la información, realice cargos a su tarjeta y tal vez incluso, le cobren compañías que no conoce.

Proteja su información

- Nunca apunte su número de identificación personal (PIN, siglas en inglés);

memorícelo.
- Nunca dé su PIN a nadie.
- No escriba su número PIN en su tarjeta.
- No escriba el número de su cuenta de tarjeta de crédito en una tarjeta postal o por fuera de un sobre que va a enviar por correo.
- No guarde su número de PIN en el mismo lugar que su tarjeta de crédito o de cajero automático.
- Nunca proporcione su número de tarjeta de crédito u otra información personal por correo electrónico o por teléfono, a menos que usted pueda verificar que está hablando con su institución financiera de confianza o con un comerciante honrado.
- No le preste su tarjeta a nadie, porque usted es responsable por todos los cargos. Usted no estará protegido contra el uso desautorizado, si se comprueba que los cargos los hace alguien a quien usted le proporcionó la tarjeta.

Uso adecuado de su tarjeta

- Vigile bien cuando empleados de tiendas y restaurantes utilizan su tarjeta y asegúrese que no están copiando su número de tarjeta de crédito (*skimming*). A veces los dispositivos usados para copiar se parecen a teléfonos móviles.
- Después de que usted hace una compra y le devuelven su tarjeta, verifique que efectivamente sea la suya.
- Proteja su código de seguridad. Los códigos de seguridad son tres o cuatro números que se encuentran en la parte de atrás de las tarjetas de crédito y que algunos comerciantes usan para verificar que usted tiene la tarjeta en su posesión cuando hace compras por teléfono o Internet.

  Los números se encuentran en la esquina superior derecha de la tarjeta en las tarjetas de crédito Visa y MasterCard, o en la parte de atrás, después del número de la tarjeta de crédito impreso, cerca del espacio donde usted firma la tarjeta.

  Si le robaron su número de tarjeta y fecha de vencimiento, pero no la tarjeta misma, el ladrón no tendrá acceso al código de seguridad requerido por muchos comerciantes cuando usted haga las compras por Internet.

- Guarde copias de sus comprobantes y recibos de cajero automático para poder verificarlos contra las facturas.
- Si usted va a salir de viaje y piensa usar su tarjeta fuera de casa, notifique a su compañía de tarjeta de crédito. Esto puede evitar que le marquen la cuenta por posible fraude y las molestias que pueden surgir si su emisor bloquea la cuenta, porque usted la está usando en lugares inusuales.
- Si usted va a hacer compras grandes y fuera de lo normal, notifique a la compañía de su tarjeta que no le marquen la cuenta por posible fraude. Por ejemplo, si usted está renovando su casa y piensa comprar los materiales, adornos o electrodomésticos, infórmele por adelantado a la compañía de la tarjeta de crédito.
- Es importante mantener vigente el seguro de fraude, por que esto podrá

garantizar la devolución de los cargos por la utilización de la tarjeta de crédito sin autorización del titular de la misma. Este seguro es opcional para el tarjetahabiente.

Su estado de cuenta

- Revise bien el estado de cuenta el mismo día que llega.
- Si tiene acceso al Internet, considere usar una tarjeta de crédito emitida por un banco, que le permita tener acceso a su cuenta en línea. Entre cada estado de cuenta podrá verificar los cargos realizados y darse cuenta si hay alguna anomalía.
- Informe inmediatamente al emisor de su tarjeta sobre cualquier cargo dudoso. Para reclamar por cargos errados o no reconocidos, usted cuenta con un periodo previamente establecido en el contrato suscrito, por lo general es de 30 días desde la fecha del mismo.
- Cuando reclame cargos, hágalo por escrito. Puede llamar al banco o empresa emisora de la tarjeta y enviar posteriormente una carta.
- Si el estado de cuenta de la tarjeta no llegó en su debido momento, llame al emisor de la tarjeta sin demora. Un estado de cuenta perdido podría indicar que fue robado (Usted es responsable de pagar sus facturas, haya recibido o no el estado de cuenta).
- Guarde los estados de cuenta y recibos anteriores en un lugar seguro y rómpalos antes de desecharlos.

Si tiene un percance con su tarjeta de crédito

- Llame al emisor de la tarjeta inmediatamente si su tarjeta está perdida o fue robada.
- Después de su llamada telefónica, envíe una carta al emisor de la tarjeta. La carta debe contener el número de su tarjeta, la fecha en que extravió la tarjeta, y la fecha en que usted le informó sobre la pérdida de la tarjeta.
- Una vez que usted informa al emisor sobre la tarjeta perdida, ya no es responsable por cualquier cargo desautorizado.

  Usted podría perder las protecciones, si por negligencia no informa sobre la pérdida de la tarjeta o los cargos desautorizados en su estado de cuenta de manera oportuna.

Recuerde, usted es su principal frente de seguridad ante los fraudes. Tome precauciones y ponga en práctica las normas necesarias de seguridad y podrá evitar mayores complicaciones en un futuro.

Fuente: http://www.consumer-action.org/spanish/articles/1248.