



Aviso al consumidor

Cómo evitar el “Robo de información de tarjetas” en los ATM y otras máquinas automáticas

Proceda con cautela cuando utiliza cajeros automáticos (ATM, por las siglas en inglés) y otras máquinas que procesan pagos. Es posible que los ladrones utilicen herramientas de alta tecnología en las estafas que cometen para capturar información de su cuenta y robarle su dinero.

Estas estafas, conocidas como “robo de información de tarjetas”, consisten en colocar dispositivos a los ATM y máquinas similares que leen la información de sus tarjetas de débito y crédito cuando las pasa por el lector electrónico. Al combinar esta acción con una cámara oculta cercana para registrar su número de identificación personal (PIN, por las siglas en inglés), los ladrones pueden obtener todos los datos que necesitan para extraer dinero de su cuenta o realizar compras no autorizadas. Además de utilizar su información directamente, los ladrones pueden venderla a otros.

Los ATM y las máquinas de cobro automático de aeropuertos, tiendas de conveniencia, áreas de recepción de los hoteles y otros lugares públicos muy transitados son los más vulnerables dado que los ladrones consideran que los propietarios de tales máquinas no las inspeccionan regularmente. Sin embargo, el robo de información de tarjetas puede ocurrir en cualquier ATM o máquina procesadora de tarjetas, incluso las existentes en los bancos. A medida que la tecnología realiza dispositivos más pequeños y potentes, el riesgo de robo de información de tarjetas aumenta.

Cómo operan los ladrones *high-tech*

Los ladrones disponen de diversas maneras para robar la información de su cuenta. Pueden colocar un dispositivo que captura los datos de las tarjetas que aparenta ser una parte auténtica del ATM o de otra máquina similar y que actúa como tal. Puede tratarse de una funda plástica sencilla y curvada sobre la ranura donde se inserta la tarjeta que lee la banda magnética o el chip de la tarjeta y transmite la información de su cuenta a los ladrones o la guarda hasta que se recupera ese dispositivo.

Los ladrones también pueden utilizar una cámara inalámbrica cercana, oculta en una caja que contiene

folletos o en una lámpara. La cámara fotografía o filma sus dedos cuando ingresan el PIN en el teclado o la pantalla. Al igual que el dispositivo que captura los datos de las tarjetas, la cámara puede transmitir imágenes en forma instantánea o guardarlas hasta que los ladrones recuperen la cámara más tarde. La cámara y el dispositivo se pueden utilizar en conjunto.

Cómo proteger la información de su cuenta bancaria personal

Para ayudar a protegerlo, los bancos y los minoristas adoptan medidas tendientes a minimizar el riesgo de uso fraudulento de su tarjeta de débito o crédito, especialmente cuando esas compras se realizan por teléfono o en línea.

Antes de aprobar las compras telefónicas, por lo general, los minoristas confirman su identidad pidiendo información personal. Pueden pedirle su domicilio, los últimos cuatro dígitos de su número de Seguro Social o respuestas a preguntas de seguridad que usted creó cuando abrió la cuenta. También pueden solicitar el código de seguridad de tres dígitos impreso en el anverso o reverso de su tarjeta de débito o crédito. Para proteger su transacción en línea del fraude electrónico, muchos sitios web comerciales le exigen que descifre una palabra o un número que se visualiza como una imagen confusa o distorsionada que dificulta su lectura por el software.

Protéjase con medidas de seguridad que dicta el sentido común

En última instancia, usted debe protegerse de los ladrones y de las herramientas que utilizan para acceder a sus cuentas y robarle. Para protegerse, tome las siguientes precauciones que dicta el sentido común.

- Aléjese de un ATM si nota que alguien lo está observando o si percibe que algo malo pasa con la máquina; reporte de inmediato sus sospechas a la empresa que opera la máquina o a algún oficial encargado de aplicar la ley que esté cerca.

- Antes de utilizar un ATM, examine los objetos cercanos que podrían ocultar una cámara; compruebe si hay una funda plástica en la ranura de inserción de la tarjeta antes de colocar la suya.
- Nunca guarde una copia escrita de su PIN en la billetera o cartera, ya que podrían ser robados; memorícelo y guarde un registro en papel en su hogar.
- Al ingresar su PIN, quédese cerca de la máquina y mantenga la mano sobre el teclado o pantalla para que sea más difícil que lo observe una persona o cámara.
- Cuidado con los extraños que le ofrecen ayudarlo con un ATM que parece deshabilitado, y notifique a alguna persona responsable de la seguridad de la máquina.
- Revise con regularidad sus estados de cuenta, ya sea en línea o en papel, y compruebe retiros y compras no autorizados. Si encuentra alguno, póngase en contacto inmediatamente con su banco o proveedor de tarjetas de crédito, puesto que así limitará su responsabilidad financiera por cargos fraudulentos.

Las leyes federales limitan su responsabilidad en casos de fraude con tarjetas de débito y crédito. En particular, dos leyes federales protegen a usted.

La Ley de Veracidad en Préstamos (Truth in Lending Act), en general, limita su responsabilidad a

§50 por cualquier uso no autorizado de su tarjeta de crédito. Sin embargo, usted no es responsable por cargos no autorizados en su cuenta—si reporta la pérdida o robo de una tarjeta de crédito antes de que se la utilice. Tampoco es responsable si el fraude ocurre porque alguien utiliza solamente el número de su tarjeta de crédito, y no la tarjeta en sí.

La Ley de Transferencia Electrónica de Fondos (Electronic Fund Transfer Act) también limita su responsabilidad por uso no autorizado de sus tarjetas de débito o ATM —si reporta rápidamente la pérdida o robo de la tarjeta. No se lo considera responsable por cargos no autorizados si reporta el fraude antes de que se realicen transacciones no autorizadas. En caso de que ocurran esas transacciones no autorizadas antes de que reporte su tarjeta como perdida o comprometida, su responsabilidad depende de cuán rápidamente reporte la pérdida.

Información adicional

La Comisión Federal de Comercio (Federal Trade Commission) brinda más información sobre qué hacer si su tarjeta se pierde o es robada, en su hoja de datos “Tarjetas de Crédito, ATM y de Débito: Qué Hacer si se Pierden o Son Robadas”, en www.ftc.gov/bcp/edu/pubs/consumer/credit/cre04.shtm.

La Oficina del Contralor de la Moneda (Office of the Comptroller of the Currency) responde sobre qué hacer con cargos no autorizados y otros problemas bancarios en HelpWithMyBank.gov.

Cómo funciona el robo de información de tarjetas

