Los fraudes y estafas en los cajeros automáticos, el pan de cada día

Mercado libre para la clonación de tarjetas

Sylvia Ubal

Lunes 26 de octubre de 2009, puesto en línea por Barómetro Internacional, Sylvia Ubal

El delito electrónico o fraude es una modalidad delictiva que en Venezuela y en la mayoría de los países de Latinoamérica, EEUU y Europa viene en ascenso y que perjudica considerablemente a la ciudadanía al momento de realizar consultas, retiros o transferencias a través de medios electrónicos de la banca.

Especialistas en materia jurídica definen el delito informático o electrónico como toda conducta que revista características antijurídicas y culpables que atentan contra el soporte lógico de un sistema de procesamiento de información, sea sobre programas o datos relevantes, a través del empleo de las tecnologías de la información y que afecten a terceras personas.

En Venezuela este tipo de delitos se ha hecho cada vez más común, motivado fundamentalmente por la masificación del Internet y la facilidad de información a través de la Web, situación que ha obligado al sistema bancario a nivel nacional a mantener una actualización constante de sus sistemas de seguridad en los cajeros automáticos y otros medios electrónicos a fin de resguardar a sus clientes.

Existen diferentes modalidades para el fraude electrónico, uno de ellos tiene que ver con la mal llamada clonación de tarjetas, por ello el sistema bancario está avanzando en un cambio hacia la tecnología de Chip, se ha demostrado que esta es más efectiva en cuanto a la seguridad de la información de los clientes.

Desde su aparición, los cajeros automáticos, o ATMs (Automatic Teller Machines) han facilitado las transacciones rutinarias a los usuarios de la banca. Anteriormente a su arribo, los clientes de los bancos debían pasar horas en colas interminables para realizar operaciones de retiro, consulta de saldos y transferencias entre cuentas.

Las redes venezolanas Conexus y Suiche 7B funcionan desde junio de 1986, pero, pese a su confiabilidad, abrieron la puerta para una serie de delitos y estafas que sembraron desconfianza en los tarjetahabientes afectados y generaron dolores de cabeza a las instituciones financieras involucradas. Los fraudes y estafas cometidos con los cajeros automáticos revelan un modus operandi con alto grado de sofisticación. En la mayoría de los casos los autores de estos delitos son expertos conocedores de la tecnología informática.

Tan importante y variada es la experiencia desarrollada en Venezuela en materia de fraude y vandalismo a los cajeros automáticos que muchos expertos de firmas como Siemens-Nixdorf, IBM, NCR y otras conocidas marcas fabricantes de ATMs vienen al país para observar de cerca los casos y diseñar soluciones para la nueva generación de cajeros. Gran parte de las modificaciones y mejoras de los nuevos ATMs se han generado específicamente obedeciendo a la experiencia venezolana.
Aunque la "clonación" de tarjetas comenzó en los 90, era limitada. Actualmente es creciente el número de usuarios de plásticos, incluso se pagan por ese medio los salarios, las misiones, jubilaciones y pensiones. Realizamos diferentes tipos de transacciones bancarias, retiro de dinero, consultas, transferencias entre cuentas, hasta pagamos los servicios básicos (electricidad y teléfono) todo a través de esta tecnología.

Un peligro que enfrentan los usuarios de tarjetas de crédito o débito, es la "clonación" del plástico, mediante la cual pueden duplicarse los códigos ocultos en la banda magnética para usarlos con fines fraudulentos. Los consumos que se efectúen con la tarjeta duplicada perjudican al titular de la tarjeta, pero el delito se comete en primera instancia contra la institución de crédito emisora del plástico.

Según nos informa Ángela Rendón, coordinadora de la Oficina contra El Fraude con Tarjetas de Crédito y Otros Instrumentos de Pago, para obtener los datos la mafia usa un lector de tarjeta como el de la entrada al cajero automático, con capacidad de hasta cien códigos.

Existe un pequeño aparato llamado Skimmer, que es un lector de bandas magnéticas de tarjetas de crédito y débito y permite obtener información con sólo deslizar la tarjeta. Simplemente basta con pasar la tarjeta por este scanner y ya fuiste clonado, luego toda la información contenida es vaciada a la computadora para falsificar una nueva tarjeta con los datos obtenidos, como la clave de confidencialidad. Un lector de este tipo suele ser colocado en los cajeros automáticos y es del tamaño de la cabeza de una alfiler.

"Los fraudes no son en volúmenes gigantescos, sin embargo, multiplique 300 bolívares por cien usuarios. Ese fraude hormiga puede ser de proporciones increíbles", destacó Rendón.

Para combatir el fraude los bancos cuentan con sistemas de “monitoreo inteligente” llamados redes neurales. Estos programas aprenden la forma en la que el tarjetahabiente se comporta y, en el momento en que se rompe el patrón normal del consumo, el sistema genera una alerta", detalló Javier Calderón subdirector de riesgos de VISA.

Otras Estafas "online" y "off-line" con su tarjeta de Crédito

Los PIRGs (Public Interest Research Groups) han recibido innumerables denuncias de consumidores que han sido objeto de fraude. Para cometerlo, basta que alguien consiga una copia de un recibo de compra con el número de la tarjeta y como el uso de ésta no requiere el marcado de un PIN (número personal de identificación), fácilmente se puede acceder a la cuenta bancaria del titular. También existe el fraude de personas que de alguna manera han averiguado el PIN de una tarjeta ajena.

En su página de internet, la Privacy Rights Clearinghouse, relata el caso de una mujer que fue objeto de fraude con su tarjeta de débito: "Un buen día me llegó una factura de una aerolínea donde me notificaban que habían cobrado el pago de varios billetes de avión por todo el país. No sabía de qué hablaban. Cuando llamé a la aerolínea me confirmaron que habían sido pagados con mi tarjeta de débito y a mi nombre".

Las tarjetas de débito pueden utilizarse con el número personal de identificación (PIN) o sin él. Las transacciones que se completan sin marcar este número son conocidas como "off-line" y requieren la firma de un recibo de compra, según informó SUDEBAN (Superintendencia de Bancos).

Las diferentes formas de clonar tarjetas de crédito y débito, ahora en cajeros automáticos según nos advierte la Superintendencia de Bancos.

– Falsifican un dispositivo para colocarlo encima de la ranura donde se desliza la tarjeta y así copia el contenido de la banda magnética cuando la tarjeta es introducida por el cliente, y un aparato de alta tecnologia capaz de leer y copiar la información de las tarjetas. Ésta es la que contiene toda la información sobre el número de cuenta y el banco al que pertenece, así como los datos del cuenta habiente. Este aparato lo instalan sobre los cajeros, después de haber bloqueado con papeles o plásticos la abertura del cajero donde se introduce la tarjeta

– Igualmente, colocan una mini cámara (del tamaño de una cabeza de alfiler) denominados "pescadoras" que capturan la información contenida en la banda magnética del plástico de los clientes y pueden grabar en video los pines o claves de las tarjetas que estaban clonando.

– Una vez copiadas un número determinado de tarjetas, se dirigen a un laboratorio y comienzan a generar tarjetas con los números clonados.

– Una vez generados los plásticos clonados, proceden a retirar el efectivo de un cajero automático.

– Las máquinas "pescadoras" son introducidas en los cajeros automáticos por los delincuentes en las

noches y fines de semana y son dejadas allí durante cinco horas durante las cuales recaban información de los usuarios de los cajeros. Además utilizan las pantallas por circuitos idénticos a los de los cajeros, que on maquetas de los cajeros auténticos y son montados sobre éstos, cuando la persona introduce la tarjeta queda grabada toda la información, este método es utilizado en los cajeros alejados y solitarios

Un experto en seguridad comenta

– Si usted ve algo raro en el dispositivo donde va la ranura donde se introduce la tarjeta, busque otro cajero automático.

– Siempre, bloquee y proteja su clave secreta. Cuando usted vaya a introducir su pin ó clave secreta en el cajero automático, bloquee la visión de su mano cuando está marcando el pin y tápela con la otra mano. De esa forma, si su tarjeta es clonada no podrán utilizarla si no pueden grabar el PIN

Consejos de expertos

Para prevenir el mal manejo de las tarjetas de crédito y débito siga estas recomendaciones:

– No pierda de vista su tarjeta. En comercios donde se la entrega a un dependiente considere un tiempo razonable para que ésta le sea devuelta.

– Revise a detalle su estado de cuenta. Verifique que el saldo corresponda al consumo.

– Si detecta un consumo que no realizó notifíquelo a su banco de inmediato.

– Antes de que deslicen por segunda vez su plástico pida que esperen a que llegue la autorización.

– Nunca acepte ayuda o sugerencias de extraños dentro de un cajero automático.

– No entregue su tarjeta a desconocidos o personas que le visiten en su domicilio a nombre del banco con la finalidad de darle una nueva tarjeta.

– Nunca debe estar condicionada la entrega de un premio o de un servicio contra la información o datos de la tarjeta de crédito. En todo caso verifíquelo con su banco.

– No revele su PIN a nadie, ni lo traiga consigo.

– Tenga a la mano los teléfonos para notificar robo o extravío.

Para enfrentar la clonación de tarjetas, la banca cambiará las actuales tarjetas de banda magnética por tarjetas con un chip. La solución incluye los puntos de venta inalámbricos para facilitar que el cliente no pierda de vista su tarjeta, pues el punto de venta le será llevado a sus manos. Todos los tarjetahabientes tendrán su nueva tarjeta en un lapso de dos años, pues ya se lograron acuerdos entre la SUDEBAN y la Asociación Bancaria de Venezuela (ABV).

Otro de los aspectos acordados entre ambas instituciones, es mejorar la educación de los usuarios y clientes para que contribuyan a evitar los fraudes. SUDEBAN afirma, que la banca "está respondiendo de modo positivo", y más de 90% de los reclamos ha sido satisfecho. Aún no hay cifras de las pérdidas de la banca, pero los fraudes siguen aumentando.

Los bancos saben que todo su prestigio se basa en la seguridad e integridad que brinden al dinero de los ahorristas. Es por ello que ante la ola de fraudes electrónicos que azota a toda la banca nacional han decidido tomar medidas a corto, mediano y largo plazo. En los próximos meses todos los cajeros automáticos deben tener claves maestras individuales, de carácter secreto y confidencial. Asimismo, las llaves de trabajo o transporte entre cajeros automáticos y los bancos, y entre los bancos y redes, deben ser generadas de forma aleatoria. Deben establecerse los procedimientos para garantizar el acceso seguro a los equipos por parte del personal autorizado por los bancos; y por último, debe eliminarse el

almacenamiento y registro de información sensible de archivos de los cajeros automáticos, punto de venta, autoservicios o cualquier dispositivo que posea banda magnética. Actualmente se estudia la incorporación de un chip de seguridad que garantiza el blindaje en las tarjetas de débito y crédito. Sin embargo, una fuente consultada aseguró que esta tecnología no es la de vanguardia en el mundo sino los sistemas biométricos que funcionan con el reconocimiento retinal o de huellas digitales de los dedos índices. Sin embargo, estos mecanismos son mucho más costosos

Sitios de mayor riesgo de delito electrónico

Fuentes de seguridad indicaron que las bandas de los llamados "tarjeteros" operan con mayor frecuencia en los estados Nueva Esparta, Anzoátegui y Bolívar, así como también en los hoteles cinco estrellas de las grandes ciudades. La razón es que en esos lugares es más probable encontrar a usuarios de cajeros automáticos que posean tarjetas internacionales. Una vez obtenida la información sobre sus cuentas, los "tarjeteros" se dirigen a países centroamericanos, especialmente Panamá, donde pueden hacer retiros de hasta 2.000 dólares en efectivo. La moneda estadounidense es revendida posteriormente en el mercado negro venezolano.

Los "tarjeteros" están divididos en zonas de influencia, y atacan a las instituciones financieras cuyas tecnologías de información son más vulnerables. Estos delincuentes conocen las deficiencias en seguridad de la información de los bancos debido a que poseen contactos con empleados de los departamentos de Sistemas, o trabajaron en ellos.

"Estos individuos viven como nómadas: van de ciudad en ciudad usando vehículos de lujo, y sacando dinero. Están identificados. La policía sabe quiénes son, puesto que no son más de diez. Pero no los agarran porque siempre están en movimiento", señaló un asesor de seguridad bancaria.

Otras formas de fraude electrónico

1. El Cambiazo: Consiste en el cambio de tarjetas durante las operaciones que se realizan en cajeros automáticos. Se recomienda que el usuario no acepte ayuda de desconocidos, no pierda de vista de sus manos la tarjeta, ni facilite la clave secreta.

2. Colocación de pantallas falsas en cajeros: Consiste en la colocación de un aparato similar al cajero de un banco y con teclado que posee una pescadora. De esta manera los delincuentes logran apoderarse de la información de la banda magnética y la clave secreta. Se recomienda a los usuarios revisar el cajero antes de introducir la tarjeta y la clave, si se observa que está flojo absténgase de utilizarlo.

3. Colocación de cámaras en accesorios adheridos a los cajeros destinadas a capturar la clave secreta vía inalámbrica. Se recomienda la revisión del cajero automático antes de realizar cualquier transacción. Desconfiar de accesorios externos del cajero colocados cerca del teclado.

4. Pishing o duplicar página Web de la banca. Se crea una página Web falsa para generar mensajes de correo para hacer creer al usuario de que la banca quiere actualizar sus datos. La banca reiteradamente informa a sus clientes que no envía este tipo de mensajes a sus clientes.

5. Bitching. Es una modalidad parecida al Pishing pero a través de la línea telefónica. El delincuente llama al cliente en nombre del banco para actualizar datos. Se recomienda abstenerse de suministrar información personal a través de llamadas telefónicas.

---

sylviaubal[AT]gmail.com