Fraude

Le mantenemos informado sobre las prácticas fraudulentas que afectan a los clientes.

AMERANT

Asesor de Fraude

El fraude puede impactar a cualquiera en cualquier momento. La prevención es la forma más económica para hacer frente a las pérdidas potenciales e inconveniencias que pueden derivarse del fraude. Amerant está comprometido a dar los pasos necesarios para prevenir la actividad fraudulenta antes de que suceda, ayudándole a obtener un gran conocimiento sobre fraude y asistiéndole para que conozca algunas de las medidas preventivas que puede tomar para evitar o mitigar el fraude.

FRAUDE EN LÍNEA Y POR CORREO ELECTRÓNICO

Phishing

Phishing es lo que ocurre cuando personas dedicadas a cometer fraudes electrónicos crean una identidad falsa de una empresa legítima, envían un correo electrónico o e-mail con el intento de "pescar" información personal. El e-mail puede indicar al usuario que visite un sitio Web haciendo clic en un enlace, y/o incluye un documento adjunto o formulario con el fin de actualizar información personal, tales como contraseñas, números de tarjetas de crédito, de la seguridad social y de sus cuentas bancarias. Sin embargo, el sitio web es falso y solamente está establecido para robarle su información. Estos e-mails normalmente tienen un sentido de urgencia.

Amerant nunca solicitará información personal identificable o números de PIN en un e-mail:

- No suministre información financiera personal.
- Sospeche de cualquier e-mail que solicite datos personales con mucha urgencia.
- No utilice enlaces incluidos en e-mails sospechosos y no deseados.
- No llene formularios por e-mail que soliciten información financiera personal.

Consejos para minimizar las oportunidades de Phishing:

- Nunca abra e-mails enviados por desconocidos.
- Nunca suministre información por medio de un e-mail o fuera de un sitio web seguro.
- No siga las instrucciones de enlaces no solicitados, ni abra documentos adjuntos en mensajes por e-mail.

- Nunca reenvíe e-mails no solicitados, ni inicie cartas en cadena.
- Evite negocios "demasiado buenos para ser verdad".
- Verifique la autenticidad de las organizaciones de beneficencia cuando haga una donación a través de un sitio web por medio de https:// e íconos de candado.
- Esté prevenido de ataques engañosos de mensajes de texto ("smishing") en su teléfono celular.
- Utilice cortafuegos (firewalls) y programas contra espionaje y contra virus y manténgalos actualizados.
- Evite el uso de redes públicas Wi-fi cuando realice operaciones financieras.

Malware/Spyware

Malware (abreviado de "programa malicioso") incluye virus y spyware, roba información personal, envía spam y comete fraude. Los delincuentes crean sitios y descargas atractivas para atraerlo a enlaces que descargan malware, sobre todo en equipos que no utilizan programas adecuados de seguridad.

Consejos para minimizar las oportunidades de malware/spyware:

- Hable con sus hijos sobre utilizar con seguridad la computadora. Evite los juegos gratis o brindar información personal.
- Si sospecha que su computadora está sufriendo de malware, suspenda sus operaciones bancarias por Internet, no realice compras y otras actividades en-línea que necesiten nombre de usuario, contraseña u otra información sensible.
- Actualice su programa de sistema operacional y navegador en la red.
- Utilice programas anti-virus y anti-spyware, así como un firewall, y actualícelos a menudo.
- Baje programas gratis de sitios que usted conoce y confía.
- No marque ningún enlace dentro de pop-ups.

E-Mail Spoofing

Se conoce como e-mail spoofing a la actividad fraudulenta de los mensajes electrónicos en los cuales la dirección de la persona que lo envía y otras partes del título del mensaje son alteradas para que parezca que ese mensaje proviene de una fuente distinta. Esto involucra la solicitud de un delincuente, que parece ser una agencia del gobierno, un negocio oficial, pagos en línea o un banco.

Algunos consejos para tener en cuenta:

- Evite mensajes electrónicos con logotipos distorsionados o de tamaño poco común, errores gramaticales, enlaces extraños, sentido de urgencia y/o solicitud de información personal.

FRAUDE DE TARJETA

Fraude de Tarjeta ATM, Tarjeta de Débito y Tarjeta de Crédito

El fraude de tarjetas tiene el potencial de drenar su cuenta de cheques e incursionar dentro de cualquier línea de crédito de respaldo que haya podido establecer. La vigilancia y una rápida acción es la mejor manera de limitar las pérdidas. Los cargos son simplemente deducidos directamente de su cuenta corriente o cuenta de ahorros, y puede que no se dé cuenta de esta actividad fraudulenta hasta que revise su estado bancario.

Cómo Evitar el Fraude en sus Tarjeta ATM, Tarjeta de Débito y Tarjeta de Crédito

- Solamente brinde su número de su Tarjeta cuando usted inicie la comunicación y considere que el comerciante es confiable.

- Nunca brinde la información de su Tarjeta cuando reciba una llamada de alguien preguntándole que verifique su información. (Por ejemplo, no ofrezca su número de tarjeta si la persona que le llama le dice que ha habido "un problema con la computadora" y necesitan verificar la información).
- Mantenga la vista en su Tarjeta cada vez que la utilice y asegúrese de que se la devuelvan lo más rápido posible. No pierda de vista su Tarjeta siempre que sea posible para evitar el "skimming".
- Nunca ofrezca la información de su Tarjeta en un sitio de la red que no sea seguro. El URL de un sitio seguro comienza con https:// y/o muestra el símbolo de un candado cerrado.
- Firme el dorso de sus Tarjetas tan pronto como las reciba.
- Esté al tanto de Cajeros Automáticos defectuosos o de personas que puedan estar cerca de usted cuando marca el Número de Identificación (PIN).
- Nunca escriba su Número de Identificación (PIN) en la Tarjeta o donde la guarda.

FRAUDE DE CHEQUES

¿Qué es el Fraude de Cheques?

El fraude de cheques es uno de los mayores retos que enfrentan las personas, los negocios y las instituciones financieras. La avanzada tecnología de las computadoras permite a delincuentes novatos, ya sean independientes o en grupos organizados, alterar la apariencia de sus cheques actuales, crear cheques falsos o falsificar su firma en un cheque legítimo. Los programas de autoedición (Desktop) para computadoras y las fotocopias son usadas a menudo para crear o duplicar un documento financiero actual; las alteraciones químicas pueden eliminar alguna o toda la información del cheque; y el robo de cheques y falsificación de su firma para retirar fondos de su cuenta o realizar un pago fraudulento son algunos de los tipos más comunes del fraude de cheques.

Existen varias maneras que los delincuentes utilizan para cometer el fraude de cheques:

- Falsificación.
- Falsificación (cheque, documento, firma o moneda).
- Alteración.
- Check Kiting.

Cómo Evitar el Fraude de Cheques:

Consejos a Individuos

- Mantenga su chequera en un lugar seguro y considere cuidadosamente quiénes tienen acceso a ella, aun posibles miembros de la familia (algunos fraudes de cheques son cometidos entre miembros de la familia).
- Revise frecuentemente los estados de cuenta mensuales y esté alerta por cualquier cheque sospechoso o falsificado.
- Nunca imprima ni escriba información personal innecesaria en su cheque, tal como número de Seguridad Social, Cédula de Identidad o Documento Nacional de Indentidad o número de tarjeta de crédito o número de teléfono.
- Pase por una trituradora de papel los cheques viejos, estados de cuenta y cualquier otra información bancaria después que haya verificado que todos sus estados están correctos y ha balanceado su chequera. No firme cheques con antelación pensando que los va a tener a mano "en caso de emergencia" o por cualquier otra razón.

Consejos para Comerciantes

La falsificación de una cuenta de negocios típicamente se realiza cuando alguien emite un cheque sin la autorización apropiada. Los delincuentes también robarán un cheque, lo endosarán y lo presentarán al cobro en un lugar de ventas al detalle o al cajero de un banco, utilizando información personal falsa.

- Establezca controles internos para asegurar que ninguna persona en su empresa, tenga autorización para acceder a todos los aspectos de emitir cheques a mano o por impresión.
- Los cheques de nómina son los cheques más frecuentemente alterados así es que inspeccione cada cheque de nómina que firme para estar seguro de que el cheque esté completo y los números de cheques están en secuencia.

MUESTRA DE SISTEMA DE FRAUDE

Llamadas Ficticias

Las llamadas ficticias son las que se realizan para obtener la confianza de alguien pretendiendo ser otra persona. El objetivo de estas llamadas es obtener información personal, tales como número de seguro social, pasaporte, fecha de nacimiento o número de cuenta bancaria, bajo falsas pretensiones. Esto lo puede hacer alguien haciéndose pasar por una institución financiera, una agencia de cobros o una agencia del gobierno.

Otra manera en que los delincuentes obtienen información personal en forma inapropiada de clientes bancarios es comunicándose con el banco, pretendiendo ser un cliente o alguien autorizado para recibir la información del cliente, y mediante el uso de artimañas y engaños, convencen al empleado del banco a que le de la información que identifica al cliente.

Fraude Nigeriano por Correo Electrónico

El Fraude Nigeriano por correo electrónico ofrece grandes sumas de dinero a individuos en los Estados Unidos que ayudan a los delincuentes, haciéndose pasar como oficiales del gobierno mueven millones de dólares fuera de Nigeria u otro país extranjero. Los personificadores prometen transferir fondos a una cuenta bancaria de la víctima en los Estados Unidos después de recibir un honorario. Los honorarios son presentados como impuestos, o gastos de procesamiento violando la sección 419 del código criminal de Nigeria. El fraude es a menudo conocido como “el Fraude 419”. Debido a que los honorarios son pagados antes de recibir la elevada cantidad de dinero prometida, este tipo de fraude es conocido como Fraude con Honorario Anticipado. Este fraude llega normalmente a las víctimas a través de salas de chat, teléfono y fax, así como a través de citas, contactos y sitios de juego.

Fraudes de Lotería y Premios

La lotería y la concesión de premios llevan a las víctimas a pagar altos honorarios con anterioridad al recibo de los premios de la lotería inexistente. Debido a que el honorario es pagado antes de recibir la gran cantidad de dinero prometida, este tipo de fraude se conoce como Fraude de Honorario Anticipado.

Fraude de Falsificación de Cheques de Cajero

Los planes alrededor de los cheques de cajero fraudulentos normalmente comienzan recibiendo un cheque por correo. Usualmente los delincuentes sitúan el cheque como dinero de premio otorgado a la víctima. Se le indica a la víctima que deposite el cheque y devuelva una parte, a los falsos organizadores del concurso como pago por honorarios, normalmente por transferencia electrónica a un país extranjero. Debido a que los bancos liberan los fondos de cheques de cajero antes de que los fondos sean compensados, la víctima asume que los fondos están compensados y prepara la transferencia electrónica.

Trabaje desde la Casa/ Estafas sobre Compradores Misteriosos

Las víctimas de Trabaje desde la Casa/ Compradores Misteriosos son empleadas por compañías sin escrúpulos para comprar en tiendas minoristas y tomar nota de la experiencia de la compra, la mercancía u otras dimensiones asociadas con el detallista. A cambio, el delincuente envía a la víctima un cheque de cajero para pagar por los servicios de compra. Típicamente, el cheque es por una cantidad significativamente mayor que la cantidad que se le debe. A la víctima se le notifica que deposite el cheque y que devuelva por transferencia electrónica la cantidad excedente. O, se le indica que devuelva la cantidad del cheque para cubrir los honorarios iniciales con la promesa de que recibirá un cheque mayor. Debido a que los bancos liberan los fondos de cheques de cajero antes de que los fondos sean compensados, la víctima asume que los fondos están compensados y prepara la transferencia electrónica. Una variante de esta estafa es que el delincuente solicita la información bancaria del comprador con el fin de realizar un depósito directo por los servicios prestados.