

Política de lucha contra el fraude

Concientización sobre el fraude:

En Broxel proteger a los clientes es nuestra prioridad. Nuestro objetivo es instruir a los consumidores sobre las formas de proteger y salvaguardar su dinero, así como su información personal, además de evitar que se conviertan en víctimas de fraude. Creemos que instruir a los clientes sobre el fraude es importante para que puedan tomar medidas para protegerse. Para informarse sobre los tipos más comunes de estafas al consumidor, sírvase consultar la sección Tipos de fraude/estafas. Tenga en cuenta que todos los días surgen nuevos tipos de estafas fraudulentas. Los estafadores crean constantemente nuevas formas de estafar a los consumidores. Por ello, es importante tener presente, en todo momento, utilizar el sentido común cuando se vea implicado el envío de dinero y el uso de tarjetas de prepago.

Prevención del fraude:

La regla número uno en la prevención del fraude es "conocer a la persona con la que se está tratando". Envíe dinero sólo a personas conocidas. Nunca lo envíe ni facilite los datos de su tarjeta de prepago a un desconocido o a alguien a quien no conozca personalmente.

El objetivo de un estafador es engañarle para que les dé dinero sabiendo que no podrá recuperarlo una vez enviado. La mejor manera de detenerlos es saber cómo pueden intentar engañarle. Por tal motivo, Broxel se compromete a proporcionar a los consumidores la información necesaria para evitar que sean víctimas de fraude.

Broxel realiza un seguimiento diario y continuo de las transacciones a través de un proveedor externo con el fin de investigar y responder a posibles actividades fraudulentas o inusuales. Diversas autoridades encargadas de la aplicación de la ley pueden considerar apropiado solicitar esta información.

Por todo ello, Broxel ha establecido indicadores clave de riesgo (KRI) o indicadores clave de desempeño (KPI) que supervisan la eficacia del programa de gestión del riesgo de fraude interno. Broxel puede verse obligada a presentar copias de los informes con fines de revisión, incluyendo, de manera enunciativa mas no limitativa, la detección, prevención y mitigación de actividades fraudulentas. Las actualizaciones de los análisis de tendencias deben producirse con regularidad para garantizar que se cubren los escenarios de fraude conocidos y se identifican nuevos escenarios.

Recuerde que la mayoría de los fraudes al consumidor comienzan con el contacto de un desconocido. Protéjase de las estafas, NUNCA envíe dinero a alguien que no conozca o con quien no tenga una relación comercial legítima.

El objetivo de Broxel es ayudar a prevenir el fraude al consumidor instruyéndoles sobre los distintos tipos de fraude/estafa que este puede sufrir.

Si Broxel no puede explicar la actividad, puede ponerse en contacto con el titular de la cuenta y preguntarle si la actividad es válida o no.

En los casos de posibles notificaciones de usurpación de identidad, Broxel puede verificar más a fondo la identidad del titular de la cuenta, ya sea llamándolo para realizar preguntas de autenticación o solicitando documentos de identificación al titular de la cuenta.

Dr. TIMOTHY JOHN HAVARD



Tipos de fraude/estafa

A continuación se indican algunos de los tipos más comunes de fraudes/estafas que debe conocer:

Robo de identidad

Los ladrones de identidad utilizan información personal (por ejemplo, números de Seguro Social, números de identificación, información de cuentas bancarias, números de tarjetas de crédito, etc.) para hacerse pasar por otra persona. Pueden utilizar esta información para enviar una transferencia no autorizada, abrir una cuenta de acceso prepago o vaciar la cuenta de un cliente existente. Consulte a continuación algunas de las señales de alerta frecuentes en el robo de identidad.

Señales de que alguien ha robado su información

- Se percata de retiros de fondos de sus cuentas que no puede explicar.
- No recibe sus estados de cuenta u otra correspondencia.
- Los comerciantes declinan sus cheques y/o tarjetas de crédito/débito.
- Recibe llamadas de cobradores por deudas que no son suyas.
- Se percata de cuentas o cargos desconocidos en su historial de crédito.
- Hacienda le notifica que se ha presentado más de una declaración de impuestos a su nombre o que tiene ingresos de una empresa para la que no trabaja.
- Recibe un aviso de que su información se ha visto comprometida por una filtración de datos en una empresa en la que tiene relaciones comerciales o tiene una cuenta.

Desafortunadamente, los robos de identidad ocurren. Sin embargo, hay ciertas medidas que puede tomar para evitar que su información personal caiga en manos equivocadas. A continuación se indican algunas formas de estar pendiente de su identidad y su información personal para minimizar el riesgo de convertirse en víctima de un robo de identidad:

- Lea detenidamente y con frecuencia sus estados de cuenta.
- Conozca las fechas de vencimiento de sus pagos. Si no recibe un estado de cuenta en la fecha prevista, investigue por qué.
- Lea los estados de cuenta de su seguro de gastos médicos. Asegúrese de que los cargos aplicados corresponden con la atención recibida.
- Destruya los documentos con información personal y financiera.
- Revise cada uno de sus tres informes crediticios al menos una vez al año. Es fácil y gratuito.

Para obtener más información y consejos sobre cómo detectar y prevenir el robo de identidad, visite www.consumer.ftc.gov.

Para denunciar un robo de identidad, visite www.IdentityTheft.gov, obtendrá instrucciones e información sobre cómo presentar una denuncia.

Estafas de extorsión tipo fiscal/ autoridad tributaria

¿Recibió una llamada telefónica de una persona que dice pertenecer a una dependencia gubernamental y le solicita dinero para cubrir "deudas atrasadas" con Hacienda? Es posible que le digan que puede transferir el dinero o enviar una tarjeta de débito prepagada para saldar dicha deuda y que, si no lo hace, se enfrentará a un periodo de encarcelamiento. Aunque estas llamadas pueden tener un código de área de Washington, D.C. o información engañosa en el identificador de llamadas, tenga la seguridad de que cualquier "empleado del gobierno" que se ponga en contacto con usted y le pida dinero por adelantado es un estafador.

Dr. TIMOTHY JOHN HAVARD



La víctima es contactada por alguien que dice pertenecer a una dependencia gubernamental y le comunica que adeuda dinero por concepto de impuestos y que debe pagarlos inmediatamente para evitar su detención, deportación o suspensión de la licencia de conducir/pasaporte. Se indica a la víctima que envíe una transferencia o compre una tarjeta de débito precargada para pagar los impuestos. Las dependencias gubernamentales nunca exigirán el pago inmediato ni llamarán para temas de impuestos sin haber enviado antes un requerimiento de pago.

Estafas por reembolso

¿Ha recibido una llamada de alguien que dice trabajar con la para la Comisión Federal de Comercio (FTC)? ¿La persona que llamó le prometió ayudarle a obtener un reembolso de la dependencia? Esto es una ESTAFA. Nunca envíe dinero ni facilite números de cuentas bancarias u otra información confidencial a quienes le prometan reembolsos. Recuerde: la FTC no hace llamadas telefónicas salientes para ponerse en contacto con la gente, no les solicita a los consumidores que proporcionen información bancaria o sensible, tampoco les solicita que envíen dinero, y si los reembolsos fueran parte de un acuerdo de la FTC, la FTC proporciona los fondos por cheque. Incluso si el identificador de llamadas dice el nombre de una dependencia que usted reconoce o en la que confía, sea escéptico. Los estafadores utilizarán tecnología que puede mostrar números legítimos que le obligan a responder.

Estafa por una supuesta obra benéfica

La víctima suele ser contactada por correo electrónico, correspondencia o vía telefónica por alguien que solicita el envío de una donación mediante transferencia de dinero a un particular para ayudar a las víctimas de un suceso reciente, como una catástrofe o una emergencia (por ejemplo, una inundación, un ciclón o un terremoto). Las organizaciones benéficas formales nunca solicitarán que se envíen donativos a un particular a través de un servicio de transferencia de dinero.

En tiempos de catástrofe, es importante ser consciente de las estafas por supuesta obra benéfica. Hay muchas formas legítimas de prestar ayuda a las personas afectadas por inundaciones, terremotos, incendios, otras catástrofes naturales o incluso catástrofes provocadas por el hombre. Si desea hacer una donación, hágalo de una forma en la que haya donado antes o a través de una organización o empresa de confianza en la que entienda perfectamente cómo se recaudan y utilizan los fondos. Es importante no enviar nunca fondos a alguien que no conozca.

Lotería extranjera

Recientemente, muchos gobiernos locales emitieron una advertencia nacional sobre el continuo fraude a los ciudadanos que tiene lugar a través de una estafa de lotería o sorteo en el extranjero. Tenga en cuenta que, si recibe un aviso de que ganó la lotería, por muy oficial que parezca, y se le solicite que pague una cuota para reclamar su premio, se trata de una estafa.

Las loterías o sorteos legítimos NUNCA exigen que la gente pague dinero por adelantado. ¿Recibe una carta, una llamada o un correo electrónico diciéndole que ha ganado algo (dinero o un premio), pero antes de poder cobrarlo tiene que enviar dinero para pagar impuestos, aranceles o cualesquier derechos? Pero usted no ha comprado un boleto ni ha participado en un sorteo. Se trata de una ESTAFA. No envíe ni transfiera dinero a las personas que le afirman que ha "GANADO" algo, pero que necesita enviarles dinero para cobrar sus premios.

A la víctima se le dice que ha ganado la lotería, un premio o un sorteo y que debe enviar dinero para cubrir los impuestos o derechos sobre tales ganancias. La víctima podrá recibir un cheque por una parte de las ganancias y, una vez depositado el cheque y enviado el dinero, el cheque rebota.

Estafa por compras en Internet

La víctima envía dinero para la compra de un artículo pedido por Internet (por ejemplo, mascotas, coches). Los artículos suelen anunciarse en Craigslist, eBay, Alibaba, etc. Una vez enviado el dinero, la víctima nunca recibe la mercancía.

¿Encontró algo en Internet que le interese: un cachorro, un coche, la renta de un departamento o cualquier artículo en venta? ¿Le parece que el precio del artículo es demasiado bueno para ser cierto y le piden que lo pague mediante una transferencia? Por desgracia, se trata de una ESTAFA. No envíe dinero al vendedor por dicho artículo. Puede que incluso le envíen una carta o un correo electrónico de autenticación diciéndole que ha adquirido el artículo, pero que

Dr. TIMOTHY JOHN HAVARD



primero tiene que transferir los fondos. No envíe el dinero. Se trata de una ESTAFA. No recibirá ninguna mercancía. Una vez transferido y recibido el dinero, no podrá recuperarlo y, lamentablemente, perderá el dinero transferido.

Compra de un vehículo

¿Ha encontrado un gran vehículo en Internet o en un anuncio con un precio demasiado bueno para ser verdad? ¿Le piden que envíe el anticipo por transferencia bancaria? Por desgracia, se trata de una ESTAFA. No envíe dinero por el vehículo al vendedor ni a un representante de pagos. El estafador de la compra del vehículo puede incluso intentar convencerle para que pague a través de MoneyGram para evitar el impuesto sobre las ventas y obtener un muy buen precio. Puede que incluso le envíen una carta o un correo electrónico de autenticación diciéndole que ha comprado el artículo, pero que para poder entregárselo tiene que transferir fondos primero. No recibirá ningún tipo de vehículo. Una vez transferido y recibido el dinero, no podrá recuperarlo y, lamentablemente, perderá el dinero transferido.

Estafa de emergencia

Se hace creer a la víctima que está enviando fondos para ayudar a un amigo o ser querido que lo necesita urgentemente. La víctima envía el dinero con urgencia al aprovecharse de su genuina preocupación por un ser querido.

Familiar en busca de apoyo

¿Recibió una llamada telefónica de un nieto o de un familiar? ¿O un "abogado" o "policía" sugiriendo que están con su familiar? ¿Están desesperados porque han sido detenidos? ¿Han sufrido un accidente de tráfico? ¿Le solicitan dinero para pagar multas o para reparar el coche? ¿Recibió la llamada de un pariente porque necesita dinero para un familiar que requiere atención médica o medicamentos? ¡SE TRATA DE UNA ESTAFA! Sea precavido al enviar dinero en cualquiera de estas situaciones. Estas personas pueden pedirle que envíe dinero a cualquier parte del mundo. Si no puede verificar con su familiar (llamando al número que tenía antes de esta llamada, no al "nuevo número" que le da la persona que llama) que le están solicitando dinero y no está seguro de la transacción, no envíe el dinero. Se perderá todo el dinero que se envíe.

Estafa familiar, pariente en apuros

Esta estafa es una variación de la estafa de Emergencia. La víctima es contactada por un individuo que finge ser un nieto en apuros o una persona con autoridad, como un médico, un policía o un abogado. El estafador describe una situación urgente o de emergencia (fianza, gastos médicos, fondos para viajes de emergencia) en la se implica al nieto y que requiere el envío inmediato de una transferencia de dinero. No se ha producido ninguna emergencia y la víctima que envió dinero para ayudar a su nieto ha perdido su dinero.

Préstamos

¿Recibió una carta o un correo electrónico sobre la obtención de un préstamo? ¿Le solicitaron que enviara dinero en concepto de comisiones de préstamo, impuestos, comisiones de servicio, anticipos o cualquier otro motivo? Se trata de una ESTAFA. No envíe dinero a una compañía de préstamos para obtener un préstamo. Si el dinero se transfiere y se recibe, no se puede recuperar. Se perderá todo el dinero que ha enviado.

Cheque/Giro bancario

¿Recibió un cheque o giro bancario por correo con instrucciones de cobrarlo primero en su banco y luego enviar parte de los fondos a otra persona mediante una transferencia? Si es así, el cheque/giro bancario es falso y su banco le hará cubrir la pérdida. Tenga en cuenta que los cheques falsos son muy difíciles de identificar. Es posible que le hayan prometido un porcentaje del cheque por el empleo o por haber pagado de más. Se trata de una ESTAFA. No envíe el dinero ni cobre el cheque.

Estafa de romance/relación en línea

¿Conoció a alguien a través de un anuncio personal, un correo electrónico, una sala de chat o un mensaje instantáneo? ¿Le pidieron que les enviara dinero para viajar o que les ayudara económicamente? No envíe el dinero, se trata de una ESTAFA. El dinero recibido por esta persona no podrá recuperarse y usted perderá el dinero enviado.

Dr. TIMOTHY JOHN HAVARD



Se hace creer a la víctima que tiene una relación personal con alguien a quien conoció en Internet, a menudo a través de las redes sociales, en un foro en línea o en un sitio web de citas. La víctima suele implicarse emocionalmente y, con frecuencia, se refiere al destinatario/a como su prometido/a.

Anuncios en periódicos

¿Ha encontrado algo en venta en los anuncios clasificados o en cualquier tipo de anuncio de periódico? ¿Le pidieron que pagara el artículo mediante una transferencia de MoneyGram? Se trata de una ESTAFA. No realice ninguna transferencia de dinero para comprar un artículo a un desconocido. No es seguro utilizar un servicio de transferencia de dinero cuando se intenta comprar un artículo.

Estafa de abuso financiero a adultos mayores

Un desconocido inicia una relación estrecha con usted y se ofrece a manejar sus finanzas y patrimonio, o las firmas de los documentos no se parecen a su propia firma. No se deje engañar y pierda su dinero mediante estafas de abuso financiero. Los estafadores intentarán manipularle para que les entregue bienes o dinero, lo que puede acabar con su dinero en efectivo, su cuenta corriente o incluso los ahorros de toda una vida en una sola transacción. Las estafas de abuso financiero pueden adoptar muchas formas, entre ellas el fraude de telemarketing, el robo de identidad, los préstamos abusivos y las estafas de mejora del hogar y planificación del patrimonio. Nunca confíe su dinero a nadie que no conozca.

Todos los demás tipos de fraude al consumidor mencionados anteriormente también podrían estar dirigidos a personas mayores o de la tercera edad.

Fraude por pago anticipado

Se le solicita a la víctima que pague comisiones por adelantado por servicios financieros que nunca se prestan. Las víctimas suelen enviar una sucesión de transacciones para el pago de diversas comisiones por adelantado. Los métodos habituales pueden ser: subvenciones de tarjetas de crédito, préstamos, herencias o inversiones.

Fraude por soporte técnico, virus detectado

La víctima es contactada por alguien que afirma pertenecer a una conocida empresa informática o de software y que se ha detectado un virus en su computadora. Se informa a la víctima que se puede eliminar el virus y proteger la computadora por un módico precio mediante pago con tarjeta de crédito o transferencia de dinero. En realidad, no había ningún virus en su computadora y la víctima acaba de perder el dinero que envió para la protección.

Estafa laboral

La víctima responde a una oferta de empleo y es contratada para el trabajo ficticio y se le envía un cheque falso para los gastos relacionados con el trabajo. El importe del cheque supera los gastos de la víctima y ésta devuelve los fondos restantes mediante una transferencia. El cheque rebota y la víctima es responsable del importe total.

Extorsión

Amenazas de muerte, detención u otras exigencias por parte de los estafadores para obtener ilícitamente dinero, bienes o servicios de una víctima mediante coacciones que supuestamente debe y amenazas si no coopera.

Estafa con cheques falsos

A menudo se envía a las víctimas un cheque como parte de una estafa y se les dice que lo depositen y utilicen los fondos para gastos de empleo, compras por Internet, compras misteriosas, etc. El cheque es falso y la víctima es responsable de los fondos utilizados. Recuerde que los fondos de un cheque depositado en una cuenta no deben utilizarse hasta que el cheque se compense oficialmente, lo que puede tardar semanas.

Estafa por supuestos funcionarios de inmigración

Dr. TIMOTHY JOHN HAVARD



La víctima recibe una llamada de alguien que dice ser un funcionario de inmigración diciendo que hay un problema con el registro de inmigración de la víctima. Es posible que se facilite información personal y detalles sensibles relacionados con la situación migratoria de la víctima para que la historia parezca más real. Se exige el pago inmediato para solucionar cualquier problema con los antecedentes de la víctima y se puede amenazar con su deportación o encarcelamiento si no se efectúa el pago inmediatamente a través de una transferencia de dinero.

Estafa por cambio de divisa

Las redes sociales se están utilizando para atraer a nuevas víctimas a un viejo timo para hacerse rico rápidamente, en el que los usuarios anuncian formas de convertir \$100 en \$1,000 mediante la "conversión de dinero". La propuesta sugiere que los inversionistas pueden aprovechar las peculiaridades del sistema monetario para obtener más dinero y convertir unos pocos cientos de dólares en miles. Una vez que los estafadores tienen acceso al dinero en efectivo, suelen bloquear a la víctima para que no pueda ponerse en contacto con ellos a través de las redes sociales o el número telefónico.

Supuestos miembros del servicio militar

Los miembros del servicio militar son un objetivo atractivo para los estafadores por varias razones. Se aprovechan de la admiración generalizada por los militares y se hacen pasar por hombres y mujeres de servicio para engañar a la gente y que les envíen dinero.

Estafa de *Mystery Shopping*

El estafador se pone en contacto con la víctima a través de un sitio web de empleo o la víctima responde a un anuncio sobre una oportunidad laboral para evaluar un servicio de transferencia de dinero. El estafador suele enviar a la víctima un cheque para su depósito y le indica que envíe una transferencia, quedándose con una parte del cheque para su pagá. La víctima envía el dinero, el estafador lo recoge y, cuando el cheque no tiene fondos, la víctima se hace responsable del importe total.

Estafa por exceso de pago

El estafador envía a la víctima un cheque que parece válido como pago de un servicio o producto. Normalmente, el importe del cheque supera lo que la víctima espera recibir y el estafador le dice que le devuelva el excedente mediante una transferencia de dinero. Cuando el cheque no tiene fondos, la víctima debe hacerse cargo del importe total.

Estafa de suplantación de identidad (*phishing*)

Comunicación que se hace pasar por una entidad de confianza, como un banco o una compañía hipotecaria, con la intención de engañar a la víctima para que facilite información personal o contraseñas. Un *Phish* es un intento fraudulento, normalmente realizado a través de correo electrónico (aunque también puede hacerse por teléfono o SMS), para robar su información personal o propagar códigos o programas maliciosos en su computadora.

Estafa inmobiliaria

La víctima envía dinero para depositar en una inmueble alquilado y nunca recibe acceso a dicho inmueble o la víctima también puede ser el propietario de este a quien el arrendatario envía un cheque y le pide que devuelva una parte del mismo mediante una transferencia de dinero y el cheque rebota.

Estafa en las redes sociales

Si un ciberdelincuente accede a sus cuentas en las redes sociales, también tendrá acceso a sus amigos y familiares más cercanos. Los delincuentes y los estafadores pueden aprovecharse de la cantidad de información personal que la gente comparte en Internet y utilizarla para hacer propuestas hábiles y muy específicas a sus amigos y familiares, a menudo con peticiones de dinero.

Estafa por mensaje de texto (SMS/*Smishing*)

Dr. TIMOTHY JOHN HAVARD

Se recomienda extremar precauciones frente a textos que generen un sentido de urgencia, que le pidan que haga clic en un enlace que le lleve a un sitio comprometido o que le hagan divulgar involuntariamente algún dato personal que pueda ser utilizado en su contra.

Telemarketing

En general, el telemarketing abarca casi cualquier transacción comercial que implique el uso de un teléfono para realizar o recibir llamadas entre un consumidor y un agente telefónico (*telemarketer*) o vendedor para la transferencia de fondos, como transferencias de dinero en efectivo o fondos cargados en una tarjeta de prepago, como pago por bienes o servicios ofrecidos o vendidos a través del telemarketing, a menudo relacionados con una promoción de vacaciones "gratis" o con grandes descuentos, estafas de premios o sorteos, o la venta de revistas "de oferta".

Sensibilización sobre el tema de fraude:

Protéjase del fraude. Envía dinero sólo a amigos y familiares. Nunca envíe dinero a alguien que no conozca personalmente. Nunca comparta la información de su tarjeta prepago con nadie. Además, si conoce a la persona que le pide dinero, compruebe siempre que es quien dice ser. Si no reconoce el número desde el que le llaman, devuélvalas la llamada a su número de teléfono conocido para verificar su identidad.

Muchas veces los estafadores crean un sentido de urgencia para persuadir a la gente de que transfiera dinero rápidamente sin tener tiempo de verificar su historia. Nunca envíe dinero a nadie antes de verificar quién es o confirmar que la solicitud es legítima.

Confirme siempre cualquier situación de emergencia con otra persona cercana a la situación o con la propia persona devolviéndole la llamada a un número de teléfono conocido.

Nunca envíe nunca dinero por transferencia para una compra en línea. Los comerciantes legítimos dispondrán de métodos de pago en su sitio web.

Nunca envíe dinero por transferencia para un depósito o pago de un inmueble en alquiler si se trata de una persona o empresa que no conoce o con la que no ha establecido una relación comercial.

Nunca envíe dinero por transferencia para reclamar premios de lotería o premios ganados, especialmente si nunca ha jugado a la lotería y no recuerda haber participado en un sorteo o lotería. Sospeche siempre de los avisos de ganadores extranjeros de lotería.

Nunca envíe dinero por transferencia para pagar impuestos. EL IRS nunca enviará a un contribuyente una solicitud por correo electrónico o llamada telefónica para que pague los impuestos mediante transferencia electrónica.

Nunca envíe dinero por transferencia para una donación a una institución de beneficencia. Las instituciones de beneficencia legítimas dispondrán de diferentes opciones de pago que no requieren el envío de una transferencia electrónica.

Nunca envíe dinero por transferencia para un encargo de compra misteriosa o una oportunidad de empleo. Las oportunidades de empleo legítimas nunca le exigirán que envíe dinero antes de aceptar un encargo o trabajo.

Nunca envíe nunca dinero por transferencia a cambio de una comisión por tarjeta de crédito o préstamo. Las empresas constituidas no solicitarán una transferencia de dinero para el pago de comisiones. Dispondrán de otras opciones de pago para sus clientes.

Nunca envíe dinero por transferencia para resolver un asunto de inmigración. El gobierno nunca llamará o enviará un correo electrónico a alguien para solicitarle el pago mediante transferencia de dinero por un asunto de inmigración.

Nunca envíe dinero por transferencia para pagar algo en respuesta a una llamada de telemarketing. Es ilegal que los agentes telefónicos soliciten el pago mediante transferencia de dinero a cualquier persona en Estados Unidos.

Su dinero no es el único objetivo del fraude. Sus datos personales también son un objetivo. ¿Por qué? Esto es muy sencillo. Los estafadores rara vez actúan bajo su propio nombre. Utilizan sobre todo datos de terceros. Para ello, los adquieren robando la identidad de otras personas.

Dr. TIMOTHY JOHN HAVARD



Otro método consiste simplemente en robar una identificación personal. Por ello, en caso de pérdida o robo de su documento de identidad o pasaporte, debe presentar inmediatamente una denuncia a la policía. También debe informar a su banco. Tomar estas medidas le ayudará a evitar la desagradable sorpresa de descubrir que alguien solicitó un préstamo o cometió un delito utilizando sus datos.

Correos electrónicos de suplantación de identidad (phishing)

Las contraseñas y los identificadores tienen un gran valor para los ciberdelincuentes. Enviar correos electrónicos de *phishing* a un montón de direcciones de correo electrónico aleatorias es una forma fácil que tienen los estafadores de robar información a personas desprevenidas. Probablemente sea un correo de *phishing* si:

- el correo electrónico está mal escrito, con faltas de ortografía y gramática incorrecta, o el nombre de una empresa conocida está mal escrito.
- su nombre no está en la línea "Para". Es probable que este correo electrónico se haya enviado a miles de personas.
- la dirección de correo electrónico del remitente es sospechosa; podría tener una empresa u organización gubernamental conocida que esté mal escrita.
- el correo electrónico no utiliza su nombre. Cualquier institución financiera en la que tenga una cuenta conoce su nombre. Los correos electrónicos que empiece por "Estimado cliente", "A quien corresponda" o incluso "Hola" puede ser un indicio de estafa.
- la URL es falsa. Pasa el ratón por encima del enlace "haga clic aquí" o "actúe ahora". Si ve una URL extraña en lugar del sitio web legítimo de una empresa, no haga clic en ella.
- se le informa que hay una vulneración en la seguridad en su cuenta y, si no tomas las medidas recomendadas en el correo electrónico, su cuenta será suspendida.
- El correo electrónico le solicita información personal sobre su tarjeta de crédito o cuenta en línea o le lleva a un sitio web que se la solicita. Las empresas legítimas que manejan su información financiera no se lo solicitarán.

Si recibes un correo electrónico sospechoso:

- No lo abra; elimínalo inmediatamente y por completo. Asegúrate de eliminarlo también de la carpeta de correos eliminados.
- nunca haga clic en ninguno de los enlaces del correo electrónico, aunque sea para "darse de baja" del remitente. Tampoco abra ningún archivo adjunto al correo electrónico sospechoso.
- recuerde en todo momento que Broxel nunca le enviará un correo electrónico solicitándole su ID, contraseña o información personal. Si no está seguro de si un correo electrónico proviene de nosotros o no, póngase en contacto con nosotros para verificar la solicitud de información. Mientras tanto, no abra ningún enlace, no haga clic en ningún archivo adjunto ni facilite ninguna contraseña o identificación de usuario hasta que verifique la legitimidad de la solicitud.

Otra técnica de extorsión de dinero es la acción de los estafadores que intentan instalar malware en su ordenador. Esto les permite tomar el control del dinero cuando usted está haciendo una transferencia de dinero en línea. Los programas maliciosos pueden instalarse inconscientemente al abrir un archivo adjunto a un correo electrónico de un destinatario desconocido. Este tipo de software puede cambiar el número de cuenta bancaria del destinatario al enviar una transferencia de dinero en línea. Se puede contrarrestar comprobando minuciosamente los detalles de la transferencia durante su autorización, por ejemplo, a través de un mensaje de texto.

Protegerse contra el fraude al consumidor

Dr. TIMOTHY JOHN HAVARD



¿Cómo protegerse de los estafadores que quieren quedarse con su dinero? Debe conocer sus trucos, utilizar el sentido común y seguir los consejos que se mencionan a continuación. De usted depende que los estafadores puedan quedarse con su dinero. Recuerde siempre que el estafador puede tener éxito o fracasar en función de que usted participe en la estafa. Estos son algunos consejos que debe recordar para protegerse del fraude en las transferencias bancarias:

- Sepa siempre con quién está tratando, sobre todo si se trata de un premio no solicitado o de una oferta de regalo. No te fíes de los mensajes que provengan de personas o instituciones desconocidas.
- Investigue siempre una oferta para asegurarte de que es real. Si parece demasiado bueno para ser verdad, probablemente lo sea.
- Recuerde siempre que enviar una transferencia bancaria es como enviar dinero en efectivo. Una vez que lo envíe y lo haya recibido el beneficiario, no podrá recuperarlo.
- Nunca envíe una transferencia bancaria a alguien que no conoce.
- Nunca envíe una transferencia de dinero a alguien que le pida que deposite un cheque y luego le devuelva una parte del dinero sin esperar a que el cheque se abone primero en su cuenta bancaria.
- Nunca envíe una transferencia a un familiar en crisis sin comprobar antes la historia. Realice preguntas para verificar la identidad de la persona.
- Nunca envíe una transferencia para recibir dinero o algo de valor a cambio después de que el dinero ya haya sido enviado.

Preguntas frecuentes sobre el fraude:

Cuanto más sepa, menos probabilidades tendrá de ser víctima de un fraude. A continuación le presentamos las preguntas más frecuentes relacionadas con el fraude:

¿Qué hago si me han estafado?

Póngase en contacto inmediatamente con la policía local.

Denuncie cualquier sospecha de fraude telefónico o por Internet enviando una denuncia en línea al Centro de Fraudes de la Liga Nacional de Consumidores (*National Consumers League's Fraud Center*).

Presente una queja ante la Comisión Federal de Comercio o llame gratis al 1-877-FTC-HELP

Presente una denuncia ante su Fiscal General.

Si ha utilizado Broxel para enviar dinero o ha utilizado su cuenta de tarjeta de prepago como resultado de una estafa, póngase en contacto con nosotros al número 1-855-279-2720 o por correo electrónico o denuncie el fraude a través de nuestro formulario en línea.

¿Qué hago si me han estafado en línea?

Si ha sido víctima de un fraude a través de Internet, presente una denuncia ante la policía local y el Centro de Denuncias de Delitos por Internet (CCCC), una asociación entre el FBI y el Centro Nacional de Delitos Patrimoniales (*National White Collar Crime Center*).

Si ha utilizado Broxel para enviar dinero o ha utilizado su cuenta de prepago como resultado de una estafa, póngase en contacto con nosotros al número 1-855-279-2720 o por correo electrónico o denuncie el fraude a través de nuestro formulario en línea.

¿Cuáles son los tipos de fraude más comunes?

Sírvase consultar la sección Tipos de fraude/estafa para ver los distintos tipos de fraude/estafa.

Dr. TIMOTHY JOHN HAVARD



¿Cuáles son las señales de advertencia de fraude en las transferencias de dinero?

- Alguien que no conoce le pide que le transfiera dinero.
- Alguien le solicita que deposite un cheque y le devuelvas una parte del dinero.
- Alguien se hace pasar por un amigo o familiar y llama en un momento de crisis pidiéndole que le envíe dinero de inmediato.
- Alguien le dice que ha ganado un premio o un concurso en el que no recuerda haber participado y le solicita que envíe dinero para pagar aranceles, impuestos o derechos.

¿Existe algún riesgo en el envío de dinero?

Sí, cuando no sabes a quién se le envía el dinero. Enviar una transferencia bancaria es lo mismo que enviar dinero en efectivo. Una vez que lo envíe, no podrá recuperarlo, ya que los estafadores suelen recoger el dinero en cuestión de minutos.

¿Cuáles son las señales de alarma del fraude con tarjetas de prepago?

- Alguien que no conoces te pide que le facilites los datos de tu cuenta de prepago.
- Ofertas que le piden que pague una cuota por adelantado utilizando su cuenta de prepago para cobrar un premio o sorteo.
- Se le pide que proporcione la información de su cuenta de prepago para una compra en línea.

Denuncie el fraude:

Póngase en contacto con Broxel si alguien intenta estafarle o defraudarle o si ha sido víctima de un fraude:

Llámenos al: 1-855-279-2720

O bien, puede enviarnos un correo electrónico a reportfraud@broxel.com

También puede considerar la posibilidad de denunciar el fraude a las siguientes autoridades:

- Póngase en contacto con el departamento de policía local y presente una denuncia.
- Formulario de denuncia en línea de la FTC
- Línea directa gratuita de la FTC: 877-FTC-HELP (877-382-4357)
- Centro de Fraudes de la Liga Nacional de Consumidores
- Centro de Denuncias de Delitos por Internet (CCCC)

Dr. TIMOTHY JOHN HAVARD