

NO SEA
ESTAFADO



www.tn.gov/consumer

NO SEA ESTAFADO

Índice

Fraudes en subastas	1
Cheques de gerencia falsos	1
Fraudes con tarjetas de crédito	1
Eliminación de deudas	2
DHL/UPS	2
Oportunidades de empleo o negocios	2
Fraudes con servicios de depósitos en garantía (escrow)	3
Hurto de identidad	3
Extorsión por Internet	4
Inversiones fraudulentas	4
Loterías	4
La Carta de Nigeria o “419”	5
Suplantación de identidad (Phishing/Spoofing)	5
Fraudes de Ponzi o de pirámide	5
Reenvíos	6
Cobro de fondos por terceros	6
Transferencias de dinero fraudulentas	6
Loterías y concursos fraudulentos:.....	6
Fraudes de sobrepagos.....	6
Fraudes por relaciones.....	7
Fraudes de “comprador misterioso”.....	7
Fraudes de compras en Internet.....	7
Fraudes de alquileres de apartamentos.....	7
Fraudes de tarifas adelantadas para préstamos.....	8
Fraudes de emergencias o familiares en apuros.....	8

NO SEA ESTAFADO

Fraudes en subastas

- Antes de hacer una oferta, contacte al vendedor y haga las preguntas que sean necesarias.
- Examine las respuestas del vendedor.
- Tenga cuidado cuando trate con personas que estén fuera de su país.
- Comprenda las políticas de reembolsos, retornos y garantías.
- Verifique los cargos de envío antes de hacer la compra.
- Tenga cuidado si el vendedor solo acepta transferencias cablegráficas o efectivo.
- Si se utiliza un servicio de depósitos en garantía, asegúrese de que sea legítimo.
- Considere asegurar su compra.
- Tenga cuidado con ofertas no solicitadas.



Cheques de gerencia falsos

- Inspeccione el cheque de gerencia.
- Asegúrese que los montos en letras y números sean iguales.
- Asegúrese que no se brille el número de cuenta en el cheque.
- Asegúrese que la firma del girador no haya sido calcada.
- Generalmente los cheques oficiales tienen un lado perforado.
- Busque añadiduras, borraduras u otras alteraciones en el cheque.
- Contacte a la institución financiera emisora para verificar la autenticidad del cheque.
- Obtenga el número telefónico del banco de una fuente confiable, no del mismo cheque.
- Tenga cuidado cuando trate con personas que estén fuera de su país.

Fraudes con tarjetas de crédito

- Asegúrese de que un sitio de Internet sea seguro y confiable antes de dar su número de tarjeta de crédito.
- No confíe en un sitio de Internet solo porque indique que es seguro.
- Si compra mercancía, asegúrese de que provenga de una fuente confiable.
- Concilie prontamente los estados de cuenta de sus tarjetas de crédito para evitar cargos no autorizados.



- Indague usted mismo la autenticidad de una persona o empresa.
- Tenga cuidado con proporcionar su información sobre tarjetas de crédito cuando se pide en cartas postales no solicitadas.

Eliminación de deudas

- Sepa con quién está tratando — haga su propia investigación.
- Obtenga el nombre, la dirección y el número telefónico de la persona o compañía.
- Investigue a la persona o compañía para verificar su autenticidad.
- Contacte a la Oficina de Buenas Prácticas Comerciales (Better Business Bureau) para verificar la autenticidad de la compañía.
- Tenga cuidado cuando trate con personas que estén fuera de su país.
- Asegúrese de que comprenda los términos y condiciones de cualquier acuerdo.
- Cuídese de negocios cuya dirección sea un apartado o una casilla de correo.
- Solicite nombres de otros clientes de la persona o compañía y contáctelos.
- Si suena demasiado bueno para ser cierto, probablemente lo sea.



DHL/UPS

- Cuídese de personas que usan el logotipo de DHL o UPS en correos electrónicos.
- Sea precavido si le piden que transfiera dinero para pagar bienes antes de que sean enviados.
- Recuerde que DHL y UPS generalmente no cobran pagos directamente a los clientes.
- DHL o UPS solamente cobran tarifas asociadas con envíos de mercancía y nunca con otros costos relacionados con transacciones en línea.
- Contacte a DHL o UPS para confirmar la autenticidad de los correos electrónicos que reciba.

Oportunidades de empleo o negocios

- Tenga cuidado con afirmaciones exageradas sobre la efectividad de un producto.
- No confíe en afirmaciones exageradas de posibles ganancias o rendimientos.
- Cuídese si le piden dinero por adelantado para obtener instrucciones o productos.

- Sea cauteloso si la oferta de empleo indica “no requiere experiencia previa”.
- No entregue su número de seguro social durante el contacto inicial con un empleador posible.
- Tenga cuidado cuando trate con personas que estén fuera de su país.
- Sea precavido cuando responda a correos electrónicos no solicitados que le ofrecen trabajar desde su hogar.
- Investigue a la compañía para verificar su autenticidad.
- Contacte a la Oficina de Buenas Prácticas Comerciales (Better Business Bureau) para verificar la autenticidad de la compañía.

Fraudes con servicios de depósitos en garantía (Escrow)

- Escriba siempre la dirección del sitio web en vez de hacer clic en el vínculo proporcionado.
- Un sitio web legítimo es siempre único y no imita la labor de otras compañías.
- Tenga cuidado si un sitio web solicita pagos a nombre de un “agente” en vez de a una entidad corporativa.
- Cuídese de sitios que aceptan depósitos en garantía solamente a través de transferencias o dinero electrónico.
- Fíjese si hay errores ortográficos, defectos gramaticales o información inconsistente.
- Tenga cuidado con sitios web que cobran tarifas muy bajas para depósitos en garantía.



Hurto de identidad

- Verifique la seguridad de los sitios web antes de proporcionar su número de tarjeta de crédito.
- Investigue la empresa o el sitio web para verificar su autenticidad.
- Intente obtener una dirección física en vez de un apartado o una casilla de correo.
- Nunca deseche sus tarjetas de crédito o estados de cuenta bancarios de forma que los puedan utilizar.
- Fíjese si no le ha llegado alguna cuenta ya que podría indicar que ha sido intervenida.
- Cuídese de estafas en las cuales le piden que divulgue información personal.
- Nunca dé su número de tarjeta de crédito por teléfono a menos que usted haya hecho la llamada.
- Revise mensualmente sus estados de cuenta crediticios para detectar actividades fraudulentas.
- Reporte tan pronto sea posible cualquier transacción no autorizada a su banco o empresa de tarjeta de crédito.

- Examine su informe de crédito como mínimo una vez al año.

Extorsión por Internet

- Proteja su seguridad detrás de múltiples barreras para interponer numerosos obstáculos ante los intrusos.
- Instale sistemas de seguridad en todos los posibles puntos de entrada.
- Identifique todas las unidades que están conectadas a Internet y evalúe el mecanismo de defensa que utilizan.
- Determine si sus servidores utilizan puertos que tienen vulnerabilidades conocidas.
- Asegúrese de que su software tenga instaladas las revisiones más actualizadas.



Inversiones fraudulentas

- Si una “oportunidad” parece demasiado buena para ser cierta, probablemente lo sea.
- Cuidado con promesas de obtener ganancias rápidamente.
- No invierta en nada a menos que comprenda las condiciones.
- No asuma que una empresa es legítima por el “aspecto” del sitio web.
- Sea cauteloso cuando responda a ofertas de inversiones que reciba a través de cartas no solicitadas.
- Tenga cuidado con inversiones que ofrecen grandes retornos a cambio de poco o ningún riesgo.
- Verifique por cuenta propia los términos de cualquier inversión que vaya a hacer.
- Investigue las partes involucradas y la naturaleza de la inversión.
- Tenga cuidado cuando trate con personas que estén fuera de su país.
- Contacte a la Oficina de Buenas Prácticas Comerciales (Better Business Bureau) para verificar la autenticidad de la compañía.



Loterías

- Si los premios de una lotería parecen demasiado buenos para ser ciertos, probablemente lo sean.
- Tenga cuidado cuando trate con personas que estén fuera de su país.
- Sea cauteloso si no recuerda haberse inscrito en una lotería o un concurso.
- Tenga cuidado si lo llaman por teléfono para informarle que ha ganado una lotería.

- Cuídese de loterías que cobran una tarifa antes de entregarle el premio.
- Cuídese de solicitudes de enviar dinero adicional con el fin de calificarlo para futuros premios.
- Las leyes federales prohíben participar en loterías del extranjero por correo o teléfono.

La Carta de Nigeria o “419”

- Si una “oportunidad” parece demasiado buena para ser cierta, probablemente lo sea.
- No responda a correos electrónicos que soliciten su información bancaria personal.
- Cuídese con personas que aseguran ser funcionarios de gobiernos extranjeros.
- Tenga cuidado cuando trate con personas que estén fuera de su país.
- Sea precavido si le piden que ayude a colocar grandes sumas de dinero en una cuenta bancaria de otro país.
- No crea en promesas de pagarle grandes sumas de dinero a cambio de su cooperación.
- Proteja cuidadosamente la información de sus cuentas.
- Tenga cuidado si le piden pagar tarifas adicionales para continuar una transacción.



Suplantación de identidad (Phishing/Spoofing)

- No confíe en correos electrónicos no solicitados que le pidan información personal.
- No llene formularios en correos electrónicos que le pidan información personal.
- Compare siempre los vínculos en el correo electrónico con el vínculo al cual lo envían.
- Conéctese al sitio web oficial en vez de hacerlo a través del vínculo en el correo electrónico no solicitado.
- Contacte a la empresa desde la cual se le envió supuestamente el correo electrónico para verificar su autenticidad.



Fraudes de Ponzi o de pirámide

- Si una “oportunidad” parece demasiado buena para ser cierta, probablemente lo sea.
- Cuidado con promesas de obtener ganancias rápidamente.
- Estudie cuidadosamente cualquier inversión antes de seleccionarla.
- Investigue bien con quién elige hacer inversiones.
- Asegúrese de comprender bien la inversión antes de involucrarse.

- Tenga cuidado si le piden que solicite la participación de más inversionistas.
- Verifique independientemente la autenticidad de cualquier inversión.
- Tenga cuidado con las referencias que le proporcione el promotor de la inversión.

Reenvíos

- Tenga cuidado si le piden que envíe paquetes a la “sede de una empresa situada en otro país”.
- Tenga cuidado cuando trate con personas que estén fuera de su país.
- Sea cauteloso si la persona indica que su país no permite recibir envíos comerciales directamente de los Estados Unidos.
- Tenga cuidado si la dirección del destinatario es la suya pero no así el nombre en el paquete.
- Nunca proporcione su información personal a desconocidos en salones de chat.
- No acepte paquetes que no haya pedido.
- Si recibe paquetes que no ha pedido, rechácelos en la entrega o contacte a la compañía que los envió.



Cobro de fondos por terceros

- No se comprometa a aceptar pagos electrónicos por subastas en las que no ha participado.
- Tenga cuidado si la persona afirma que el gobierno de su país dificulta la transferencia de este tipo de fondos.
- Sea cauteloso si la oferta de empleo indica “no requiere experiencia previa”.
- Tenga cuidado cuando trate con personas que estén fuera de su país.

Transferencias de dinero fraudulentas

Las transferencias de dinero fraudulentas pueden involucrar relatos dramáticos o persuasivos. Algunos ejemplos de estos relatos son:

Loterías y concursos fraudulentos: La carta dice que usted ha ganado una lotería. Lo único que tiene que hacer es depositar un cheque de gerencia que se adjunta y transferir dinero para cubrir “impuestos” y “tarifas”. Independientemente de lo legítimo que parezca el cheque, es falso. Cuando rebote, usted habrá perdido el dinero que envió.

Fraudes de sobrepagos: Alguien responde su aviso para vender un producto y ofrece pagarle con cheque de gerencia, cheque personal o cheque corporativo. Pero en el último momento, el comprador (u otra persona relacionada) encuentra una razón para entregarle un cheque por una cantidad superior al precio de venta

y le pide que transfiera la diferencia electrónicamente. El cheque falso podría engañar a los cajeros del banco, pero eventualmente rebotará y usted tendrá que cubrirlo.



Fraudes por relaciones: Usted conoce a alguien a través de un servicio de citas en Internet y comienzan a corresponderse. Se envían mensajes, hablan por teléfono, se intercambian fotografías y hasta planifican su boda. Pero él le informa que tiene que viajar a Nigeria u otro país por motivo de trabajo. Una vez ahí, solicita su ayuda: ¿Puede transferirle dinero para ayudarlo temporalmente? La primera transferencia podría ser pequeña, pero después le pide más –para ayudarlo a recuperar dinero que le debe el gobierno, a cubrir costos por una enfermedad o una cirugía repentina para su hijo o hija, para pagar el vuelo de regreso a los Estados Unidos– siempre con la promesa de que le devolverá el dinero. Usted podría recibir documentos o llamadas de abogados que “comprueban” lo anterior. Pero por más real que parezca la relación, es una estafa. Usted perderá el dinero que transfirió, junto con la persona que pensaba que conocía tan bien.

Fraudes de “comprador misterioso”: Lo contratan para ser un comprador misterioso y le piden que evalúe el servicio de atención al cliente de una empresa de transferencia de dinero. Se le envía un cheque para que lo deposite en su cuenta bancaria e instrucciones para que retire la cantidad en efectivo y la transfiera, generalmente a Canadá u otro país, a través de su servicio cablegráfico. Cuando se descubre que el cheque es falso, usted ya ha perdido su dinero.



Fraudes de compras en Internet: Usted compra algo en línea y el vendedor insiste que el único método de pago aceptable es una transferencia de dinero. Solicite pagar con tarjeta de crédito, un servicio de depósitos en garantía u otro método. Si paga en línea con una tarjeta de crédito o tarjeta de cargo, su transacción estará protegida por la Ley de facturación crediticia justa (Fair Credit Billing Act). Si le insisten que pague con una transferencia de dinero, es probable que nunca reciba su producto, ni su dinero.

Fraudes de alquileres de apartamentos: Al buscar un apartamento o propiedad vacacional en alquiler, encuentra una opción perfecta por un excelente precio. Puede reservar la propiedad si transfiere dinero para cubrir la tarifa de reserva, el depósito de garantía y el primer mes de alquiler. Después de transferir el dinero usted descubre que ha desaparecido y no existe tal propiedad. Un estafador obtuvo un aviso de alquiler de propiedad legítimo, cambió la información de contacto y publicó el aviso modificado en otros sitios. O bien, publicó un sitio que no está en alquiler o no existe por un precio inferior al del mercado para

atraerlo. Si usted es quién ofrece una propiedad en alquiler, cuídese de lo contrario: un posible arrendatario le informa que ha decidido cancelar su depósito y le pide que le devuelva su dinero mediante una transferencia antes de que usted se dé cuenta de que le había entregado un cheque falso.

Fraudes de tarifas adelantadas para préstamos: Usted lee un aviso o un sitio web, o recibe una llamada telefónica, que le garantiza un préstamo o una tarjeta de crédito, independientemente de su historial crediticio. Mientras completa la solicitud descubre que tiene que pagar una tarifa por adelantado. Si tiene que transferir dinero a cambio de un préstamo o una tarjeta de crédito, está tratando con un estafador: no recibirá ningún préstamo ni la tarjeta de crédito.



Fraudes de emergencias o familiares en apuros:

Usted recibe una llamada o un correo electrónico inesperado que le informa sobre una persona que dice ser un familiar o amigo, que necesita que le transfiera dinero para sacarlo de un apuro: para arreglar su automóvil, salir de prisión o del hospital o regresar de otro país. Pero quiere que no se lo diga a nadie en la familia.

Desafortunadamente, es probable que se trate de un estafador utilizando el nombre de un familiar. Verifique lo que le comunican con otras personas en su familia. También puede hacer preguntas sobre su familia que una persona desconocida no podría responder a la persona que lo ha llamado.





División de Asuntos del Consumidor de Tennessee



Formulario para quejas

500 James Robertson Parkway, 12th Floor
Davy Crockett Tower
Nashville, TN 37243
615-741-4737

www.tn.gov/consumer



Contáctenos



Departamento de Comercio y Seguros, autorización No. 335397, 3,000 copias, julio de 2011. Este documento público fue promulgado a un costo de \$0.49 por copia.

El costo para esta publicación provino de un fondo de reserva sin costo alguno para los contribuyentes de Tennessee.