Guía para estudiantes
FRAUDES Y ESTAFAS

Guía para estudiantes: Fraudes y estafas

ÍNDICE

Tipos de estafas

1. Estafa con tarjetas de débito – Robo de Tarjetas

¿En qué consiste la práctica conocida como Robo de Tarjetas?

Un estudiante abre una nueva cuenta bancaria, generalmente con poco dinero ($10-$25). El estudiante le da su tarjeta de débito y su PIN a un tercero. Este deposita cheques robados o falsificados en la cuenta y retira el dinero antes de que los cheques sean rechazados. Luego le dice al estudiante que denuncie al banco el extravío de la tarjeta de débito. Si le preguntan cómo obtuvo el PIN el estafador, el estudiante debe responder que escribió el PIN en un trozo de cinta adhesiva y lo pegó en el reverso de la tarjeta.

Técnicas de reclutamiento

Los estafadores suelen usar redes sociales para reclutar estudiantes con la promesa de dinero rápido. Aquí hay algunos ejemplos extraídos de cuentas de redes sociales:

CONSEJOS DE PREVENCIÓN

- Nunca compartas tu tarjeta de débito o PIN con nadie.
- Nunca deposites cheques ni giros de origen desconocido en tu cuenta.
- No participes de un plan delictivo. Defraudar a un banco es ilegal.

En casos recientes se presentaron cargos penales contra estudiantes por asociación ilícita y hurto.

**Visita guardyourstash.com para ver videos de prevención.*

2. Estafa del impuesto estudiantil

Durante varios años se han cometido estafas impositivas contra víctimas en todo Estados Unidos. Estas estafas suelen aumentar en la temporada de impuestos, pero últimamente los estafadores están llevando a cabo este fraude durante todo el año. Existen distintos tipos de estafas "impositivas". En una de ellas, el estudiante recibe una llamada telefónica o un correo electrónico donde se le notifica que no ha pagado el impuesto estudiantil. Luego se le pide que transfiera el impuesto impago a una cuenta designada. El impuesto estudiantil suele ser un valor nominal, de menos de $100.

En otro caso, el estafador informa al estudiante que existe una orden judicial en su contra por impuestos impagos y que debe pagar para no ser arrestado. La estafa funciona así:

- El estudiante recibe una llamada desde un número de teléfono que parece tener un código de área de Washington, DC. A continuación se incluye la transcripción de un mensaje de voz de un estafador real:

  *"Mi nombre es **** y llamo en relación con una acción de ejecución iniciada por el Tesoro de los Estados Unidos. Se trata de una acción muy seria. Si ignora esta llamada, se entenderá que se ha negado por segunda vez a comparecer ante un juez o un gran jurado por un delito federal. Mí número es (***) ***-****. Repito (***) ***-****). Le aconsejo que coopere con nosotros y nos ayude a ayudarlo. Gracias".*

- Cuando el estudiante llama al número de teléfono, el estafador responde: "Servicio de Impuestos Internos". A veces el estafador usa un lenguaje amenazante para conseguir que el estudiante coopere, le dice que debe pagar el dinero inmediatamente, y lo amenaza con arrestarlo y posiblemente deportarlo.

- El estafador informa al estudiante que puede pagar sus impuestos por medio de tarjetas de regalo, transferencias bancarias o en efectivo.
- Así convencen a algunos estudiantes de pagar los impuestos adeudados con tarjetas de iTunes, Green Dot, Google Pay y Steam. El estafador le pide al estudiante que le dé los números impresos en el reverso de la tarjeta. Esto agiliza la estafa.

CONSEJOS DE PREVENCIÓN

- Algunas facultades y universidades cobran una cuota (impuesto) a los estudiantes matriculados. Antes de pagar la cuota, contacta a la Tesorería para verificar que sea legítima.
- El Servicio de Impuestos Internos **no** contacta contribuyentes por correo electrónico, mensaje de texto ni redes sociales para solicitar información personal o financiera. La mayoría de las comunicaciones se realizan por correo a través del Servicio Postal de los Estados Unidos.
- El Servicio de Impuestos Internos nunca llamará para exigir un pago inmediato a través de un medio específico, como una tarjeta de débito prepaga, una tarjeta de regalo o una transferencia bancaria.
- El Servicio de Impuestos Internos nunca amenazará con hacerte arrestar por la policía local, oficiales de inmigración u otras fuerzas de seguridad por falta de pago. El Servicio de Impuestos Internos tampoco puede revocar tu licencia de conducir, licencias comerciales ni situación migratoria. Este tipo de amenazas son tácticas comunes usadas por los estafadores para engañar a sus víctimas.

3. Estafas de soporte técnico

El estafador contacta al estudiante para ofrecerle un servicio de soporte técnico. Las víctimas suelen ser usuarios de Microsoft Windows. El estafador afirma ser un Empleado de Soporte Técnico de Microsoft. Estas llamadas se originan principalmente desde centros de atención al cliente en la India. El estafador intentará que la víctima le conceda acceso remoto a su computadora. Una vez obtenido el acceso remoto, el estafador realiza trucos con herramientas integradas en Windows y otros programas para ganarse la confianza de la víctima y convencerla de que le pague por sus servicios. El estafador roba información de la tarjeta de crédito de la víctima o la persuade para que inicie sesión en la página de su banco. Para ello, le dice que está conectada a un servidor seguro y no puede acceder a la información necesaria para realizar un reembolso.

Funcionamiento – Estas estafas se basan en la ingeniería social. Los estafadores usan numerosos trucos para ganarse la confianza de los estudiantes y convencerlos de instalar un software de escritorio remoto. Una vez que tienen acceso a la computadora, toman el control de este y usan varios componentes y herramientas de Windows para hacer creer al estudiante que la computadora tiene problemas que deben ser reparados.

Inicio – Estas estafas de soporte técnico comienzan de diversas formas. Suelen comenzar con una llamada en frío de un supuesto prestador de servicios de Soporte Técnico de Microsoft o Windows. También se publicitan en motores de búsqueda como Bing o Google. Algunas estafas se inician a través de ventanas emergentes en sitios web infectados, en los que se indica a los estudiantes que llamen a un número de teléfono. Estas ventanas emergentes suelen simular mensajes de error, como la pantalla azul de la muerte.

Acceso remoto – El estafador indica al estudiante que descargue e instale un programa de acceso remoto, como Team Viewer, LogMeIn GoToAssist o ConnectWise Control, y le da instrucciones para poder controlar su computadora a distancia con ese programa.

CONSEJOS DE PREVENCIÓN

- **Nunca cedas el control de tu computadora** a un tercero a menos que sepas que es el representante de un equipo de soporte técnico con quien tú te has puesto en contacto. Los estafadores pueden robar tu información personal e instalar software maliciosos que luego se utilizan para cometer robos de identidad.
- **Desconfía de las llamadas no solicitadas.** Las empresas de tecnología legítimas no hacen llamadas no solicitadas a sus clientes. Esta es una táctica de estafa muy popular. Recuerda que los estafadores pueden falsificar números de teléfono de aspecto oficial, así que no confíes en tu identificador de llamadas.
- **Cuídate de las ventanas de advertencia.** Casi la mitad de las estafas de soporte técnico comienzan con una advertencia en la computadora del estudiante. Estas ventanas emergentes incluyen un número de teléfono al que llamar para pedir ayuda. En lugar de llamar, apaga tu computadora y reiníciala.
- **No hagas clic en enlaces incluidos en correos electrónicos de remitentes desconocidos.** Los estafadores también utilizan el correo electrónico para llegar a los estudiantes. Estos mensajes dirigen a los consumidores a sitios web que abren ventanas emergentes con advertencias falsas y números de teléfono.
- **Ten cuidado si alguien te pide un pago imposible de rastrear.** Los estafadores suelen solicitar pagos por transferencia bancaria, tarjetas de regalo o tarjetas de débito prepagas. Las empresas legítimas no solicitan pagos por estos medios.
- **Descarga software sólo de sitios de proveedores oficiales o de la tienda de Microsoft.** Desconfía de las descargas de software de sitios de terceros. Estos sitios pueden incluir software modificados sin el conocimiento del propietario que incluyan software malicioso de soporte u otras amenazas.
- **Usa Microsoft Edge para navegar por Internet.** Este navegador bloquea los sitios de estafa de soporte técnico conocidos a través de Windows Defender SmartScreen. Nunca llames a los números que aparecen en ventanas emergentes. Los mensajes de error y advertencias de Microsoft nunca incluyen un número de teléfono.
- **Activa el antivirus Windows Defender en Windows 10.** Este detecta y elimina el software malicioso de estafa de soporte conocido.

4. Estafa de Instagram

Recientemente, los estafadores han comenzado a contactar estudiantes a través de Instagram. El tema del mensaje suele ser de interés para un estudiante universitario, como “ahorra dinero con esta nueva app”. Este mensaje irá seguido de un enlace (normalmente una URL acortada con bit.ly).

Al hacer clic en el enlace, se autoriza a un tercero a acceder a tu cuenta de Instagram. Los estafadores utilizarán tu cuenta para publicar anuncios en tu perfil, enviar mensajes a tus amigos y comentar anuncios/spam en las publicaciones de otras personas.

CONSEJOS DE PREVENCIÓN

- **No abras mensajes de usuarios desconocidos.** Si no conoces al remitente, ignora el mensaje. Si ves un enlace que no conoces, no hagas clic en él.
- **Si ya hiciste clic en el enlace** y detectas una actividad sospechosa, revisa tu lista de aplicaciones autorizadas. Para ello, inicia sesión en un navegador web y ve a Editar perfil > Aplicaciones autorizadas > Revocar Acceso. Para mayor seguridad, cambia también tu contraseña.

5. Estafas de becas/préstamos estudiantiles

Los estudiantes son blanco de varias estafas que incluyen ofertas de becas garantizadas, asistencia financiera y ofertas de cancelación de deuda por préstamos estudiantiles. Los estafadores se aprovechan de las necesidades financieras del estudiante con la promesa de una beca importante o de un préstamo más barato. En realidad, su objetivo es conseguir que el estudiante pague por adelantado o pague aranceles por los que no recibirá ningún beneficio, o bien obtener la información personal identificable (IPI) del estudiante, sus números de cuenta bancaria o datos de tarjeta de crédito.

Becas

Muchas de estas estafas ofrecen una beca garantizada falsa. Los estafadores no garantizan ninguna beca y suelen pedir un arancel de gestión, procesamiento o inscripción por adelantado. Una vez pagado el arancel, el estafador solicita pagos adicionales o no vuelve a contactar al estudiante. Las solicitudes de becas deben ser presentadas por el estudiante, no por un tercero. El estudiante debe escribir sus propios ensayos y reunir sus propias cartas de recomendación. El hecho de que un tercero se ofrezca a hacer todo esto por ti debería ser una señal de que se trata de una estafa. Otra señal de alarma es un correo electrónico o una llamada telefónica informándote que has obtenido una beca que nunca solicitaste. Los estafadores suelen utilizar tácticas de presión y aconsejar al estudiante que actúe rápido a riesgo de perder la beca. En realidad, sólo intentan obtener tu información financiera.

Préstamos y cancelación de deuda

En algunos casos, las empresas de préstamos fraudulentas te dirán que pueden conseguirte las mejores tasas de interés a cambio del pago de un arancel nominal. Los préstamos estudiantiles legítimos no requieren el pago de aranceles por adelantado. Los gastos de procesamiento se incluyen en el importe a devolver o se deducen del monto prestado. Las ofertas fraudulentas de consolidación de préstamos suelen exigir a los estudiantes que paguen un arancel de consolidación por adelantado y luego no cumplen la promesa. Los préstamos estudiantiles pueden consolidarse gratuitamente en **https://studentloans.gov/myDirectLoan/index.action**

La eliminación de deudas por préstamos estudiantiles también es una estafa conocida. La deuda por préstamos estudiantiles legítimos debe cancelarse en su totalidad y sólo se condona en raras circunstancias, por causas como incapacidad permanente, muerte o falsificación de documentos.

CONSEJOS DE PREVENCIÓN

- Ignora las ofertas que exijan una respuesta inmediata.
- Nunca reveles información personal identificable, incluyendo tu número de Seguridad Social, cuenta bancaria o información de tarjetas de crédito.
- Nunca compartas tu número de identificación de FSA ID ni firmes un poder o una autorización para que un tercero actúe en tu nombre en relación con un préstamo estudiantil.
- No pagues a un tercero para que gestione y realice pagos en tu nombre.
- Verifica la existencia de la empresa a través de un servicio de información y de Internet.
- Visita el sitio web de Asistencia Federal del Departamento de Educación de los Estados Unidos: **https://studentaid.ed.gov/sa/repay-loans/avoiding-loan-scams. Este sitio tiene mucha** información sobre empresas de cancelación de deuda de confianza y las medidas que debes tomar si ya has compartido información personal con una empresa de cancelación de deuda por préstamos estudiantiles.
- Ignora a las empresas que afirmen estar afiliadas al Departamento de Educación.

6. Robo de identidad

El robo de identidad consiste en robar información de identificación personal (IPI) clave y usarla para acceder a las cuentas bancarias y personales de la víctima, abrir nuevas cuentas de crédito y/o cuentas bancarias, comprar vehículos, rentar apartamentos, contratar servicios públicos o telefónicos, etc. La información de identificación personal puede incluir tu nombre, fecha de nacimiento, número de Seguridad Social y el apellido de soltera de tu madre.

Controla tu crédito:

1. Revisa tus extractos de tarjeta de crédito y cuentas bancarias, y concilia tus compras todos los meses.
2. Solicita un Informe de Crédito de Consumo gratuito anual y comprueba que la información sea correcta. Puedes solicitar un informe de crédito gratuito en línea en annualcreditreport.com.
3. Si crees que puedes ser víctima de un robo de identidad, puedes congelar tu archivo de crédito de consumo contactando a las tres Agencias de Información Crediticia a través de sus sitios web. Selecciona la pestaña de congelación de crédito. Esto dificultará enormemente que un estafador pueda abrir nuevas cuentas con tu identidad.

CONSEJOS PARA PROTEGER TU IDENTIDAD:

- Nunca reveles información personal por teléfono o Internet, a menos que hayas sido tú quien inició el contacto.
- Nunca reveles información de tu tarjeta de crédito o cuenta bancaria en un sitio web, a menos que ofrezca una transacción segura. Los indicadores de transacción segura incluyen un icono de un candado en la barra inferior de la página del navegador web. La URL de la página web cambiará de “http” a “https”.
- Destruye los documentos importantes no deseados que contengan información personal antes de desecharlos.
- Memoriza tu número del Seguro Social. **No** lleves tu tarjeta del Seguro Social en la cartera o el bolso.

7. Estafas de Apple/iCloud

Los estudiantes suelen recibir llamadas telefónicas y correos electrónicos de personas que fingen contactarse en nombre de Apple para obtener información personal identificable (IPI), números de cuentas bancarias o información de tarjetas de crédito.

Llamadas telefónicas falsas:

Los estafadores llaman haciéndose pasar por el servicio técnico de Apple. Al igual que sucede con las llamadas falsas de Microsoft, estas llamadas se originan principalmente desde centros de atención al cliente en la India. El estafador afirma que alguien intentó acceder a tu cuenta de Apple/iCloud o que han detectado actividad sospechosa en tu cuenta. Para resolver el problema, el estafador te pedirá tu nombre, correo electrónico, número de teléfono, contraseña y otros datos personales.

CONSEJOS DE PREVENCIÓN

- **Desconfía de las llamadas no solicitadas.** El soporte técnico de Apple nunca te llamará de forma inesperada, sólo lo hará cuando tú los hayas contactado primero.
- **Las empresas legítimas nunca te solicitarán tu contraseña.** Incluso si contactas al soporte técnico real de Apple, nunca te solicitarán tus contraseñas.
- **Los estafadores son insistentes** y te presionarán para que les des información alegando que es necesaria. Los verdaderos representantes de soporte técnico no intentarán persuadirte para que les des información personal. Los estafadores también te llamarán constantemente si creen que eres vulnerable a sus trucos.
- **Los representantes de soporte técnico legítimos deben conocer tu nombre.** Una vez que hayas contactado al soporte técnico de Apple, los representantes se dirigirán a ti por el nombre que hayas proporcionado al solicitar que se contacten contigo.
  - **Ejemplo:** “Hola, soy Jean, de Apple, ¿hablo con John?”

Correos electrónicos falsos de Apple:

Los estafadores saben que la mayoría de los estudiantes usan Apple y iCIoud y suelen enviar correos electrónicos de suplantación de identidad de aspecto realista (pero falsos). Estos son algunos ejemplos reales de estos correos:

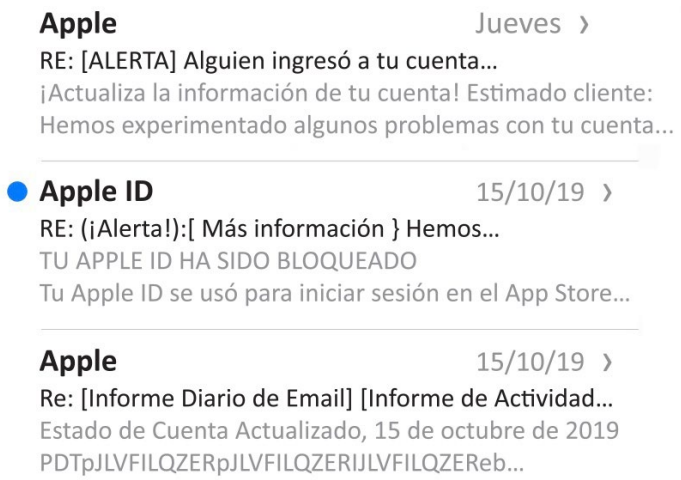
Estimado Cliente:

Tu cuenta de Apple ID ha sido bloqueada por motivos de seguridad.

Tu cuenta está desactualizada. Verifica tus datos y actualiza la dirección de facturación para que podamos proteger tu cuenta y mejorar nuestro servicio para mantener tu privacidad.

Te recomendamos que verifiques tu dirección de facturación dentro de las próximas 24 horas o tu cuenta será bloqueada permanentemente.

Actualizar tu cuenta



Apple Jueves ›
RE: [ALERTA] Alguien ingresó a tu cuenta...
¡Actualiza la información de tu cuenta! Estimado cliente:
Hemos experimentado algunos problemas con tu cuenta...

Apple ID 15/10/19 ›
RE: (¡Alerta!):[Más información } Hemos...
TU APPLE ID HA SIDO BLOQUEADO
Tu Apple ID se usó para iniciar sesión en el App Store...

Apple 15/10/19 ›
Re: [Informe Diario de Email] [Informe de Actividad...
Estado de Cuenta Actualizado, 15 de octubre de 2019
PDTpJLVFILQZERpJLVFILQZERIJLVFILQZEReb...

Los estafadores pueden falsificar fácilmente la dirección de correo electrónico del remitente. Por ejemplo, puede parecer que el remitente es "Apple" cuando en realidad es **hfn3an3ggt@awalannew25.com**. Los estafadores más avanzados pueden falsificar direcciones de correo electrónico para que el remitente parezca ser **support@apple.com** u otras direcciones legítimas. Al hacer clic en "Responder" podrás ver la verdadera dirección de correo electrónico del remitente.

Los correos electrónicos fraudulentos suelen afirmar que alguien ha accedido a tu cuenta sin autorización o que tu cuenta de Apple/iCloud ha sido bloqueada por motivos de seguridad. Una vez que abras el correo electrónico, verás un enlace para "Actualizar/Verificar tu cuenta" o un archivo PDF/DOC para descargar con "más información". No hagas clic en el enlace ni descargues nada. Esa es su manera de robar tu información personal u obtener acceso remoto a tu dispositivo.

CONSEJOS DE PREVENCIÓN

- **Las empresas legítimas nunca se referirán a ti como "Usuario" o "Cliente".** Apple y otras empresas siempre se dirigirán a ti por el nombre que figura en tu cuenta.
- **Al hacer clic en "Responder" podrás ver la verdadera dirección de correo electrónico del remitente.** Los estafadores tienen tácticas para hacer que la dirección de correo electrónico del remitente parezca real.
- **Los correos electrónicos falsos suelen contener errores ortográficos.** Esta es una forma fácil de determinar si el correo electrónico es falso.

8. Estafas de Amazon

Al igual que sucede con las estafas de Apple, los estafadores llaman y envían correos electrónicos a los estudiantes haciéndose pasar por Amazon para tratar de obtener sus datos de acceso e información personal.

Llamadas telefónicas falsas:

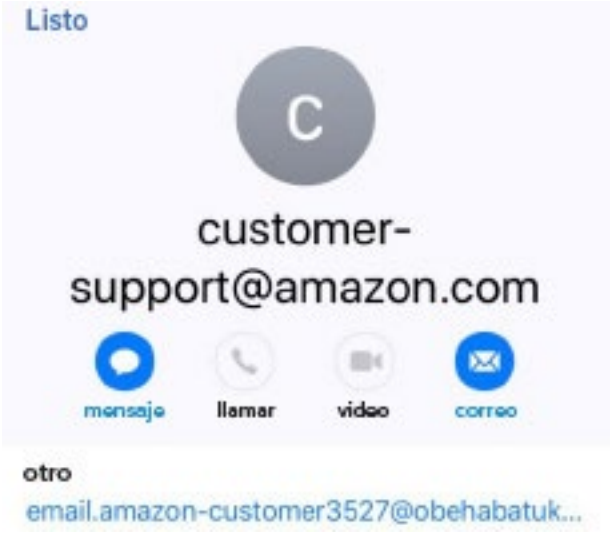
Es posible que recibas una llamada grabada informándote que se ha realizado una compra importante con tu cuenta de Amazon y solicitándote que marques “1” para contactar al soporte técnico de Amazon y resolver el problema. Una vez que lo hagas, el estafador te pedirá tu nombre, número de teléfono, información de tarjeta de crédito, contraseñas, etc. Amazon nunca te llamará a menos que tú te hayas comunicado con ellos primero, ni te solicitará tus contraseñas o información de tarjeta de crédito.

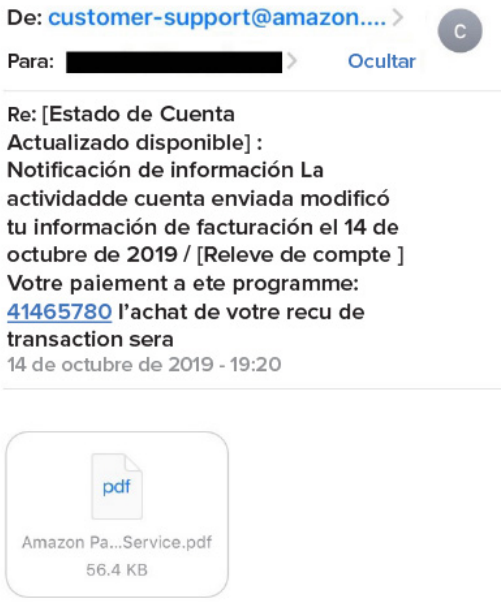
Correos electrónicos falsos de Amazon:

Amazon suele ponerse en contacto con sus clientes por correo electrónico. Los estafadores intentan engañar a los estudiantes por medio de correos electrónicos de suplantación de identidad que imitan los correos del servicio técnico de Amazon. Estos correos electrónicos afirman que ha habido un problema de facturación o un inicio de sesión sospechoso en tu cuenta.

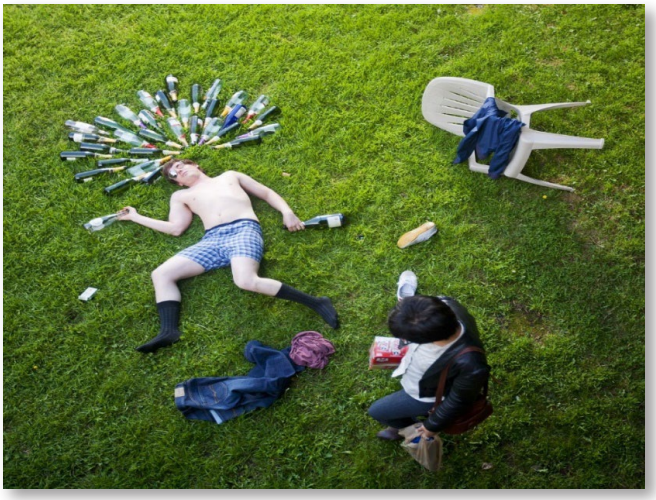
Haz clic en “Responder” para revelar la verdadera dirección del remitente. No hagas clic en los enlaces incluidos en el correo electrónico ni descargues archivos. Esos son los medios que usan para suplantarte o controlar tu dispositivo de forma remota.

Este es un ejemplo de un correo electrónico falso de Amazon. Observa que al hacer clic en el campo “De” puedes ver la verdadera dirección del remitente.





9. Extorsión



Existen casos de estudiantes universitarios a los que se les exige que paguen sumas de dinero para mantener su reputación en el campus o con sus familias o amigos. Alguien filma a un estudiante haciendo algo inapropiado o le pide fotos íntimas. Luego, el chantajista amenaza con publicar el vídeo o las fotos en redes sociales a menos que el estudiante le pague una suma de dinero inmediatamente.

Existen casos de estudiantes que conocieron a alguien en un sitio de citas que los convenció de enviar fotos íntimas. Una vez hecho esto, la otra persona exigirá más fotos comprometedoras y/o favores sexuales al estudiante. Si el estudiante no coopera, el otro amenazará con publicar/compartir las fotos en redes sociales, por correo electrónico o por otros medios de difusión en línea.

Otros estudiantes han sido engañados para que envíen fotos íntimas a alguien que se hace pasar por una celebridad, un cazatalentos, un cantante o un deportista. Una vez hecho esto, el impostor chantajea al remitente y le exige dinero, favores sexuales, o más fotos o vídeos íntimos. Al agresor le genera placer poder controlar al alumno.

Estos tipos de extorsión tienen graves consecuencias y pueden tener resultados devastadores. Algunos estudiantes han llegado incluso a quitarse la vida. Otros casos resultaron en la presentación de graves cargos penales contra quienes publicaron fotos de estudiantes menores de edad.

CONSEJOS DE PREVENCIÓN:

- En una época en que todos tenemos un teléfono y existe una multitud de aplicaciones de redes sociales, los estudiantes deben ser conscientes de que cada una de sus acciones puede llegar a Internet con sólo presionar un botón.
- Mantén la configuración de privacidad de tu teléfono y tus aplicaciones en los niveles más estrictos posibles.
- No compartas fotos comprometedoras con nadie, ni siquiera con tu pareja. No todas las relaciones duran para siempre o terminan de forma amistosa. No guardes fotos íntimas en tu dispositivo.
- Respeta a las personas que puedan actuar de forma inapropiada como resultado de una discapacidad y no tomes ni publiques fotos de ellas en línea. Internet es para siempre, y un error de juicio hoy puede volverse en tu contra en el futuro.

10. Estafa de alquiler de vivienda

Esta estafa es una de las muchas variaciones de las estafas con cheques falsos. El estafador responde a un anuncio en línea o llama a un número de teléfono publicado en el campus y dice ser un posible compañero de piso. El estafador envía un cheque por una cantidad superior al alquiler inicial acordado. El estudiante deposita el cheque y este es aparentemente aprobado. Los fondos se acreditan en la cuenta. El posible compañero de piso (estafador) solicita que se le devuelva el dinero extra a través de una transferencia bancaria, una transacción digital por Venmo, Apple Pay, etc. o un depósito móvil, si el titular de la cuenta facilitó las credenciales de acceso. El estudiante devuelve el dinero sobrante al potencial compañero de piso (estafador). En una fecha posterior, el banco notifica al estudiante que el cheque depositado es falso y el estudiante ha perdido el dinero.

Una variante de esta estafa se da cuando un estudiante responde a un anuncio en línea que incluye fotos de un apartamento y el alquiler solicitado. El estafador dice que está fuera de la ciudad y no puede mostrar la unidad, y le pide al estudiante que realice un depósito reembolsable para reservar el apartamento hasta que pueda mostrárselo. El estudiante realiza un depósito electrónico al estafador. El estafador no es el propietario de la vivienda y el estudiante termina perdiendo el dinero (depósito).

CONSEJOS DE PREVENCIÓN PARA ESTUDIANTES

- Confía en tu instinto: si el apartamento parece demasiado bueno para ser verdad, probablemente lo sea.
- Desconfía de un compañero de piso o propietario que no pueda reunirse contigo en persona. Si tu única forma de comunicarte con ellos es por correo electrónico, desconfía.
- Si te presionan para que envíes un depósito inmediatamente, retrasa las cosas hasta que puedas investigar adecuadamente la oferta.
- Investiga sobre el apartamento y las personas involucradas. Sé siempre escéptico.
- Busca “estafas de alquiler” en Internet para conocer las estafas más recientes.

11. Estafas de PayPal

PayPal suele contactar a sus clientes por correo electrónico. La siguiente información puede ayudarte a asegurarte de que se trata realmente de PayPal, y no de alguien que intenta acceder a tu cuenta.

Direcciones de correo electrónico falsas:

Los estafadores pueden falsificar fácilmente el nombre de PayPal en la dirección de correo electrónico del remitente. Por ejemplo, puede parecer que el remitente es "PayPal Services" cuando en realidad es spfr2013qz7@nomail.com.

Si colocas el mouse sobre el nombre o haces clic en "Responder" deberías poder ver la dirección completa del remitente. Los estafadores más sofisticados pueden falsificar el nombre completo para que parezca un remitente legítimo, así que ten cuidado.

Si haces clic en un enlace de un correo electrónico, asegúrate de revisar la URL del sitio al que te envíe. Para los delincuentes es muy fácil reproducir el aspecto de un sitio web legítimo, por lo que debes comprobar que te encuentras en el sitio web correcto.

Un correo electrónico de PayPal:

- No te solicitará información confidencial, como tu contraseña, cuenta bancaria o tarjeta de crédito.
- No contendrá archivos adjuntos ni te pedirá que descargues o instales ningún software.

CONSEJOS DE PREVENCIÓN

- No proporciones información personal a una persona o empresa que no conozcas.
- Desconfía de cualquier oferta que no pague un salario regular o que implique trabajar para una empresa extranjera.
- Investiga a la empresa en la página de la Comisión Federal de Comercio (FTC), la Oficina de Buenas Prácticas Comerciales *(Better Business Bureau)* o la Fiscalía General del Estado.

VERIFICA LA INFORMACIÓN EN TU CUENTA DE PAYPAL:

- Si recibes un correo electrónico que dice que recibiste un pago de PayPal, tómate un momento para iniciar sesión en tu cuenta de PayPal antes de enviar cualquier mercancía. Asegúrate de que el dinero se haya transferido realmente y de que no se trata de una estafa.

12. Estafa de reenvío

La mayoría de las estafas de reenvío se originan cuando un estudiante responde a un anuncio en línea o solicita un puesto en una bolsa de trabajo u otro sitio web de aspecto oficial que ofrece “trabajo desde casa”.

Estos sitios prometen miles de dólares a los solicitantes por trabajar desde sus casas sin ninguna habilidad especial y con una capacitación mínima. Estos empleos son muy atractivos para los estudiantes, las personas con hijos y las personas mayores.

Los puestos suelen ser gestor de mercancías, especialista en importación/exportación o asistente de procesamiento de paquetes.

El empleador (estafador) dice que las funciones del puesto incluyen:

- Recibir productos de comerciantes (normalmente productos electrónicos).
- Consolidar y reempaquetar los productos.
- Colocar etiquetas de correo con franqueo pagado.
- Reenviar los paquetes a una dirección en el extranjero.

Lo que la mayoría de las víctimas no sabe es que los productos se compraron con tarjetas de crédito robadas o cheques falsos y que los empleados son cómplices del delito.

Este es un ejemplo de un posible anuncio de trabajo:

CL | Trabaje desde casa

- 27 de feb******TRABAJE DESDE CASA******Especialista en en-víos
- 20 de feb ¡¡¡¡¡¡¡TRABAJE DESDE CASA EN 2019!!!!!!!
- 13 de feb Se buscan especialistas en envíos para trabajar MEDIO TIEMPO DESDE CASA
- 13 de feb Gane $1200 POR SEMANA ***DESDE CASA***

CONSEJOS DE PREVENCIÓN:

- Evita los anuncios de trabajo en los que la descripción del puesto implique reempaquetar o reenviar mercancías.
- No proporciones información personal identificable en solicitudes de empleo en línea. Pueden usar tu información para robar tu identidad.
- Si el salario no coincide con las tareas que debes realizar, se trata de una estafa.

13. Estafas de viajes compartidos

Cuando viajes con Uber, Lyft, Via, o cualquier otra empresa de red de transporte (TNC), el paso más importante que puedes tomar para asegurar un viaje seguro es comprobar que subes al vehículo correcto. Antes del comienzo del viaje, cada TNC proporciona al cliente información valiosa para asegurarse de que suba al vehículo correcto. Esta información debe incluir la marca y el modelo del vehículo, el nombre del conductor, la fotografía del conductor y la matrícula del vehículo. Cuando llegue el conductor, pregúntale amablemente su nombre y comprueba que sea el nombre proporcionado por la aplicación. Asegúrate de que la marca y el modelo del vehículo sean correctos y de que la matrícula coincida con la información proporcionada en la aplicación. Si alguno de los datos observados **no** coincide con los de la aplicación**, no subas al vehículo.**

Una vez dentro del vehículo, el conductor nunca debe pedirte que pagues en efectivo. Si el conductor te presiona para que le des dinero en efectivo, pide salir del vehículo y llama al 911. Si el conductor se niega a dejarte salir del vehículo, llama al 911.

El lugar donde vives es un dato importante y es posible que no quieras compartir esta información con otras personas. En lugar de pedir que te dejen en la puerta de tu apartamento, casa o dormitorio, elige un lugar cercano a tu residencia.

La mayoría de las veces, tu pago será procesado inmediatamente después de salir del vehículo. Si observas un cargo de limpieza (de $100 a $300) injustificada (si no has ensuciado el vehículo ni vomitado en él), accede inmediatamente al sitio web de la empresa, selecciona el viaje en cuestión y ve a la sección de ayuda. Allí encontrarás un enlace llamado “Disputar cargo de limpieza”. Haz clic en ese enlace y disputa el cargo. También debes ponerte en contacto con la emisora de tu tarjeta de crédito y disputar el cargo.

Si encuentras un cargo no autorizado en el extracto de tu tarjeta de crédito, denúncialo inmediatamente a la policía local y a la emisora de tu tarjeta. Algunas TNC también disponen de una aplicación de soporte para las transacciones no autorizadas. Por ejemplo, en caso de compras no autorizadas a través de Uber, visita: **https://help.uber.com/h/fe547761-4384-42d4-8531-4cfb0e0e523e** y completa la información requerida. Uber te reembolsará el importe de cualquier viaje no autorizado y te proporcionará información sobre las transacciones no autorizadas, como el número de teléfono y el correo electrónico asociados a la cuenta utilizada, y los lugares de inicio y finalización del viaje.

14: Estafas a estudiantes internacionales

- Los estudiantes internacionales pueden ser víctimas de estafadores que fingen contactarlos en nombre del gobierno federal y los asustan para que les paguen dinero.
- Los estudiantes extranjeros, sobre todo de países del sur de Asia, pueden recibir llamadas telefónicas que parecen ser del gobierno.
- La persona que llama suele conocer la situación migratoria del estudiante y el programa o la universidad al que asiste.
- El estafador afirma que existe un problema con los documentos migratorios del estudiante o con la renovación de su visa. Luego exige el pago inmediato de un cargo o arancel falso de migraciones, a menudo por miles de dólares.
- El estafador puede amenazar al estudiante con arrestarlo o deportarlo en caso de que no pague, y suele exigir que se le pague con tarjetas de regalo (como Google Play o iTunes) o criptomonedas (como Bitcoin).

¿Cuáles son los indicios de que se trata de llamadas fraudulentas?

- El gobierno federal no haría estas llamadas o amenazas, ni pediría estos pagos.
- Quienes llaman pidiendo que se les pague con tarjetas de regalo o criptomonedas son estafadores que prefieren esos medios de pago porque pueden obtener el dinero y desaparecer sin dejar rastro.

Los estafadores también intentan sacar dinero a los estudiantes internacionales

- Si recibes una llamada como esta, cuelga el teléfono.
- Si no estás convencido de que se trate de una estafa, habla con alguien de confianza al respecto. Varias personas afirman que descubrieron que una llamada era una estafa después de hablar con un familiar, la policía local o un empleado de la universidad. Es probable que otras personas de tu comunidad hayan recibido la misma llamada, por lo que hablar de ello podría ayudar a otras personas de tu zona.
- Si te preocupa tu visa o tus documentos migratorios, contacta al Centro Nacional de Atención al Cliente del Servicio de Ciudadanía e Inmigración de los Estados Unidos (USCIS) al 800-375-5283.

15: Pagos entre pares (P2P)

- Las aplicaciones P2P están diseñadas para simplificar las transacciones financieras entre personas que se conocen y confían una en la otra.
- Las aplicaciones P2P permiten a los usuarios enviar dinero desde sus dispositivos móviles a través de una cuenta bancaria o tarjeta vinculada.
- El uso de aplicaciones móviles de pago P2P, como CashApp, Venmo y Zelle, está aumentando.
- Estas aplicaciones suele usarse para dividir la cuenta de un restaurante o enviar el pago de servicios a un compañero de cuarto o apartamento.
- En general, los pagos P2P son seguros porque están encriptados e incluyen funciones de control de fraude.

A medida que los estadounidenses se sienten más cómodos con estas aplicaciones, los estafadores adaptan sus tácticas para aprovechar el acceso rápido y generalmente anónimo a dinero en efectivo que proporcionan.

Algunas medidas para evitar ser estafado al usar aplicaciones de pago:

- No uses aplicaciones P2P para pagar bienes y servicios.
- Antes de donar dinero con una app P2P, comprueba siempre el sitio web de la organización benéfica para verificar que aceptan donaciones por este medio.
- Incluso una transacción legítima puede salir mal si se introduce un número de teléfono incorrecto o se escribe mal el nombre del destinatario y se envían los fondos a la persona equivocada.
- Verifica siempre la información del destinatario antes de realizar cualquier pago.
- Nunca envíes pagos P2P a personas que no conozcas ni aceptes pagos de personas que no conozcas.
- Usa contraseñas seguras y nunca entregues tu teléfono celular a alguien que no conozcas por ningún motivo. Un estafador puede enviar dinero desde una app P2P a su cuenta en 10 segundos sin que lo sepas.
- ¡¡Una vez transferidos los fondos, el dinero se pierde para siempre!!

16: Mejores consejos para prevenir fraudes

1. Solicita un informe de crédito gratuito en **annualcreditreport.com.** Cada año puedes recibir 1 informe de crédito gratuito de cada una de las 3 Agencias de Información Crediticia (TransUnion, Equifax o Experian). Al recibirlo, comprueba que no incluya cuentas o consultas no autorizadas, o direcciones desconocidas.

2. Solicita una declaración de beneficios de Seguridad Social en www.ssa.gov. Cuando la recibas, revisa tu registro de beneficios y su ganancias estimados. También debes asegurarte de que nadie está usando tu número del Seguro Social en su empleo o para obtener otros beneficios.

3. Verifica la identidad de las personas a quienes envías pagos con aplicaciones P2P, como Zelle, Venmo, etc. Envía dinero únicamente a personas que conozcas y acepta dinero únicamente de personas que conozcas. No realices pagos a extraños con aplicaciones P2P. La mayoría de las transacciones "entre pares" son instantáneas e irreversibles.

4. No pagues compras en línea o por teléfono con tarjeta de débito. Las tarjetas de débito son vulnerables porque están vinculadas a una cuenta bancaria. Es mucho más fácil revertir una transacción fraudulenta abonada con una tarjeta de crédito que una abonada con una tarjeta de débito. Tampoco facilites los números de tu tarjeta de débito/crédito por teléfono o correo electrónico, o en páginas web, a menos que hayas sido tú quien inició la llamada o el pedido.

5. Mantén registros exhaustivos. Si te roban una computadora, ¿puedes darle una descripción completa a la policía? Anota la marca, el modelo, el color y, sobre todo, el número de serie de tu computadora, que es un identificador clave similar al número de identificación de un vehículo (VIN). También puedes necesitar esta información para presentar un reclamo a tu aseguradora.

6. No uses un cajero automático si observas cables o dispositivos de copiado conectados a la ranura para la tarjeta, y cubre el teclado con la mano, un sombrero u otra prenda de vestir cuando introduzcas los números de tu PIN. Notifica al banco o a la policía local si observas cualquier dispositivo conectado a un cajero automático.

7. No realices compras con tarjeta de débito sin antes verificar el saldo de tu cuenta. La mayoría de las instituciones financieras permitirán que se procese la transacción aunque no tengas fondos suficientes para cubrir el cargo. Esto dará lugar a penalizaciones y comisiones innecesarias.

8. No asumas que un correo electrónico o una llamada telefónica son auténticos. El hecho de que alguien conozca tus datos básicos (nombre, fecha de nacimiento, dirección, etc.) no significa que un correo electrónico o llamada telefónica sean legítimos. Los delincuentes usan distintas técnicas de ingeniería social para obtener información personal identificable.

9. Cuando salgas de bares o restaurantes a altas horas de la noche, no aceptes que te lleve una persona que dice ser empleado de un servicio de transporte privado o una empresa de red de transporte conocidos, a menos que tú hayas solicitado el servicio. Existen casos de estudiantes que han sido llevados a zonas aisladas para robarles. También se han dado casos de clientes ebrios a quienes condujeron a cajeros automáticos y obligaron a retirar dinero de sus cuentas.

10. No te ofrezcas a depositar un cheque en tu cuenta para un desconocido. Cualquiera puede afirmar que no tiene una cuenta y contarte una historia triste. Tú eres responsable por los depósitos realizados en tu cuenta. No reveles a nadie los datos de acceso a tu cuenta. Si lo haces, pueden depositar cheques robados o falsificados en tu cuenta. El banco te hará responsable económicamente.

Confía en tu instinto — si parece que algo anda mal, probablemente sea así.

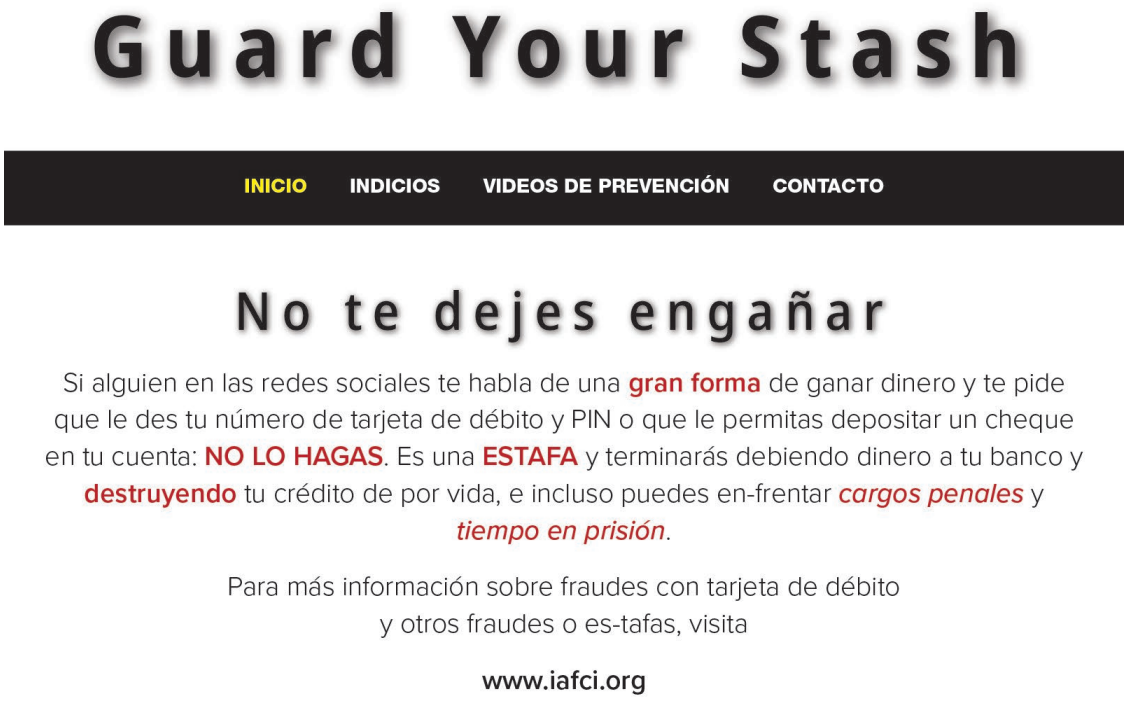
Recursos para la prevención de fraudes

Asociación Internacional de Investigadores de Delitos Financieros

La IAFCI es una organización internacional sin fines de lucro que ofrece servicios y un entorno en el que se puede reunir, intercambiar y enseñar información sobre fraudes financieros, investigaciones de fraudes y métodos de prevención de fraudes para el bien común de las fuerzas de seguridad, la industria de pagos financieros y la sociedad en general. **Puedes encontrar información sobre estafas en https://www.iafci.org.**

La Comisión Federal de Comercio (ftc.gov) - tiene mucha información sobre estafas dirigidas a estudiantes universitarios. Puedes entrar en su página web e inscribirte para recibir alertas diarias.

Visita www.guardyourstash.com/ para acceder a información y vídeos de prevención sobre estafas con tarjetas de débito.



Agradecimientos

- **Phil Bartlett,**
  Servicio de Inspección Postal de los Estados Unidos
- **Michael Carroll,**
  Servicio de Inspección Postal de los Estados Unidos
- **Brian O'Connor,**
  Departamento de Policía de Cambridge
- **Missy Coyne,**
  Oficina Nacional de Delitos de Seguros (NICB)
- **Wade Stormer,**
  Uber

ASOCIACIÓN INTERNACIONAL DE INVESTIGADORES DE DELITOS FINANCIEROS
1020 SUNCAST LANE, SUITE 102
EL DORADO HILLS, CA 95762

WWW.IAFCI.ORG
TEL. 916-939-5000