Como Protegerse de Estafas

Todos los días, miles de personas son engañadas por delincuentes y estafadores que usan métodos astutos y sofisticados para robar el dinero del público. Incluso cuando el crimen está siendo cometido, la víctima no está consciente del engaño y/o la estafa. Frecuentemente, las víctimas se sienten humilladas por haber depositado la confianza en las personas que les robaron, experimentan confusión y vergüenza. Tanto así, que no reportan el delito a las autoridades. Si usted ha sido víctima de algún crimen y/o estafa financiera, usted no está solo.

La mejor manera de prevenir las estafas financieras es estar debidamente informado. El Departamento de Banca y Valores de Pennsylvania ha creado esté folleto que incluye información sobre las estafas más comunes de hoy en día, así como consejos útiles para defenderse usted y proteger su dinero.

También puede encontrar información sobre cómo comunicarse con las agencias gubernamentales, organizaciones sin fines de lucro y agencias de crédito que pueden ayudarle a eludir crimines de fraudes futuros y/o asistirle si usted ha sido víctima de alguna estafa financiera o crimen cibernético

¡Tenga en cuenta, si la situación le suena demasiado buena para ser cierta, probablemente lo es! ¿Parece algo sensacional? Pues es un fraude.

TABLA DE CONTENIDO

ESTAFAS DE PAGOS POR ADELANTADO

Los pagos por adelantado son instantáneamente una "**bandera roja**".
Los estafadores predadores se presentan como representantes de empresas y/o comerciantes de negocios legítimos. Con frecuencia se enfocan en individuos con un historial de crédito deficiente prometiendo una aprobación fácil o "garantizada". Sin embargo, para aprovechar la oferta, la víctima debe pagar por adelantado altos pagos por honorarios aparentemente legítimos por la solicitud, préstamos falsos, modificaciones, refinanciamiento de préstamos o tarjetas de crédito seguro e otros "servicios". Al final, el estafador se desaparece con el pago y la víctima no recibe nada a cambio.
Las estafas por adelantado involucran una variedad de métodos incluyendo llamadas de telemercadeo, mensajes de texto, correos electrónicos, documentos diseñados profesionalmente, anuncios clasificados y el Internet, incluyendo las redes sociales.

COMO PROTEGERCE DE ESTAFAS DE PAGO POR ADELANTADO

- Evite cualquier oferta de crédito que requiera un pago inicial. Aunque un prestamista pueda cobrar por su solicitud, informe de crédito y otros honorarios, generalmente esta se deduce del préstamo después de su aprobación.
- Si se le piden que pague cuotas a través de una transferencia bancaria o tarjeta de débito prepagada, especialmente a alguien en otro país, tenga cuidado. Estos pagos son extremadamente difíciles de recuperar o investigar.
- Verifique con quién está tratando. Si no conoces a la persona o la compañía, tome su tiempo y investigue sobre ellos.

Si usted se ha convertido en una víctima de una **estafa de pago por adelantado**, comuníquese con el Departamento de Pennsylvania de Banca y Valores, la oficina del Fiscal General de Pennsylvania o la Comisión de Comercio Federal.

ESTAFAS PONZI

Las estafas Ponzi llevan el nombre del Charles Ponzi quien a principios del siglo XX hizo famoso estos crímenes de robo financiero. El más infame sucesor moderno es Bernie Madoff. Las estafas Ponzi toman muchas formas, pero todas dependen de una corriente constante de los inversores que se les prometen tasas de pagos regulares, exageradamente altas. Sin un flujo constante de nuevos inversionistas, el esquema Ponzi se convierte en una "casa de naipes" que colapsa bajo su propio peso, pero antes el estafador desaparece con el dinero de los inversores.

Los esquemas Ponzi pueden ser difíciles de detectar, pero aquí las "**banderas rojas**":

- Cuando a las víctimas se les urge a invertir en un rápido y especulativo pago.
- Cuando al inversionista se les promete que su inversión es "libre de riesgo".
- Los promotores del fraude Ponzi a menudo dependen de sus círculos sociales: los primeros inversionistas alinean sus más cercanos amigos, parientes y asociados profesionales como nuevas víctimas.
- A los primeros inversionistas se les paga generosamente. Estos pagos pasan hacer "prueba" para así convencer hasta el más incrédulo de sus futuras víctimas o de quienes insisten en ver pruebas antes de invertir su dinero con el fin de persuadir a nuevas víctimas/inversores.

COMO PROTEGERCE DE ESTAFAS POZI

- Todas las inversiones legítimas implican un grado de riesgo. Cuidado con las promesas garantizadas de altos beneficios y/o "sin riesgo".
- No permita que los promotores se nieguen a proporcionar explicaciones claras y detalladas de sus inversiones.
- No se apresure a tomar una decisión. Tenga cuidado con los vendedores que crean un falso sentido de urgencia para que usted invierta su dinero de inmediato.
- Revise a fondo los antecedentes del asesor a través del FINRA
- Asegurarse de que la inversión está registrada como una oferta legítima de valores con el Departamento de Banca y Valores de Pennsylvania o de la Comisión Federal de Bolsa de Valores.
- Solicite información detallada por escrito y verifique las declaraciones del promotor.
- Sea cauteloso de las ofertas que no pueden ser revisadas en persona.
- Este atento a la conducta no-profesional del promotor o de la interrupción de los servicios prometidos.

Si usted se convierte en una víctima de este **esquema Ponzi**, comuníquese con la oficina del Fiscal General de Pennsylvania, el Departamento de Pennsylvania de Banca y Valores o su cuartel local de policía.

ESTAFAS IRS

Usted ha recibido una llamada telefónica o un correo electrónico de alguien alegando estar trabajando para una agencia del gobierno como el Servicio de Impuestos Internos (IRS) o el tesoro de Estados Unidos. Aunque usted no haya recibido ningún aviso del gobierno anteriormente, el solicitador alega que usted debe dinero por impuestos no pagados, atrasados o que te perdiste un plazo de pago.

El solicitador le amenaza con arresto o una demanda legal si ustedes no les pagan ni les da información personal (por ejemplo, su número de seguro social o fecha de nacimiento). La persona que llama exige que los envié dinero vía remesas, giro, o con una tarjeta de débito prepagada, o de otra manera en el cual el dinero no podrá rastrearse.

El solicitador suena exigente y autoritario.
¿Que se supone que usted debes hacer?

COMO PROTEGERCE DE ESTAFAS IRS

- **Recuerda**: el gobierno de Estados Unidos o agencia estatal nunca les va a llamar y pedir dinero o información.
- En ocasión de que se ponga en contacto con usted a través del teléfono, el gobierno de Estados Unidos y las agencias estatales siempre le enviara información legal antes por correo tradicional.
- Si usted no reconoce un número de teléfono en el identificador de llamadas, no tiene que responder (incluso si el identificador de llamadas dice que es el IRS o alguna otra agencia del gobierno).
- Llamadas legítimas le dejarán un mensaje de voz.
- Si usted cree que la llamada es legítima, tome el nombre de la persona que llama y cuelgue. No llame al número proporcionado, más bien busque el número de teléfono en un directorio y asegúrese de que está llamando a una agencia real y legítima y no a un estafador.

Si usted ha sido víctima de este crimen de **estafa del IRS,** comuníquese con la oficina del Fiscal General de Pennsylvania.

ESTAFAS DE AFINIDAD

El **fraude de afinidad** ocurre cuando un estafador afirma ser un miembro de la misma etnia, religión, trabajo o grupo comunitario. "Usted puede confiar en mí", dice el estafador, "Porque soy como tú." “Compartimos los mismos intereses. "Y puedo ayudarte a ganar dinero".

Estos fraudes frecuentemente pagan altos rendimientos a los primeros inversores del grupo con el dinero generado del que ha invertido más tarde. Como resultado, los primeros inversionistas se sienten muy entusiasmados con sus ganancias y del esquema que se derrumba una vez que la víctima haya invertido su dinero y el estafador se desaparece con el todo el dinero de sus víctimas.

El **fraude de afinidad religiosa** es un problema general con estafadores que se encuentran en todas las denominaciones religiosas e iglesias. Los consumidores se han quejado de fraude y abuso por los asesores financieros, estafadores que piden ofrendas y donaciones a sus iglesias y dan consejos para invertir sus finanzas por medio de supuestas “inspiraciones divinas ".

Muchas de estos fraudes basan sus predicciones en calamidades de inminente caos financiero o social, como la fuerte caída del mercado de valores. Fraudes utilizan los medios de comunicación como, revistas religiosas, periódicos, estaciones de radio y televisión por cable que se enfocan en programación religiosa alcanzando a devotos feligreses, facilitando así a este tipo de **fraude de afinidad religiosa**.

COMO PROTEGERCE DE ESTAFAS DE AFINIDAD

- Tenga cuidado con el uso de nombres o testimonios de otros miembros del grupo.
  No se apresure a tomar una decisión. Tenga cuidado con los vendedores que crean un falso sentido de urgencia para invertir de inmediato.
- Obtenga un prospecto u otra forma de información escrita que detalle los riesgos de la inversión, así como los procedimientos para obtener su ganancias y dinero.
- Pida consejo profesional de un experto externo y neutral que no participe del grupo-un contable, abogado o asesor certificado en finanzas -para evaluar la inversión.
- Investigue antes de invertir: llame al Departamento de Bancos y Valores de Pennsylvania para asegurar que la inversión esté registrada legalmente y revise a fondo los antecedentes del asesor a través del FINRA.

Si usted se convierte en una víctima de **fraude de afinidad**, comuníquese con la oficina del Fiscal General de Pennsylvania, el Departamento de Pennsylvania de Banca y Valores o su cuartel de policía local.

ESTAFAS DE ORGANIZACIONES BENEFICAS

Hay muchas organizaciones que hacen un buen trabajo caritativo y merecen el apoyo y/o donación. Desafortunadamente, hay personas que ven la generosidad de los demás como una oportunidad para estafar y enriquecer sus propios bolsillos.

Las estafas por medio de organizaciones benéficas ocurren todo el tiempo, pero son especialmente comunes después de un gran desastre o tragedia, como el maratón de Boston por medio de ataques terroristas o para las víctimas del huracán Sandy, cuando el público está más *susceptible a apoyar y dar sus* donaciones. El público debe estar consciente de los criminales que buscan aprovecharse de la generosidad haciéndose pasar por organizaciones caritativas para obtener dinero o información privada de contribuyentes bien intencionados. Tales esquemas fraudulentos pueden incluir el contacto por teléfono, las redes sociales, correos electrónico o peticiones en persona.

A menudo, los delincuentes envían correos electrónicos, o son visitados por “voluntarios”. (Algo que una organización legítima nunca haría). Estos correos electrónicos se dirigen a los destinatarios a sitios web falsos que parecen estar afiliados con causas caritativas legítimas. Estos sitios con frecuencia imitan los sitios de nombres legítimos o usan nombres similares a las organizaciones benéficas legítimas, o afirman estar afiliados con organizaciones benéficas legítimas con el fin de persuadir a la gente a enviar “donaciones” y/ o proporcionar información financiera y personal que es luego utilizada para robar identidades y/o recursos financieros.

COMO PROTEGERCE DE ESTAFAS DE ORGANIZACIONES BENEFICAS

- Ignorar las solicitudes para donaciones por correo electrónico de organizaciones desconocidas: estas son casi siempre estafas.
- Consulte con el servicio de impuestos internos para asegurarse de que la organización está registrada como una corporación 501 (c). Eso significa que las donaciones son legítimas y deducibles de impuestos.
- **NUNCA** dé, ni envíe dinero en efectivo. Para fines de seguridad e impuestos, contribuya con un cheque o tarjeta de crédito u otra forma que provea documentación de dicha donación. Al escribir un cheque, que sea pagadero a la organización, nunca a un individual o "cash".
- No proporcione información financiera personal, como números de seguro social o números de tarjeta de crédito o de cuenta bancaria y/o contraseñas, a cualquier persona que solicite una contribución. Los estafadores pueden usar esta información para robar la identidad y el dinero de un donante.
- Si una organización benéfica afirma estar ayudando a un organismo local como la policía o los de bomberos, consulte con ese organismo y verifique si están recaudando fondos y si conocen y usan a la organización benéfica para adquirir sus fondos.
- Contacte el Departamento de Estado de Pennsylvania para verificar que la organización está legalmente registrada con el Estado.
- Contacte el Better Business Bureau’s Wise Giving Alliance para obtener información sobre organizaciones caritativas sin fines de lucro.

Si usted ha sido víctima de este crimen, presente una queja ante la Comisión Federal de Comercio, el Internet Crime Complaint Center o su policía local.

FRAUDE DE CHEQUE DE CAJERO

Hubo un tiempo en que los cheques del cajero se consideraban como el conducto más efectivo para hacer pagos. Hoy en día, debido a sofisticadas falsificaciones de estos cheques, este método de pago a perdido la confianza de comerciantes y vendedores debido a las grandes pérdidas de suma de dinero por medio de falsos cheque de cajero.

Los cheques de caja se consideran instrumentos relativamente libres de riesgo, por lo tanto, son utilizados frecuentemente como una forma de pago confiada por los consumidores de bienes y servicios. Últimamente, los cheques de caja se han convertido en un atractivo medio para cometer fraude cuando son utilizados para pagar a los consumidores.

Esta estafa se dirige a personas que venden artículos de mucho valor como coches, apartamentos, o incluso caballos, a través de clasificados de publicidad y subastas en línea o Internet. El falsificador, quien a menudo residen en otros países, se plantea como un comprador interesado y ofrece pagar con un cheque de cajero. Después de que la víctima presenta el cheque al banco, el comprador de "repente" retrocede la oferta y pide un reembolso. Porque los fondos del cheque están disponibles en el Banco después de unos días, la víctima asume que el cheque se ha despejado y acuerda devolver el dinero. Para cuando el banco descubre la falsificación, hasta 60 días más tarde, el comprador falso se ha desaparecido y la víctima debe ahora pagar al banco por el total de la cantidad del cheque falso. Aunque la cantidad de un cheque de caja se vuelve rápidamente "disponible" al consumidor después de que él deposita el cheque, estos fondos no pertenecen al consumidor si se llegara a comprobar que el cheque es fraudulento. Descubrir que un cheque de caja es fraudulento puede llevar semanas. Mientras tanto, el consumidor puede haber transferido irrevocablemente los fondos o puede haber utilizado los fondos, solo para descubrir más tarde, cuando el fraude es detectado – que el consumidor debe al banco la cantidad total del cheque de caja que había depositado.

ESTAFAS COMUNES — Cada estafa relacionada con un cheque de caja fraudulento puede ser diferente, pero algunos de los escenarios más comunes son:

• *Venta de artículos*– Usted vende artículos en el mercado – por ejemplo, a través del Internet. Un comprador le envía un cheque de caja por el precio que usted ha acordado, y usted le envía los productos al comprador. El cheque de caja resulta ser fraudulento.
• *Precio de compra excedido*– Este escenario es similar al descrito anteriormente, sin embargo, el comprador le envía a usted un cheque de caja por un valor mayor que el precio de la compra y le pide que haga una transferencia bancaria por una parte o todo el excedente, con frecuencia en un país en el exterior. El comprador puede explicar que este procedimiento le permite cumplir con las obligaciones que tiene con usted y con un tercero usando un solo cheque. El cheque de caja resulta ser fraudulento.

COMO PROTEGERCE DEL FRAUDE DE UN CHEQUE DE CAJERO

- Conozca la diferencia entre los fondos que están a disposición para retiro de su cuenta y un cheque que ha sido finalmente librado. Por ley, a su banco se le puede solicitar que ponga a su disposición los fondos, aunque el cheque no ha sido librado. Sin embargo, podría llevarse varias semanas en saber si el cheque será librado o no.
- **Recuerde:** usted es responsable de los fondos que deposita hasta que su banco haya recibido el dinero de la institución donde se originó el cheque (esto podría tardar más de 60 días).
- Tenga precaución al hacer transacciones con extraños que pagan con cheques de cajero. Asegúrate de decirle al comprador que usted enviará el artículo solamente después de que el cheque haya despejado. Si no conoce la persona que presenta el cheque, sostenga los fondos en su cuenta bancaria hasta que su banco confirme que el cheque haya sido despejado.
- **Nunca** acepte un cheque por más cantidad que su precio de venta, especialmente si se espera que usted pague el excedente del cheque a otra persona.

Si usted se convierte en una víctima de **fraude de cheques de caja**, comuníquese con la oficina del Fiscal General de Pennsylvania, el Servicio Secreto de Estados Unidos o el Departamento de Pennsylvania de Banca y Valores.

ESTAFAS DE REPACION DE CREDITO

Muchas compañías afirman que pueden "borrar" o "reparar" su historial de crédito – por un pago inicial.
La verdad es que solamente el transcurso del tiempo y un plan de repago de deudas personales mejorará su informe crediticio.
Las compañías de reparación de crédito deshonestas pueden cobrar cientos, incluso miles de dólares por servicios que nunca realizan. Otros facturan sus clientes por cosas que usted pueden hacer por su cuenta libre y gratuitamente, como la disputa de errores y la eliminación de elementos obsoletos.

En una estafa de reparación de crédito común, la empresa de reparación de crédito
disputa toda la información negativa en el informe de crédito de un individuo. Esto suele ocasionar que la información quede retirada temporalmente por las agencias de crédito, mientras que las controversias
se repasan. Durante este tiempo, el crédito del individuo aparece haber mejorado.
Sin embargo, esto no es ni una solución legítima ni permanente.

Otro truco es aconsejar a un individuo para solicitar un nuevo número de Identificación de Empleado (EIN) (por su sigla en inglés) ante el Servicio de Impuestos Internos (IRS, por su sigla en inglés). Los números EIN son legítimos, y usualmente, los usan los negocios para reportar información financiera al IRS y a la Administración del Seguro Social — pero un número EIN no puede usarse como un sustituto de su número de Seguro Social. Esto se conoce como "segregación de archivos" y es un delito grave. Si por seguir el consejo de una compañía de reparación de crédito usted comete un fraude, podría verse involucrado en un problema legal. Es considerado delito federal.

COMO PROTEGERCE DE ESTAFAS DE REPACION DE CREDITO

- Nadie puede borrar la información negativa de sus informes de crédito si es exacto.
- Usted puede corregir los errores en su informe de crédito por usted mismo.
- Usted tiene derecho a una copia gratuita de su informe de crédito de cada una de las tres agencias de crédito una vez cada 12 meses.
- Contacte el National Foundation for Credit Counseling para encontrar un asesor de acreditado legítimo cerca de usted.

Si usted es una víctima de una **estafa de reparación de crédito**, comuníquese y presente una queja con la Comisión Federal de Comercio (FTC, por sus siglas en inglés).

ESTAFAS ROMANTICAS

Si usted ha conocido a alguien en otra ciudad, estado o país en línea/internet a través de un perfil de citas o redes sociales.
ADVERTENCIA: Esta persona puede ser un "farsante" y no ser quien aparenta ser. Esta persona dice estar atraída por usted y comienza a enviarle mensajes de texto, correo electrónico o incluso llamarle regularmente. Él o ella dice estar repentinamente enamorado de usted formando así un rápido apego emocional. En un principio se muestran muy interesados por la vida de la víctima y hacen muchas preguntas. Con esa información inventan la pareja perfecta y le dicen a la víctima todo lo que esta desea escuchar. Ya cuando la "relación" se halla establecido es cuando la **estafa romántica** y monetaria comienza.

Espontáneamente, este nuevo interés romántico y amoroso le ha sucedido algún tipo de "crisis" y necesita su ayuda rápidamente. O tal vez ambos han hecho planes para matrimonio y de casamiento, lo que requerirá viajes, una visa, u otros gastos relacionados con la boda.

Esta persona necesita dinero y pide su ayuda-a través de un transmisor de dinero como Western Unión, Money Gram, o cargando una tarjeta de débito prepagada. O le pide que proporcione acceso a su cuenta bancaria para hacer transferencias de dinero con mayor facilidad.

Él o ella permanecerá en contacto con usted y le prometerá cualquier cosa hasta permanecer en la supuesta relación romántica siempre y cuando usted continúe enviando dinero. Él o ella siempre encontrará una razón para pedir dinero y favores.
Usted nunca llegara a conocer en esta persona o individuo y/o usted no podrá rastrear el dinero que usted haya enviado e remitido.

COMO PROTEGERCE DE ESTAFAS ROMANTICAS

- Evite dar demasiados detalles personales sobre sí mismo hasta que estés usted seguro de quien es la persona que está interesada en usted.
- No aceptes ni crea todo lo que le diga la persona en línea.
- Google tu "nuevo amor" y presta atención si su foto aparece con varios nombres unido a ella.
- Si el perfil de la persona desaparece de tu página de citas por internet, o página web dentro de varios días, para comunicarse con usted vía mensajería instantánea o Skype, esto indica una buena posibilidad de que este sea un estafador en busca de su próxima víctima
- Ignore las peticiones a su perfil o página de parte de desconocidos, es por este medio que los estafadores y delincuentes buscan a sus potenciales víctimas.

Si usted se ha convertido en una víctima de **fraude romántico**, comuníquese con la oficina del Fiscal General de Pennsylvania.

ESTAFAS DE LOTERIA INTERNACIONAL

Alguien que usted no conoces acaba de informarle que usted ha ganado el premio “mayor” en una lotería extranjera. Usted no recuerdas haber nunca participado, pero el premio está dirigido a su nombre.

Desafortunadamente, este aparente golpe de fortuna no es nada más que una estafa. Las estafas de lotería funcionan persuadiendo a la víctima para que envíe dinero para reclamar el premio ya sea este dinero en efectivo, un viaje u otro artículo de valor. El estafador, afirma que está representando una organización de gobierno, ser una celebridad o representante de la lotería extranjera, este convence a su víctima que para hacer efectivo el premio, este necesita un monto de dinero para cubrir el seguro del premio, u otros "costos de procesamiento" asociadas con el desembolso del premio. La cuenta bancaria o su número de Seguro Social también pueden ser solicitados para "verificar" la identidad del ganador. Sin embargo, el premio nunca llega y el estafador se roba el dinero de su víctima y hasta su identidad.

Otras veces, la víctima recibirá un cheque o giro postal no solicitado con instrucciones para depositar el dinero y transferir una parte del mismo al remitente para cubrir las "tarifas de procesamiento" o impuestos. El cheque es falso; sin embargo, el dinero que la víctima ha transferido al estafador es real. La víctima no podrá recuperar los fondos enviados por la transferencia bancaria y este será responsable a su banco o tarjeta de crédito por el dinero que obtuvieron contra el cheque falso.

COMO PROTEGERCE DE ESTAFAS DE LOTERIA INTERNACIONAL

- Nunca le dé su número de cuenta bancaria a alguien para que pueda reenviar las ganancias de la lotería u otro ingreso inesperado para ti. Los estafadores pueden usar su número de cuenta bancaria para tomar dinero de su cuenta en lugar de poner dinero en ella. Los estafadores oportunistas suelen pedir estos datos para robar su dinero o su identidad.
- Sospeche de cualquier persona que afirme que usted ha ganado un premio, especialmente si usted no recuerda entrar en ningún concurso.
- Es contra la ley federal comprar boletos de lotería extranjeras por teléfono o por correo. Si usted juega a una lotería extranjera — ya sea a través del correo o por teléfono — está infringiendo la legislación federal.
- Las loterías legítimas y los sorteos no requieren que los ganadores paguen dinero antes de reclamar un premio.

Si usted ha sido víctima de una **estafa de lotería internacional**, presente una queja en el Centro de Quejas por Internet, (Internet Crime Complaint Center, por sus siglas en inglés).

FRAUDE DE “MICROSOFT”

Microsoft u otra compañía ha detectado una estafa en la que delincuentes cibernéticos llaman a consumidores de todo el mundo, haciéndose pasar por personal de soporte técnico de Microsoft, informando de un virus que ha infectado su PC, (computadora personal) y ofrecen una “solución”, pero no antes de que usted pague una cuota con su tarjeta crédito o débito (el costo podría ser de

$50.00 dólares o más). Es muy importante informar de que Microsoft nunca realiza este tipo de llamadas.

El consumidor recibe una llamada de alguien que se identifica como personal de Microsoft u otra compañía conocida indicando que su PC, computadora personal tiene un problema y se ofrece para resolverlo. Una vez ganada la confianza del consumidor, le piden que inicie una sesión en un sitio Web para descargar un archivo que facilita la resolución del problema. Mientras realizan la llamada para “solucionar” verá movimiento del cursor en la pantalla de su computadora, controlada por el estafador.

Esta persona puede incluso abrir una ventana en su pantalla que muestra todos los virus y malware que supuestamente han sido descubiertos durante la "reparación". Lo que realmente está sucediendo es que están descargando software, malware e incluso virus a tu PC, computadora. Es de este modo que su sistema, archivos e información han sido comprometido e infectado. Puede que no descubras que su computadora ha sido tomada por un estafador durante días, semanas, o incluso meses - y durante este tiempo, el estafador ha estado observando todos sus movimientos desde su propia computadora. Es posible que el estafador haya descargado "ransomware" en su computadora: usted no podrá acceder a los archivos de su computadora hasta que pague un rescate a el estafador. En muchos casos, aunque usted haya pagado, es posible que no recupere el acceso a los archivos de su computadora. De este modo logran acceder a la información personal del usuario, incluso a su información bancaria. En algunos casos solicitan los datos de su tarjeta de crédito y en otros, además de acceder a sus datos personales, también pueden llegar a infectar su PC con un virus o software.

COMO PROTEGERCE DE UN FRAUDE DE “MICROSOFT”

- Asegúrese de tener instalado un software actual y eficaz de antivirus en su computadora y sistema.
- Si recibe una llamada de una persona identificándose como personal de Microsoft o Norton, ofreciéndole su ayuda para solucionar una incidencia técnica dígales los llamarás de vuelta. Llame a esa empresa utilizando un número de teléfono que ha verificado como legítimo (de la guía telefónica, o del sitio web real de la empresa).
- Si usted ha recibido un correo electrónico, póngase en contacto con el sitio web de asistencia al cliente de la compañía y solicite la empresa para verificar que esta persona es en realidad uno de sus empleados**.**
- Si cree que su PC o equipo está infectado, evite usar Internet y:
  1. Ejecute un escaneo usando su software antivirus; o
  2. Póngase en contacto con un técnico de renombre o empresa de reparación de computadoras y hacer que compruebe su PC, y/o ordenador.

Si usted cree ser una víctima de un **fraude o esquema de Microsoft** u otra compañía cibernética, comuníquese con la con la oficina del Fiscal General de Pennsylvania.

CONTACTOS

National Federation for Credit Counseling
• 1-800-388-2227 • 1-800-682-9832 (Spanish)
nfcc.org
Financial Industry Regulatory Authority (FINRA)
BrokerCheck® (research Brokers, Brokerage Firms, Investment Adviser Representatives and Investment Adviser Firms)
finra.org/Investors/ToolsCalculators/BrokerCheck/
Area Agencies on Aging
aging.pa.gov/local-resources/pages/AAA.aspx

REPORTES DE CREDITO GRATUITOS

Annual Credit Report Request Service • P.O. Box 105281, Atlanta, GA, 30348-5281
1-877-322-8228
annualcreditreport.com

AGENCIAS Y OFICINAS DE CREDITO

Equifax • 1-800-685-1111
equifax.com
Experian • 1-888-397-3742
experian.com
TransUnion • 1-888-567-8688

OFICINAS DE NEGOCIOS

Western Pennsylvania • 877-267-5222 (Pittsburgh)
westernpennsylvania.bbb.org
Northeastern Pennsylvania • 570-342-5100 (Scranton)
nepa.bbb.org
Eastern Pennsylvania • 215-985-9313 (Philadelphia) • 610-966-8780 (Bethlehem)
• 717-364-3250 (Harrisburg)

CONTACTOS PARA SU PROTECCION

OFICINAS DEL GOBIERNO

Pennsylvania Department of Banking and Securities
Tratar de encontrar información sobre los servicios financieros puede ser confuso, si usted no está seguro de dónde empezar, llámenos hoy at **1.800.PA.BANKS** o **1.800.600.0007**.
dobs.pa.gov

Pennsylvania Office of Attorney General
• 1-800-441-2555
attorneygeneral.gov

Pennsylvania Department of State, Bureau of Charitable Organizations
• 1-800-732-0999
dos.pa.gov

Federal Trade Commission
• 1-877-FTC-HELP
ftc.gov

Consumer Financial Protection Bureau
• 1-855-411-2372
consumerfinance.gov
consumerfinance.gov/es (Sitio web en Español)

Internet Crime Complaint Center • www.ic3.gov

U.S. Secret Service
• Harrisburg 717-234-0214 • Philadelphia 215-861-3300
• Pittsburgh 412-281-7825 • Scranton 570-346-5781
secretservice.gov
Internal Revenue Service
(Para información sobre organizaciones caritativas)
• 1-877-829-5500
irs.gov/charities

Tome medidas hoy:

Conéctese: PA Banking and Securities on

Facebook and LinkedIn. @PAFinancialReg on Twitter.
Manténgase conectado para aprender de eventos en su comunidad, así como las últimas noticias y tendencias financieras y regulatorias.

Educate: dobs.pa.gov | The Quarter
Contamos con numerosas publicaciones gratuitas y recursos para los consumidores y las organizaciones comunitarias.

Llámenos: 1.800.pa. BANKS o (1.800.600.0007). Operadores telefónicos desde las 8:00 am hasta las 5:00 pm de lunes a Viernes. Una persona responderá su llamada o le devolverá su llamada en 24 horas entre días de la semana.