Como evitar estafas

Grupo INT – https://www.grupo-int.com
dpto.ciberseguridad@grupo-int.com

Indice

Notas y aclaraciones

El objeto de esta pequeña guiá sobre estafas es la de ayudar a las personas a prevenir las mismas. Los estafadores cada día se esmeran más y depuran sus técnicas para conseguir sus objetivos. **El sentido común** es la primera defensa que tenemos y si a esto le añadimos **un poco de esfuerzo a la hora de verificar la información**, tenemos mucho ganado.

Este "manual" ha sido adaptado del original, publicado por la ACCC (Australian Competition & Consumer Commission) titulado "El pequeño libro negro sobre estafas" y con la siguiente licencia:

ISBN 978 1 920702 00 7
Comisión Australiana de Competencia y Consumo
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

ACCC 12/16_1129
www.accc.gov.au

Nuestra intención es la de difundir y ayudar en la detección de estafas porque en nuestro día a día hemos tratado casos que han resultado demoledores para los estafados. **Si al compartir este documento, incumplimos cualquier licencia o derecho de autor, notifiquenoslo enviando un correo a**: info@grupo-int.com para que podamos subsanarlo. No esta en nuestros objetivos dañar, molestar o incumplir ningún derecho de nadie.

Introducción

Todos los años, las estafas les cuestan a los usuarios, las empresas y a la economía cientos de millones de euros, causando daños emocionales a las víctimas y a sus familias.

La mejor manera de protegerse es a través del conocimiento y la educación. Este documento puede ser una herramienta importante para que los consumidores y las pequeñas empresas sepan más sobre las estafas e incluye:

- ✔ Las estafas más comunes a tener en cuenta.
- ✔ Las diferentes maneras en las que los estafadores pueden ponerse en contacto con usted.
- ✔ Los recursos que los estafadores usan para engañarlo
- ✔ Las señales de advertencia
- ✔ Cómo protegerse, y
- ✔ Dónde se puede encontrar ayuda.

Queremos recordarle que nadie da nada gratis, que si algo nos parce increíble, lo más seguro es que lo sea y por supuesto, usar el sentido común.

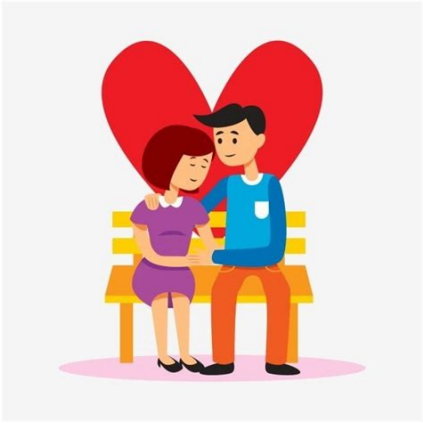
Principales estafas a evitar

Todos somos vulnerables a las estafas, por eso, todos necesitamos información sobre cómo identificarlas y evitar ser estafados. Algunas personas piensan que solo los crédulos y codiciosos son víctimas de estafas. La verdad es que los estafadores son inteligentes y si no se sabe a qué debemos prestar atención, cualquiera puede ser víctima de una estafa. ¿Ha recibido una oferta que parece demasiado buena para ser cierta, tal vez una llamada telefónica para ayudarlo a reparar su computadora o una amenaza para que pague dinero que no debe, una alerta de su banco o proveedor de telecomunicaciones sobre un problema con su cuenta o incluso una invitación a “ser amigo” o a conectarse en línea?

Los estafadores saben cómo aprovecharse de las debilidades para obtener lo que quieren. Se están volviendo más inteligentes, y se adaptan a los tiempos que corren para aprovechar nuevas tecnologías, nuevos productos o servicios y eventos importantes, para crear historias creíbles que lo convencerán de desprenderse de su dinero o de sus datos personales.

Sin embargo, gracias a las decenas de miles de denuncias de estafas recibidas todos los años, hemos preparado una lista de estafas comunes para revelar los secretos y las tácticas que los estafadores no quieren que usted conozca.

Estafas de citas y romances



Las estafas de citas y romance les cuestan millones a los estafados todos los años y pueden arruinar a personas y a sus familias. Este tipo de estafa tiene un fuerte componente emocional que lo hace doblemente dañino.

Cómo funciona la estafa

Los estafadores de citas y romance crean perfiles falsos en sitios web de citas, aplicaciones móviles o plataformas de redes sociales legítimos como Facebook, utilizando fotos e identidades que frecuentemente roban a otras personas. Usan estos perfiles para intentar entablar una relación con usted que puede durar meses o incluso años, solo para poder quedarse con su dinero. El estafador pedirá dinero para ayudarle con enfermedades, lesiones, costos de viaje o una crisis familiar. Son desalmados y le mentirán para aprovechar su buena disposición.

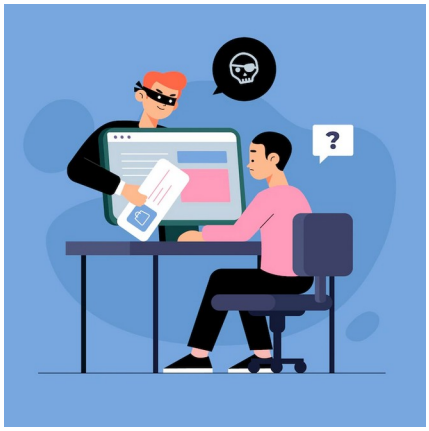
Los estafadores generalmente estarán en el extranjero y tendrán una excusa para explicar por qué están allí. Dirán, por ejemplo, que están haciendo el servicio militar,

trabajando como ingeniero o cuidando a un amigo o a un familiar. Nunca son quienes dicen ser y algunos estafadores astutos incluso pueden enviar pequeños regalos. Esto es sólo parte de un plan para sacarle aún más dinero en el futuro.

Protéjase

- ✗ Nunca envíe dinero ni informe sus datos personales a alguien que solo haya conocido por Internet.
- ✗ Tenga cuidado si un admirador/a que conoció por Internet le pide comunicarse fuera del sitio web de citas o de la plataforma de redes sociales después de solo unos pocos "contactos" o conversaciones, podría ser un estafador/a.
- ✗ Realice una búsqueda de imágenes de su admirador/a para ayudar a determinar si realmente es quien dice ser. Puede utilizar servicios de búsqueda de imágenes como Google o TinEye.
- ✗ Tenga cuidado cuando comparta fotos o videos íntimos en Internet. Se sabe que los estafadores/as chantajean a sus víctimas usando fotos o videos de ellos que no quieren que sean vistos por otras personas.

Estafas de inversión



¿"Inversión sin riesgo" u oportunidad para el infortunio?

Como funciona la estafa

Las **estafas de inversión** adoptan muchas formas incluso compra de criptodivisas, comercio de opciones binarias, emprendimientos comerciales, planes de jubilación, fondos administrados y la compraventa de acciones o propiedades. Los estafadores

adornan las “oportunidades” con folletos y sitios web de aspecto profesional para enmascarar sus operaciones fraudulentas. En general, comienzan con una llamada telefónica o un mensaje de correo electrónico inesperado que ofrece una oportunidad que “no se puede perder”, de “alta rentabilidad” o “garantizada”. El estafador generalmente opera desde el extranjero y no tiene una licencia para ofrecer servicios financieros.

Las **estafas de software de predicción** prometen predecir con precisión movimientos del mercado de valores, resultados de carreras de caballos, eventos deportivos o loterías. Son simplemente una forma de apuesta disfrazada de inversiones. La mayoría de los planes o programas no funcionan y los compradores no pueden recuperar su dinero. En muchos casos el proveedor simplemente desaparece.

Las **estafas de fondos de jubilación** ofrecen acceso anticipado a su fondo de jubilación, a menudo a través de un fondo de jubilación autogestionado o a cambio del pago de honorarios. El estafador puede pedirle que acepte una historia confabulada para permitir la liberación anticipada de su dinero y luego, actuando como su asesor financiero, engañará a su empresa de fondos de jubilación para que le pague sus beneficios de jubilación directamente a él. Una vez que tenga su dinero, el estafador puede retener fondos en concepto de” honorarios” elevados, o incluso dejarlo sin nada en absoluto.

Protéjase

- ✗ No permita que nadie lo presione para tomar decisiones sobre su dinero o sus inversiones, especialmente si la oferta ha salido de la nada.
- ✗ Antes de separarse de su dinero, haga su propia investigación sobre la empresa de inversiones y compruebe si la misma tiene una Licencia para ofrecer servicios financieros. Pregúntese: si un extraño supiera un secreto para ganar dinero, ¿por qué lo compartiría?
- ✗ Si no está en edad de jubilarse, tenga cuidado con las ofertas que promueven el acceso fácil a sus beneficios de jubilación depositados. Si accede de manera temprana a su fondo de jubilación ilegalmente, es posible que tenga que pagar multas en virtud de la legislación fiscal.

Estafas de amenazas y multas

Si una autoridad gubernamental o una compañía de confianza le dice que pague, tómese su tiempo, piense y vuelva a verificar.

Cómo funciona la estafa

En lugar de ofrecer un premio, dinero o reembolso, estas estafas utilizan amenazas diseñadas para coaccionarlo a que entregue su dinero. Es posible que el estafador lo llame y lo amenace con un arresto o le envíe un mensaje de correo electrónico para informarle que adeuda dinero por una multa por exceso de velocidad, una deuda con la oficina de impuestos o una factura impagada.

Durante la llamada telefónica, los estafadores lo presionarán para que pague de inmediato y le informarán que enviarán la policía a su casa si se niega a pagar. Se sabe que los estafadores se dirigen a personas vulnerables en nuestra comunidad, como los inmigrantes recién llegados. Se hacen pasar por funcionarios del Departamento de Inmigración y amenazan a las víctimas con la deportación a menos que paguen tarifas para corregir errores en sus visas. Una estafa muy similar consiste en un estafador que pretende ser de la Agencia Tributaría y les dice a sus víctimas que tienen una factura impositiva pendiente.

Los estafadores también pretenden ser empresas de confianza, como su banco, proveedor de gas, electricidad, agua o de servicios telefónicos. Lo amenazarán con cancelar su servicio o con cobrarle multas excesivas si no paga la factura de inmediato. En ocasiones, pueden hacerse pasar por una empresa como Correos y decirle que tiene un paquete para recoger y se le cobrará una tarifa de retención por cada día que lo tengan almacenado. Cualquiera sea el caso, intentan preocuparlo y hacer que actúe sin

detenerse a pensar y verificar que la historia sea cierta. Si la estafa se envía por correo electrónico, es probable que incluya un archivo adjunto o un enlace a un sitio web falso, en el que se le pedirá que descargue una prueba de la "factura", "multa" o "detalles de la entrega". Si abre el archivo adjunto o lo descarga, se infectará su computadora con un programa malicioso (malware).

Protéjase

- ✗ No se deje presionar por una persona que llame amenazando. Tómese su tiempo, piense y verifique si la historia es verdadera.
- ✗ Una agencia gubernamental o una empresa de confianza nunca le pedirá que pague por medios inusuales como tarjetas de regalo, transferencias o Bitcoins.
- ✗ Verifique la identidad del contacto llamando directamente a la organización correspondiente; búsquelo a través de una fuente independiente, como una guía telefónica, una factura anterior o una búsqueda en Internet.
- ✗ No utilice los datos de contacto proporcionados en los mensajes de correo electrónico o durante las llamadas telefónicas. Le repetimos, búsquelos a través de una fuente independiente.

Estafas de dinero inesperado

Si se le pide que haga pagos antes de recibir bienes o dinero, piénselo dos veces.

Cómo funciona la estafa

Inesperadamente, los estafadores le dicen que tiene derecho a recibir dinero, piedras preciosas, oro o acciones valiosas, pero que debe hacer **pagos por adelantado**

para obtenerlos. Nunca recibirá lo que se le prometió y siempre habrá una excusa para explicar por qué tiene que pagar más. Si paga el importe, perderá su dinero.

Las **estafas de reembolso o reclamo** consisten en un estafador que le dice que se le debe dinero por razones tales como impuestos pagados en exceso, honorarios bancarios o algún tipo de compensación. Sin embargo, para poder recibir su dinero, se le pide que pague una pequeña tarifa por gastos administrativos.

En las **estafas de herencia**, los estafadores se hacen pasar por abogados, banqueros o funcionarios extranjeros y le informan que tiene derecho a cobrar una gran herencia o le ofrecen que participe en una argucia porque tiene el mismo nombre que alguien que falleció. Generalmente, utilizan documentos que parecen oficiales y le piden que realice pagos en concepto de honorarios e impuestos antes de poder recibir la herencia. También pueden solicitar sus datos personales para completar la "documentación oficial". Esto significa que podrían robarle su identidad, además de su dinero.

Es posible que las comúnmente llamadas **estafas nigerianas** se hayan originado en África Occidental, pero pueden provenir de cualquier parte del mundo. Se trata de estafadores que le dicen que necesitan su ayuda para recibir una gran fortuna que están tratando de transferir fuera de su país desesperadamente. Pueden afirmar que la fortuna es una cantidad de dinero escondida, oro o activos abandonados por un gobierno o funcionario corrupto y, si acepta recibirla, le otorgarán un porcentaje elevado del total cuando sea seguro hacerlo. Al igual que todas estas estafas, dirán que primero debe pagar impuestos, cargos bancarios u honorarios por controles de antiterrorismo y lavado de dinero, para poder enviarle el dinero. Estas estafas comúnmente provienen del extranjero y solicitan el pago mediante transferencia electrónica, pero también pueden solicitar transferencias bancarias u otros métodos de pago.

Si se deja engañar por este tipo de estafas, nunca recibirá nada del estafador y perderá el dinero que haya enviado.

Protéjase

- ✗ Recuerde que no existen planes para hacerse rico de la noche al día: si suena demasiado bueno para ser verdad, probablemente lo sea.

- ✗ Evite cualquier acuerdo con un extraño que solicite un pago por adelantado mediante giro postal, transferencia electrónica, transferencia internacional de fondos, tarjeta precargada o moneda electrónica. Rara vez se logra recuperar el dinero enviado de esta manera.
- ✗ Si un mensaje de correo electrónico espontáneo parece sospechoso, simplemente elimínelo. No haga clic en ningún enlace.
- ✗ Los departamentos gubernamentales, bancos o empresas de servicios públicos nunca se comunicarán con usted para pedirle que pague dinero por adelantado para reclamar una tarifa o reembolso.
- ✗ Si no está seguro, verifique la identidad del contacto de forma independiente. No utilice los datos de contacto proporcionados en el mensaje que le enviaron; obtenga los datos de contacto correctos a través de una fuente independiente, como una guía telefónica o una búsqueda en Internet.
- ✗ Realice una búsqueda en Internet utilizando el texto exacto de la oferta: muchas estafas pueden identificarse de esta manera.

Estafas de premios y loterías

No se deje tentar por haber ganado algo sorpresivamente, solo el estafador se lleva a casa dinero caído del cielo.

Cómo funciona la estafa

Estas estafas intentan engañarlo para que entregue dinero por adelantado o para que entregue sus datos personales a cambio de recibir un premio de una lotería, un sorteo o una competencia en la que nunca participó. Los estafadores afirman que debe pagar tarifas o impuestos para poder liberar sus "ganancias" o premios. También es

posible que tenga que llamar o enviar un mensaje de texto a un número de teléfono con tarifa de recargo para reclamar su premio.

Las **estafas de "raspadita"** consisten en recibir correo con folletos de papel satinado y varias tarjetas para raspar, una de las cuales será la tarjeta ganadora. Para hacerlo más creíble, generalmente será el segundo o el tercer premio. Cuando llame para reclamar su premio, los estafadores solicitarán el pago de tarifas o impuestos para poder recibir sus ganancias.

Las **estafas de lotería** pueden usar los nombres de loterías reales del extranjero para afirmar que ganó dinero en efectivo, aunque nunca haya participado en ellas. Los estafadores normalmente piden el pago de honorarios o impuestos para liberar los fondos. También le informarán que necesitan sus datos personales para demostrar que usted es el ganador correcto, pero luego usarán esta información para robar su identidad o dinero de su cuenta bancaria.

Los **vales y las tarjetas de regalo falsos** consisten en estafadores que le envían un mensaje de correo electrónico o un mensaje de texto o un mensaje en las redes sociales diciendo que usted ha ganado una tarjeta de regalo de una tienda conocida, pero que debe proporcionar algunos datos antes de poder recibirla. Este es un intento para obtener información personal que puede usarse para el robo de identidad o para hacerlo objeto de otra estafa. También se sabe que ofertas como éstas descargan ransomware en su dispositivo.

En las **estafas de premios de viajes** los estafadores afirman que usted ha ganado vacaciones o pasajes aéreos gratuitos. De hecho, lo que realmente ha ganado es la posibilidad de comprar alojamiento o vales de vuelo. Estos vales de viaje con frecuencia incluyen tarifas y condiciones ocultas, o pueden ser falsos y no tener valor alguno. Del mismo modo, los estafadores pueden ofrecerle increíbles paquetes de vacaciones con descuento que simplemente no existen.

Protéjase

- ✗ Recuerde: no puede ganar dinero en una lotería o sorteo a menos que haya participado.

- ✗ Las loterías y sorteos no requieren que pague una tarifa para cobrar las ganancias. Realice una búsqueda en Internet utilizando el texto exacto de la oferta. Esto puede servir para confirmar que se trata de una estafa.
- ✗ Piense dos veces antes de llamar o enviar un mensaje de texto a un número de teléfono que comience con "803, 806, 807": se cobran a tarifas con recargo.

Estafas de compras, clasificados y subastas por Internet

A los estafadores también les encanta la facilidad de comprar por Internet.

Cómo funciona la estafa

Cada vez más, los consumidores y las empresas compran y venden por Internet. Desafortunadamente, a los estafadores les gusta comprar víctimas por Internet.

Los estafadores pueden crear **sitios web de tiendas falsos** muy convincentes, que parecen reales, incluso en redes sociales como Facebook. El mayor indicio de que un sitio web de una tienda es una estafa es la forma de pago. Tenga cuidado si le piden que pague por transferencia electrónica o por otros medios inusuales de pago.

En una **estafa de subasta en línea**, el estafador afirma que usted tiene una segunda oportunidad para comprar un artículo por el que hizo una oferta porque el ganador se retiró. El estafador le pedirá que pague fuera del servicio de pago seguro del sitio de subastas; si lo hace, perderá su dinero, no obtendrá el artículo por el que pagó y el sitio de subastas no podrá ayudarlo.

La **estafa de anuncios clasificados en Internet** es una estafa común dirigida tanto a compradores como a vendedores. Los compradores deberían cuidarse de los estafadores que publican anuncios falsos en sitios web de anuncios clasificados legítimos. Los anuncios pueden ser para cualquier cosa, desde propiedades en alquiler hasta mascotas, autos usados o cámaras, y con frecuencia el precio es bajo. Si muestra interés en el artículo, el estafador puede decir que está de viaje o que se ha mudado al extranjero y que un agente le entregará los productos luego de recibir el pago. Tras el pago, no recibirá los artículos ni podrá ponerse en contacto con el vendedor.

En el caso de los vendedores, un estafador de anuncios clasificados responderá a su anuncio con una oferta generosa. Si usted la acepta, el estafador pagará con cheque o giro postal. Sin embargo, la cantidad que recibirá será mayor que el precio acordado. En esta **estafa de pago en exceso**, el "comprador" puede decirle que hubo un error y le solicitará que reembolse el monto excedente mediante una transferencia de dinero. El estafador espera que usted transfiera el dinero antes de descubrir que el cheque ha rebotado o que el giro postal fue falso. Perderá el dinero, y también el producto que vendió si ya lo despachó.

Protéjase

- ✗ Averigüe exactamente con quién está tratando. Si es una tienda nacional, tiene muchas más posibilidades de resolver el problema si algo sale mal.
- ✗ Compruebe si el vendedor tiene buena reputación, si cuenta con una política de reembolso y un servicio de gestión de quejas.
- ✗ Evite cualquier acuerdo en el que le soliciten un pago por adelantado mediante giro postal, transferencia electrónica, transferencia internacional de fondos, tarjeta precargada o moneda electrónica. Rara vez se recupera el dinero enviado de esta manera. Nunca envíe dinero ni proporcione datos de tarjetas de crédito ni de cuentas en línea a alguien que no conozca o en quien no confía, y nunca envíe estos datos por correo electrónico.
- ✗ Solo pague a través del método de pago seguro del sitio web, busque una dirección en Internet que comience con "https" y un símbolo de candado cerrado.
- ✗ Nunca acepte un cheque o giro postal como pago por un importe mayor de lo acordado ni envíe dinero a nadie en nombre de otra persona.

Estafas dirigidas a computadoras y dispositivos móviles

Recuerde: todo lo que se conecta a Internet es vulnerable.

Cómo funciona la estafa

Los **estafadores de acceso remoto** lo llaman por teléfono y le dicen que su computadora está infectada por un virus. Si sigue sus instrucciones, les permitirá acceder y controlar su computadora donde pueden robar información o instalar malware. También pueden tratar de convencerlo de que compre un software "antivirus", que generalmente resulta ser demasiado caro o está disponible en Internet en forma gratuita.

Malware es un término que se refiere a cualquier tipo de software malicioso que puede instalarse en su computadora o en otros dispositivos, e incluye virus, software espía, ransomware, troyanos y registradores de pulsaciones de teclas.

Los **registradores de pulsaciones de teclas** y el **software espía** permiten a los estafadores grabar exactamente lo que escribe en su teclado y averiguar contraseñas y datos bancarios o acceder a información personal y enviarla a cualquier lugar que deseen. Una vez instalados, los estafadores pueden controlar su correo electrónico y sus cuentas de redes sociales y capturar cualquier información que haya en su dispositivo, incluidas las contraseñas. También pueden usar sus cuentas para enviar más estafas a sus amigos y familiares.

El **ransomware** es otro tipo de malware que encripta o bloquea su dispositivo para evitar que lo use hasta que se realice un pago para desbloquearlo. El pago no garantiza que se desbloqueará ni que estará libre de virus ocultos, que también pueden propagarse e infectar otras computadoras o dispositivos en su red.

El malware generalmente se pasa por correo electrónico y aparentemente puede provenir de fuentes legítimas, como su proveedor de servicios públicos, una agencia gubernamental o incluso la policía, que pretende emitir una multa. No haga clic en el enlace ni abra ningún archivo adjunto del que no esté absolutamente seguro. Es posible que descargue software malicioso. Estas estafas se dirigen tanto a individuos como a empresas.

Protéjase

- ✗ Tenga cuidado con descargas gratuitas que ofrecen música, juegos, películas y acceso a sitios para adultos. Pueden instalar programas dañinos sin que usted lo sepa.
- ✗ Mantenga sus redes de oficina, computadoras y dispositivos móviles seguros. Actualice su software de seguridad, cambie las contraseñas y haga una copia de seguridad de sus datos con regularidad. Almacene sus copias de seguridad fuera de la oficina y fuera de línea.
- ✗ No abra archivos adjuntos ni haga clic en enlaces de mensajes de correo electrónico ni en mensajes de redes sociales que haya recibido de extraños, simplemente presione eliminar.

Robo de identidad

Todas las estafas conllevan la posibilidad del robo de identidad. Protegerse de las estafas también implica mantener su información personal segura.

El robo de identidad es una amenaza en todas las estafas

La mayoría de las personas asocian las estafas con intentos de engaño para obtener dinero. Sin embargo, su información también es valiosa para los estafadores. Los estafadores roban sus datos personales para cometer actividades fraudulentas, como realizar compras no autorizadas con su tarjeta de crédito o usar su identidad para abrir cuentas bancarias o telefónicas. Es posible que pidan préstamos o lleven a cabo otras transacciones ilegales usando su nombre. Incluso pueden vender su información a otros estafadores para otros usos ilegales.

Que le roben la identidad puede ser devastador tanto financiera como emocionalmente. Puede demorar meses en recuperar su identidad y el impacto de que se la hayan robado puede durar varios años.

Phishing: Un estafador lo contacta de la nada por correo electrónico, por teléfono, por Facebook o por mensaje de texto y simula pertenecer a una empresa legítima, como un proveedor de servicios bancarios, telefónicos o de Internet. Lo dirige a una versión falsa del sitio web de la empresa que le solicitará sus datos personales para verificar los registros de clientes debido a un error técnico. Pueden llamar haciéndose pasar por una tienda de artículos de lujo y decir que alguien está intentando usar su tarjeta de crédito. Le aconsejarán ponerse en contacto con su banco, pero no colgarán y mantendrán la línea abierta. Cuando usted trate de llamar al banco, todavía estará hablando con los estafadores, quienes simularán que se trata de una llamada real, imitarán al personal del banco y le pedirán los datos de cuenta y de seguridad. En ambos casos, el estafador captura cualquier información que usted le dé y luego la usa para acceder a sus cuentas.

Encuestas falsas: Los estafadores ofrecen premios o recompensas, como tarjetas de regalo de tiendas conocidas, a cambio de completar una encuesta en línea. La encuesta requiere que responda una serie de preguntas, que incluyen la divulgación de datos de identificación importantes o datos bancarios.

Como parte de una estafa: Con frecuencia los estafadores solicitan información personal en otras estafas. En una estafa de lotería, los estafadores suelen solicitar la licencia de conducir o el pasaporte para “comprobar su identidad para poder liberar el dinero del premio”. En estafas de citas y romance, pueden solicitar información “para patrocinar la solicitud de visa para visitarlo en su país”.

Recuerde: Entregar información personal a un estafador puede ser tan malo como entregar dinero. Mantenga sus datos personales en secreto y en un lugar seguro.

Protéjase

- **Piense dos veces sobre lo que dice y hace en un entorno en línea**. Tenga cuidado al compartir información sobre usted en Internet, incluso en redes sociales, blogs y otros foros en línea. Reflexione antes de completar encuestas, participar en concursos, hacer clic en enlaces o archivos adjuntos, o incluso "hacerse amigo", "expresar que le gusta" o "compartir" algo en Internet.
- **Tenga cuidado con cualquier pedido de sus datos o de dinero**. Los estafadores tratarán de engañarlo para que entregue sus datos usando nombres de compañías conocidas o de departamentos gubernamentales Si cree que es una estafa, no responda. Utilice la guía telefónica o haga una búsqueda en Internet para verificar los datos de contacto de la organización. Nunca utilice los datos de contacto proporcionados en la solicitud original.

Si ha proporcionado información de identificación personal a estafadores, comuníquese lo antes posible con la policía o llamando al INCIBE (Instituto Nacional de Ciberseguridad) en el número 017.

Estafas de trabajo y empleo

¿Altos ingresos garantizados? ¡Improbable!

Cómo funciona la estafa

Las **estafas de trabajo y empleo** consisten en ofertas para trabajar desde el hogar o generar una "oportunidad de negocios" e invertir en ella. Los estafadores prometen un empleo, un salario alto o un gran retorno de la inversión después de efectuar pagos iniciales por adelantado. Estos pagos pueden ser para un "plan de negocios", un curso de capacitación, software, uniformes, permisos de seguridad, impuestos u honorarios. Si paga los honorarios, es posible que no reciba nada o que no obtenga lo que esperaba o lo que le prometieron.

Algunas ofertas de empleo pueden ser una pantalla para **actividades ilegales de lavado de dinero**, donde se le pide que actúe como "administrador de cuentas" o "asistente personal", que reciba pagos en su cuenta bancaria a cambio de una comisión y que luego transfiera el dinero a una empresa en el extranjero. Generalmente, las estafas de trabajo se promueven a través de mensajes de correo electrónico no deseados o de anuncios clasificados bien conocidos y en sitios web de buscadores de empleo, incluso en sitios web gubernamentales de buscadores de empleo.

Un gran peligro relacionado con estas estafas de trabajo es que pueden pedirle una gran cantidad de datos personales que no debería proporcionar, incluidos su número de contribuyente fiscal y copias de su pasaporte o licencia de conducir. Esta información podría ser utilizada más adelante para robarle la identidad.

Protéjase

- ✗ Tenga cuidado con ofertas o planes que afirman garantizar ingresos o que requieren un pago por adelantado.
- ✗ Nunca acepte transferir dinero en nombre de otra persona, se trata de lavado de dinero y es ilegal.
- ✗ No proporcione su número de contribuyente fiscal, licencia de conducir o pasaporte cuando se postule para un trabajo. Es posible que tenga que proporcionar esta información, pero solo después de haber comenzado a trabajar.

El lavado de dinero es un delito penal: No acepte transferir dinero en nombre de un desconocido.

Estafas de beneficencia y médicas

Los estafadores no tienen escrúpulos y pueden actuar en momentos de desesperación.

Cómo funciona la estafa

Los estafadores se aprovechan de las personas que buscan donar a una buena causa o encontrar una respuesta a un problema de salud.

En las **estafas de beneficencia** los estafadores recaudan dinero simulando trabajar para una causa legítima o benéfica, o para una ficticia creada por ellos. Generalmente, los estafadores se aprovechan de un desastre natural o de una crisis reciente que apareció en las noticias.
Estas estafas impiden la realización de donaciones muy necesarias para organizaciones benéficas legítimas. Las organizaciones benéficas deben estar registradas ante el gobierno; para hacer una donación de manera segura, primero verifique que estén registradas.

Las **estafas de curación milagrosa** ofrecen una gama de productos y servicios que pueden parecer medicinas alternativas legítimas y que generalmente prometen remedios rápidos y efectivos para afecciones médicas graves. Generalmente, los tratamientos se promueven utilizando testimonios falsos de personas que han sido "curadas".

Las **estafas de pérdida de peso** prometen una pérdida de peso espectacular con poco o ningún esfuerzo. Este tipo de estafa puede implicar una dieta inusual o restrictiva, ejercicios revolucionarios, un dispositivo para "eliminar la grasa", píldoras, parches o cremas innovadores. Es posible que le soliciten que realice un pago elevado por

adelantado o que firme un contrato a largo plazo para recibir suministros de manera constante.

Las **farmacias en línea falsas** ofrecen fármacos y medicamentos falsificados a precios muy económicos y, a veces, los proporcionan sin receta médica. Estos medicamentos pueden tener ingredientes activos limitados o carecer de ellos, lo que puede tener consecuencias letales para los usuarios.

Protéjase

- ✗ Si se le acerca un recaudador de beneficencia en la calle, pida ver su identificación. Si tiene alguna duda sobre de quién se trata, no pague.
- ✗ Consulte la lista de organizaciones benéficas registradas en la Asociación de organizaciones benéficas sin fines de lucro de España.
- ✗ Consulte a un profesional de la salud si está considerando probar medicamentos, suplementos u otros tratamientos que aseguran ser "milagrosos" o "instantáneos".
- ✗ Pregúntese: Si verdaderamente se trata de una cura milagrosa, ¿su profesional de la salud no le habría hablado al respecto?

Estafas a empresas

Los estafadores aprovechan que muchas empresas llevan un ritmo muy acelerado para timarlas.

Cómo funciona la estafa

Las estafas dirigidas a empresas tienen todo tipo de apariencias y es probable que se realicen en las épocas de mayor actividad, como el final del ejercicio fiscal.

Una **estafa de facturación falsa** es el truco más común que usan los estafadores contra las empresas. Los estafadores emiten facturas falsas por publicaciones, anuncios, productos o servicios no deseados o no autorizados. La **estafa de la guía comercial** es un ejemplo bien conocido, en el que se recibe una factura por la publicación en una guía supuestamente conocida. Los estafadores lo engañan para que se registre, disfrazando la oferta como una factura pendiente o una publicación gratuita, pero con un acuerdo de suscripción oculto en la letra pequeña.

La **estafa de nombres de dominio** es otra táctica utilizada por los estafadores, en la que se lo engaña para que se inscriba en un registro de dominio de Internet no solicitado muy similar al suyo. También puede recibir un aviso de renovación falso para su nombre de dominio real y pagar sin darse cuenta.

Una **estafa de productos de oficina** consiste en que usted recibe y le cobran productos que no pidió. Estas estafas a menudo involucran productos o servicios que usted compra regularmente, como papelería y artículos de limpieza. Los estafadores suelen llamar a su empresa fingiendo que un servicio o producto ya ha sido solicitado.

Las **estafas de redirección de pagos** consisten en un estafador que usa información que ha obtenido al piratear sus sistemas informáticos. Luego, se hace pasar por uno de sus proveedores habituales y le informa que sus datos bancarios han cambiado. Es posible que le informen que han cambiado de banco recientemente y pueden usar membretes y marcas copiados para convencerlo de que son legítimos. Le proporcionarán un nuevo número de cuenta bancaria y le pedirán que todos los pagos futuros se procesen a dicha cuenta. Con frecuencia, la estafa solo se detecta cuando su proveedor habitual pregunta por qué no le pagaron.

El **ransomware** puede ser extremadamente perjudicial para cualquier empresa. La mejor defensa es hacer una copia de seguridad de sus datos con regularidad y almacenar esas copias en otro lugar y sin conexión a Internet.

Protéjase

- ✗ No acepte ofertas ni transacciones de inmediato: Siempre pida que la oferta se haga por escrito y solicite asesoramiento independiente si la transacción implica dinero, tiempo o un compromiso a largo plazo.

- ✗ Nunca proporcione datos bancarios, financieros ni contables de su empresa a alguien que se comunique con usted de forma inesperada y a quien no conozca o en quien no confíe.
- ✗ Contar con procedimientos administrativos efectivos puede contribuir en gran medida a prevenir estafas: Cuente con procesos claramente definidos para verificar y pagar cuentas y facturas, y analice con mucha atención pedidos de cambio de datos bancarios.
- ✗ Capacite y conciencie a su personal para reconocer estafas.
- ✗ Mantenga copias de seguridad de los datos de su empresa en otro lugar y sin conexión a Internet.
- ✗ Tenga cuidado con los mensajes de correo electrónico que soliciten cambios en los datos de pago. Siempre verifique los cambios en los datos de pago directamente con la empresa o persona.

Cómo funcionan las estafas: Anatomía de una estafa

La mayoría de las estafas siguen el mismo patrón y, una vez que entienda eso, los trucos del estafador se vuelven más fáciles de detectar.

Si observa detenidamente todos los distintos tipos de estafas descritos en este libro, pronto notará que la mayoría de las estafas pasan por tres etapas: 1-Contacto; 2-Comunicación y 3-Pago, envío de dinero.

Comprender las partes básicas de una estafa lo ayudará a evitar la oleada actual de estafas y a estar en guardia para protegerse de las nuevas estafas que surjan en el futuro.

1. Contacto: Forma de ejecución

Cuando los estafadores se dirijan a usted, siempre será con una historia diseñada para hacerle creer una mentira. El estafador pretenderá ser algo que no es: un funcionario del gobierno, un inversor experto, un funcionario de lotería o incluso un admirador romántico.

Para hacerle creer estas mentiras, los estafadores utilizarán una variedad de métodos de comunicación.

Por Internet

Los estafadores acechan en el entorno anónimo de Internet.

El correo electrónico es un método preferido de ejecución de estafas, que da acceso a una forma barata y sencilla de comunicarse a gran escala. Los correos electrónicos de phishing que "buscan" su información personal son el tipo de estafa de correo electrónico más común.

Las plataformas de redes sociales, los sitios de citas y los foros en línea permiten que los estafadores se conviertan en "amigos" y entren en su vida personal para acceder a sus datos personales, que luego pueden ser utilizados en contra de usted o de su familia y amigos.

Los estafadores utilizan s**itios de compras en línea**, **anuncios clasificados** y **sitios de subastas** para captar compradores y vendedores. En general, el contacto inicial se realiza a través de sitios confiables y de buena reputación, o a través de sitios web falsos que parecen reales. Busque opciones de pago seguras y tenga cuidado con los métodos de pago inusuales, como transferencia electrónica, Bitcoins o tarjetas de dinero precargadas. Las tarjetas de crédito suelen ofrecer cierta protección.

Por teléfono

Los estafadores también llaman por teléfono y envían mensajes de texto.

Los estafadores utilizan **llamadas telefónicas** a hogares y empresas en una amplia variedad de estafas, desde amenazas impositivas hasta ofertas de premios o "ayuda" contra virus informáticos. La disponibilidad de llamadas telefónicas de voz sobre protocolo de Internet (VOIP) baratas significa que los centros de llamadas pueden operar desde el exterior con números de teléfono que parecen números locales. La identificación telefónica de la persona que llama puede disimularse fácilmente y es uno

de los muchos trucos que usan los estafadores para hacerle creer que son otras personas.

Los estafadores utilizan **mensajes de texto SMS** para enviar una gran variedad de estafas, incluidas las de competencia o de premios. Si responde, es posible que le cobren tarifas con recargo o que se vea inscrito en un servicio de suscripción. Es más seguro no responder ni hacer clic en los enlaces de los mensajes de texto a menos que sepa de quiénes proceden. También pueden contener archivos adjuntos o enlaces a software malicioso en forma de fotos, canciones, juegos o aplicaciones.

A domicilio

Cuidado, algunos estafadores irán directamente a su domicilio para tratar de estafarlo.

Las **estafas puerta a puerta** generalmente consisten en que el estafador promociona bienes o servicios que no se entregan o son de muy mala calidad. Incluso es posible que le facturen un trabajo que no deseaba o que no aceptó. Una estafa común puerta a puerta es la que realizan trabajadores poco fiables que se desplazan de un lugar a otro y realizan reparaciones de viviendas de mala calidad o simplemente toman su dinero y escapan.

Las empresas legítimas pueden vender puerta a puerta, pero los vendedores deben identificarse claramente a sí mismos y a su empresa y cumplir otras reglas. Usted tiene derechos específicos en lo que respecta a las prácticas de venta puerta a puerta, incluida la posibilidad de cambiar de opinión.

Los estafadores pueden hacerse pasar por **falsos trabajadores de beneficencia** para recaudar donaciones. Aprovecharán eventos recientes como inundaciones e

incendios forestales. Antes de donar pida una identificación y vea el libro oficial de recibos.

El correo masivo todavía se utiliza para enviar **estafas de lotería y sorteos**, **oportunidades de inversión**, **estafas nigerianas y cartas de herencia falsas**. Un folleto de papel satinado no es garantía de que una oferta sea legítima. Independientemente de la forma de ejecución que utilicen, la historia que presentan es siempre el anzuelo y, si usted "pica", el estafador intentará hacerlo pasar a la siguiente etapa.

2. Comunicación: Preparación

Si les da la oportunidad de hablar con usted, a usar trucos de su conjunto de recursos de estafadores para convencerlo de que se deshaga de su dinero.

Entre los recursos de los estafadores se encuentran los siguientes:

- ✗ Los estafadores crean historias elaboradas pero convincentes para conseguir lo que quieren.
- ✗ Utilizan sus datos personales para hacerle creer que ha tenido contacto con ellos anteriormente y para hacer que la estafa parezca legítima.
- ✗ Los estafadores pueden ponerse en contacto con usted regularmente para generar confianza y convencerlo de que son su amigo, compañero o que tienen un interés romántico en usted.
- ✗ Juegan con sus emociones utilizando el entusiasmo de una victoria, la promesa de amor eterno, la compasión por un accidente desafortunado, la culpa por no ayudar o la ansiedad y el temor de ser arrestados o de recibir una multa.
- ✗ A los estafadores les encanta crear una sensación de urgencia para que no tenga tiempo de razonar y reaccione según las emociones en lugar de la lógica.
- ✗ Del mismo modo, utilizan tácticas de venta de alta presión. Dicen que se trata de una oferta limitada, que los precios subirán, o que el mercado cambiará y se perderá la oportunidad.
- ✗ Una estafa puede tener todas las características de una empresa real mediante el uso de folletos de papel satinado con la jerga técnica de la industria respaldada por frentes de oficinas, centros de llamadas y sitios web profesionales.
- ✗ Con acceso a Internet y a software inteligente, es fácil para los estafadores crear documentos falsificados y de aspecto oficial. Un documento que parece tener la

aprobación del gobierno o que está plagado de jerga legal puede dar a una estafa un aire de importancia.

Los recursos del estafador están diseñados para hacer que baje sus defensas, confíe en la historia y actúe de manera rápida o irracional y pase a la etapa final: enviar el dinero.

3. Pago, envío de dinero

Algunas veces, la pista principal que tendrá de que se trata de una estafa es la manera en la que el estafador le pedirá que pague.

El pedido de dinero puede hacerse a los pocos minutos de la estafa o después de meses de preparación cuidadosa. Los estafadores tienen preferencias sobre la manera en que usted envíe su dinero. Se sabe que los estafadores indican a las víctimas que utilicen el sitio de remesas de dinero (oficina de correos, servicio de transferencia electrónica, o incluso el banco) más cercano a ellos para enviar el dinero. En algunos casos permanecen en el teléfono, dan instrucciones específicas, e incluso pueden enviar un taxi para ayudar con el procedimiento. Los estafadores están dispuestos a aceptar dinero por cualquier medio, entre otros, transferencias bancarias directas, tarjetas de débito precargadas, tarjetas de regalo, tarjetas de Google Play, Steam o iTunes o moneda virtual como Bitcoin. Cualquier solicitud de pago por un método inusual es un signo revelador de que se trata de una estafa. Las tarjetas de crédito generalmente ofrecen algo de protección. Usted también debería buscar opciones de pago seguras donde aparezca “https” en la dirección web y el sitio tenga un símbolo de candado cerrado. No envíe dinero a alguien que solo haya conocido en línea o por teléfono, especialmente si dicha persona está en el extranjero. Tenga en cuenta que los estafadores también pueden solicitar pagos en forma de bienes valiosos y regalos caros, como joyas o artículos electrónicos.

Pagar dinero a los estafadores no es lo único de lo que debería preocuparse: si usted ayuda a un extraño a transferir dinero, es posible que se vea involucrado en actividades ilegales de lavado de dinero sin saberlo.

Las reglas de oro para protegerse

Esté alerta al hecho de que existen estafas. Al tratar con contactos no invitados de personas o empresas, ya sea por teléfono, por correo, correo electrónico, en persona o en un sitio de redes sociales, siempre considere la posibilidad de que el acercamiento pueda ser una estafa. Recuerde, si algo parece demasiado bueno para ser verdad, probablemente lo sea.

Sepa con quién está tratando. Si solo ha conocido a alguien por Internet o no está seguro de la legitimidad de una empresa, tómese un tiempo para investigar un poco más. Busque fotos en imágenes de Google o busque en Internet a otras personas que puedan haber estado en contacto con esa persona.

No abra textos sospechosos, ventanas emergentes ni correos electrónicos: elimínelos. Si no está seguro, verifique la identidad del contacto a través de una fuente independiente, como una guía telefónica o una búsqueda en Internet. No utilice los datos de contacto suministrados en el mensaje que le enviaron.

Mantenga sus datos personales seguros. Ponga un candado en su buzón y destruya sus facturas y otros documentos importantes antes de tirarlos. Guarde sus contraseñas y números de pin en un lugar seguro. Tenga mucho cuidado con la cantidad de información personal que comparte en las redes sociales. Los estafadores pueden usar su información e imágenes para crear una identidad falsa o para hacerlo víctima de una estafa.

Tenga cuidado con formas de pago inusuales. Generalmente, los estafadores solicitan pagos mediante transferencias electrónicas, tarjetas precargadas e incluso tarjetas de Google Play, Steam o iTunes y Bitcoin. Esto casi siempre es una señal de que se trata de una estafa.

Mantenga sus dispositivos móviles y computadoras seguros. Utilice siempre la protección con contraseña, no comparta el acceso con otros (ni siquiera de forma remota), actualice el software de seguridad y haga copias de seguridad del contenido. Proteja su red WiFi con una contraseña y evite usar computadoras públicas o puntos de acceso WiFi para acceder a la banca en línea o para suministrar información personal.

Elija sus contraseñas con cuidado. Elija contraseñas que sean difíciles de adivinar para los demás y actualícelas regularmente. Una contraseña segura debería incluir una combinación de mayúsculas y minúsculas, números y símbolos. No use la misma contraseña para cada cuenta/perfil, y no comparta sus contraseñas con nadie.

Desconfíe de cualquier pedido de sus datos o de dinero. Nunca envíe dinero ni proporcione números de tarjetas de crédito, datos de cuentas en línea ni copias de documentos personales a quien no conozca o en quien no confíe. No acepte transferir dinero ni bienes para otra persona: el lavado de dinero es un delito penal.

Tenga cuidado al comprar en línea. Desconfíe de ofertas que parecen demasiado buenas para ser ciertas y siempre use un servicio de compras en línea que conozca y en el que confíe. Piense dos veces antes de usar monedas virtuales (como Bitcoin): no tienen las mismas protecciones que otros métodos de transacción, lo que significa que no podrá recuperar su dinero una vez que lo envíe.

Dónde encontrar ayuda o apoyo

Si ha perdido dinero por una estafa o le ha dado sus datos personales a un estafador, es poco probable que recupere su dinero. Sin embargo, hay pasos que puede dar de inmediato para limitar el daño y protegerse contra pérdidas adicionales.

Póngase en contacto con su banco o cooperativa de crédito. Si envió dinero o información bancaria personal a un estafador, comuníquese con su banco o cooperativa de crédito inmediatamente. Es posible que puedan anular una transferencia de dinero o cheque, o cerrar su cuenta si el estafador tiene los datos de la misma. Es posible que su proveedor de tarjeta de crédito pueda realizar un "reembolso" (anular la transacción) si se hizo una facturación a su tarjeta de crédito de manera fraudulenta.

Recupere su identidad robada. Si sospecha que es víctima de robo de identidad, es importante que actúe rápidamente para reducir el riesgo de pérdida financiera u otros daños. Póngase en contacto con INCIBE: Un servicio gratuito financiado por el gobierno que brinda apoyo a las víctimas de delitos de ciberseguridad. INCIBE puede ayudarlo a

diseñar un plan de respuesta para seguir los pasos apropiados a fin de reparar daños a su reputación, historial de crédito e identidad. Visite el sitio web de INCIBE en www.incibe.es o llame al 017.

Denuncie que ha sido víctima de un delito de identidad para poder restablecer sus credenciales ante el gobierno o instituciones financieras.

Si usted o alguien que conoce ha sido estafado y puede estar padeciendo estrés emocional o depresión, hable con su médico de cabecera, con un profesional de la salud local o con alguien en quien confíe. También puede considerar ponerse en contacto con servicios de asesoramiento psicológico o de apoyo.

Recuerde, usted es la victima, no el delincuente.