Lo que debe saber para detectar estafas de impostores

(BPT) - Aunque el fraude no es nada nuevo, las estafas actuales están en constante evolución. Los últimos avances tecnológicos, como la inteligencia artificial (IA), hacen que estos fraudes sean aún más difíciles de detectar. La Comisión Federal de Comercio (Federal Trade Commission, FTC) realiza un seguimiento del costo astronómico que supone el fraude para los consumidores, como los $15.900 millones en pérdidas declaradas solo en 2025. Aunque las estafas adoptan muchas formas, la mayoría tiene un rasgo en común: los impostores. Los estafadores se hacen pasar por una persona, una empresa o un organismo público que no son. Las estafas de impostores son el tipo de fraude más denunciado en el país.

Las estafas actuales pueden potenciarse fácilmente con la IA, usando herramientas como la IA generativa, la clonación de voz y la tecnología deepfake para crear contenido personalizado y muy convincente que puede incluso ayudar a los estafadores a entablar relación con las víctimas a lo largo del tiempo. Las identidades falsas generadas por IA se utilizan en muchos tipos de estafas, desde estafas sentimentales y de inversión hasta estafas en las que se hacen pasar por un nieto o una pareja sentimental.

Para ayudarlo a proteger el dinero que tanto le ha costado ganar, el Servicio de Inspección Postal de los Estados Unidos® ofrece consejos que le ayudarán a detectar y prevenir los tipos más comunes de fraude.

Inversiones en criptomonedas para "hacerse rico rápidamente"

A todo el mundo le gusta soñar con ganar dinero fácil. Por desgracia, a los estafadores también. Las estafas más habituales abarcan desde valores y materias primas hasta pozos de petróleo y monedas de oro. La estafa en auge hoy en día se basa en inversiones falsas en criptomonedas, en las que incluso los inversores más avispados pueden caer. Los estafadores que se dedican a las inversiones en criptomonedas pueden publicar sitios web de inversión que parecen auténticos, pero usted se dará cuenta de que no puede retirar el dinero que ha "invertido".

Si recibe una llamada telefónica o un correo electrónico en el que se utilizan tácticas de presión y se prometen grandes beneficios, es una señal de alarma. Es posible que alguien se ponga en contacto con usted diciendo que ha ganado mucho dinero y que quiere enseñarle cómo hacerlo. Pero las inversiones legítimas nunca garantizan resultados. Si suena demasiado bueno para ser verdad, es que lo es.

Protéjase: no tome decisiones precipitadas en materia de dinero, aunque el vendedor le diga que es una "oportunidad única en la vida" con una fecha límite. Investigue para comprobar por usted mismo las promesas de rentabilidad y nunca invierta basándose únicamente en lo que lea en una sola fuente de información. Compruebe la reputación de cualquier empresa en la oficina local de defensa del consumidor o en la Fiscalía General de su estado.

Estafas dirigidas a abuelos

Una de las estafas más preocupantes, potenciada por la IA, utiliza fotos falsas y la clonación de voz para hacerle creer que un familiar, como un nieto, se está poniendo en contacto con usted, y le pide con urgencia dinero para una fianza, gastos legales o facturas de hospital. Para que la historia resulte creíble, los estafadores agregan detalles sobre cómo o dónde se produjo esa "emergencia", o le dicen que un abogado, un médico o un agente de policía se "lo explicará todo" si los llama. En cuanto se envía el dinero, los estafadores se esfuman y el abuelo o la abuela pierde cientos o miles de dólares.

Protéjase: Piense antes de actuar. Estas llamadas o correos electrónicos pueden llegar a altas horas de la noche, cuando no se piensa con claridad. Es a propósito. Póngase en contacto con su familiar (o con sus padres) por el medio que suele utilizar para comunicarse con ellos y compruebe la historia. Las peticiones urgentes de dinero siempre son señales de alarma, al igual que las formas en que los estafadores quieren que se les envíe el dinero. Los métodos de pago preferidos por los estafadores son las transferencias bancarias o las tarjetas de prepago recargables, lo que hace imposible recuperar el dinero.

Estafas sentimentales

Las redes sociales y los sitios web de citas son plataformas perfectas para engañar a consumidores vulnerables y atraerlos hacia relaciones sentimentales. Cualquier persona que se encuentre socialmente aislada podría caer en una estafa romántica. Los estafadores fingen estar interesados en usted y, tras ganarse su confianza, pueden pedirle que les envíe dinero o que cobre un cheque o un giro postal. Los estafadores crean una sensación de urgencia alegando que tienen una emergencia médica. O bien, puede que le prometan venir a Estados Unidos para estar con usted, pero que necesitan un cheque o un giro postal para cubrir los gastos. Ninguna de estas historias es cierta.

Protéjase: en cualquier relación que surja a través de Internet, no revele sus datos personales. Busque en Internet el nombre de la persona y la ciudad en la que dice vivir. Actúe con cautela y preste atención a las incongruencias que puedan aparecer en el perfil y la información de la persona. Mantenga las conversaciones en la plataforma de la página web oficial de citas. Algunas señales de alerta son mostrar interés romántico por usted muy rápidamente, insistir en pasar a un correo electrónico privado y pedirle dinero para visitarle o para una emergencia.

Servicio técnico falso

Es posible que reciba una falsa advertencia sobre un problema en su computadora, como una ventana emergente o un correo electrónico que parezca proceder de una empresa conocida. El aviso le pedirá que llame a un número de teléfono para obtener ayuda o que haga clic en un vínculo. Otras estafas relacionadas con el soporte técnico pueden comenzar con una llamada o un mensaje de texto de un estafador que se hace pasar por un técnico informático. Es posible que le pidan acceso remoto a su computadora y finjan estar buscando virus. A continuación, dirán que han detectado un programa malicioso y se ofrecerán a eliminarlo a cambio de una cantidad de dinero.

Una señal de alarma importante es que le insistan en que pague con tarjetas de regalo, mediante transferencia bancaria, criptomonedas o con una aplicación de pago. Quieren que pague de alguna de estas formas porque es como usar dinero en efectivo: una vez que paga, es difícil recuperar su dinero.

Protéjase: si recibe una llamada de asistencia técnica que no haya solicitado, simplemente cuelgue. Si recibe un correo electrónico o un mensaje de texto, ignórelo y bórrelo. No facilite información de carácter personal (personally identifiable information, PII) a desconocidos, como su número de Seguridad Social, fecha de nacimiento, números de cuentas bancarias o dirección particular. No haga clic en los vínculos ni responda a este tipo de correos electrónicos. Bloquee los mensajes de spam y borre el correo electrónico o el mensaje de texto. Revise la factura de su teléfono móvil para detectar cargos sospechosos y mantenga actualizado el software de seguridad de todos sus dispositivos.

Para obtener más información sobre la prevención del fraude, visite uspis.gov/imposter-scams. Si cree que ha sido víctima de fraude o de cualquier delito relacionado con el Servicio Postal de los Estados Unidos, denúncielo en uspis.gov/report o llame al 877-876-2455.