Protegiendo Su Dinero

¿Puede reconocer una estafa con Inteligencia Artificial (IA)?

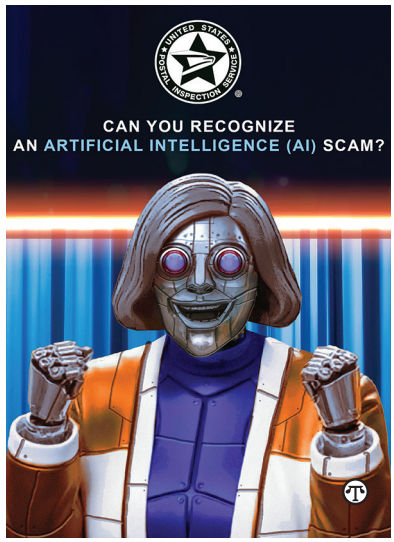
(NAPS)—Los inspectores postales desean ayudarle a usted y a todos los clientes del USPS a mantenerse seguros durante la Semana Nacional de Protección al Consumidor (NCPW), del 1 al 7 de marzo de 2026, y durante todo el año.

Los estafadores aprovechan cada oportunidad para engañarle y hacerle creer que sus mentiras son ofertas legítimas, premios e incluso solicitudes de emergencia de amigos y familiares. Ahora, con la proliferación de la inteligencia artificial (IA), los estafadores están utilizando este nuevo método para personalizar sus trucos y fraudes con el fin de que parezcan aún más reales, legítimos y creíbles—desde fotos generadas por IA y clonaciones de voz que imitan a una persona real, hasta mensajes cuidadosamente redactados que construyen una relación con la víctima durante semanas. Pero una falsificación sigue siendo una falsificación. Como en cualquier otra estafa, estas falsificaciones se crean para separarle de su dinero o bienes obtenidos con tanto esfuerzo.

Las falsificaciones creadas con IA se utilizan en muchos tipos de estafas prolongadas, desde estafas románticas hasta estafas de inversión, estafas con criptomonedas e incluso fraudes que afirman ser de soporte técnico. Sea cual sea la estafa, todas implican impostores que buscan a su próxima víctima, pero no tiene que ser usted.

Puede ser difícil reconocer las estafas que utilizan IA, pero aquí hay algunas características reveladoras:

- La "persona" que se comunica con usted tiene una presencia inconsistente o limitada en las redes sociales—pocos amigos, creación reciente de la cuenta, comentarios que no parecen naturales o que están demasiado bien redactados, o imágenes que no coinciden con los detalles del nombre o perfil.
- Pequeños errores ortográficos, sitios web no seguros que solicitan información de inicio de sesión, o una dirección de correo electrónico que no coincide con el dominio del sitio web que solicita información (ejemplo: john.doe@USPSUS.com, cuando USPS.com es el nombre de dominio real).
- "Pruebas" excesivamente elaboradas—PDF o capturas de pantalla que pueden fabricarse fácilmente.
- Solicitudes para trasladar la comunicación fuera de la plataforma—por ejemplo, insistir en comunicarse por WhatsApp, Telegram o una dirección de correo electrónico privada separada para que no se apliquen las protecciones de seguridad de la plataforma.
- Inconsistencias en audio o video—la sincronización de labios puede no coincidir, puede haber iluminación extraña o movimientos bruscos, o una voz que no coincide del todo con la persona que usted conoce.
- Rendimientos financieros demasiado buenos para ser verdad—rendimientos y ganancias altas garantizadas, presión para reclutar a otras personas, u oportunidades privadas "exclusivas".



La inteligencia artificial ayuda a los estafadores a despojar a las personas de dinero real—pero usted puede protegerse.

Para protegerse de los estafadores, siga estos consejos y compártalos con los clientes y su comunidad:

- Nunca envíe dinero a alguien que solo conoce en línea—especialmente a través de criptomonedas, transferencias bancarias, tarjetas de regalo o métodos de recarga prepagados.
- Considere las solicitudes financieras inusuales como señales de alerta. Peticiones como "préstame para comprar un boleto" o "invierte a través de esta billetera privada" son advertencias para DETENERSE y verificar.
- Active la autenticación multifactor (MFA) en sus cuentas de correo electrónico, redes sociales y cuentas financieras.
- Utilice métodos de pago con protección al comprador (tarjetas de crédito, servicios de depósito en garantía) cuando realice transacciones con personas desconocidas.
- Limite el intercambio de información de identificación personal. Proporcionar su fecha de nacimiento completa, número de Seguro Social, fotos de identificaciones o direcciones de domicilio puede facilitar el robo de identidad.
- Mantenga sus dispositivos y programas actualizados. Utilice software antivirus y un administrador de contraseñas para crear contraseñas fuertes y únicas.
- Tenga precaución con desconocidos "demasiado serviciales". Si alguien le ofrece abrir una cuenta de inversión o "ayudarle" a registrarse, desacelere y verifique.
- Informe a sus contactos. Advierta a amigos y familiares si ve un contacto sospechoso que finge ser usted.

Y si cree que ha sido víctima de una estafa, tome medidas inmediatas:

1. Detenga toda comunicación con el estafador y conserve todos los mensajes y registros de transacciones.

2. Comuníquese de inmediato con el banco o proveedor de pagos para intentar detener o rastrear las transferencias.

3. Denuncie ante las autoridades:

- Reporte al Servicio de Inspección Postal en www.uspis.gov/report; a la Comisión Federal de Comercio (FTC) en reportfraud.ftc.gov; y al Centro de Quejas de Delitos por Internet (IC3) del FBI en ic3.gov.
- Reporte el perfil y los mensajes en la plataforma donde ocurrió el contacto.

4. Cambie sus contraseñas y active la MFA si compartió información de inicio de sesión.

5. Coloque alertas de fraude y un congelamiento de crédito si compartió datos financieros sensibles.

6. Comuníquese con la policía local si perdió sumas significativas de dinero o fue amenazado.

7. Busque apoyo. Las estafas causan daño emocional, así que hable con amigos de confianza, familiares o un consejero.

8. Si utilizó criptomonedas, comuníquese con las autoridades de inmediato. El rastreo es difícil, pero si se reporta temprano, puede haber una posibilidad de recuperar sus fondos.

Si cree que ha sido víctima de cualquier estafa relacionada con el correo de los EE. UU., repórtelo a los inspectores postales al 877-876-2455 o en www.uspis.gov/report.

Para obtener más información sobre la prevención del fraude, visite www.uspis.gov.