Protecting Your Money

Can You Recognize An Artificial Intelligence (AI) Scam?

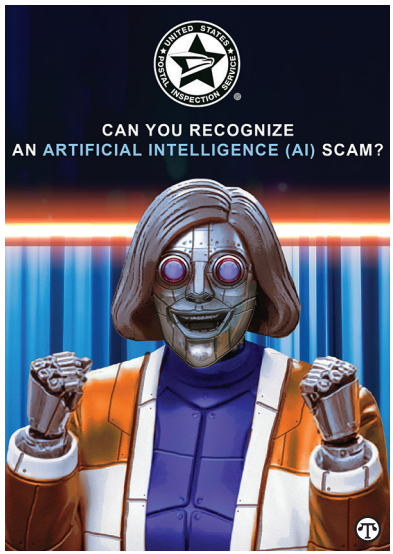
(NAPS)—Postal inspectors want to help you and all USPS customers stay safe during National Consumer Protection Week (NCPW), March 1-7, 2026, and throughout the year.

Scammers take every opportunity to trick you into believing their lies are legitimate offers, wins, and even emergency requests from friends and family. Now, with the prevalence of artificial intelligence (AI), scammers are using this new method to personalize their tricks and cons to make them appear even more real, legitimate, and believable—from AI-generated photos and voice clones that mimic a real person to wording that builds a relationship with a victim over weeks. But a fake is still a fake. As in any other scam, these fakes are created to separate you from your hard-earned money or property.

AI fakes are used in many types of long-running scams, from romance to investment scams, cryptocurrency scams, and even scams claiming to be tech support. Whatever the scam, they all involve impostors looking for their next victim, but it doesn't have to be you.

It can be difficult to recognize scams that use AI, but here are some tell-tale characteristics:

- The "person" contacting you has an inconsistent or thin social media footprint—few friends, recent account creation, comments that don't seem natural or are too well-written, or images that don't match name/profile details.
- Tiny misspellings, non-secure websites that ask for login info, or an email address that doesn't match the website domain asking for information (example: john.doe@USPSUS.com, when USPS.com is the actual domain name).
- Overly polished "evidence"—PDFs or screenshots that can be easily fabricated.
- Requests to move communication off-platform—e.g., insisting on speaking via WhatsApp, Telegram, or a separate private email address so platform security protections won't apply.



Artificial intelligence helps scammers cheat people out of real money—but you can protect yourself.

- Inconsistencies in audio/video—lip sync timing may be off, weird lighting/jerky motion, or a voice that doesn't quite match the person you know.
- Too-good-to-be-true financial returns—guaranteed high returns and rewards, pressure to recruit others, or "exclusive" private opportunities.

To protect yourself from scammers, follow these tips, and share them with customers and your community:

- Never send money to someone you know only online—especially through cryptocurrency, wire transfer, gift cards, or prepaid reload methods.
- Treat unusual financial asks as red flags. Requests to "loan me to buy a ticket" or "invest through this private wallet" are warnings to STOP and verify.
- Enable multi-factor authentication (MFA) on email, social, and financial accounts.
- Use payment methods with buyer protection (credit cards, escrow services) when transacting with unknown parties.
- Limit sharing of personally identifiable information. Providing your full date of birth, Social Security number, photos of IDs, or home addresses can enable identity theft.
- Keep devices and software updated. Use antivirus software and a password manager for strong, unique passwords.
- Be cautious with "too helpful" strangers. If someone offers to set up an investment account or "help" you sign up, slow down and verify.
- Inform your contacts. Warn friends and family if you see a suspicious contact pretending to be you.

And if you believe you have been a victim of a scam, take immediate action:

1. Stop communication with the scammer and preserve all messages and transaction records.

2. Contact the bank/payment provider immediately to attempt to stop or trace transfers.

3. Report to authorities:

- Report to the Postal Inspection Service at www.uspis.gov/report; Federal Trade Commission (FTC) at reportfraud.ftc.gov; and the FBI's Internet Crime Complaint Center (IC3) at ic3.gov.
- Report the profile and messages to the platform where the contact occurred.

4. Change passwords and enable MFA if you shared login info.

5. Place fraud alerts and a credit freeze if you shared sensitive financial data.

6. Contact local police if you lost significant sums of money or were threatened.

7. Seek support. Scams cause emotional harm, so talk to trusted friends, family, or a counselor.

8. If you used cryptocurrency, contact law enforcement immediately. Tracing is difficult, but reported early, there may be a chance of recovering your funds.

If you believe you have been a victim of any scam connected to the U.S. Mail, report it to postal inspectors at 877-876-2455, or at www.uspis.gov/report.

For more information on fraud prevention, visit www.uspis.gov.