



FEDERAL BUREAU OF INVESTIGATION

Public Service Announcement



Alert Number: I-072026-PSA | 20 July 2026 FBI Warns of Scammers Impersonating the IC3

This Public Service Announcement (PSA) is an update to Alert Number I-04182025-PSA titled, "[FBI Warns of Scammers Impersonating the IC3](#)." This PSA contains updated information about an ongoing fraud scheme where criminal scammers are impersonating FBI personnel facilitating Internet Crime Complaint Center (IC3) complaints to deceive and revictimize individuals.

This scheme combines several exploitation tactics to include the targeting of previous victims,¹ the use of artificial intelligence (AI)-generated videos to create fictitious or misleading promotional materials for their fraud schemes; and the creation of spoofed websites with the purpose of gathering personally identifiable information entered by a user into the site. Each of the tactics give victims a false sense of safety and security, while the actors impersonate or falsely affiliate themselves with government personnel or entities.

How the Scam Works

Complainants report scammers use a variety of methods to initiate contact with victims. Some individuals received an email or a phone call, while others were approached, or observed an advertisement via social media or forums. Almost all complainants indicated the scammers claimed to have recovered the victim's lost funds or offered to assist in recovering funds. However, the claim is a ruse to revictimize those who have already lost money to scams.

Scheme 1

A recent example of the impersonation scheme variant indicates scammers create fraudulent persona profiles and fake pages on social media networking sites, impersonating FBI personnel to lure victims into "re-targeting"² scams.

- After the victim of a scam begins to realize they are being defrauded, the victim informs the scammers they will report them to the FBI and file an IC3 report. The victim is later contacted by an individual impersonating an FBI agent on Facebook Messenger (FM). The impersonator communicates via Telegram and FM and sends a link to update the submitted IC3 report. The link may contain malicious code or may be used to collect more financial data to revictimize the person.

Scheme 2

Another recent example of the impersonation scheme involves scammers creating AI-generated videos (commonly referred to as "deepfakes"³) on social media

platforms, impersonating FBI personnel and promoting the FBI IC3 government website.

- A social media platform shared AI-generated videos depicting a senior FBI leader encouraging users to submit victim complaints on a spoofed IC3 website.
- The site features similar structure and content to the FBI IC3 government website. However, the spoofed website only allows users to interact with the complaint submission, and clicking on any further links returns the user to the home page.
- The complaint structure differs from the FBI IC3 intake in that it is a singular form step requiring only name, phone number, email address, scam type, and estimated financial loss.
- Upon submission the site gives a reference number and indicates that someone will be in touch with the submitter.

AI-Generated Videos

Scammers use AI-generated videos to create believable depictions of public figures to bolster their fraud schemes.

- Scammers rely on fear, urgency, and high-tech tricks like AI-generated video and caller ID spoofing to appear legitimate.
- Scammers generate videos for real time video chats with alleged company executives, law enforcement, or other authority figures.
- Scammers create videos for private communications to "prove" the online contact is with a "real person."

TIPS TO PROTECT YOURSELF

- IC3 does not maintain a social media presence and does not investigate crimes or recover funds through Facebook, Telegram, or similar platforms. Any social media profiles or pages claiming to represent IC3 or offering to recover lost money are fraudulent and are actively attempting to steal your personal or financial information.
- IC3 will never directly communicate with individuals via phone, email, social media, phone apps, online chat, or public forums. If further information is needed, individuals will be contacted by FBI employees from local field offices or other law enforcement officers.
- When navigating to IC3's official website, type www.ic3.gov directly into the address bar located at the top of your Internet browser, rather than using a search engine.
- If using a search engine, avoid any "sponsored" results as these are usually paid imitators looking to deter traffic from the legitimate IC3 website.
- Verify that the URL of the IC3 website ends in [.]gov and is correctly entered as www.ic3.gov.
- Avoid clicking on any link whose URL differs from the legitimate IC3 site to mitigate risk of fraud.

- Never click on links that may include suspicious artifacts or graphics, such as unprofessional or low-quality graphics used to imitate a legitimate website.
- Never share sensitive information if you are unsure of the website's legitimacy.
- Report any incidents to the legitimate FBI IC3 website only at www.ic3.gov
- IC3 will never ask for payment to recover lost funds, nor will IC3 refer someone to a company requesting payment for recovering funds.
- Do not send money, gift cards, cryptocurrency, or other assets to people you do not know or have met only online or over the phone.
- IC3 does not maintain any social media presence. Report any accounts impersonating IC3 to that social media's safety or support contacts.

Spotting a Fake Video or Message

- Carefully examine the email address, messaging contact information, including phone numbers, URLs, and spelling used in any correspondence or communications. Scammers often use slight differences to deceive you and gain your trust. For instance, actors can incorporate publicly available photographs in videos, use minor alterations in names and contact information, or use AI-generated voices to masquerade as a known contact.
- Look for subtle imperfections in images and videos, such as distorted hands or feet, unrealistic facial features, indistinct or irregular faces, unrealistic accessories such as glasses or jewelry, inaccurate shadows, watermarks, voice call lag time, voice matching, and unnatural movements.
- Listen closely to the tone and word choice to distinguish between a legitimate phone call or voice message from a known contact versus AI-generated voice cloning, as they can sound nearly identical.
- AI-generated content has advanced to the point that it is often difficult to identify. When in doubt about the authenticity of someone wishing to communicate with you, contact your relevant security officials or the FBI for help.
- Be wary of online content that elicits strong emotion - anger, fear, disbelief. Take a moment to verify that what you are seeing or hearing is true before responding. If you see a surprising video or image online, verify its authenticity through reputable news sources or known official channels.

REPORT IT

If you or someone you know has fallen victim to this scam, file a complaint with the IC3 at www.ic3.gov. Be sure to include as much information as possible:

- Identifying information about the person or company that contacted you.
- Methods of communication used, including websites, emails, the fake social media profile name, and telephone numbers.
- Financial transaction information, such as the date, type of payment, amount, account numbers involved, the name and address of the receiving financial institution, and receiving cryptocurrency addresses.

- Description of your interaction with the individual, including how contact was initiated, such as the type of communication, purpose of the request for money, how you were told or instructed to make payment, what information you provided to the scammer, and any other details pertinent to your complaint.
- Victims aged 60 or over who need assistance filing an IC3 complaint can contact the DOJ Elder Justice Hotline, 1-833-FRAUD-11 (or [833-372-8311](tel:833-372-8311)).

For additional information on similar scams, please see previous Public Service Announcements:

- IC3 | "[Threat Actors Spoofing the FBI IC3 Website for Possible Malicious Activity](#)"
- IC3 | "[FBI Warns of the Impersonation of Law Enforcement and Government Officials](#)"
- IC3 | "[Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud](#)"
- IC3 | "[ABA Foundation and FBI Release New Infographic to Help Americans Spot and Avoid Deepfake Scams](#)"

DISCLAIMER: The information in this document is being provided "as is" for informational purposes only. The FBI does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by FBI.

¹Unless otherwise stated, the use of the term "victim" in this product does not imply that the individual or entity meets the definition of "victim" in the Victims' Rights and Restitution Act (VRRRA), *34 U.S.C § 20141* or the Crime Victims' Rights Act (CVRA), *18 U.S.C § 3771*, or that the individual or entity has been identified as a victim in an FBI investigation.↩

²Re-targeting scams, often called "recovery" or "double-dip" scams, are manipulative schemes where scammers target individuals who have already been defrauded. Posing as law enforcement, banks, or cybersecurity firms, scammers promise to recover the victim's lost money or track down the original thieves, only to steal more funds.↩

³Deepfake refers to the broad range of generated or manipulated digital media (e.g., images, videos, audio, or text; collectively referred to as "synthetic content" or "synthetic media") created using artificial intelligence and machine learning processes. Deepfakes can depict the alteration or impersonation of a person's identity to make it appear as if they are doing or saying things they never did.↩