ARMY CRIMINAL INVESTIGATION DIVISION

7 March 2025

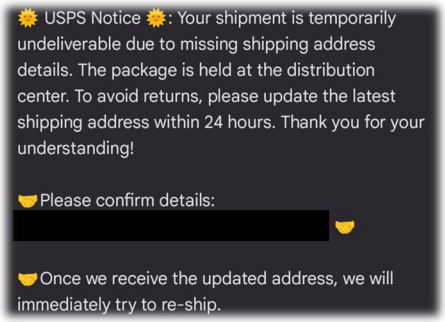
Cybercrime Prevention Flyer

Government Agency Text Scams

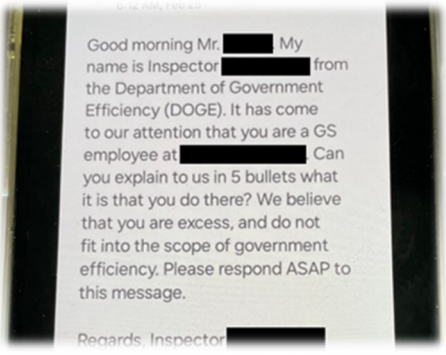
Due to convenience and immediacy in communication offered by text messaging, many people are more likely to readily check these messages and respond quickly as compared to email or answering a phone call. As cybercriminals and scammers are well acquainted with the most effective means to communicate with unsuspecting victims, and due to the proliferation of cell phones (approximately 310 million in the U.S. as of 2024), sending a convincing scam via text can be an effective method for criminal elements to engage unsuspecting individuals. A single reply by one victim can net a cybercriminal hundreds or even thousands of dollars; the potential amounts are even higher with multiple replies.

To add authenticity, scammers often draft a convincing text message purported to come from an official local, state, or federal agency. Some common scam themes include:

- **IRS Scam** – Often seen during tax season, IRS themed messages request personal information to process a refund or recalculate tax amounts. Payment might be requested to allow the recipient of the text to avoid prosecution or having their social security number canceled.
- **Social Security Scam** – Frequently targeting older adults, Social Security scams often revolve around overpayment, suspension of benefits, or requests for additional information necessary for a payment increase.
- **U.S. Postal Service** – Using notification of an incoming package, scammers request recipients to click on a provided link which then leads to a website requesting personal or financial information.



- **Speeding and Parking Ticket Scams** – This scam involves a text indicating recipient's vehicle was exceeding the speed limit or parked illegally, and a citation was issued; it then requests payment to avoid a court appearance.
- **Jury Duty Text Scam** – Seemingly sent from a court with a claim the recipient missed jury duty and is required to pay a fine or provide personal information to avoid jail time or fines.
- **Other Government Agency Scams** – Within a month of the establishment of the Department of Government Efficiency (DOGE), scammers began targeting government personnel with DOGE themed scams.



Text Scam Protection Tips

- Bear in mind that the IRS does not text taxpayers; the IRS contacts taxpayers through the U.S. Postal Service unless in special circumstances wherein taxpayers would be contacted by phone.
- Do not click on links received in text messages, or reply to text messages, if the sender is unknown or the message looks questionable.

- If a scam text is received, block the number and delete the message; most smartphones offer a way to block phone numbers.
- Contact the government agency identified in the text through the agency's official contact methods provided on the agency website; do not use the contact information provided in the text.
- Avoid responding to unrecognized phone numbers.
- Report the scam number to cell phone service providers.
- Do not provide personal or financial information via text.
- Report the scam to the Federal Trade Commission (FTC), Federal Communications Commission (FCC), and Internet Crime Complaint Center (IC3).

If you are a victim of an email scam and affiliated with the Army, notify the Department of the Army Criminal Investigation Division via the Submit a Tip – Report a Crime website.

To receive Cyber Field Office Cybercrime Prevention Flyers, send an email to: CYDIntel@army.mil

Cyber Field Office
Russell Knox Building
27130 Telegraph Road
Quantico, VA 22134

CPF 0020-2025-CID461