OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Washington, DC 20528 | www.oig.dhs.gov

FOR IMMEDIATE RELEASE
May 20, 2024

For Information Contact:
DHS-OIG.OfficePublicAffairs@oig.dhs.gov

FRAUD ALERT:
Department of Homeland Security Impersonation Schemes

This U.S. Department of Homeland Security (DHS) Office of Inspector General (OIG) Public Service Announcement highlights how scammers impersonate DHS personnel to defraud the public and how to avoid becoming a victim.

Background

Each year, DHS OIG receives hundreds of reports of scammers impersonating DHS employees to defraud the public. Impersonators spoof actual DHS phone numbers and create email addresses that resemble DHS emails to appear legitimate. Some even send pictures of real or doctored law enforcement credentials. Impersonators try to convince victims to provide personally identifying information, passwords, credit card or bank numbers, or make payments using money transfer services or unconventional methods.

Recent Trends

Scammers often target immigrants, elderly adults, and minority groups or persons with foreign ties. The most common ruses include claims of:

- Violations of immigration or customs laws.
- Offers to expedite immigration paperwork or resolve issues with immigration forms.
- Seized packages containing drugs or other illegal items.
- Identity theft requiring a new social security number.
- Active warrants for money laundering, terrorist financing, or other serious crimes.
- Threatening arrest, visa cancellation, or deportation.
- Warning against telling anyone about the call(s).

Ways to Protect Yourself

1. Be suspicious of calls or emails claiming to be from DHS. Scammers can fake caller ID information and email addresses. DHS will never use the main contact numbers listed on dhs.gov to make calls of this nature. If you receive calls from these numbers, do not provide any personal information.

2. Legitimate government email addresses end in *.gov*. In rare instances, impostors impersonate a *.gov* email. [1]

3. Imposters may send images or videos of a DHS or law enforcement uniform or wear a uniform on video calls. Many provide victims with fictitious case and/or badge numbers or images of badges. You should not believe a caller just because they appear in uniform or provide this information and may consider asking to meet at a police station.

4. Scammers often use incorrect language such as "DHS agent," "DHS private investigator" or "detective with DHS." They may misuse agency names such as "Department of Customs and Border Security," or "U.S. Immigration Agency." Be suspicious of any caller who does this.

5. Your call may be transferred to another scammer impersonating a more senior government official or allege multiple agencies are investigating you. This can include attorneys, local law enforcement, DHS, Internal Revenue Service (IRS), U.S. Marshals Service, Drug Enforcement Agency (DEA), and U.S. Department of the Treasury. This does not make the call authentic in any way.

6. Scammers often have personal information when they call. This may include residence(s) or family addresses, family member names, social security numbers, date of birth, etc. Scammers can obtain or purchase this information online (for example, following company data breaches). Knowing details about you does not make any call legitimate.

7. Some scammers claim you need a new social security number. The government rarely issues new social security numbers without your request.[2]

8. Do not send money to anyone claiming to be DHS. DHS employees will not ask you to pay a fine over the phone.

9. Scammers may ask for payment in unconventional forms, including gift cards, prepaid debit cards (Green Dot, Visa, Mastercard), Google/Apple pay, money transfer services (Zelle, Venmo, CashApp), cryptocurrency (Bitcoin), gold bars,[3] and cash. If you are ever asked to place money in a vehicle, contact local law enforcement immediately.

Reporting Fraud

Anyone who believes they may have been a victim of this scam is urged to call the DHS OIG Hotline (1-800-323-8603) or file a complaint online via the DHS OIG website at https://www.oig.dhs.gov/hotline. Internet crime victims can file a complaint with the FBI at www.ic3.gov and with the Federal Trade Commission.

---

[1] Microsoft has published helpful information about identifying email phishing scams here: https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

[2] See Social Security Administration notification, dated October 7, 2022: https://faq.ssa.gov/en-us/Topic/article/KA-02220

[3] See FBI IC3 Alert Number I-012924-PSA dated January 29, 2024: https://www.ic3.gov/Media/Y2024/PSA240129