UNITED STATES ARMY
CRIMINAL INVESTIGATION COMMAND

Media contact: 571-305-4041 FOR IMMEDIATE RELEASE

Government Imposter Scams on the Rise

QUANTICO, VA (Jan. 5, 2021) – The holiday season revealed an increase in government impersonator scams. Knowing the warning signs will help to reduce vulnerability, and prevent the consumer from being scammed.

The U.S. Army Criminal Investigation Command warns that government impersonator scams are on the rise and is asking the Army community and American public to help the Army maintain its readiness by reporting any and all scams or suspicious activity believed to be a possible scam.

Scammers count on everyday distractions, especially during the holiday season, to prey on unsuspecting people. This time of year scammers are getting creative and finding more opportunities for creating fake offers and phony fraud alerts by using the reputation of official government officials or agencies. The scammer impersonates a trusted source or vendor to send convincing and malicious emails to individuals in the hopes of gathering personal and financial information.

The scammers will make contact via phone or email and will claim to be affiliated with the government. Criminals are using alert type, pre-recorded messages about compromised social security numbers or how to claim unissued COVID-19 relief checks; tricking recipients into giving up protected information.

“No government agency will send you an unsolicited email or phone call asking for personal information,” said Edward LaBarge, director of CID’s Major Cybercrime Unit. “For the most part, if a government agency is looking to get ahold of you, they will send a letter via the U.S. Postal System on official letterhead.”

Fraudulent “collection agency” or police department calls are also being used by scammers to threaten jail time or legal action if payment or personal information is not provided immediately.

“For someone that lost their job as a result of the pandemic, keeping the lights on is a higher priority than cybersecurity and because of that vulnerability, one may be more apt to fall victim to an unemployment or other type of benefits scam,” said LaBarge.

According to CID officials, many individuals think they can easily detect a scam because they are a government employee, Soldier, contractor, or family member of one of the three. However, this is not always the case.

“No one is immune to becoming a victim of an online scam, it can happen to anyone,” said LaBarge. “When it comes to being a victim, it really comes down to psychology. Cybercriminals thrive during stressful world events such as the pandemic and play on people’s fears, stress, anxiety and vulnerabilities.”

Types of government impersonator scams.
Below are scams you may encounter. This list is not meant to be all-inclusive.

Debt Collector
Scammers claim to be affiliated with the government, such as law enforcement or a U.S. attorney. The scammer will say you owe a debt, and you must pay immediately otherwise you will face criminal charges and arrest. The scammer explains you can pay the debt by wiring or loading money to gift cards.

Internal Revenue Service (IRS)
A phony IRS representative contacts you and says you owe a tax debt. If you do not pay immediately, you will be arrested. The COVID-19 pandemic has provided scammers with another avenue to trick victims. Faux IRS representatives claim they can expedite economic impact payments, once you provide your personal information or pay a fee.

Social Security
The scammer claims to be a government representative from the Social Security Administration and your Social Security number (SSN) has been compromised. The scammer might tell you that your SSN has been associated with a crime or someone has used your SSN to apply for credit cards. The scammer will want to “verify” your SSN and will need money to reactivate or reissue your SSN.

Service Member
A scammer poses as a military service member of any rank or branch. They may even pose as you, targeting your friends and family. Scammers will communicate by social media or messaging applications; for example, the scammer says they are deployed to a combat zone or in a remote area of the world on a dangerous “secret” mission. The scammer pleads for financial help, claiming they need the money to come home, pay for food, or necessary medical care. The scammer tells their victims they can send much needed help via gift cards, wire transfers, or cryptocurrency.

Government Impersonator Scam Warning Signs

- You receive an unsolicited call, email, or text saying you owe a debt, overpaid a bill, or your personal information has been compromised.
- Scammers demand immediate payment via gift cards, wire transfers, or cryptocurrency.
- Scammers threaten action by law enforcement if you do not pay immediately.
- Scammers threaten to revoke benefits, block your SSN, or confiscate official documents such as your driver's license or passport.

To reduce your vulnerability, keep the following in mind:

- If a government agency needs to contact you, you will receive official correspondence in the U.S. mail.
- Do not trust caller ID – phone numbers can be spoofed just as simply as email addresses.
- A government agency will never demand the payment of a debt via gift cards, wire transfers, or cryptocurrency.
- Do not give or confirm your Personally Identifiable Information, banking, or credit card information to anyone who contacts you.
- Make sure your family and friends know that the U.S. military does not charge its service members to come home, eat, or receive medical care.

Government Impersonator Scam Victim Reporting

- If you provided personal or bank information, contact your bank and any relevant financial institutions as soon as possible.
- Notify local law enforcement.
- Report it to commercial, state, and federal agencies.
- The Better Business Bureau
- The Federal Trade Commission
- Internet Crime Complaint Center
- State Consumer Protection Offices
- U.S. Postal Inspection Service

Army personnel or their families who are victims of an Internet-based crime should report the crime to their local CID office. Individuals can also report crime tips to CID anonymously via a specialized application at https://www.cid.army.mil/report-a-crime.html.

-30-

For more information about computer security, other computer-related scams, and to review previous cybercrime alert notices and cyber-crime prevention flyers visit the Army CID MCU website at https://www.cid.army.mil/mcu-advisories.html. To report a crime to Army CID, visit www.cid.army.mil.