Cybercrime Prevention Flyer

CPF 00018-2020-CID361-9H **3 December 2020**

Government Impersonator Scams

Have you received a phone call, email, or text message from someone claiming to be a “representative” from a government agency who says you owe a debt, overpaid a bill, or your personal information has been compromised? Does the government representative say that in order to fix the problem you will need to send money immediately? Do they say that if you do not send money immediately something bad will happen to you? No matter the ruse they use to get money out of you, scammers depend on your trust and fear, and this is especially evident when dealing with government impersonator scams. As a service member, dependent, veteran, federal employee, or contractor, you might engage with government agencies on a regular basis; so when someone claiming to be from a government agency contacts you, your initial reaction may be to cooperate without asking questions. However, if armed with information, the risk of you becoming the victim of a government impersonator scam can be reduced.

What is a government impersonator scam?

Government impersonator scams are attempts to convince you to send money or share your personal information with someone pretending to be a government official.

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.

Report a crime to U.S. Army Criminal Investigation Command

Major Cybercrime Unit

27130 Telegraph Road
Quantico, Virginia 22134

Email

MCU Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

Cybercrime Prevention Flyer

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 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.

Cybercrime Prevention Flyer

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

Resources

Internal Revenue Service

Social Security Administration

National Do Not Call Registry

IRS Phone Scam Cybercrime Prevention Flyer

Social Media Scamming Cybercrime Prevention Flyer

Telephone Frauds and Scams Cybercrime Prevention Flyer

To receive future MCU Cybercrime Prevention Flyers, send an email to: Subscribe CPF