BusinesSafe is designed to aid businesses in protecting the safety and well-being of Florida's residents and visitors from threats. BusinesSafe provides private sector partners with open source information, analysis and resources to help protect their businesses and communities.

Florida Fusion Center 22-051 **May 2022, Issue #76**

BusinesSafe Threat Topic: Government Impersonation Scams

Government impersonation scams occur when criminal actors contact individuals or businesses claiming to be from a local, state, or federal agency. The government impersonators may try to get individuals or businesses to give them personal identifiable information or money using multiple tactics such as threats of fines or arrest. This article includes an overview of common methods and indicators of attacks used by government impersonators to obtain money or personal information for fraudulent means. While these lists are not all encompassing, they offer individuals and businesses information to better recognize and protect from government impersonation scams.

Common methods of attack

- Government impersonators may use tactics such as phone calls, texts, emails, or in some cases, physically show up to a residence or business, and threaten arrest or request personal information such as a social security number.
- Government impersonators may tell individuals or businesses that they need information to verify their account or to fix a fraudulent discrepancy.
- Government impersonators may impersonate federal or law enforcement agents and threaten businesses or individuals with fees or jail time by claiming a failure to make a past due payment or file a report. Criminal actors may also claim there is a warrant out for the individual or business owner's arrest unless they pay a fee.
- Government impersonators that appear in person may have official looking clothing, badges or other identification that may appear authentic to make the scam more believable.
- Some emails or texts from government impersonators may have links that contain malware or lead to spoofing websites that look like legitimate government websites but are set up to collect personal identifiable information for future fraudulent use.

Potential signs and indicators

- The person claiming to be with the government is aggressive and threatening or hangs up when you request further information.
- The requested method of payment is wire transfer, cash, gift cards, or crypto currency.
- The email or text message you receive contains a suspicious looking link or grammatical errors.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8600, HSEC:1 FSIN:1.3.1, 3.1, 3.1.5 FFC: 4.1, 4.3, 4.4

- You receive a message from someone claiming to be from a government agency through social media or your businesses website.

Mitigation strategies

- If it seems suspicious, it probably is. Cease all contact with the individual until you can verify their legitimacy.
- Always ask for identification verification. Some government impersonators may also give you a fraudulent employee ID number to try to trick you into thinking they are legitimate.
- If you are unsure of the authenticity of a government official, contact the agency the person claims to be with from the agency's phone number from their public website. Do not rely on the information given to you by the suspected government impersonator.
- Do not wire money, send gift cards, pay with crypto currency or send cash. Legitimate government agencies will never demand payments made using gift cards, crypto currency or wire transfer methods.
- Never give out any financial or personal information to anyone claiming to be with the government without first verifying the person you are dealing with works for that agency.
- Government impersonators may be able to spoof caller ID to make it appear the phone call is coming from a legitimate government agency. Do not trust caller ID and verify the phone number prior to providing sensitive information.

Ways victims can report

- Report government imposters to your local law enforcement agency.
- File a complaint about online impersonations with the Federal Bureau of Investigation (FBI) on their website.
- Report government impersonator fraud to the Federal Trade Commission (FTC).
- In Florida, file a complaint on the Florida Office of the Attorney General website.
- ***"If You See Something, Say Something®"*** *– Report suspicious activity to your local law enforcement agency, on the FDLE website using Florida's See Something, Say Something Tool Kit, via the Florida See Say app, or by calling 855-FLA-Safe. In an emergency, call 911.*

Resources

- If you feel you may have unknowingly given your personal information to a government impersonator, go to IdentityTheft.gov for steps you can take to protect your identity.
- The FTC offers information and resources on how to avoid government impersonator scams.
- The FBI's public service announcement provides additional resources and information to help individuals and businesses identify government impersonations.
- The Florida Division of Consumer Services provides information on multiple frauds and scams to help individuals and businesses recognize and avoid different scam types and tactics
- The Florida Office of the Attorney General offers additional resources to help identify and mitigate against imposter scams or additional scams.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8600, HSEC:1 FSIN:1.3.1, 3.1, 3.1.5 FFC: 4.1, 4.3, 4.4