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 20-240 **December 2020, Issue #40**

BusinesSafe Threat Topic: Government Impersonation Scams

Government impersonation scams involve scammers posing as government officials to steal money or gain access to sensitive information. According to the Federal Trade Commission (FTC), nearly 1.3 million government impersonation scams have been reported nationwide since 2014 with a total loss of more than $450 million. Some of the top scams involve individuals claiming to be from the Social Security Administration (SSA), Internal Revenue Service (IRS), Health and Human Services/Medicare agencies, and law enforcement agencies. Scammers' tactics continue to evolve, and targeted scams may increase after natural disasters, economic downturns, and health crises. For a general overview of variations of the government impersonation scam, visit the FTC website.

Scammers may use robocalls and spoofing when impersonating government agencies. Spoofing is when a caller falsifies the information sent to your caller ID display to disguise their identity. Scammers may also create a sense of urgency or fear by saying money is owed and must be received immediately to avoid penalties or loss of benefits.

- In October 2020, the Federal Bureau of Investigation (FBI) saw an increase in fraudulent callers spoofing their Midland, Texas, office and trying to obtain financial and personal information.
  FBI Warns Scammers Spoofing Midland FBI Office Phone Number in Government Impersonation Fraud
- In July 2020, six individuals from Kansas, Tennessee, Florida, Louisiana, and Texas were arrested and charged with money laundering. One of their scams involved telling victims they owed back taxes and threatened legal action if they did not pay.
  Six Charged in Transnational Money Laundering Operation Involving Elder Fraud

Scammers may also use other tactics such as going go door-to-door or online scams. Scammers will disguise themselves as government representatives and may send emails or social media messages promising money in exchange for personal information. This is known as phishing. Scammers may also use false credentials or badges to gain victims' trust when going door-to-door.

- In September 2020, a Maryland man pled guilty to impersonating a Secret Service Agent and committing bank and credit card fraud using the victims' identities.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8791, Approval: FL8600, HSEC-1, FSIN-1, FSIN-3

Baltimore County Man Pleads Guilty To Federal Charges Related To Impersonation Of Officer To Commit Credit Card Fraud, Aggravated Identity Theft

- In June 2020, a COVID-19 scam targeting senior citizens was identified. Scammers used a fake website claiming affiliation with the U.S. Department of Treasury. They also hacked Facebook accounts and sent messages requesting payment for non-existent grant money. Attorney General Moody Takes Action to Stop COVID-19 Grant Scam Targeting Seniors
- In October 2018, the Florida Lottery warned citizens about an email scam saying they may have won $1 million, which was an attempt to obtain personal and financial information. Florida lotto officials warn of Mega Millions scam

Ways to Protect Yourself from Government Impersonation Scams

1. **Do not wire money, pay by gift card, or give any personal financial information.** Scammers often request payment immediately via wire, prepaid card, or by providing your personal bank account information. Government agencies do not require individuals to pay fines or fees with prepaid debit or gift cards.
2. **Do not pay to collect prizes.** Legitimate lotteries and sweepstakes will not make you pay to obtain a prize you have won. For more information on avoiding lottery and sweepstakes scams, visit the Florida Attorney General's website.
3. **Learn more about spoofing, phishing, and staying safe online or on a mobile device.** Visit the Secure Florida website.
4. **If you are concerned or think you owe money to a government agency, contact them directly.** Independently obtain the agency's official contact information and confirm that you are speaking with a legitimate representative.
5. **Keep yourself updated on current scams.** Learn more about some common government impersonation scams and how to protect yourself using the links below.
    - SSA: Fraud Prevention and Reporting
    - HHS: COVID-19 fraud is rapidly evolving
    - IRS: Tax Scams/Consumer Alerts
6. **If you believe you are a victim, file a complaint.** Reporting the incident allows agencies to alert the public about new scams, increase awareness, and protect others from becoming a victim.
    - Report fraud, scams, and bad business practices to the FTC online or by phone at 1-877-FTC-HELP. They can help you understand the next steps that may be taken after filing the complaint.
    - Report online scams to the Internet Crime Complaint Center.
    - Report government impersonation scams to the Florida Office of the Attorney General at MyFloridaLegal.com or by phone at 1-866-9NO-SCAM.

To sign up to receive BusinesSafe directly to your email, visit our website.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8791, Approval: FL8600, HSEC-1, FSIN-1, FSIN-3