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 22-058 **June 2022, Issue #78**

BusinesSafe: Scams Targeting Seniors

In 2021, the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) reported that citizens over the age of 60 reported a combined loss of $1.7 billion in scams across the United States. Due to its high senior population, Florida had the second highest number of these reports. This article includes an overview of common methods and scenarios used by fraudsters, ways to report and how to protect your assets from future scams.

Common Methods of Attack:

- **Tech Support Scams** – This scam includes unsolicited offers of tech support received by phone call, email, or through a website. The scammer claims to be with a tech support company posing as an employee from a major computer or other technology-based companies (e.g., Microsoft), offering to fix a fraudulent issue with one of your devices.
- **Confidence and Romance Scams** - Scammers using these schemes try to make a victim believe they are someone else or pretend to develop a new friendship or romantic interest. They use this supposed relationship to convince the victim to send them money under the guise of legal trouble, car trouble, an investment opportunity that seems too good to be true, or for a ticket to travel to see the victim. Sometimes they will even allege that a family member (like a grandchild) is in trouble and needs immediate funds.
- **Charity Scams** – Fraudulent charities or false relief fundraisers rely on the goodwill of their victims. Scammers seek to capitalize on recent tragedies, trends, disasters, or even advertise a fraudulent charity named to imitate a legitimate one. Some indicators of a charity being fraudulent include donations requested or required to be made in cash, by gift card, or by wiring money.
- **Health Insurance and COVID-19 Scams** – Scammers may pose as a Medicare representative to get victims to share their personal information. They may also provide fake services in pop-up mobile clinics or other locations, and then bill Medicare while pocketing the money. Some scammers also used COVID-19 as a new opportunity to target older Americans' concerns about their health and medical providers.

Potential Signs You Could be a Victim of a Scam:

- A pop-up window appears on your computer screen with an urgent message instructing you to call a phone number for assistance. This pop-up might look like an error message from your operating system or antivirus software, and even potentially include the logos from the trusted source and a fraudulent source.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8600, HSEC:1 FSIN: 1.13, 3.1.5, 3.1.7, 3.12 FFC: 4.1, 4.3, 4.6

- You are in contact with a charity that only accepts or heavily promotes payments made by cash, gift-cards, wiring money, or other ways where you can't stop the payment process and get your money back once you suspect fraud.
- You are unexpectedly contacted by a person claiming to be a Medicare representative who asks for personal information, or you receive a call that offers to send you COVID-19 testing kits, vaccines, prescriptions, and other supplies in exchange for payment.

Tips to Protect Yourself:

- If it sounds too good to be true, it probably is.
- Install trusted antivirus software to protect you and your computer from attacks and ensure all software is up to date and patched.
- Be wary of any links or information in a pop-up message or emails. Never call the phone number provided and if the criminal actor calls you, hang up or do not answer.
- If you receive urgent requests for financial assistance from friends, family or romantic interests, talk to someone you trust before making any decisions. They may be able to help confirm if the person actually needs assistance or identify a potential scam.
- Prevent future calls from potential scammers by having your phone block calls from unknown numbers.
- Check your bank and credit card statements regularly for any unauthorized or suspicious spending.
- Do not feel pressured by charities to give money immediately. Properly vet a charity or fundraiser by using the Florida Department of Agriculture and Consumer Services' Check-a-Charity tool to verify if the supposed charity is registered in Florida.
- Do not give out your Medicare number, Social Security number, or personal identifiable information to unsolicited callers.

Ways Victims Can Report:

- For victims of online scams, you can contact the Florida Attorney General's Office of Citizen Services either by calling the Attorney General's Fraud Hotline at 1-866-966-7226 or by filing out an online complaint form at My Florida Legal.
- The Federal Trade Commission (FTC) gives citizens the resources and ability to report various scams ranging from Health, Phone, Internet, or TV Service, or Impersonator Scams.
- Report elder fraud to the FBI's IC3 website.
  Report a consumer complaint through the Florida Department of Agriculture and Consumer Services (FDACS) online Consumer Complaint Form or by calling 1-800-HELP-FLA (435-7352) or 1-800-FL-AYUDA (352-9832) en Español.

Resources:

- The IC3 serves as the FBI's central repository for the collection of Internet crime complaints and publishes annual reports on various topics including an Elder Fraud Report from 2021 (PDF) which provides more information and resources.
- The Florida Department of Agriculture and Consumer Services provides information and resources on various scams and includes specific information on scams targeting Florida's elder population.
- The Office of the Florida Attorney General offers advice and resources on identifying and fighting against senior fraud on their website.
- The Florida Department of Law Enforcement provides information and reporting resources on multiple elder fraud scams on their Secure Florida website.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8600, HSEC:1 FSIN: 1.13, 3.1.5, 3.1.7, 3.12 FFC: 4.1, 4.3, 4.6