TALLAHASSEE SENIOR SERVICES

CORONAVIRUS (COVID-19) Scams to Avoid

COVID-19 Scams

Unfortunately, the COVID-19 pandemic, like other crises, is the perfect opportunity for scammers to take advantage of vulnerable individuals. Many of us are doing things in a different way, using more technology, and the uncertainty involved in navigating these new experiences can make us more susceptible to fraud. The delivery of stimulus checks, for example, has provided new opportunities for scammers. The Federal Trade Commission has warned people not to respond to any texts or emails from individuals claiming to have information about checks from the government. The federal government will not contact you asking for your social security number or banking details in order for you to receive a stimulus check. Information on reporting fraud involving payment of federal taxes can be found here.

Another prominent text message scam involves contact tracing. Contact tracing is the process by which a state's health department works with an infected individual to notify anyone who may have been exposed to this person while contagious. Individuals who came in contact with the infected person receive a text message from the health department informing them they will receive a call with further information. Scammers will send a fake text warning of potential exposure to infection, but then also ask for personal information, like a social security number. Actual contact tracers will not ask for any personal information.

In addition to email and text fraud, COVID-19 scams also come in the form of fake websites and phone scams, designed to obtain an individual's personal information and access to accounts. Fake charitable organizations purporting to collect donations to assist those suffering during this crisis also exist. When making donations, research the organization and do not donate in cash, with a gift card, or by wiring money.

For more information on COVID-19 scams review the Federal Trade Commission's Coronavirus Advice for Consumers.

For a list of the most prevalent coronavirus scams check out the Better Business Bureau's list of the Top Six Coronavirus Scams Reported.

Fake Websites

Fraudulent websites can be designed to look like legitimate government websites providing information about COVID-19, or stores purporting to sell hand sanitizer, masks and other essential supplies. These sites are often laced with malicious ads seeking personal information, or simply collect credit card information upon checkout, in the case of fraudulent sites for purchasing supplies.

- While a fake website can be made to look quite convincing, the URL will give it away. Check your address bar, fraudulent website will often use domains ending in 'com.co,' '.ma,' or '.co.' Legitimate domains typically end in '.com' or '.org.'
- Installing an ad blocker can help prevent your browser from loading fraudulent ads designed to obtain personal information.
- Ignore online offers for vaccinations, no proven treatment to prevent COVID-19 is currently available.

Further information on fraudulent websites and other scams is available here.

OVER

Email and Text Messages

Fraudulent emails and texts typically contain links to fake websites or malicious software. Many email and text message scams are designed to appear legitimate by impersonating government agencies. The Federal Communications Commission (FCC) is aware of a scam purportedly offering $30,000 in COVID-19 relief. There is no such relief program, and the text is likely a phishing attempt. Phishing involves a scammer attempting to trick you into revealing sensitive account information, usernames and passwords, or the use of imbedded links that will download malware to your device.

- Check the phone number that a text is coming from, scam texts often come from numbers with more than ten digits.
- Check email addresses to ensure they are legitimate, often fraudulent email addresses will be off by a character or two.
- Review hyperlinks before clicking on them; hover your curser over the link and check the URL, if it looks suspicious in any way (including the domain endings listed above) mark as spam and delete.

For more information on COVID-19 text message scams check out the Federal Trade Commission's COVID-19 Contact Tracing Text Message Scams.

Phone Scams

Phone scams typically involve a caller spoofing phone numbers to trick you into thinking the call is coming from a legitimate number. As with the phishing scams mentioned above, the goal of the scammer it to retrieve sensitive account information and gain access to your finances. The World Health Organization (WHO) has urged caution regarding any phone calls claiming to be from the WHO seeking account information or money. Additionally, there are reports of phone scams targeting individuals with preexisting conditions, offering COVID-19 testing kits, diagnostic equipment and even fake cures, and asking for payment over the phone.

- Do not respond to calls from unknown numbers, and remove any businesses from you address book. If a fraudster spoofed the number of you bank or credit card company, the institutions name would display on your phone giving you false confidence that the call is legitimate.
- Hang up and call the customer service number to ensure you are speaking with someone legitimate.

Additional information from the Federal Communications Commission is available here.

Resources

Tallahassee Police Department *TeleServe*		**850-891-4660**
• Report scams and fraud locally.		
National Center for Disaster Fraud Hotline		**866-720-5721**
• Report COVID-19 fraud to the hotline or by visiting: Justice.gov/DisasterComplaintForm.		
Office of the Attorney General	Myfloridalegal.com	**850-245-0150**
• The Attorney General is warning Floridians to only use secure sites when looking for COVID-19 information. Refer to this resource or the Federal Trade Commission to avoid scammers.		

Federal Trade Commission Consumer Information www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing

- Tips on scams, how to avoid scams, and what the Federal Trade Commission is doing to address scams.