

SCAMS AND FRAUD

There are many types of scams and fraud. Some examples of what to look out for include the following:

Fraudulent websites can be designed to look like legitimate government websites, or retail spaces. 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 items.

- While a fake website can be made to look quite convincing, the URL will usually give it away. Check your address bar, fraudulent websites 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.

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 is to retrieve sensitive account information and gain access to your finances.

- Do not respond to calls from unknown numbers and remove any businesses from your address book. If a fraudster spoofed the number of your bank or credit card company, the institution's 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.

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. 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, scam texts often come from numbers with more than ten digits.
- Check the email addresses, fraudulent email addresses will often be off by a character or two.
- Review hyperlinks before clicking on them; hover your cursor 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.

To report fraud or financial exploitation start by contacting your local law enforcement. Also, review the reporting information included below for specific types of fraud.

Scams and Fraud Resources	
The National Council on Aging (NCOA) Provides a list of the top ten financial scams targeting seniors.	ncoa.org/article/top-10-financial-scams-targeting-seniors
United States Department of Justice For a list of specific fraud types and where to report them.	justice.gov/criminal-fraud/report-fraud
Secure Florida An initiative of the Florida Department of Law Enforcement, Secure Florida provides education, training and resources.	secureflorida.org/SF/Home.aspx

AARP Fraud Watch Network aarp.org/money/scams-fraud/?intcmp=AE-SCM-FRD-CTA	877-908-3360
AARP's Fraud Watch Network can help you spot and avoid scams. Sign up for free "watchdog alerts," review a scam-tracking map, or call the fraud helpline above.	
Consumer Financial Protection Bureau consumerfinance.gov/consumer-tools/educator-tools/resources-for-older-adults/protecting-against-fraud/	855-411-2372
Provides a variety of information designed to help protect older adults from fraud and financial exploitation.	
Federal Bureau of Investigation fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud	
For a list of common elder fraud schemes visit the website above.	
usa.gov/stop-scams-frauds	844-872-4681
For a list of common scams and frauds, tips for online safety and reporting information.	
Seniors vs. Crime seniorsvscrime.com	800-203-3099
This program uses retired citizens not only to educate Floridians on consumer fraud but also to help in some consumer investigations. In addition, the volunteers regularly conduct seminars on how seniors can protect themselves from becoming crime victims.	
Federal Trade Commission Consumer Information consumer.ftc.gov/features/scam-alerts	
Tips on scams, how to avoid them, and what the Federal Trade Commission is doing to address scams.	
Military and Veterans Assistance Program (MVAP) myfloridalegal.com/MVAP	866-966-7226
The MVAP was created to help educate military members and veterans on the types of scams that target their communities, what they can do to protect themselves, and how they can help protect others by reporting scams and deceptive business practices.	
Office of the Attorney General Myfloridalegal.com	850-245-0150
The Office of the Attorney General provides information and training concerning how to avoid scams and fraud, as well as online complaint forms.	
Reporting Scams and Fraud	
Tallahassee Police Department talgov.com/publicsafety/tpd-onlinecrimereporting.aspx	850-891-4660
Report scams and fraud locally.	
Florida Department of Economic Opportunity mobile.connect.myflorida.com/prweb/PRAuth/app/DEOReemp_g1eNZfpW-iXvYsT47L1K1toiqe6SG1Pt*/!STANDARD	833-352-7759
If you are the victim of unemployment fraud, report it by visiting the website or calling the number above.	
Federal Trade Commission reportfraud.ftc.gov/#/	877-FTC-HELP 877-ID-THEFT
Protect your community by reporting fraud, scams, and bad business practices.	
Internal Revenue Service (IRS) irs.gov/pub/irs-pdf/f14039.pdf	
Please visit the link above and follow the instructions for submitting an affidavit to the Internal Revenue Service to report tax fraud.	
National Center for Disaster Fraud Hotline Justice.gov/DisasterComplaintForm	866-720-5721
Report COVID-19 fraud to the hotline or by visiting the website above.	