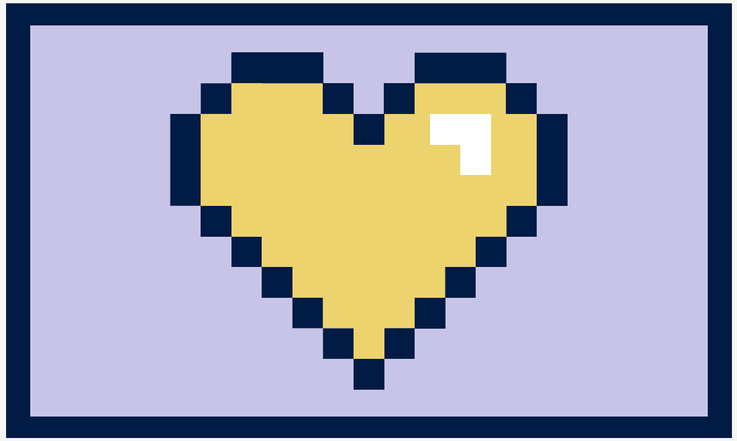
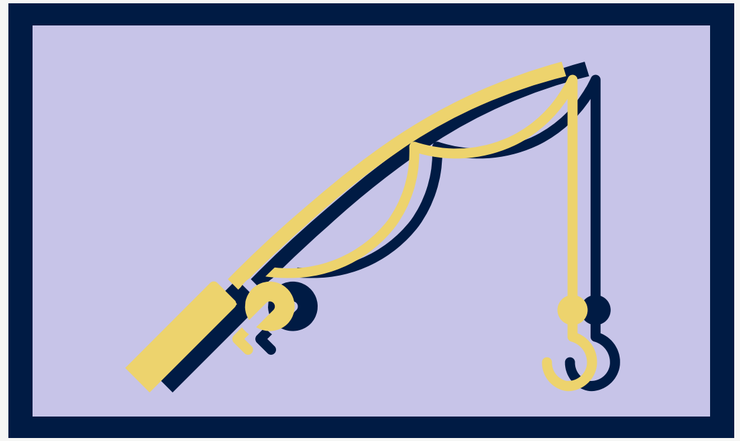
CYBERCRIME & Seniors

THREAT OVERVIEW



TOP SENIOR SCAMS

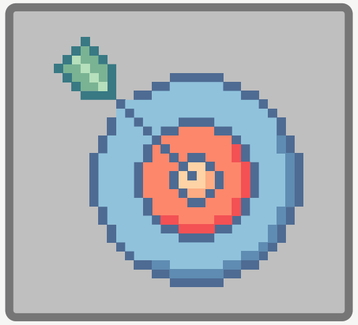


RESOURCES

Guide

An Overview Of The Threat Against Seniors

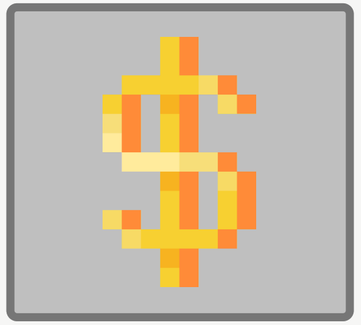
HOW OFTEN ARE SENIORS TARGETED?



Reports show that more than **3.5 million seniors** are victims of fraud or financial exploitation each year.

Most of these instances occur online, with tech-related schemes being one of the most common.

HOW MUCH DO SENIORS LOSE TO SCAMS?



The IC3 Elder Fraud Report shows seniors lost more than **$3.1 billion** in 2022.

This is a **84% increase** in reported losses from 2021.

The average amount of money lost per person is **$35,000**.

Cybercrime & Seniors

File Edit View Help

An Overview Of The Threat Against Seniors

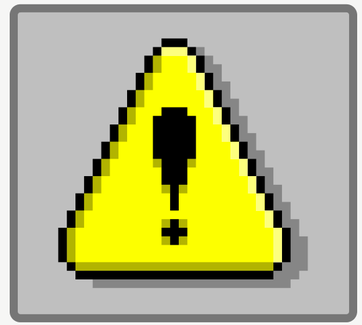
WHY ARE SENIORS TARGETS OF SCAMS?

Scammers time schemes around monthly social security or pension checks, and also scan obituaries, striking after a spouse's death.

Fear of losing financial independence may cause a senior to not report a scam.

Physical and mental impairments can lead to easier targeting.

WHERE DO SENIOR SCAMS HAPPEN?



- Dating Apps
- Emails
- Investment Apps
- Online Advertisements
- E-Commerce Websites
- Phishing Messages
- Robocalls
- Social Media

Top Senior Scams

PHISHING MESSAGES

GOVERNMENT IMPERSONATION

Scammers pose as representatives from a government agency to trick a victim into taking urgent action and providing personal information or to send money. For more information and examples, click here.

SWEEPSTAKES & LOTTERY

Fraudulent messages claiming a user won a lottery or sweepstakes can lead to a victim paying countless fees and providing information to 'claim' winnings. For more information and examples, click here.

TECH SUPPORT

Fake firewall notices will pop up on a computer, showing a helpline. Calling the number will lead to a fake tech support scammer who may try to steal money. For more information and examples, click here.

PRESSURE TO SCREENSHARE

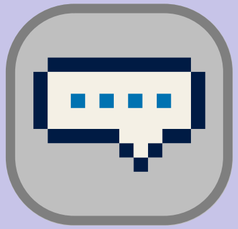
Associated with a large assortment of scams, all screensharing schemes reach a point where a fraudster tricks citizens into allowing the scammer to have full remote access of the victim's computer.

THE BEST WAY TO AVOID PHISHING MESSAGES IS BY DELETING THE SUSPICIOUS MESSAGE AND BLOCKING THE SENDER

Top Senior Scams

SOCIAL MEDIA

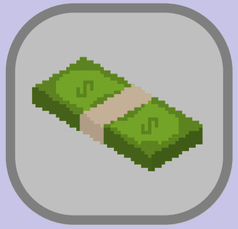
FAKE POSTS



Through fake or hacked accounts, scammers create fake posts on social media. Often reshared by people with good intentions, these posts can contain malware or encourage donations to fake sources.

Avoid these scams by researching information on a more reliable news source. Ignore and report anything that seems suspicious.

INVESTMENT SCHEMES



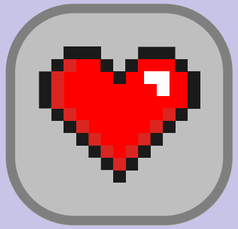
Scammers can pose as finance moguls on social media, offering helpful classes or investment advice to unwary consumers. All with the goal of stealing their personal information and money.

Avoid these scams by blocking the suspicious users who reach out through direct messages and never give information to an unknown person.

Top Senior Scams

SOCIAL MEDIA

ROMANCE SCAMS



A scammer uses fake accounts on dating apps, pretending to be a potential lover, to lure in targets to send money. In 2021, consumers lost more than $1 billion nationwide to romance scams.

Avoid these scams by meeting with the potential love interest in person, in a safe, well-populated environment. Be extremely cautious of anyone who refuses to meet in person.

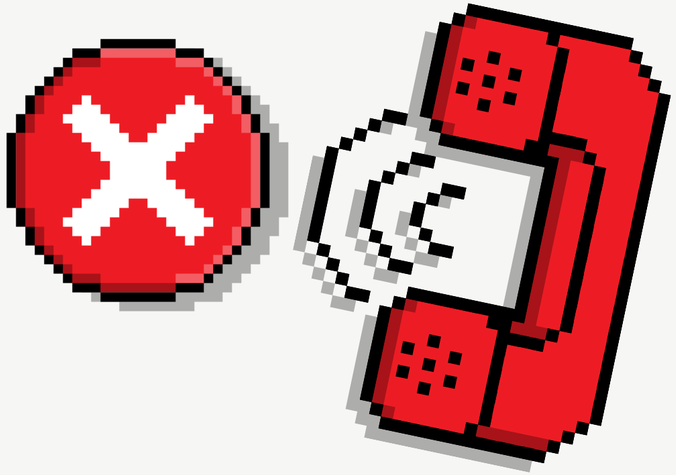
FRAUDULENT CHARITIES

Scammers may pose as a fraudulent charity and ask for donations from generous people. Natural disasters and other major world events are when scammers usually push these fraudulent charities.

Avoid these scams by only donating to trusted charities and avoiding suspicious crowdfunding programs.

OTHER COMMON SCAMS

TAKING ADVANTAGE OF GRANDPARENTS	When a scammer pretends to be a child or grandchild, spoofs a caller ID and calls family members claiming to have been arrested and requesting bail money. It could be just a simple "I need money" ask, but other times they may pretend to be kidnapped, urging for money to be sent immediately or else.
ONLINE SHOPPING DEALS	Online shopping ads that are too good to be true, most likely are. Make sure the online shopping site is trusted before purchasing. For more information and examples, click here.

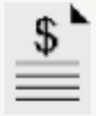


AVOID THESE SCAMS BY HANGING UP AND CALLING THE LEGITIMATE NUMBER OF THE PERSON OR COMPANY OF THE SUSPECTED SCAM CALL

Cybercrime & Seniors

File Edit View Help

How To Stay Protected From Scams



Check for unauthorized charges regularly on credit reports and bank statements.

Be wary of a deal that seems too good to be true.

Ask for more information when dealing with someone suspicious—if they refuse, stop talking to them.

Talk to family and friends and get a second opinion, even if it may lead to embarrassment.

Never give out personal information to an untrusted source.

Keep security software up to date

If a solicitor is demanding an immediate decision, ask for more time. End the conversation if they refuse.

Avoid clicking on links or attachments from unknown sources.

Don't trust pop-up ads, even if they claim immediate tech support is required.

Know that the government will not initiate contact over the phone, text or email about late payments and will never request payment via gift card.

Never use the same passwords for multiple accounts.

Never access personal apps or files when using public Wi-Fi.

Helpful Resources

CYBERCRIME & Seniors

ADDITIONAL RESOURCES ON HOW TO SPOT, REPORT AND AVOID CYBERCRIMES THAT TARGET SENIORS:

- CONSUMER ALERTS
- REPORT IDENTITY THEFT
- SCAM SCAMS AT A GLANCE
- ANNUAL CREDIT REPORT
- SENIOR PROTECTION TEAM
- FLORIDA ABUSE HOTLINE
- FTC REPORT FRAUD
- FBI INTERNET CRIME COMPLAINT CENTER
- CONSUMER PROTECTION BASICS
- DEPARTMENT OF ELDER AFFAIRS