

HOW TO RECOGNIZE AND AVOID SCAMS

OLLI CLECAT

24 October 2022




AARP FRAUD PREVENTION

- AARP offers a resource for its members as well as non-members to get guidance and support on scams
- [AARP Fraud Watch Network Helpline](#) connect you to specialists to help people who are victims of a scam or possible fraud attempts

Your membership helps support free resources from the AARP Fraud Watch Network™.

AARP Fraud Prevention

Trusted guidance.




Getting targeted by scams can leave you wondering what to do, but there's a resource to turn to for trusted guidance and support. Our [AARP Fraud Watch Network Helpline](#) connects you to trained specialists to help when you've been the victim of a scam or to talk through fraud attempts you've experienced.

Call us if you or a loved one has been targeted by a scam.
877-908-3360 Monday – Friday, 8 a.m. to 8 p.m. ET.

[LEARN MORE](#)

The AARP Fraud Watch Network Helpline helps support those who have experienced scams. Explore more resources.



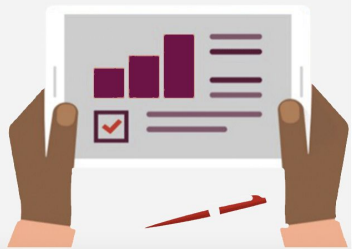
Watch Anytime

STAYING SAFE AS SCAMS EVOLVE
Watch AARP's free, on-demand video to learn how you and your loved ones can identify and avoid evolving scams.

[SIGN ME UP!](#)

FRAUD WATCH NETWORK
Learn how to recognize and avoid scams with resources, tools, articles and more from the AARP Fraud Watch Network.

[EXPLORE NOW](#)



WHAT IS A SCAM

- A scam is a dishonest or fraudulent scheme that attempts to take money or something of value from people. It is a confidence trick that dishonest groups, individuals, or companies perform. The person who carries out a scam is a scammer, trickster, or swindler



Better Business Bureau found that nearly 70% of those who are scammed are under the age of 45, and almost 80% held college degrees. Anyone can be vulnerable to being scammed; it's not just the gullible or trusting.

LATEST SCAM NEWS - ZELLE FRAUD IS ON THE RISE

- Zelle is a peer-to-peer payment system (like PayPal) operated by Early Warning Services, an Arizona tech company owned by Bank of America, Wells Fargo, JPMorgan Chase, PNC Bank, U.S. Bank, Capital One and Truist
- Consumers enroll in Zelle through one of more than 1,700 participating banks or through the Zelle app, then use it to send money directly from their bank account to another Zelle user's bank account
- People can't collect money through Zelle without enrolling their U.S. bank or credit union account into the system
- **What to do:**
 - ✓ If it's an email, look carefully at the sender's address...If the sender's domain doesn't match the company's, it's not from the company
 - ✓ If it's a text warning you about Zelle fraud, do not reply to the text. Call your bank's fraud hotline instead



Never reveal anything to an unknown caller, texter or emailer professing to be from your bank, no matter how persuasive their credentials are or how urgent the supposed problem with Zelle. Instead, call the bank yourself, on the number listed on the back of your ATM card, to see if there is a problem with your account.

SOBERING STATISTICS

- In 2021, the FBI's Internet Crime Complaint Center (IC3) received 13,900 tech support fraud complaints from older victims who lost a total of \$238 million
- Older victims account for 58% of the total reports of tech support fraud to the IC3 Center and 68% of the total losses
- Overall, scams that target older adults have "risen at an alarming rate, while the loss amounts are even more staggering," according to the IC3's Elder Fraud Report 2021.
- In 2021, over 92,000 victims over the age of 60 reported losses of \$1.7 billion to the IC3, representing a 74% increase in losses over those reported in 2020



AARP has found that financial exploitation of older adults has more than doubled since COVID-19

SOBERING STATISTICS – SPAM TEXTS ARE THE NEW SPAM CALLS

- Spam texts are surpassing robocalls as the preferred choice of scammers
- According to the Federal Trade Commission, 2022 is on track to be the first year **where more people report being contacted by scammers via text than by phone call**
- Americans received 87.8 billion spam texts in 2021, compared to 72 billion spam calls. The previous year, there were 55.5 billion spam texts, compared to about 54.5 billion calls
- Americans received 15.6 billion spam texts in September, **nearly 57 spam texts for every person in the United States**



WHY FINANCIAL EXPLOITATION HAS FLOURISHED

- An AARP report surmises that the growth in financial exploitation during/after the pandemic is related to:
 - ✓ **Tech evolution and reliance:** Seniors have been forced to increasingly rely on technology to limit face-to-face transactions, which offers criminals new avenues for theft. And because it's evolving so quickly, it can be difficult for people to keep up, leaving them vulnerable to misinformation and scams.
 - ✓ **Isolation:** With less frequent interactions, loved ones may be less likely to notice signs of financial abuse. Isolation also might make a person more dependent on others for assistance with daily tasks, including the management of their finances
 - ✓ **Loneliness:** An older person who feels lonely due to that increased isolation or the death of a loved one from COVID-19 (or another cause) might be more receptive to a criminal who pretends to care about them



FIGHTING SENIOR FRAUD **BEFORE** IT HAPPENS

- Tucked into the 2022 appropriations bill that President Biden signed into law earlier this year is a little-known measure that aims to tackle the financial exploitation of seniors
- The Fraud and Scam Prevention Act promises a new level of prevention and response to this exploitation by recruiting a new army to fight it...
 - ✓ Clerks and shopkeepers that seniors interact with as they go about their daily business
 - ✓ Creates a new task force, the Senior Scam Prevention Advisory Group, with representatives from government agencies, consumer advocates and industry organizations
 - ✓ Tasked with developing a training program that teaches retailers, financial institutions and wire-transfer services to recognize scams and stop senior fraud before it happens
- Retail cashier may be able to alert customers to a potential fraud before they purchase several hundred dollars in gift cards, a very common scam tactic



Task force has orders to actively monitor the latest fraud schemes and use that information for targeted outreach not only to seniors but their families and caregivers, too. A dedicated website of identified scams and resources is also part of the plan.

COMMON TYPES OF FRAUDS AND SCAMS

- Charity scams
- Debt collection scams
- Debt collection scams that target survivors
- Debt settlement and debt relief scams
- Foreclosure relief or mortgage loan modification scams
- Grandparent scams
- Ransomware
- Imposter scams
- Lottery or prize scams
- Mail fraud
- Money mule scams
- Mortgage closing scams
- Romance scams
- Wire or money transfer fraud



CHARITY SCAM

- A charity scam is when a fraudster poses as a real charity or makes up the name of a charity that sounds real in order to get money from you
- These kinds of scams often increase during the holiday season **as well as around natural disasters and emergencies, such as storms and wildfires**
- Be careful when any charity calls to ask for donations, especially ones that suggest they're following up on a donation pledge you don't remember making
- **What to do:** Ask for detailed information about the charity, including address and phone number. Look up the charity through their website or a trusted third-party source to confirm that the charity is real



GRANDPARENT SCAM

- Someone calls or contacts you saying they're a family member and they need money to get out of trouble
- You need to check that there's an emergency first because it could be a scammer calling
- **What to do:**
 - ✓ Resist the pressure to send money immediately...Hang up
 - ✓ Call or message the family member or friend who (supposedly) contacted you. Call them at a phone number that you know is right, not the one someone just used to contact you
 - ✓ Call someone else in your family or circle of friends, even if the caller said to keep it a secret. Do that especially if you can't reach the friend or family member who's supposed to be in trouble

This is how a family emergency scam call may go:

Caller: Hi Grandpa, it's me.

Grandpa: [*Name of the grandson*]? Is that you?

Caller: Yes, it's me. [*Repeats name Grandpa said.*]
Grandpa, I'm in trouble, and I need money for bail.

Grandpa: What happened?

Caller: Please don't tell Mom or Dad. I'll get in so much trouble.

Grandpa: Where are you?

Caller: Hurry, Grandpa. A lawyer is going to call you. Please help me!

Grandpa then gets a second call from the fake lawyer.

Attorney: This is your grandson's lawyer. He's in a lot of trouble. The only way he can get out of jail is if you pay.

IMPOSTER SCAM - SPAM TEXTS

- According to the FTC, scammers use spam texts to trick people into giving the scammers personal information such as passwords, account numbers and Social Security numbers
- Scammers also try to get you to click on links in text messages
- Texts might notify you of a bill paid, or say they've noticed suspicious activity in your account, or inform you of winning a gift card or a contest
- **What to do:**
 - ✓ Do not respond to suspicious texts, even if the message requests that you "text STOP" to end messages
 - ✓ Do not click on any links you receive in texts
 - ✓ Do not provide any information via text or website
 - ✓ Contact the company using a phone number or website you know is real and not the information in the text



To: 7726

HUGE SALE
95% OFF
go.g/18jpxv12

How to report spam texts

Forward spam messages to **7726** or SPAM. From there, your carrier will ask for the phone number of the spam text and launch an investigation.

RANSOMWARE SCAM

- Ransomware is a type of malicious software (malware), that prevents you from accessing your computer files or network and demands you pay a ransom for their return
- You can unknowingly download ransomware onto your device by opening an email attachment, clicking an ad, following a link, or even visiting a website that's embedded with malware
- You usually discover it when you can no longer access your data, or you see computer messages letting you know about the attack and demanding ransom payments
- **What to do:**
 - ✓ Keep operating systems, software, and applications current and up to date
 - ✓ Make sure anti-virus and anti-malware solutions are set to automatically update and run regular scans
 - ✓ Back up data regularly and double-check that those backups were completed



One of our OLLI members was recently a victim of such a scam. The member was tricked into clicking on a pop-up message indicating malware detection. The member was told to call and then was threatened with data destruction if they didn't comply. Thankfully, the incident was thwarted by a quick-thinking bank employee

HOW TO RECOGNIZE A SCAM

Recognizing these common signs of a scam could help you avoid falling for one

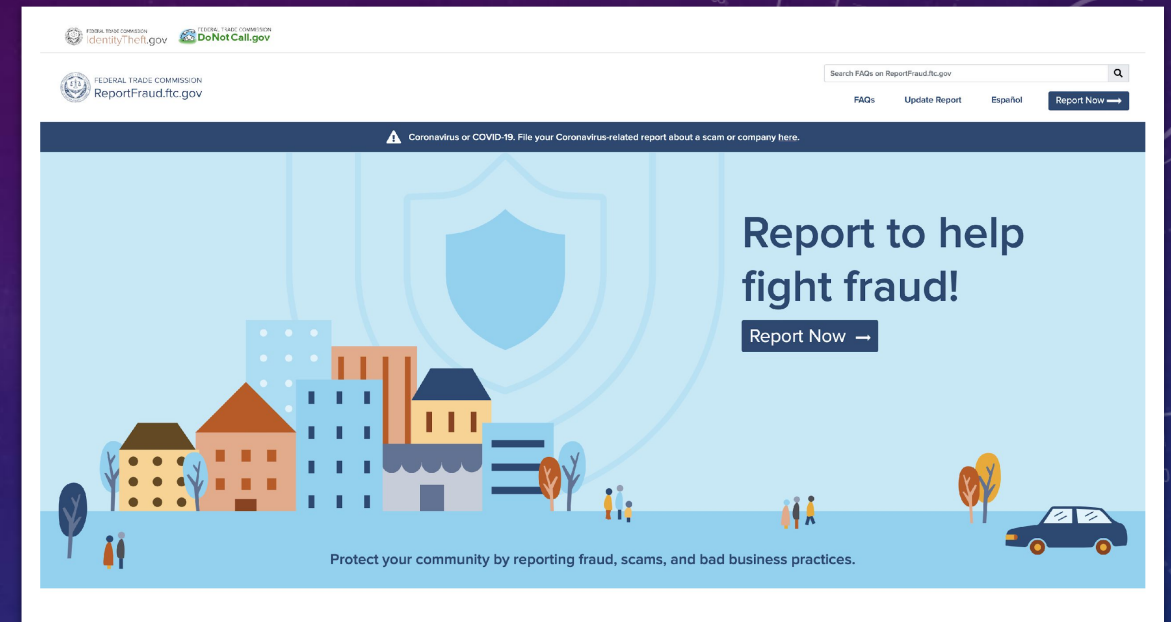
1. Scammers **PRETEND** to be from an organization or someone you know
2. Scammers say there's a **PROBLEM** or a **PRIZE**
3. Scammers **PRESSURE** you to act immediately
4. Scammers tell you to **PAY** in a specific way



Cybercriminals use social engineering techniques to conceal their identity and present themselves as trusted sources or individuals

WHAT YOU CAN DO TO AVOID A SCAM

- Don't give your personal or financial information in response to a request that you didn't expect
- Resist the pressure to act immediately
- Know how scammers tell you to pay...NEVER use a gift card
- Stop, think, and talk to someone you trust
- Learn and practice good cybersecurity measures (e.g., strong password, malware protection)
- Keep your system software up to date and maintain preventative software programs (anti-virus and anti-malware)
- Look for visual clues (spelling, grammar, address bar) in emails or texts



If you were scammed or think you saw a scam, report it to the Federal Trade Commission

CYBERSECURITY MEASURES EVERYONE NEEDS

- When cybersecurity is inadequate, it can lead to stolen identity and financial loss
- Most scams and scammers have two main goals--to steal your money and your identity
- Maintaining cybersecurity is very important
- It all starts with a **STRONG Password** (random and unique)

As a minimum, strengthen your passwords



Enabling features like two-factor authentication on all your accounts also helps add more security

CYBERSECURITY MEASURES – PASSWORD MANAGER

- A password manager is a service that helps you generate and store long, unique passwords for all your online accounts
- Instead of memorizing all the login information you use for each site, you only must remember one **Master Password** when using a password manager
- The autosave and autofill features, will enable connection to all your accounts easily



CYBERSECURITY MEASURES – TWO-FACTOR AUTHENTICATION

- Having a strong password isn't always enough to keep your personal and financial information safe
- Security experts recommend safeguarding your accounts with another layer of defense, namely two-factor authentication (2FA) {aka multifactor authentication}
- 2FA is an extra layer of security used to make sure that people trying to gain access to an online account are who they say they are
- With 2FA, a potential compromise of just one of the (e.g., password) factors won't unlock the account




Common forms of 2FA include:

- ❑ SMS Text-Message and Voice-based
- ❑ Software-generated time-based, One-Time Passcode (OTP)
- ❑ Push Notification

WHAT TO DO IF YOU WERE SCAMMED

- You paid a scammer with a credit or debit card
 - Contact your credit card company or bank that issued your card and tell them there was a fraudulent charge
- You gave the scammer your social security number
 - Go to **IdentityTheft.gov** for next steps...should also monitor your credit
- You gave the scammer access to your computer or phone
 - Run a scan with your computer's security software and delete anything that's flagged
 - Check your bank account and/or credit card for fraudulent charges
- Contact the **Federal Trade Commission** to report the scammer and hopefully help prevent other people from falling victim to scams; file a report with your local police



The screenshot shows the FTC Consumer Advice website. At the top, there is a navigation bar with the FTC logo and the text 'FEDERAL TRADE COMMISSION CONSUMER ADVICE'. To the right of the logo are several menu items: 'Shopping and Donating', 'Credit, Loans, and Debt', 'Jobs and Making Money', 'Unwanted Calls, Emails, and Texts', 'Identity Theft and Online Security', and 'Scams'. Below the navigation bar, there is a breadcrumb trail 'Home / Articles' and a link 'Vea esta página en español'. The main heading of the article is 'What To Do if You Were Scammed', which is circled in orange. Below the heading, there is a sub-heading 'Article' and a paragraph of text: 'Find out what to do if you paid someone you think is a scammer, or if you gave a scammer your personal information or access to your computer or phone.' Below this paragraph, there are four links: 'If You Paid a Scammer', 'If You Gave a Scammer Your Personal Information', 'If a Scammer Has Access to Your Computer or Phone', and 'Report a Scammer to the FTC'. At the bottom of the article, there is a paragraph of text: 'Scammers can be very convincing. They call, email, and send us text messages trying to get our money or sensitive personal information — like our Social Security or account numbers. And they're good at what they do. Here's what to do if you paid someone you think is a scammer or gave them your personal information or access to your computer or phone. If you paid a scammer, your money might be gone already. No matter how you paid, it's always worth asking the company you used to send the money if there's a way to get it back.'

<https://consumer.ftc.gov/articles/what-do-if-you-were-scammed>

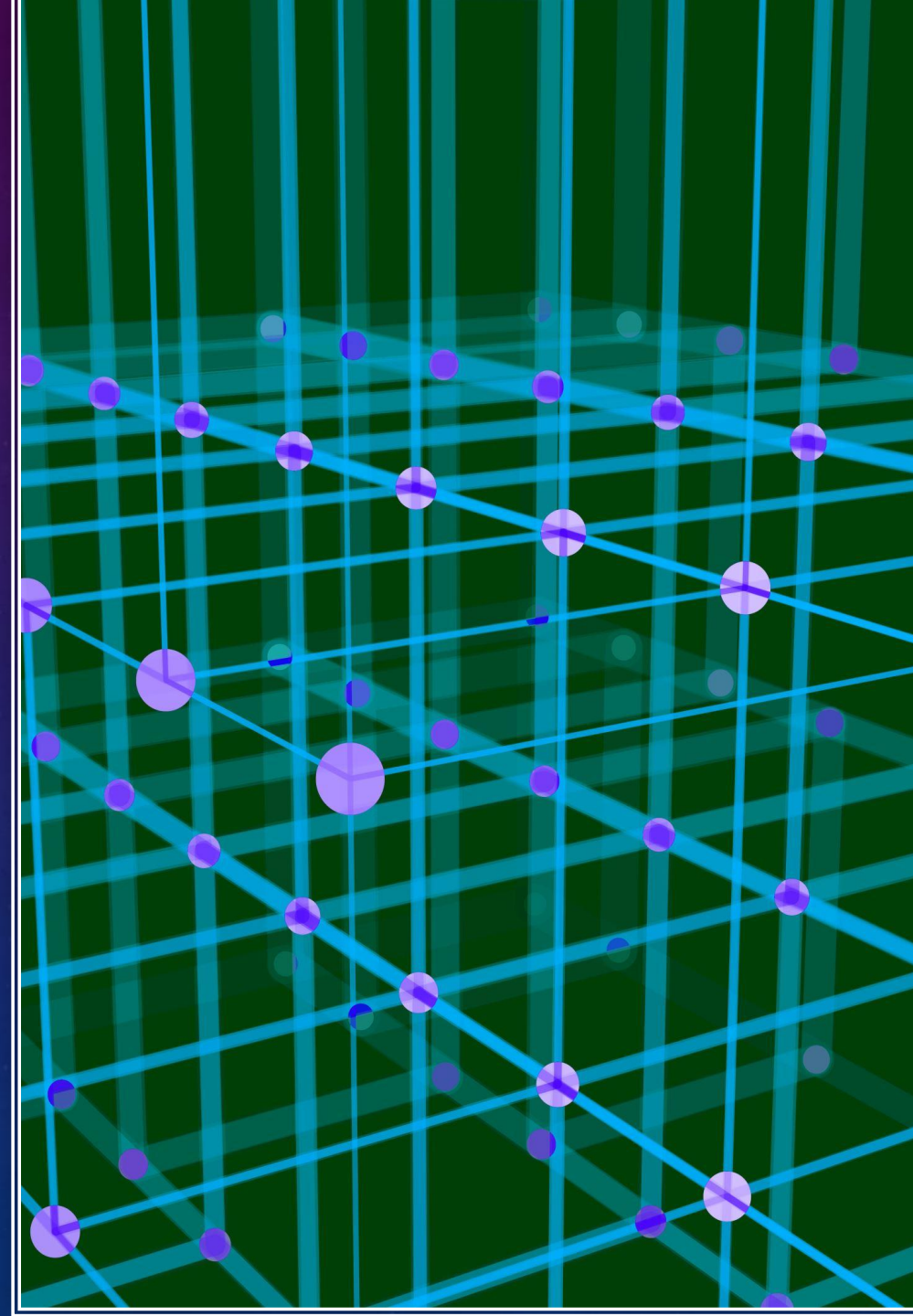
LET'S REVIEW

- A scam is a dishonest or fraudulent scheme that attempts to take money or something of value from people
- NEVER give your personal or financial information in response to a request that you didn't expect
- Social engineering attacks center around the attacker's use of persuasion and confidence...you are more likely to take actions you otherwise wouldn't
- Maintaining cybersecurity is very important...ensure your passwords are random, unique and NOT reused...use a Password Manager and enable 2FA whenever possible
- Keep your device's system software up-to-date, as well as anti-virus and anti-malware software
- Always practice caution...**BE VIGILANT, not afraid**, when you're looking at putting in any login information, personal information or financial information when you navigate from a QR code, SMS text, or via email

- Find information on common scams and frauds that can happen to you, refer to USA.GOV, [Common Scams and Frauds](#)
- If you were scammed or think you saw a scam, [report it to the Federal Trade Commission](#)

LINKS TO RESOURCES

- <https://www.consumerfinance.gov/consumer-tools/fraud/>
- <https://www.aarp.org/money/scams-fraud/>
- <https://reportfraud.ftc.gov/#/>
- <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes>
- <https://www.aarp.org/money/scams-fraud/info-2022/financial-exploitation-scam-report.html?intcmp=AE-FRDSC-MOR-R2-POS3>
- <https://consumer.ftc.gov/>
- <https://consumer.ftc.gov/articles/what-do-if-you-were-scammed>
- <https://www.usa.gov/common-scams-frauds>



QUESTIONS

