Protecting Ourselves from Scams
A Comprehensive Guide

Detection

Unsolicited

Emails, texts, phone calls, or door visits that you have not initiated or requested

Get An Approach

Mine is every communication is bogus until proven differently. Disregard but don’t ignore if the messaging concerns an account of importance to you.

Verify

Create a list of contact numbers or bookmarked websites for all of your accounts especially banking. Follow-up if appropriate

Phone Scams

Common Ploys:

Scammers impersonate government officials or charity workers, asking for personal info or money.

Be Vigilant:

Don't give out sensitive information and verify caller's authenticity independently.

Stay Safe:

Trust your instincts and end the call if something doesn't feel right.

Phishing Scams

What is it?

Fraudsters send emails or texts that look similar to those from reputable businesses and organizations, tricking you into sharing sensitive personal information or downloading malware.

How to Spot it?

Check the authenticity of the URL and sender's email address. Be wary of urgent requests, demands for personal information.

Protect Yourself

If you suspect an email is fraudulent, verify its authenticity independently through official channels, such as contacting the business or organization.

Email and Online Scams

1

Unsolicited Emails:

Do not click on suspicious links or download unknown attachments.

2

Verify Sources:

Check for authenticity from a known good source and be wary of too-good-to-be-true deals.

3

Analyze Content:

Don't provide sensitive data unless you're certain of the message's legitimacy.

Romance Scams

The Danger:

Scammers build fake online personas to establish emotional connections and request money or gifts.

Stay Safe:

Exercise caution when sharing personal info and financial details with individuals you meet online.

Be Skeptical:

Be wary of those who avoid face-to-face meetings or video calls and share online interactions with a trusted friend or family member.

Social Security Scams

1 The Setup:

Scammers falsely claim your Social Security benefits are in jeopardy and demand payment or personal info.

2 Stay Alert:

Remember that legitimate government agencies won't threaten you over the phone.

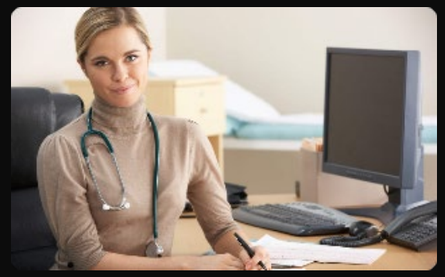
3 Verify Claims:

SSA will not ask for personal info or payment over the phone; verify such claims independently through official channels.

Medicare & Health Insurance Fraud

What is it?

Fraudsters may impersonate healthcare providers or insurers, requesting Medicare or insurance details for fraudulent billing.



How to Spot it?

Confirm the authenticity of any requests for funds or personal data with trusted individuals before disclosing health information.

Protect Yourself

Confirm the legitimacy of any healthcare provider through trusted sources before sharing personal or insurance information over the phone.

The Grandparent Scam

1

The Scare Tactics:

Scammers call claiming to be a grandchild or relative in distress and request money.

2

Ask Questions:

Verify their identity by asking personal questions only the real relative would know.

3

Be Vigilant:

Don't provide personal info or payment without verifying their identity.

The Lottery Scam

The Setup:

Scammers contact you claiming you've won a large sum of money in a foreign lottery.

Stay Alert:

Avoid clicking on links or giving out personal info to claim a prize.

Verify Sources:

Foreign lotteries are illegal in the US. Report such claims to local authorities and the FCC.

Investment Scams

Types of Investment Scams	Warning Signs	Effective Strategies
Pyramid Schemes	Promises of high returns, pressure to recruit new members	Report the incident to the relevant authorities and trusted individuals, don't invest money or share personal information
Pump and Dump Scams	Claims of insider information, high risk investments with low investment values	Don't invest money or share personal information, consult with financial professionals before investing
Ponzi Schemes	Unrealistic returns, vague financial disclosure, limited access to funds	Verify the legitimacy of the investment opportunity through trusted sources, such as regulatory bodies and financial professionals, report the scam to the relevant authorities and trusted individuals

The Tech Support Scam

The Ruse:

Scammers claim to be tech support and ask for remote access to your computer.

Stay Safe:

Don't give permission for remote access and avoid downloading unknown software or giving out personal info.

Verify Identity:

Ask for their company name or employee ID and verify their legitimacy through official sources.

The Charity Scam

The Deception:	Scammers may pose as charity workers, asking for donations or claiming to represent a legitimate charity.
Stay Safe:	Verify the charity's identity through their website, Better Business Bureau, or the National Association of State Charity Officials.
Don't Give Money or Personal Info:	Avoid giving money or personal info to charity organizations that you're not familiar with.

Stay Informed

Keep Updated

Stay informed about common scams and their warning signs to protect yourself and others. Sign up for scam alerts from trusted sources.

Share Information

Spread awareness about scams among friends and family. Share information on common scam strategies and warning signs.

Be Vigilant

Learn to spot suspicious emails, messages, or phone calls. Educate your loved ones about the red flags to watch out for.

Additional Tips

Enroll in scam alerts from reputable sources like AARP or the Federal Trade Commission (FTC).

Verify Requests

1

Identify Scammers

Independently verify the identity of anyone requesting money or personal information. Contact the reputed agency using official contact info.

2

Confirm Authenticity

Reach out to trusted individuals, like family or friends, to verify funds or personal data requests from unfamiliar sources.

3

Stay Cautious

Don't share confidential details without thorough verification. Scammers may use deceptive tactics to appear legitimate.

Use Strong Passwords & 2FA

1 Unique & Robust

Guard your online accounts by creating strong, unique passwords. Consider utilizing a password manager for added security.

2 Enable 2FA

Add an extra layer of protection by enabling two-factor authentication wherever possible.

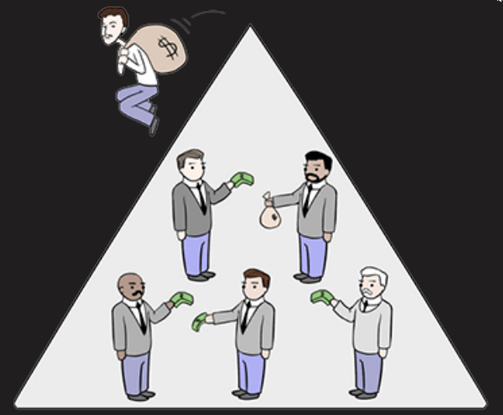
Don't Rush Decisions

Be Wary of Pressure Tactics

Scammers often employ pressure tactics to force rushed decisions. Take your time, consult with trusted individuals, and conduct thorough research.

Investigate Before Committing

Research and gather information about the offer or opportunity before making any commitments or financial decisions.



Choose Wisely

Avoid impulsive decisions driven by scammers. Weigh the pros and cons and consult experts if necessary.

Monitor Finances

1

Regular Reviews

Monitor bank and credit card statements regularly to identify any unauthorized transactions or suspicious activity.

2

Prompt Reporting

If you notice any suspicious activity, report it promptly to your financial institution for further assistance and investigation.

3

Set Alerts

Consider setting up account alerts for unusual or large transactions to stay informed about potential fraudulent activities.

Register for Do-Not-Call Lists

1

Combat Telemarketing Scams

Sign up for the National Do-Not-Call Registry to reduce unwanted telemarketing calls that often disguise scam attempts.

2

Exercise Caution

Avoid sharing personal or financial information with telemarketers, even if they claim to represent legitimate companies.

3

Stay Alert

Remain vigilant against suspicious or aggressive telemarketing calls. Hang up if necessary.

If You’ve Been Scammed

1 Don't engage

Don't respond to suspicious messages or phone calls. Block the sender or delete the message immediately.

2 Verify the source

Double-check the website or phone number before providing any personal information.

3 Report the scam

Notify your bank, credit card company, or local authorities if you suspect a scam.

Remember, scammers can be very persuasive.
Trust your instincts and prioritize your safety above everything else.

Next Steps

If you believe you've been targeted by a scam, it's important to act quickly. The first step is to report the incident to your local law enforcement agency and the Federal Trade Commission (FTC) at www.ftc.gov/complaint.

Be prepared to provide as much information as possible about the scam and any communication you've had with the fraudster. This can help authorities take action against scammers and prevent others from falling victim to the same scam.

Seek Support

If you've fallen victim to a scam, it's important to reach out to someone you trust for guidance and support. Consider talking to a trusted family member, friend, or financial advisor. Discussing the situation can provide clarity and emotional support.

Don't hesitate to involve professionals who specialize in elder abuse or financial scams for expert assistance. They can help you navigate the situation and provide valuable resources.

Protecting Against Scams: You're Not Alone

Remember, you are not alone in the fight against scams. By staying informed and taking proactive precautions, you can empower yourself and your loved ones to stay safe and secure. Together, we can protect ourselves from falling victim to fraudsters.