

Scam Tip Sheet

As part of our promise to help you enjoy financial stability and security, we've created this helpful tip sheet. Please review it to protect yourself from being scammed. Remember: Scams are a crime. They are theft by deception.

SCAM TYPE	DESCRIPTION
Phone Scams	Callers pretend to be from Medicare, IRS, or even your grandchild. Often urgent or threatening.
Investment Scams	Offering high returns on investment "opportunities" with little to no risk.
Relationship Scams	Online "friends" or "lovers" who ask for money or gift cards.
Tech Support Scams	Calls or computer pop-ups saying your computer is infected. They want remote access or payment.
Lottery or Prize Scams	"You've won but you must pay fees or taxes first." No real prize exists.
Charity Scams	Fake charities, especially after disasters.
Mail/Delivery Scams	Receiving unordered items.
Utility or Government Impersonator Scams	Overdue fines/taxes/tolls/jury summons/court order, threaten to shutoff services or arrest you unless you pay.

RED FLAGS TO WATCH OUT FOR:

- You're asked to pay in gift cards, wire transfers, cryptocurrency, or cash.
- High-pressure language: "Act now!", "You'll be arrested!", or "Don't tell anyone."
- Requests for personal or financial information (social security number, Medicare, credit card, bank account, etc.)
- Emails or messages with poor grammar, urgent threats, or inaccurate email addresses.
- Callers can "spoof" familiar phone numbers. This means your caller ID may show a familiar number but it is not real.

Scam Tip Sheet

WHAT TO DO IF YOU SUSPECT A SCAM:

1. Stop immediately. Hang up or disconnect. Do not respond.
2. Never send money or share personal information.
3. Call Security.
4. Keep records of what was said or sent.
5. Call official sources directly, if unsure (Medicare, your financial institutions, etc.)

TIPS TO STAY PROTECTED:

- Sign up for the National Do Not Call Registry: 1-888-382-1222
- Use call blocking features or apps on your phone – contact ERCS for help: 1-800-677-0211.
- Keep computer software up to date – contact ERCS for help.
- Shred mail with personal information.
- Double-check before donating or sending money online.
- Call Medicare or your financial institutions using a known phone number. Do not call a number provided in an email, text message, or letter asking for follow-up.
- Visit the AARP Scams & Fraud page for additional resources.
- Trust your instincts. If it feels wrong, it probably is.

YOU ARE PROTECTING OTHERS BY SPEAKING UP.

Remember, we're here to help. Don't be embarrassed to report a scam. Scammers are professionals. It is not your fault. Reporting as soon as possible increases the chances of potentially recouping lost funds.