SCAMS

Scammers often take advantage of emergencies, confusion or fear, tricking people into giving away money, personal information or access to their accounts. Whether after a disaster, through phone calls or online, know the signs of a scam to protect yourself and your family.

QUICK TIPS

- Never disclose personal or financial information unless you are sure of the identity of the person you are speaking with.
- Be cautious of anyone who pressures you to act immediately or pay with gift cards, wire transfers or cryptocurrency.
- Always verify the identity of a caller, door-to-door visitor or online seller before engaging further.
- Watch for spelling errors, urgent messages or unusual links in emails and texts.
- Report suspected scams to local law enforcement and the Federal Trade Commission at reportfraud.ftc.gov.

SCAMS SAFETY TIPS

SCAMS AFTER DISASTERS

Scammers often target communities recovering from hurricanes, tornadoes, floods or other disasters. They may impersonate government officials, contractors or charities.

Common Scams

- **Fake contractors**: Scammers may go door-to-door, offering quick repairs or tree removal services. They often demand upfront payment and never return.
- **FEMA impersonators**: Some scammers claim to represent FEMA or a local emergency agency and ask for Social Security numbers, bank accounts or payment for assistance.
- **Bogus charities**: Fraudulent organizations may solicit donations using names similar to those of legitimate nonprofits. They often ask for cash, gift cards or wire transfers.

- **Debris removal scams**: Scammers may offer to remove storm debris but disappear after receiving payment.
- **Rental or housing scams**: Some individuals list properties that are already occupied or non-existent and request deposits upfront.

Do's and Do Not's

- Ask for identification from anyone claiming to be from a government agency.
- Verify the contractor's credentials and request references.
- Research a charity before donating at Give.org or CharityNavigator.org.
- Pay in full for services before work begins.
- Share personal or financial information over the phone or at the door.
- Assume a logo or badge makes someone legitimate.

ONLINE SCAMS

Online scams can appear through email, websites, texts or social media. These scams may promise money, ask for login credentials or deliver malware through suspicious links.

Common Scams

- **Phishing emails or texts**: These may appear to come from a trusted source but include links that steal your information or infect your device.
- **Online shopping scams**: Fraudulent websites or sellers may collect payment for goods that are never delivered.
- **Romance scams**: Scammers may build trust over several weeks or months before requesting money.
- **Tech support scams**: Pop-up messages or calls claim there is a virus on your device and ask for remote access or payment.
- **Job offer scams**: Offers that require upfront fees or ask for personal information before hiring are often fake.

Protect Yourself

- Hover over links to see where they lead before clicking.
- Use strong, unique passwords and enable multi-factor authentication when available.
- Keep your device and antivirus software up to date.
- Avoid downloading attachments or software from unknown sources.
- Research any suspicious emails or websites before responding or providing information.

SCAMS TARGETING SENIORS

Older adults may be more frequently targeted by scams that appear credible or emotionally manipulative. Education and vigilance are key to prevention.

Common Scams

- **Grandparent scams**: A scammer pretends to be a grandchild in trouble, requesting urgent financial assistance.
- **Government impersonation**: Scammers pose as IRS, Social Security or Medicare officials requesting personal data or payment.
- **Lottery or prize scams**: Victims are told they won a prize but must pay fees to receive it.

- **Home repair scams**: Fake contractors may target older homeowners, offering unnecessary or overpriced services.
- **Health scams**: Scammers may offer fake medications, medical devices or insurance coverage.

Safety Recommendations

- Discuss common scams with family and caregivers.
- Let unknown calls go to voicemail and never press numbers in automated messages.
- Do not rush to send money, even if a caller says it is an emergency.
- Keep personal documents in a secure place and shred sensitive paperwork.
- Designate a trusted family member to review financial or legal decisions if needed.

IDENTITY THEFT

Identity theft occurs when someone uses another person's personal information to open accounts, make purchases or commit fraud. It can happen digitally or in person.

Online

- Be cautious when entering personal information on websites. Ensure the URL starts with "https."
- Do not reuse passwords across different accounts.
- Avoid using public Wi-Fi to log into financial accounts or make purchases.
- Monitor accounts regularly for suspicious activity.
- Use secure, encrypted platforms for sharing sensitive information.

In Person

- Do not carry your Social Security card unless needed.
- Keep checkbooks, passports and personal records in a locked location.
- Collect mail promptly and consider a locked mailbox.
- Shred old bank statements, credit card offers and medical records.
- Report lost or stolen ID or payment cards immediately to the issuing agency.