Types of Scams, Resources Available

Common Types of Scams

1. **Phishing Scams**
    a. **Description:** Fake emails or messages pretending to be from trusted organizations (e.g., banks, Medicare).
    b. **Example:** Emails asking for personal information or clicking on malicious links.
    c. **Protection Tips:**
        - Don't click on links or download attachments from unknown sources.
        - Verify the sender by contacting the organization directly.
        - **DON'T** use any of the information in the email received to contact the organization directly. Use the phone number on the back of your credit card, Medicare card, etc.

2. **Tech Support Scams**
    a. **Description:** Scammers pose as tech support from well-known companies, claiming there is an issue with the victim's computer.
    b. **Example:** Pop-up warnings or unsolicited phone calls asking for remote access to fix a non-existent problem.
    c. **Protection Tips:**
        - Never give remote access to your computer to unsolicited callers.
        - Contact your computer's official support directly if unsure.

3. **Medicare/Health Insurance Scams**
    a. **Description:** Scammers pose as Medicare or health insurance representatives to steal personal information.
    b. **Example:** Fake calls or emails asking for Medicare numbers or offering fake medical services.
    c. **Protection Tips:**
        - Medicare will never call or visit you to sell anything.
        - Guard your Medicare and health insurance numbers like you would a credit card.

4. **Grandparent Scams**
    a. **Description:** Scammers pretend to be a grandchild in trouble or another relative needing money.
    b. **Example:** Urgent phone calls or emails asking for money to be wired immediately.
    c. **Protection Tips:**
        - Always verify the identity of the caller by asking questions only the real person would know.
        - Never wire money or send gift cards to anyone claiming to be a relative in distress without verification.

5. **Investment and Lottery Scams**
    a. **Description:** Scams offering fake investment opportunities or claiming the victim has won a lottery.
    b. **Example:** Unsolicited calls or emails promising large returns on investments or asking for a fee to claim a lottery prize.
    c. **Protection Tips:**
        - Be skeptical of "too good to be true" offers.
        - Consult with a trusted financial advisor before making any investment decisions.

6. **The Gift Card Scam**
    a. **Description**: is a type of fraud where scammers trick victims into purchasing gift cards and then providing the scammers with the card details, which they can use to steal the funds.
    b. **Examples**: The scammer contacts the victim through various means, such as phone calls, emails, text messages, or social media. They might pose as someone the victim knows, such as a boss, a family member, or a friend, or as a representative of a reputable organization, such as the IRS, a utility company, or tech support. There is a sense of urgency.
    c. **Protection Tips**:
        - Do Not Respond: If you receive such a request, do not provide any information or purchase gift cards.
        - Report the Scam: Report the scam to the Federal Trade Commission (FTC) or the relevant authorities in your country. You can also notify the retailer where you purchased the card.
        - Keep Records: If you've fallen victim, keep any receipts and document your interactions with the scammer. This information can be helpful for reporting and possibly recovering your money.

How to Identify Red Flags

- Pressure to act quickly.
- Requests for payment via wire transfer, gift cards, or prepaid debit cards.
- Unsolicited requests for personal information.
- Emails or calls with poor grammar or spelling errors.
- Caller ID spoofing (appears to be from a trusted source but isn’t).

Phone Calls -- Caller ID and your phone's address book is you best friend. If the caller ID doesn't show the name of someone in your phone's address book, why answer the call? Screen the call first or have your answering machine answer the call. If it's important, the caller will leave a message that you can deal with afterwards.

Steps to Take if You Are a Victim

- **Report the Scam:**
  - Contact local law enforcement.
  - Report to the Federal Trade Commission (FTC) or the Consumer Financial Protection Bureau (CFPB).
- **Contact Financial Institutions:**
  - Notify your bank or credit card company to stop any unauthorized transactions.
- **Change Passwords:**
  - Update passwords ***regularly*** and enable two-factor authentication where possible.

Resources for Help

- Provide a list of trusted resources and contacts, such as:
  - Local law enforcement non-emergency line.
  - Federal Trade Commission (FTC) website.
  - AARP Fraud Watch Network.

Scam, Fraud Alerts - Protect Your Digital Identity (aarp.org)

Protect Yourself from Social Security Scams | SSA

How to place or lift a security freeze on your credit report | USAGov

10 Common Scams That Target Seniors and How to Avoid Them | Retirement | U.S. News (usnews.com)