LEARN

Lifelong Education & Aging Resource Network

Red Flags in Scams



Urgency or Pressure to Act Quickly

- Scammers often create a sense of urgency, claiming you must act immediately or face serious consequences, such as losing money, missing an opportunity, or facing legal action.
- Example: “Your account will be closed unless you verify your information now.”

Requests for Personal or Financial Information

- Legitimate organizations rarely ask for sensitive information (e.g., Social Security numbers, passwords, bank account details) via unsolicited messages, emails, or phone calls.

Unsolicited Contact

- Scammers often initiate contact out of the blue through calls, emails, texts, or direct messages on social media.
- Example: “Congratulations! You’ve won a prize. Just click here to claim it.”

Too Good to Be True Offers

- Unrealistic promises, such as free money, large prizes, or exclusive investment opportunities, are almost always scams.
- Example: “You’ve been selected to receive a $10,000 grant—no strings attached.”

Requests for Payment via Untraceable Methods

- Scammers often demand payment through gift cards, cryptocurrency, prepaid debit cards, or wire transfers, making it difficult to recover the money.

- Example: “Pay your overdue taxes with gift cards from your local store.”

Impersonation of Trusted Entities

- Scammers pretend to be from reputable organizations like banks, government agencies, tech companies, or charities.
- Example: “This is the IRS. You owe back taxes and must pay immediately.”

Emotional Manipulation

- Exploiting emotions such as fear, guilt, love, or sympathy to gain compliance.
- Example: Romance scams where scammers feign love or companionship to extract money.

Generic or Poorly Written Communications

- Emails or messages with generic greetings (“Dear Customer”), spelling errors, or awkward phrasing can indicate a scam.
- Example: “Hello User, You account is compromise. Click here to fix.”

Requests to Keep the Interaction Secret

- Scammers may urge you not to tell anyone, claiming confidentiality is necessary.
- Example: “Don’t tell your bank; they might not approve of this transaction.”

Inconsistent or Unverifiable Details

- Scammers often provide vague or changing information, avoiding specifics when questioned.
- Example: A charity representative unable to provide a website or tax ID for verification.

Fake Confirmations or Alerts

- Fraudulent messages claim you’ve made a purchase or your account has been compromised.
- Example: “Your account has been locked. Click here to reset your password.”

Threats or Intimidation

- Scammers may threaten arrest, deportation, or legal action to coerce payment or information.
- Example: “If you don’t pay now, the police will come to arrest you.”

Too Much Information Requested

- Forms or messages asking for excessive details that aren’t relevant to the context.
- Example: A fake survey asking for your Social Security number.

Suspicious URLs or Email Addresses

- Phishing scams often use links or email addresses that closely mimic legitimate ones but with slight alterations.
- Example: “www.bank-loginsupport.com” instead of “www.bank.com.”

No Contact Information or Fake Contact Details

- Scammers rarely provide reliable ways to reach them or list fake addresses and numbers.

How to Protect Yourself

★ Verify claims by contacting organizations directly using official contact details.
★ Avoid clicking on unsolicited links or downloading attachments from unknown sources.
★ Use secure payment methods and never pay with gift cards or cryptocurrency when demanded upfront.
★ Stay informed about common scams and share knowledge with others.

Curriculum sponsored by:

IDAHO Community Care Program
Case Management - Advocacy - Respite - Education

Providing statewide information, support, and education to caregivers, family, and other loved ones taking care of an individual with memory concerns, dementia, or Alzheimer’s.

www.a3ssa.com/community-care-program