IEHA Program Lesson Submission

Author(s) Names and Email(s):	Lori Bouslog lbouslog@purdue.edu
County Where Author(s)	Vermillion
Area Where Author(s) Work:	Area 5
Phone Number of Author(s):	765-492-5332
Month/Year Materials Created:	April, 2026
Topic Title:	Scams: What You Need to Know
Topic **(Information should educational, you are not the author, seek and presented in a would allow an study, and teach to copyright issues resolved before submission.**	This program helps older adults recognize common scams, including those that occur on social media, and teaches practical strategies to protect personal information. Participants learn how to spot red flags, avoid fraud, and stay safe online and offline.
Short Statement for Lesson:	1. Participants will be able to identify at least three common types of scams—including social media scams—and recognize key warning signs associated with each. Participants will learn and apply practical strategies for protecting personal information, with a focus on strengthening privacy and security settings on social media platforms. Participants will understand what steps to take if they suspect a scam, including how to stop communication, safeguard accounts, and report fraud to the appropriate agencies.

It is the policy of the Purdue University Cooperative Extension Service that all persons have equal opportunity and access to its educational programs, services, activities, and facilities without regard to race, religion, color, sex, age, national origin or ancestry, marital status, parental status, sexual orientation, disability or status as a veteran. Purdue University is an Affirmative Action institution. This material may be available in alternative formats.

Scams: What You Need to Know – Lesson Guide

This program helps older adults recognize common scams, including those that occur on social media, and teaches practical strategies to protect personal information. Participants learn how to spot red flags, avoid fraud, and stay safe online and offline.

Understanding Today's Scams – Why This Matters

Older adults are increasingly targeted by scammers.

- Adults 60+ reported $2.4 billion in losses in 2023 (FTC).
- 41% of adults 50+ say they've lost money to fraud at least once (AARP).
  Scams can happen to anyone—learning the warning signs is your best protection.

Lesson Objectives

- Participants will be able to identify at least three common types of scams—including social media scams—and recognize key warning signs associated with each.
- Participants will learn and apply practical strategies for protecting personal information, with a focus on strengthening privacy and security settings on social media platforms.
- Participants will understand what steps to take if they suspect a scam, including how to stop communication, safeguard accounts, and report fraud to the appropriate agencies.

Common Scams Targeting Older Adults

1. Imposter Scams

Scammers pretend to be:

- *Social Security, Medicare, IRS*
- *Banks or credit card companies*
- *Amazon or tech companies*
- *A grandchild or family member in trouble*
  FTC identifies imposter scams as the #1 most reported scam.

2. Tech Support Scams

Scammers claim your computer has a virus and pressure you to pay for "support."

- *Older adults are **six times more likely** to lose money to tech support scams (FTC).*

3. Prize, Lottery & Sweepstakes Scams

"You've won—but you must pay a fee first."

- *FTC has taken action against deceptive sweepstakes practices, including Publishers Clearing House.*

4. Investment & Cryptocurrency Scams

Promises of guaranteed returns or "risk-free" investments.

- *These scams cause the **highest dollar losses** for older adults (FTC).*

5. Online Shopping Scams

Fake websites or social media ads that take your money but never deliver.

- *AARP reports online shopping scams are among the **top three** affecting older adults.*

Social Media Scams & How They Work

Why Social Media Is a Hotspot for Scams

- Social media is now the **most financially damaging contact method** for scams targeting older adults (FTC).
  Losses from social-media-based scams have increased **ninefold since 2020**.

Common Social Media Scams

1. Fake Ads & Marketplace Listings

Scammers create ads that look like real retailers.

- *Payments often go to individuals, not companies.*
- *Items never arrive or are counterfeit.*

2. Romance Scams

Scammers build emotional relationships online to request money.

- *Older adults report some of the **largest losses** in this category (FTC & AARP).*

3. Phishing Links

Links in posts, messages, or comments may:

- *Install malware*
- *Steal passwords*
- *Capture personal information*

4. Fake or "Cloned" Profiles

Scammers copy a real person's profile and send friend requests to gain trust.

Protecting Personal Information on Social Media

Privacy Settings

- Set your profile to **"Friends Only."**
- Limit who can see your posts, photos, and personal details.

Avoid Oversharing

Do **not** post:

- Your address
- Travel plans
- Financial information
- Personal documents (e.g., vaccine cards, IDs)

Strengthen Account Security

- Use strong, unique passwords.
- Turn on multifactor authentication (FTC strongly recommends this).
- Log out on shared devices.

Be Cautious With Messages & Friend Requests

- Verify unexpected friend requests by contacting the person directly.
- Don't click links sent by strangers—or even friends—if the message seems unusual.

Prevention Strategies & What to Do

How to Spot a Scam

- According to the FTC and AARP, these are major red flags:

1. Urgency or Pressure

Scammers say things like:

- *"Act now!"*
- *"Your account will be closed!"*
- *"Your grandchild is in danger!"*

2. Requests for Unusual Payments

If someone asks for payment via:

- *Gift cards*
- *Wire transfers*
- *Cryptocurrency*
  …it's almost certainly a scam.

3. Unsolicited Contact

Unexpected calls, texts, or messages asking for personal information or money.

4. Too Good to Be True

Unrealistic investment returns, unbelievable discounts, or "free" prizes.

If You Suspect a Scam

1. Stop Communication Immediately

- Do not respond, click links, or send money.

2. Protect Your Accounts

- Change passwords and enable multifactor authentication.

3. Report the Scam

- **FTC:** ReportFraud.ftc.gov
- **AARP Fraud Watch Network Helpline:** 877-908-3360 (free support)

4. Monitor Your Finances

- Check bank and credit card statements for unauthorized charges.

Discussion & Reflection

- Have you or someone you know encountered a scam?
- What warning signs stood out?
- What steps can you take today to strengthen your online safety?

Sources: Federal Trade Commission (FTC) & AARP Fraud Watch Network

Scams: What You Need to Know – Handout

(Based on guidance from the FTC and AARP Fraud Watch Network)

Top Scam Warning Signs

- **Urgency or pressure:** “Act now!” “Your account will be closed!”
- **Unusual payment requests:** Gift cards, wire transfers, cryptocurrency.
- **Unsolicited contact:** Unexpected calls, texts, emails, or social media messages.
- **Too good to be true:** Unrealistic prizes, investment returns, or deals.

Common Scams to Watch For

- **Imposter scams:** Someone pretending to be Social Security, Medicare, IRS, Amazon, or a family member.
- **Tech support scams:** Claims your computer has a virus and asks for remote access or payment.
- **Prize & sweepstakes scams:** You’re told you won but must pay a fee first.
- **Investment & crypto scams:** Promises of guaranteed or “risk-free” returns.
- **Online shopping scams:** Fake ads or sellers who take your money but never deliver.

Social Media Safety Tip

- **Limit who can see your posts** — set accounts to *Friends Only*.
- **Avoid oversharing —** don’t post your address, travel plans, or personal documents.
- **Use strong passwords** and turn on **multifactor authentication**.
- **Be cautious with friend requests —** verify if unsure.
- **Don’t click unexpected links**, even from people you know.

Protecting Your Personal Information

- Never share Social Security numbers, bank info, or passwords by phone, email, or message.
- Shred sensitive documents before discarding.
- Use secure Wi-Fi and avoid logging into accounts on public networks.
- Review bank and credit card statements regularly.

If You Suspect a Scam

- Stop communication immediately.
- Do not send money or personal information.
- Report it:
    - FTC: ReportFraud.ftc.gov
- AARP Fraud Watch Network Helpline: 877-908-3360
- Change passwords and enable multifactor authentication.
- Monitor your accounts for unusual activity.

Remember

Staying safe is about staying aware. If something feels off, it probably is. Take your time, ask questions, and reach out for help—scammers rely on pressure and secrecy, and you don’t owe anyone an immediate response.