FRM-KM.012FG

University of Kentucky
College of Agriculture, Food and Environment
Cooperative Extension Service

A BAD DEAL IN DISGUISE:
TYPES OF SCAMS

Facilitator's Guide

RATIONALE: Scammers may try to trick us by appearing in disguise. This makes it difficult to know when something is "too good to be true." Learn how to avoid being a victim by recognizing common scams. Curriculum materials include publication, facilitator's guide, PowerPoint slides, two participant activities, marketing tools, and evaluation. *This lesson is part of the 2020-2023 Management & Safety Program of Work.*

PROGRAM GOAL: To raise scam and fraud awareness to reduce the likelihood that participants will fall victim in the future

MAJOR PROGRAM INDICATOR: Financial Education General 2056 (Enhance Life Skills and Build Consumer Awareness)

POSSIBLE IMPACT INDICATORS:

- Impact indicator 2056.4 – Number of individuals who implemented strategies to avoid breaches in personal or financial security
- Impact indicator 2056.1 – Number of individuals who gained knowledge related to financial management

OBJECTIVES:

1. Identify at least three imposter types of scams
2. Identify at least two advance fee types of scams
3. Name at least one organization to which you can report potential fraud

RESOURCES FOR LEADERS:

- Publication – A Bad Deal in Disguise: Types of Scams
- Facilitator's Guide
- PowerPoint Presentation (optional)
- Activity Handout – SCAM-O (bingo)
- Activity Handout – Scam Detectives
- Evaluation and Follow-Up Evaluation
- Impact Statement
- Marketing Tools – Social media post, media advisory, radio scripts, and newspaper article

RESOURCES FOR PARTICIPANTS:

- Publication – A Bad Deal in Disguise: Types of Scams
- Activity Handout – SCAM-O (bingo)
- Activity Handout – Scam Detectives
- Evaluation

ESTIMATED TIME AND ADAPTATIONS FOR AUDIENCE:

You can adapt this presentation and deliver it in a variety of time frames and settings depending upon your audience. The estimated presentation time using all included activities is 50 to 60 minutes. This time can be adjusted by using fewer activities or shortening discussion times, as follows:

- 45 minutes – Eliminate the Scam Detectives activity. Limit some discussions.
- 30 minutes – Eliminate the Scam Detectives activity. Very briefly discuss the types of scams and limit some of the examples and sharing opportunities to conserve time. Could eliminate use of SCAM-O cards if desired.
- 15-20 minutes – Eliminate the scam detectives and SCAM-O activities. Focus only on one of the two groups of scams – either imposter scams or advance fee scams. Share the reporting and prevention information. (Note that you would not be meeting one of the objectives of the lesson. The evaluation would not be complete unless you presented this shortened lesson in two parts, to cover all objectives before evaluating.)

CONSIDERATIONS FOR "MAIL-OUT" STYLE LESSON OR VIRTUAL PRESENTATION:

- The Scam Detectives activity is designed for an in-person setting. Omit when using as a mail-out or virtual lesson.
- SCAM-O cards can be used with a mail-out or virtual lesson if desired. Provide one of the cards to each participant along with the presentation information. Virtual attendees can play along the same as they would in person. For mail-out packets, participants would fill out the bingo card as they read the accompanying publication. Participants can turn in the completed cards either in person or by submitted photo to receive their prize if available.
- For virtual presentations, consider using a registration list so you can provide materials in advance. Materials may be distributed by mail, email, or porch/office pick-up. If you would like an online evaluation survey to use instead of the paper form, contact Kelly May at k.may@uky.edu.
- It may also help to have a co-facilitator who can check the chat and read questions and answers from participants during the presentation. The co-facilitator may also help with any technical difficulties if that person is set as a co-host in the meeting software.
- Try to keep virtual presentations interactive if possible. Use questions for which participants can raise their hands, respond in the chat, or reply by voice or video.

PROGRAM PREPARATION:

- Secure a meeting space.
- Preload the PowerPoint presentation (optional) and have needed equipment on site (TV or projector and screen, cables, laptop, speakers if needed, etc.).
- Prepare participant packets, including activity printables.
- Secure supplies:
    - White board or flip chart and markers (optional).
    - Activity supplies:
        - The SCAM-O Activity requires something for participants to use to mark off or cover their bingo card squares. Examples may include pens, markers, bingo chips, ink daubers, or candies of an appropriate size for the square. NOTE: If available, you might use Valentine conversation hearts to reference the Romance Scam.
        - Consider having small prizes for winners of the SCAM-O Activity (optional). Prizes might consist of marketing items, candies/treats, or a local coupon. Note that the full presentation will cover all the scams possible, so you should have prizes for the entire audience if possible.
        - The Scam Detective Activity calls for tape to secure the printable cards to participants' backs.
- If appropriate, consider:
    - Download and print or order free bulk copies of the scam placemats from the Consumer Financial Protection Bureau. They can be used as a placemat, or a supplemental worksheet or activity. In particular, there are placemats about Grandparent Scams, Romance Scams, and the Word Games Bundle. Find it at https://pueblo.gpo.gov/CFPBPubs/CFPBPubs.php?NavCode=XB&Sub2ID=256&CatID=39

INTRODUCTION:

Slide 1 – Introduction/Title Page

Introductory Activity – Icebreaker:

- **ASK: Have you ever heard an offer that sounded "too good to be true"?**
- (Have audience members raise hands and maybe share a few.)

As the facilitator, share:

- We all know to beware of things that sound "too good to be true."
- The trouble is, sometimes it is difficult to tell what is false from what is true.
- This is made more difficult by scammers who, many times, appear in disguise or use other tricks to convince us to participate.

Slide 2 – Review Objectives

- Identify at least three imposter types of scams
- Identify at least two advance fee types of scams
- Name at least one organization to which you can report potential fraud

Slide 3 – Question

- **ASK: What scams have you heard about in your local news?**
- (Record some answers on a flip chart or just repeat answers verbally.)

Slide 4 – Activity: Play SCAM-O

As the facilitator, share:

- The Federal Trade Commission received 2.9 million fraud reports in 2021.
- Of those reports, about a quarter of them resulted in a loss, equaling a total of $6.1 billion.
- The best way to steer clear of joining those statistics is to learn more about different types of scams so you can avoid falling victim.

Slide 5 – Activity: Play SCAM-O

As the facilitator, share:

- Today's whole presentation is a game!
- You each have a bingo card with common scams listed in each square.
- As I describe each scam, cross that one off your card. **This represents you protecting yourself from the scam by knowing about it!**
- Once you mark off four squares in a straight line (across, down, or diagonal), shout "Bingo!" to receive a prize (optional).

NOTE TO FACILITATOR: Scam names in this facilitator's guide are denoted in RED. When you talk about items in red type, that means that participants should cross off that scam on their SCAM-O card. Also note that participants may want to share stories or discuss their experiences with each of the scams. You may wish to allow time for these discussions if you are presenting the full version of this lesson.

OBJECTIVE ONE:

Identify at least three imposter types of scams

Slide 6 – Imposter Scams

As the facilitator, share:

- Many scams start with a scammer in disguise.

- One in five people lost money to imposter scams, at a $1,000 median loss, according to 2021 data from the Federal Trade Commission.
- In an imposter scam, the scammer pretends to be someone else – a trusted source or a business you probably already have dealings with – in order to trick you into sharing information or money.
- Sometimes scammers will play on your trust, pretending to be someone you know, such as in a phishing attempt, grandparent scam, or romance scam.
- Sometimes they try to scare you into paying something they falsely claim you owe, such as in IRS, deputy sheriff, or tech support scams.
- If they ask for money, they typically want you to use a wire transfer or pay by gift card – which can't be tracked or reversed. Let us explore a few of these scenarios in greater detail.

Slide 7 – Phishing

- In **phishing scams**, the scammer pretends to be someone else to trick you into sending money or to get your information, such as a password, account number, or Social Security number.
- Most people know your bank will never ask for your account number – they already have that information on file.
- However, when you get an email or text message that looks like it is from your bank and requests information, it is tempting to reply. The scammer is counting on this reaction.
- Phishing attempts come in many forms:
    - Someone may claim to be a long-lost relative or a prince from a far-away land with an inheritance to share.
    - It may look like a well-known shipping service with a link to track "your order" that you don't recall placing.
    - It may appear that a service you subscribe to, like a television streaming service or utility, has "declined" your payment, with a request to update your credit card information.
    - Sometimes the scammer claims to be a well-known company or store and says they need to access your account to "investigate fraudulent charges."
- Always beware of clicking on links in emails and on websites.
- These could lead to false websites with malware, malicious software that could damage your computer, phone, or tablet or make your information vulnerable.
- Check links and email addresses by hovering your mouse over them and waiting for the box to pop up to show where the link really goes.
- *NOTE: In presentation mode, if showing the PowerPoint, note that there are two extra clicks to show what the pop-up box may look like when you hover the mouse over a link. The first click will show the actual web address for the link. The next click will show the actual email address for the email link. Click again to remove the email address. Then you can click to the next slide.*

Slide 8 – "Grandparent" Scam

- A **"grandparent"** scam often targets seniors.
- A caller on the phone claims to be the senior's grandchild (or other relative) in trouble.
- In this scenario, the false relative has been arrested or stranded and needs money immediately.
- Often, they will ask for suspicious forms of payment, such as a wire transfer, pre-paid credit cards, or gift cards.
- The caller stresses urgency and secrecy, not wanting to upset "mom and dad."
- If you get a call like this from a "grandchild" or someone supposedly representing a relative, hang up.
- If you want to verify, you can contact the relative or relative's family directly to make sure they are safe.
- Note that "grandparent" is in quotes here. It could be any "person-in-need" as the focus of the scam.

Slide 9 – Romance Scam

- **Romance scams** are another type of imposter scam that often begin through online contact.
- Typically romance scams will use social media, dating platforms, or messaging apps.
- A scammer may research you and pretend to have common interests or use a profile you might find attractive.
- If your new romantic interest is reluctant to meet in person that could be a red flag.
- Another red flag is if the relationship moves along very quickly – although some scammers are quite patient.
- After some time and trust has built, your new love interest needs money.
- The premise might be that they are in trouble, or that they need money to settle accounts or pay for travel to visit or move closer.
- Watch out if requested payment methods are those that can't be tracked or reversed.

Slide 10 – Charity Scams

- Imposter scams may prey on your urge to help others in need. For example, people are often generous in times of tragedy or natural disaster.
- Scammers know this and may pretend to represent a charity.
- **Charity** scams may take the form of false charities asking for money transfers.

Slide 11 – Tech Support Scam

- Sometimes the imposters pretend to offer you help.
- In **tech support scams**, the imposter pretends to "assist" you with computer issues you may not have known about – because they don't exist.
- This may happen through phishing, phone calls, pop-up ads, or via a locked screen providing a number to call and "fix" it.

Slide 12 – Imposters Who Threaten

- Sometimes imposters use a disguise to threaten or scare you into paying money or revealing information.
- Reported disguises have included:
    - **The Internal Revenue Service (IRS) scam,**
    - **Sheriff or deputy sheriff scam,**
    - **The Social Security scam, or**
    - **The Medicare scam.**
- Threats can sound scary, like your Social Security number being linked to "criminal activity" or a warrant for your arrest.
- Sometimes they may claim that your benefits will be suspended or that your identification will be revoked.
- They ask that you wire money or use gift cards to pay fees or settle accounts.
- If you have real concerns about any of these issues, contact local officials directly in a separate call using a verified office phone number.

OBJECTIVE TWO:

Identify at least two advance fee types of scams

Slide 13 – Advance Fee Scams

- Other scams revolve around trying to get you to pay money up front in the hopes that you will receive a larger "reward" later.
- The Federal Trade Commission's top 10 fraud categories included **advance fee scams** such as online shopping, sweepstakes and lotteries, and fake check scams, among others.

Slide 14 – Online Purchase Scam

- **Online purchase scams** are on the rise according to the Better Business Bureau (BBB), making up more than 38% of scams reported to the BBB in 2020.
- More than a third of those reports were about pets and pet supplies, such as specific breeds of dogs.
- Most often, victims of this scam paid for a product or service and never received it.
- Others received a fake or lower-quality item or something else entirely.
- This could happen on an unfamiliar website, or when using seller platforms like Facebook Marketplace or Craigslist.

Slide 15 – Government Grant / Fake Loan Scam

- **Government grant scams** and **fake loan scams** work in a similar way.
- These claim to be loans or government grants for college, home repairs, home business costs, or other expenses.
- You may be asked for an advance payment for fees or taxes before you can receive the money.
- Alternatively, they may ask for your checking account information so they can "deposit the money" or "withdraw a one-time processing fee."
- Everyone has access to a free list of available federal grants at grants.gov/; you should never have to pay for this list.

Slide 16 – Prize, Lottery, or Sweepstakes Scam:

- The **prize, lottery, or sweepstakes scam** continues to circulate, possibly because the idea of winning sounds so tempting.
- Real prizes are free, and you have to enter to win.
- Scammers might surprise you with a "win" you weren't expecting.
- If you need to pay a fee, such as for taxes, processing, or shipping, then it is probably a scam.
- You also cannot increase your odds of winning by paying – that is another version of the scam.

Slide 17 – Home Improvement Scams

- Another type of advance fee scam is the **home improvement scam**, which preys on victims of natural disasters.
- Weather events – hailstorms, tornadoes, hurricanes, mudslides, fires, flooding – can leave destruction behind. When that happens, there may be door-to-door construction workers who claim to have "leftover" materials they want to use, and they offer a "discount" for their work.
- However, these scams don't have to be tied to disaster. Some scammers will visit a neighborhood with "leftover blacktop" at a deal or other supplies from supposedly completing some other project.
- Often, they take the deposit but never complete the project.

Slide 18 – Fake Checks Scam

- **Fake check scams**, conversely, are like an advance fee scam in reverse.
- Someone sends you a check or money order that is "accidentally" more than the purchase price.
- The sender says to deposit the check and wire transfer the extra money back to them.
- However, that check could be counterfeit or may bounce.

Slide 19 – Employment Scams

- Similarly, **employment scams** may involve an "employer" who sends "the employee" a check and asks you to send money back in return.
- Or the employer promises to reimburse your costs and fees for doing a service, but never pays.
- In another version, the company may need up-front money for license, registration, or insurance.
- The false employer may even supply forms or contracts that are very convincing.

OBJECTIVE THREE:

Name at least one organization to which you can report potential fraud

Slide 20 – Tips to Avoid Scammers

- Learning to check it out when something sounds "too good to be true" can be a real money saver.
- And reporting scam suspicions to the authorities could help save someone else.
- These are some of the best ways to keep yourself safe from scams.

Slide 21 – Protect Yourself

- The following are four "big tips" to protect yourself:

1. No matter who you're dealing with, it pays to **do some research**. Verify online businesses through a trusted outside source before paying.
2. When shopping online, **use sites that are encrypted**. Look for the "s" in https in the website address and/or for the lock symbol. Finally, don't trust people who contact you unsolicited. They probably don't have your best interests at heart.
3. **Don't pay with a gift card, wire transfer, or cryptocurrency**. The Kentucky Attorney General's Office reports that in 2021, victims most often paid with a gift card or other reloadable card. Scammers will ask for these forms of payment because they cannot be tracked or reversed.
4. In short, **never send money to get money**. Also, don't deposit a check into your account and then pay it back to someone else. You could lose your money if the check doesn't clear.

Slide 22 – Report Fraud

- We can all help prevent scams by **reporting fraud attempts** to the authorities.
- Unreported scams will continue to thrive and cost us all.
- Report suspected scams to the following authorities:
    - Kentucky Attorney General at ag.ky.gov/scams or 888-432-9257
    - Federal Trade Commission at reportfraud.ftc.gov or 877-FTC-HELP

- Better Business Bureau at bbb.org/scamtracker
- Cybercrime such as online phishing – Internet Crime Complaint Center (IC3) at www.ic3.gov
- Identity Theft – IdentityTheft.gov

Slide 23 – Activity: Scam Detectives Game

- *Instructions: Refer participants to the Scam Detectives card in their packets. Provide each person with a piece of tape as well.*
- Today we have discussed a number of scams. It may lead you to think: Who knows what is going on behind my back?
- In this game, you have to find out!
- Everyone should have a notecard with a scam written on it and a piece of tape. Each person should tape a card to someone else's back without showing them. This way everyone will have a mystery word on their back.
- **The best way to avoid a scammer is to do your research. You're going to find out what scam is going on "behind your back" (taped to your back) by asking good questions.**
- You can ask closed questions (yes, no, one-word answer, such as Does this scam involve a computer?) or open questions (What tactics does this scammer use? Who does this scammer usually target?).
- When you figure out the scam, you can take the note off your back.
- Players continue until all scams have been revealed or until a designated period has ended.

Slide 24 – Credits

Take questions if there are any.

Distribute evaluation forms and collect once completed.

EVALUATION:

Please distribute the evaluation form and collect the completed evaluations before the participants leave. If you wish to have them compiled for you and the results shared, you may scan and email, or copy and mail, the evaluations to:

Kelly May, Senior Extension Associate
112 Erikson Hall
Lexington, KY 40506-0050
k.may@uky.edu

Please note that a sample impact statement is included in the available materials. An online version of the evaluation form is available on request to k.may@uky.edu.

Sources and References:

- Better Business Bureau. 2021 BBB Online Purchase Scams Report. (Retrieved March 15, 2022.) https://bbbfoundation.images.worldnow.com/library/d94746d3-524e-4d00-9ae1-8e6e6d542025.pdf
- Federal Trade Commission's Consumer Sentinel Network. Data Book 2021 Snapshot. Data as of Dec. 31, 2021. (Retrieved March 15, 2022, from data published Feb. 22, 2022.) https://public.tableau.com/app/profile/federal.trade.commission/viz/ConsumerSentinel/Infographic
- Federal Trade Commission's Consumer Sentinel Network. Top 10 Fraud Categories. Data as of Dec. 31, 2021. (Retrieved March 15, 2022, from data published Feb. 22, 2022.) https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports
- Kentucky Office of the Attorney General. (2020) Consumer Alerts. Retrieved March 2, 2022, from https://ag.ky.gov/Resources/Consumer-Resources/Consumers/Pages/Comsumer%20Alerts.aspx

Kelly May
Senior Extension Associate for Family Finance and Resource Management

May 2022