Just Say No to Scams

Seminar lesson plan and class activities

Consumer Action Managing Money Project

www.managing-money.org

Just Say No to Scams
Seminar lesson plan and class activities

Lesson purpose:

To provide consumers with the information and resources that will enable them to recognize and protect themselves against scams.

Learning objectives:

By the end of the lesson, participants will understand:

- The tactics scammers often use
- How well known scams are carried out
- How to protect themselves from scam attempts
- Where to get more information about scams, including updates and alerts
- What to do if they are scammed

Lesson duration:

2 hours

Materials:

For instructor:

- *Just Say No to Scams: A guide to protecting yourself from liars, cheats and crooks* (full-length consumer guide)
- *Common Scams: Recognizing and avoiding fraud* (detailed compendium of scams for trainers)
- Visual teaching aid (PowerPoint presentation with instructor's notes)
- Lesson plan, including activities, answer keys and resources (pages 3-24)
- Class evaluation form (page 25)

Instructor will also need:

- A computer and projector for the PowerPoint presentation (the PowerPoint slides also can be printed on transparency sheets for use with an overhead projector); and
- An easel and pad, or a whiteboard, and markers.

For participants:

- *Just Say No to Scams: A guide to protecting yourself from liars, cheats and crooks*
- *Optional: Common Scams: Recognizing and avoiding fraud*
- *Optional: Just Say No to Scams: Quick tips for protecting yourself from fraud* (two-page summary of full-length guide)
- Gone phishing! (exercise) (1 page)
- Class evaluation form (1 page)

Optional:

- Printout of the PowerPoint presentation

Lesson outline:

- Welcome and training overview (5 minutes)
- Recognizing a scam (10 min)
- Phishing (10 min)
- Gone phishing! (exercise) (10 min)
- Common scams (15 min)
- Scams targeting particular demographics (15 min)
- Protecting yourself from scams (10 min)
- Bad actors (exercise) (20 min)
- Reporting a scam (10 min)
- Questions and answers (10 min)
- Wrap-up and evaluation (5 min)

Instructor's notes:

This training module consists of a consumer guide (*Just Say No to Scams: A guide to protecting yourself from liars, cheats and crooks)*, a lesson plan with class activities, and a PowerPoint presentation. It was created by the national non-profit organization Consumer Action to be used by non-profit organizations providing consumer education in their communities. The entire module can be found online at http://www.consumer-action.org/modules/module_scams.

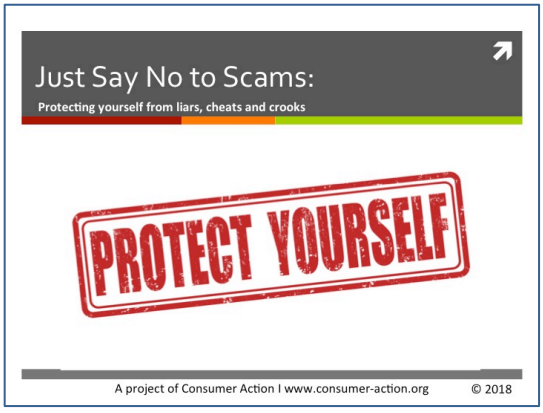
Before conducting the training, familiarize yourself with the guide, this lesson plan (including activities) and the PowerPoint visual teaching aid.

The PowerPoint presentation contains notes for each slide (appearing below the slide when in Normal view or Notes Page view). These notes offer detailed information about the items appearing on the slide. The learning objectives for each section, along with key points and questions to generate discussion, are included in the lesson plan, as are indicators telling you when to move to the next PowerPoint slide.

Why Adults Learn, a PowerPoint training for educators, provides tips for teaching adults and diverse audiences—it will be helpful to you even if you have taught similar courses before. The slide deck is available at http://www.consumer-action.org/outreach/articles/why_adults_learn/.

WELCOME AND TRAINING OVERVIEW (5 minutes)

→SLIDE #1 (onscreen as participants arrive; direct early arrivals to begin reading the brochure/guide)

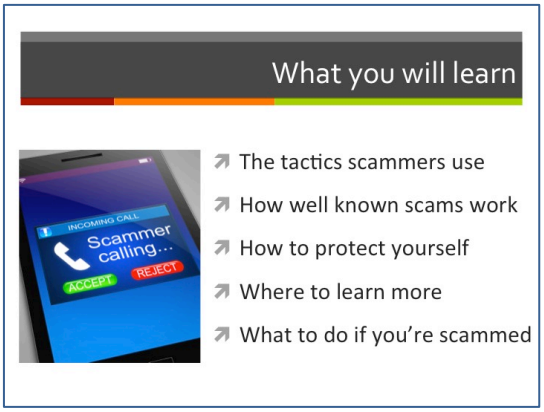


Welcome participants and introduce yourself.

If you have a small group, you can ask individuals to introduce themselves (or, if time permits, ask them to pair off with someone seated near them and then introduce each other to the group) and tell you what they hope to get out of the training. In a larger group, invite a few volunteers to share their expectations. On your whiteboard or easel pad, jot down some of the specific things participants mention. You can come back to this at the end of the class to make sure you've covered these points. (This activity is designed to serve as a brief icebreaker. It will also give you an idea what participants' expectations and needs are.)

Review the contents of participants' packets. Ask the class to take a look inside their packets and make sure they have all the materials needed.

→SLIDE #2



Present the learning objectives of the training.

By the end of the lesson, participants will understand:

- The tactics scammers often use
- How well known scams are carried out
- How to protect themselves from scam attempts
- Where to get more information about scams, including updates and alerts
- What to do if they are scammed

RECOGNIZING A SCAM (10 minutes)

Learning objective: Recognize the telltale signs of a scam so that you can avoid becoming a victim.

Key points (slide 3):

- Even though the countless ways to scam someone can vary widely, all scams have certain things in common; being able to recognize those telltale signs is key to avoiding becoming a victim.
- Scams typically involve an unexpected contact, a request (for money, information, access, etc.), a sense of urgency and, often, a sense that something is "off" (not quite right).

Questions to generate discussion:

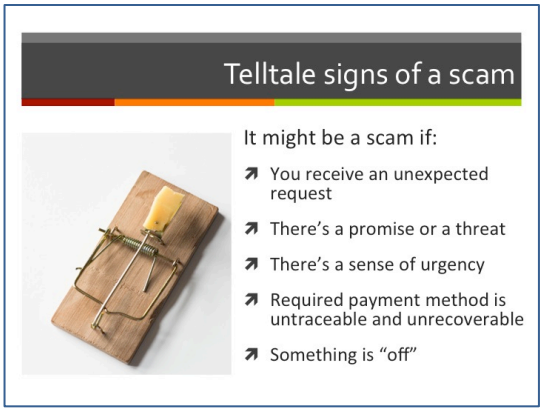
- What is intuition? When do you use your intuition? Do you trust it? Have you ever regretted not trusting your intuition?
- What might raise your suspicions that someone was trying to scam you?
- Have you or someone close to you been scammed? How? Could that happen again today? Why or why not (i.e., what have you/they learned)?

Note: When generating discussion, allow a moment or two for participants to respond. You can jot down responses on your easel pad or whiteboard.

→SLIDE #3

Introduction: Scammers seem to come up with endless ways to fleece their victims. Fortunately, you don't have to be familiar with every old and new scam in order to avoid them. There are a handful of things that all scams have in common. You just need to know what to look for—the telltale signs of a scam.

Go over slide notes.



Slide notes: Scams are as varied as their perpetrators' imagination, but they all have certain things in common. If you know what to look for—the telltale signs of a scam—you can spot a con long before the crook knows you're on to him. Not every scam raises all these warning signs, but all raise at least one.

It might be a scam if:

•Someone contacts you unexpectedly and asks for something (money, personal data, account information or remote access to your computer, for example). The request might not come immediately, but it *will* come.

•You are promised something desirable (the ability to make big money working at home, the chance to get paid for cashing a check, help with a financial problem, or the immigrant visa you want, for example) or threatened with something unwelcome (arrest, deportation, forfeited lottery winnings, etc.).

- There is a sense of urgency to the person's request—they need your payment, personal information or computer access immediately for you to avoid some unwelcome consequence (arrest, account closure, computer crash, a lost investment opportunity, etc.).
- Payment is requested in a form that is untraceable or difficult to cancel or recover (such as a wire transfer or a gift or prepaid card).
- The message sent by a supposedly legitimate business or agency contains typos, unusual capitalization, non-native English use, bad grammar and other errors, and/or the email address, phone number or website address (URL) provided in a communication supposedly coming from a well-known

business or agency doesn't match the contact information found on its legitimate website, your account statement or another valid source.

PHISHING (10 minutes)

Learning objective: Recognize phishing attempts so that you can avoid falling for them.

Key points (slide 4):

- Phishing is one of the oldest and most widely used methods of scammers to get you to reveal sensitive information or give them access to your computer or device.
- The goal of phishing is get the victim to reveal sensitive personal information or to allow access to their personal accounts, computer or device.
- Phishing relies on impersonation (including "spoofing") to get unwitting consumers to let their guard down.

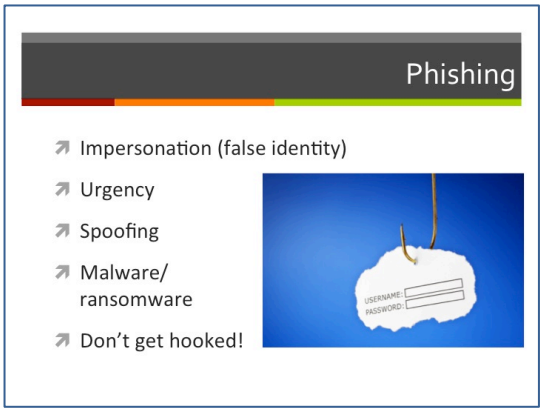
Questions to generate discussion:

- Have you or someone you know ever received a bogus email, text message or phone call? Did you fall for it? If not, what tipped you off that it was a scam?
- Do you do anything to filter out phishing attempts (for example, use a call blocker or spam filter)? Are they effective?

→SLIDE #4

Introduction: Phishing is a scammer favorite because it requires very little effort and is so effective. Despite widespread efforts to inform consumers about phishing attacks and how to avoid falling for them, every day tens of thousands of people around the world reveal their personal information to a crook in response to a phishing attempt (https://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx).

Go over slide notes.



Slide notes: Phishing is one of the oldest and most widely used methods by scammers to get you to reveal sensitive information that can be used to steal your money, identity or security. In fact, as you will notice in the common scams we'll discuss later, phishing plays a role in many different scams. Recognizing and avoiding phishing attempts is key to protecting yourself.

Whether delivered by email, phone, text message or social media, phishing messages attempt to scam you by pretending to be from a legitimate business, government agency or other trusted individual or entity that could believably have a need for your Social Security number, account numbers, passwords, birthdate or other sensitive personal information—to deliver a package, verify a transaction, send you a prize, fulfill an order, issue a refund, keep your account open, etc. Typically, there is a link to a website where you are asked to log in to your account (if you have one) or enter other personal information, or where malicious software will automatically download. In many cases, the website is "spoofed"—designed to look just like the legitimate company or agency's website—to trick you into believing you are secure.

While many phishing messages appear to be from a company or agency, some look like they come from a friend (for example, "Check out the e-card your friend sent!") or a coworker ("I need you to send me the employee W-2s right away!"). Regardless of the purported source, all phishing emails are designed to get

you to act quickly and divulge sensitive information or open yourself up to malware (typically used to gain access to your data or to encrypt your files and demand ransom).

All phishing attempts use impersonation (false identity) to fool their targets; the email, text or phone call purportedly comes from a legitimate business, a government agency, a friend, a coworker or some other familiar and trusted entity or individual. This is how the scammer gets you to let your guard down. Phishing messages instill a sense of urgency. Sometimes the urgency is a threat (for example, closing your account, not delivering your package, not issuing a refund, etc.) and other times it's a promise (there is an inheritance, lottery jackpot, romance or friend's e-card waiting for you, for example). This is how the scammer gets you to act without first thinking, verifying or consulting someone—all of which could make you realize it's a scam.

Phishing attempts often employ "spoofing"—the creation of a bogus website designed to look just like the legitimate site of a well known business or agency, or rigging caller ID so that it looks like the call is coming from a recognized business, agency or neighbor. Typically, the website will either ask you to enter your account login/password or other sensitive information or it will download malware onto your computer or device. Likewise, a phishing call (also known as "vishing") might have you enter your personal or payment information or call a fake call center back to provide such information.

Some phishing attempts are made with the goal of installing malware (malicious software) on your computer or device. Depending on the type of malware used, it could allow the scammer to access your files, track your online activity, record your keystrokes or steal your contacts. "Ransomware" is designed to encrypt your files so that you lose access to them unless you agree to pay a ransom to get the "unlock" code.

Here are some tips for evading phishing attempts:

- Pay attention to detail. Most phishing attempts reveal themselves through spelling, capitalization and grammatical errors, non-native English use (unnatural wording) and unprofessional presentation—things you wouldn't expect from a business or government agency. (View a phishing example in CNET's "How to spot a phishing email": https://www.cnet.com/how-to/spot-a-phishing-email/.)
- Be equally critical of website URLs; Techwalla explains the tricks you might come across (https://www.techwalla.com/articles/how-to-recognize-a-fake-url). Check the website address to see if it matches the known URL of the business. Beware of lookalikes. Type in the correct URL yourself rather than clicking a link. Look for the "s" (in *https*) and the key or padlock symbol at the bottom of the browser, both of which indicate a secure website. If the website looks different from the last time you visited or its appearance is in any way "off," leave—you may be a victim of "pharming." (Pharming refers to a fraudster installing malicious code on your computer that redirects you to a fraudulent website without your knowledge.)
- Remember that credit card issuers, banks and other financial institutions will never ask you to disclose your password. That is generally true for other businesses too. Federal agencies will rarely call you or ask you to confirm personal information by phone, and then typically only regarding a matter you're already aware of.
- Don't trust the "From" field in an email message. Reveal the sender's email address to see if it looks suspicious. Even if it doesn't looks suspicious, it could be a forged address. (How-To Geek explains how to find out the real sender by digging into the email's "headers": https://www.howtogeek.com/121532/htg-explains-how-scammers-forge-email-addresses-and-how-you-can-tell/). If either the sender or the subject looks suspicious, delete the email without opening.
- Don't trust caller ID. Technology has made it easy for scammers to block caller ID or to display a name or number you are likely to recognize and trust.
- Never respond directly to an email or text message from a bank, business or agency, or trust the contact information provided in the message or call. Contact customer service via the known number or website to verify that the request for your information is legitimate.

- Don't click links or open attachments from unknown sources. Be cautious even with links and attachments sent from friends and other familiar sources, since email contact lists are often hijacked for the purpose of sending out phishing messages that are more likely to be opened.

Learn more at Phishing.org (www.phishing.org). (Though the website is designed to help organizations and their IT professionals thwart phishing attempts, there are examples and tips useful for individuals too.)

Report phishing attempts to the company, agency or organization impersonated in the message. Also forward phishing emails to the Federal Trade Commission (FTC) at spam@uce.gov, and file a complaint with the Internet Crime Complaint Center (IC3) (https://www.ic3.gov/complaint/splash.aspx).

"GONE PHISHING!" EXERCISE (10 minutes)

Assign participants to work on the fill-in-the-blanks exercise on page 20 of the lesson plan. Ask for volunteers to share their answers. (Answer key is on pages 21-22.)

COMMON SCAMS (15 minutes)

Learning objective: Understand how common scams are perpetrated so that you can avoid falling for them, and use what you know about these scams to recognize other scam attempts.

Key points (slides 5-6):

- There are certain scams and variations on them that scammers attempt regularly.
- Understanding how many scams are perpetrated helps you recognize other scams and avoid falling for them.
- Avoiding any scam requires being vigilant, skeptical, protective, unhurried, proactive and informed.

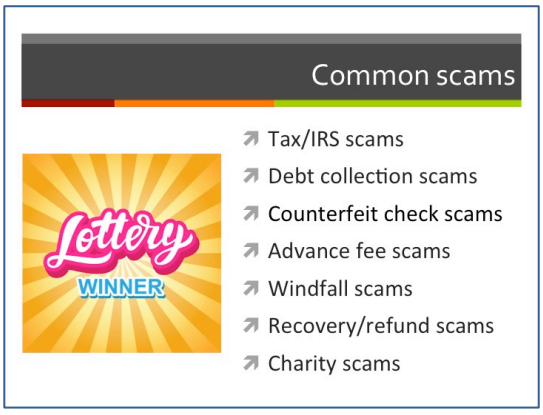
Questions to generate discussion:

- Can you describe some scams you're aware of? Explain how they work.
- If you had to advise someone how to avoid being a scam victim, what advice would you give?

→SLIDE #5

Introduction: There are certain ruses in the scammer's arsenal that are tried-and-true. These are the scams that continue to reel in victims and reward the scammer handsomely. Though there may be variations on the original, the underlying con remains the same. Consumers who are familiar with these oft-used ploys are better prepared to avoid these, and other, scams.

Go over slide notes.



Slide notes: It's impossible to be aware of all the different types of scams being perpetrated. However, there are certain scams that are carried out far more often than others, due in large part to their success rate. As we go over these, look for the warning signs that would alert you to similar ploys. See the companion "**Common Scams: Recognizing and avoiding fraud**" publication for more detail about specific scams.

Tax scams: An imposter claiming to work for the IRS threatens you with arrest, deportation or other action if you don't immediately pay taxes you supposedly owe. Or they request "verification" of personal or account information, supposedly for the purpose of processing your tax return or refund.

Tip: The IRS will always contact you by mail first, won't threaten you, and won't demand payment by wire transfer, prepaid card, gift card or cashier's check. Call the IRS (800-366-4484) to verify that a communication is legitimate. Read the "Tax Scams/Consumer Alerts" page on the IRS website to become familiar with these and other tax-related scams (https://www.irs.gov/newsroom/tax-scams-consumer-alerts). (Be aware that, beginning April 2017, private debt collectors now may call taxpayers to collect past-due taxes, making it more difficult to be certain that a caller is a scammer. However, you should still first receive a letter from the IRS notifying you that your account is being transferred to a private collection agency. You should also receive a letter from the collection agency.)

Debt collection scams: A scammer impersonating a debt collector threatens you with jail or other legal action if you don't immediately pay (typically via wire transfer, prepaid or gift card number or cashier's check) a debt you supposedly owe. In other cases, the collector is legitimate, but the debt is not valid (too old, or already paid or settled), is in the wrong amount or doesn't belong to you.
Tip: Any time you are contacted by a debt collector, you should request that a "validation notice" be mailed to you. Learn more in Consumer Action's *When a Collector Calls* (https://www.consumer-action.org/english/articles/when_a_collector_calls_an_insiders_guide_to_responding_to_debt_collectors) and in the FTC's "Fake Debt Collectors" (https://www.consumer.ftc.gov/articles/0258-fake-debt-collectors).

Counterfeit check scams: Someone gives you a (counterfeit) check and asks you to deposit it and then return part of the money to them. It is often cloaked as an accidental overpayment for something they are purchasing from you or for work you've done. When the fake check bounces, you are out the amount of the check plus whatever money you sent back to the scammer and any non-sufficient funds fees.
Tip: Don't accept a check or money order unless you know and trust the person you're dealing with. Only accept the exact amount due you. Never wire money to strangers. Learn more at the FTC's "Fake Checks" webpage (https://www.consumer.ftc.gov/articles/0159-fake-checks).

Advance fee scams: Someone contacts you offering help with some financial need—for example, getting out of debt, reducing payments on your student loans, avoiding foreclosure, getting a lump sum out of your pension, tapping the equity in your home, negotiating a tax settlement or erasing negative information in your credit report. You pay the scammer's fee upfront, but the help doesn't materialize.
Tip: Be skeptical if you didn't initiate contact. Research the company and the value of the services offered (many are available free). Avoid anyone who promises you will qualify for a loan or credit card before you even apply, particularly if you have a low or no credit score. Learn more at the FTC's "Advance-Fee Loans" page (https://www.consumer.ftc.gov/articles/0078-advance-fee-loans).

Windfall (sweepstakes, inheritance, etc.) scams: Someone informs you that you've won a lottery or sweepstakes, received an inheritance, gotten a grant or are entitled to some other windfall—*but*, you must first pay a fee or provide personal information to collect it.
Tip: Assume that anyone who demands a fee or personal information before turning over money due you is a scammer—especially if you don't remember entering or applying. Steer clear of any contest that requires you to reveal sensitive data (Social Security number, etc.) to enter.

Recovery/refund scams: Someone contacts you promising to recover money you've lost to a scam.
Tip: Assume that anyone who contacts you to recover lost money, missing prize winnings, undelivered products, etc. is trying to scam you. (Often, perpetrators of these scams work off of a "sucker" list—a compilation of people who have fallen for scams in the past and are believed to be more likely to be cheated again.) Agencies (such as the FTC or CFPB) that work on consumers' behalf never call victims to promise a refund in advance and never ask for a fee or personal information before helping. Learn more at the FTC's "Prize Scams" webpage (https://www.consumer.ftc.gov/articles/0199-prize-scams).

***Charity scams*:** You are contacted by a charity (maybe even one with a familiar name) requesting an immediate monetary donation. The representative dissuades you from thinking about it or researching the organization.

Tip: Rather than respond to random requests, research the causes and charities you want to support on sites like Charity Navigator (https://www.charitynavigator.org/) and Give.org (http://give.org/). Make donations with a credit card, which offers strong consumer protections. Read the FTC's "Before Giving to a Charity" webpage (https://www.consumer.ftc.gov/articles/0074-giving-charity).

→SLIDE #6

Go over slide notes.

Slide notes:
Pyramid schemes: This type of investment scam (also known as a Ponzi scheme) lures victims through the promise of very attractive and/or guaranteed returns. Early investors tout the too-good-to-be-true opportunity to friends and family members, unwittingly recruiting new victims. Once the supply of new investors dwindles and/or existing investors want to cash out, the scheme falls apart and everyone (except the originator) loses. Multi-level marketing (MLM) schemes are similar, but are organized as businesses where recruits are required to buy a large inventory and/or recruit new distributors.
Tip: Research investment companies and professionals using FINRA's BrokerCheck (https://brokercheck.finra.org/); the SEC's Investment Adviser Public Disclosure program (https://adviserinfo.sec.gov/IAPD/Default.aspx); and your state's securities regulator's office (http://www.nasaa.org/about-us/contact-us/contact-your-regulator/). Follow the FTC's tips for steering clear of questionable multi-level marketing schemes (https://www.ftc.gov/tips-advice/business-center/guidance/multilevel-marketing). One of the best ways to protect yourself and find legitimate investments is to learn about investing from reputable sources.

Affinity fraud: Someone offers you an attractive investment or business opportunity specifically because of your affiliation with a particular demographic or community (a religion, language, ethnicity, culture, etc.).
Tip: Do not let your guard down just because of a common background, or because someone you trust vouches for the organizer or investment (that person might be fooled too). Go through the same steps to verify the individual, company and investment that you would if there were no personal connection. (For an infamous example of affinity fraud, read about Bernie Madoff: https://en.wikipedia.org/wiki/Madoff_investment_scandal.)

Sales scams: A scammer tries to sell you counterfeit luxury goods, duplicate concert/event tickets, an invalid gift card, a lease on a home they don't own, supplies or training for bogus work-at-home jobs, a puppy that doesn't exist, ineffective or dangerous health products, etc.
Tip: Do business only with merchants you know and trust, or ones that you have investigated thoroughly. Conduct peer-to-peer transactions through an intermediary that offers some protections (PayPal, eBay and Airbnb, for example), and pay by credit card.

Tech support scams: Someone claiming to be from a well-known tech company notifies you (typically by phone or email, or through a pop-up window in your browser) that there is a serious technical problem with your computer that he or she can fix if you pay a fee or give them remote access to your computer. (Victims sometimes unwittingly initiate contact with the scammer themselves after finding a bogus tech support number online.) The scammer takes your payment and provides worthless services and/or downloads malware that locks your computer files until you pay a ransom.
Tip: Don't believe random claims that your computer needs fixing. Never click on pop-up ads or links in unsolicited messages. Don't give anyone you aren't confident you can trust remote access to your computer. Get the contact information for legitimate tech support from a trusted source. Back up your computer files regularly. Learn more at the FTC's OnGuardOnline (https://www.consumer.ftc.gov/features/feature-0038-onguardonline).

False health claims: Hucksters market weight loss, medical and youth-preserving treatments and products that turn out to be ineffective or even harmful.
Tip: There's no quick and easy way to lose weight, no "miracle" cures and no fountain of youth. Consult with a physician regarding any specific medical issues you experience as you age. Beware of "free" trial offers; most people forget to cancel before the trial period ends and wind up paying for something they don't want. Read the FDA's "Health Fraud Scams…Are Everywhere" (https://www.fda.gov/downloads/forconsumers/protectyourself/healthfraud/ucm302359.pdf), which provides tips for recognizing these types of scams.

Romance scams: Often perpetrated online through dating websites, chat rooms or social media, this ruse tricks you into believing the scammer has romantic intentions (or wants to be your friend). Once he or she has gained your confidence and emotional commitment, there will be a request for money or a "favor."
Tip: Before becoming romantically or otherwise involved, research the person's name, try to verify that they live and work where they say they do, and do an image search of their photo (https://images.google.com/). (If the photo appears under several different names, it's a scam.) Don't ignore the little signs that something isn't right, such as early professions of love or friendship, a request to move your communications off the dating or social media site, non-native English from someone claiming to be American, a story that tugs at your heartstrings, a reluctance to meet in person, etc. Don't send money or enter into any other transaction. Learn more at the FTC's "Online Dating Scams" webpage (https://www.consumer.ftc.gov/articles/0004-online-dating-scams) and in the agency's infographic (https://www.ftc.gov/sites/default/files/u46943/online-dating-scams-aba.png).

Blackmail schemes: You do something that you wouldn't want a spouse, parent, employer, school administrator, law enforcement officer or anyone else to find out about, and someone photographs or records you, or gets hold of an email or text message, and then demands money to keep your secret.
Tip: Since virtually everyone around you has a smartphone and the ability to photograph or record whatever you do, and email and text messages are not always secure, don't put yourself in a compromising position. If you submit to someone's demands for money in exchange for their silence, be aware that there's no guarantee your secret will remain private even after you have met the blackmailer's demands.

SCAMS TARGETING PARTICULAR DEMOGRAPHICS (15 minutes)

Learning objective: Help consumers recognize and avoid scams aimed at particular demographics (seniors, veterans, immigrants and students).

Key points (slides 7-10):

- While many scams are aimed at the general public, there are some that target a particular demographic because the scammer identifies an easy way in, detects a vulnerability or believes there is a great likelihood of financial gain.
- Seniors, veterans, immigrants and college students are a few demographics that often are targeted.
- For a variety of reasons, seniors can be particularly vulnerable to fraud, and they are also more likely to be financially scammed by someone they know and trust.
- Scammers often target veterans because they can appeal to their loyalty to the military and because their VA benefits provide an "in" to the veteran.
- Scammers often target immigrant communities because they can exploit a lack of English fluency, distrust of law enforcement or mainstream financial institutions, desire to achieve legal immigration status or fear of deportation.
- Scammers often target college students because they are easy to find (college campuses), have some money (from parents, student loans, part-time jobs, etc.), are away from home for the first time (so not under parents' watchful eyes) and are probably inexperienced with money management.

- The best protection for potential targets is to learn—before becoming a victim—how to recognize and avoid scams.

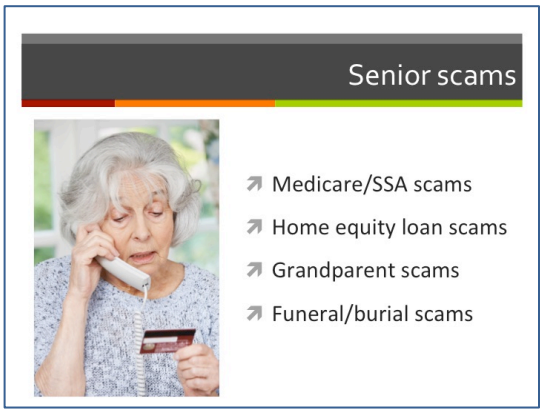
Questions to generate discussion:

- Why do you think seniors often are the target of scammers? What makes seniors more attractive to scammers and/or more susceptible to scam attempts? What could you do today to protect a senior in your life? (Ideas might include going over warning signs/tips with the senior and others in his/her life, encouraging the senior to contact you when in need of a second opinion, etc.)
- How might current events shape the types of scams being perpetrated? (For example, Medicare phishing and bogus fee scams increased with the announcement of new Medicare cards; bogus charity scams increased with the California wildfire disaster; and immigration scams and unfounded deportation threats increased with changes to federal immigration policy.)

→SLIDE #7

Introduction: For a variety of reasons, seniors are at greater risk of being scammed and may benefit from outside help to avoid scams and financial abuse. Recognizing that they can be targets and understanding how some common senior scams work can prepare them and loved ones to avert a financial loss.

Go over slide notes.



Slide notes:
While consumers of all ages should be on guard against scams, seniors can be particularly vulnerable to fraud. This can be because of changes in the brain that make it harder for the elderly to detect suspicious body language and other warning signs that someone might be untrustworthy (http://news.usc.edu/135031/senior-scams-and-fraud-due-to-aging-brain/). Or it can be because they are isolated, are more likely than young people to be home (and available to answer the phone or door), are inexperienced in managing their finances (a deceased spouse may have been the primary household money manager) or don't have access to the internet and the tools it offers for verifying claims and identifying scams. The elderly are also more likely to be financially scammed by someone they know and trust—a friend, family member, caregiver or other helper.

All states have laws to protect older people from abuse. In addition to reporting suspected elder fraud to local adult protective services agency (https://eldercare.acl.gov/Public/Index.aspx) and law enforcement, notify any financial institution holding an account that has been fraudulently accessed. Learn more about the following scams and others in the National Council on Aging's (NCOA) list of the top 10 financial scams targeting seniors (https://www.ncoa.org/economic-security/money-management/scams-security/top-10-scams-targeting-seniors/).

Medicare/Social Security scams: A scammer posing as a Medicare or Social Security Administration representative provides a bogus reason why they need your Medicare or SS number and/or financial account information (and then they use your Medicare benefits or steal your money or identity). Or, they sell you discounted prescription drugs that might be fake or even harmful, or a cheap Medicare-covered medical device and then bill Medicare for many times the value.
Tip: Don't ever give your Medicare, Social Security or other account numbers to an unexpected caller. Call Medicare (800-633-4227) or Social Security (800-772-1213) to verify a request. (Be aware that Medicare's announcement that it would be issuing new Medicare cards with non-Social Security number identifiers in 2018 and early 2019 has sparked new scams where callers posing as Medicare representatives ask for a processing fee for the new card or bank account information to issue a "refund" on the old card accounts.) Ask your healthcare provider for referrals to suppliers, or ask if the supplier you are considering doing

business with is reputable. Learn more at Medicare's "fighting fraud" webpage (https://www.medicare.gov/forms-help-resources/help-fight-medicare-fraud).

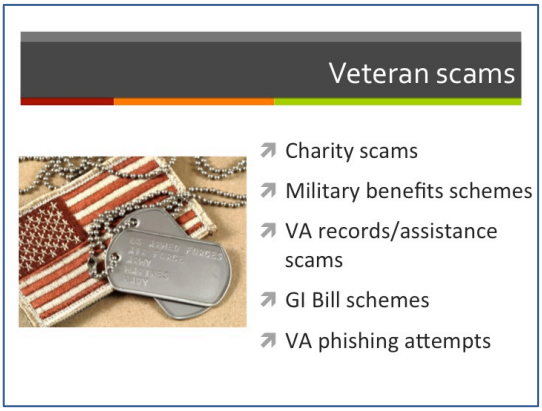
Home equity loan scams: Questionable home equity loans, which pull equity out of your home and use the property as collateral, typically have high fees and high variable interest rates (fluctuating payments). Many are "interest only," which means you never pay down your debt and your payments eventually increase, and they may require a lump sum (balloon) payment in just a few years. Some lenders encourage you to refinance repeatedly to pull more money out, each time adding additional fees to your debt. If you can't make the required payments, your home could be taken from you (foreclosure).
Tip: Do not respond to unsolicited loan offers. Borrow only from a reputable lender that you contact after shopping around. Get advice and assistance from someone you can trust. A HUD-certified housing counselor can offer guidance about loan terms, affordability, lender reputation, your rights and alternatives to borrowing (https://www.hud.gov/i_want_to/talk_to_a_housing_counselor).

Grandparent scams: A scammer pretending to be a family member—often a grandchild—or an authority figure calls and claims that your loved one needs money urgently for something like emergency medical care or bail in another country. The scammer demands immediate payment, usually via wire or a prepaid or gift card.
Tip: Don't pay the caller! If you are concerned about the person who is supposedly in need of money, try to contact him or her directly, or verify with another family member or anyone else likely to know if the story is true (even if the scammer tells you not to).

Funeral and burial scams: A scammer reads an obituary or funeral notice for your loved one and shows up claiming the deceased died with an outstanding debt that you must now pay. Another type of scam is the sale of fake burial plots, often discovered only when the plot is needed. While not technically a scam, some funeral homes try to oversell products and services in violation of the law.
Tip: Verify any claims. Ask for help from people you trust; a lawyer would be a good resource because he or she could also tell you what your rights are related to any debts the deceased did truly leave behind. Learn more at the FTC's "Debts and Deceased Relatives" webpage (https://www.consumer.ftc.gov/articles/0081-debts-and-deceased-relatives). Pre-purchase burial plots/crypts only through a reputable cemetery, and get a written receipt. Read the FTC's Funeral Rule (https://www.consumer.ftc.gov/articles/0300-ftc-funeral-rule) to understand your consumer rights when buying funeral services. Learn about "ghosting"—the theft of a deceased individual's identity to commit fraud—in Consumer Action's publication: https://www.consumer-action.org/downloads/outreach/2015_deceased_ID_theft.pdf.

→SLIDE #8

Go over slide notes.



Slide notes: A late-2017 AARP Fraud Watch Network survey found that veterans are more likely than other Americans to be the victims of scams. In fact, more than twice as many veterans as nonveterans lost money to scam artists during the previous five years. Instead of receiving deserved respect for their service to our country, veterans, and even active duty servicemembers, are instead often targeted by scammers. These are a few of the most prevalent veteran scams. Read the *AARP Watchdog Alert Handbook: Veterans' Edition: 9 Ways Con Artists Target Veterans* (http://action.aarp.org/site/DocServer/Watchdog-Alert-Handbook-Veterans-Edition.pdf) to learn more about how veterans and servicemembers can avoid becoming scam victims.

Veteran charity scams: Scammers try to appeal to veterans' and servicemembers' loyalty to the military by soliciting donations to charities that purport to help these groups. In some cases, the charity doesn't exist. In

others, a charity is established legally, but all or most of the donated funds go into the pockets of the fundraisers.
Tip: Before responding to a donation request, research the organization at sites such as Charity Navigator (https://www.charitynavigator.org/) and Give.org (http://give.org/). If you make a donation, use a credit card—never cash.

Military benefits schemes: A veteran is offered a cash buyout of his or her future pension or disability benefits, or is persuaded to take out a pension advance loan at an exorbitant cost with unaffordable payments. In other cases, the veteran is persuaded to put his or her assets into an annuity or trust so that they will qualify for the Aid & Attendance Benefit, reserved for those with few liquid assets. The veteran ends up paying high fees for the advice and financial products, and also jeopardizes their eligibility for Medicaid, loses access to their money for a long time or has to repay the benefits after an investigation.
Tip: Don't take a buyout of or borrow against your VA pension or other benefits, move your assets around to qualify for benefits, or pay someone to file a claim. Call the U.S. Department of Veterans Affairs (VA) National Pension Hotline at 877-294-6380 to speak to a counselor about any investment or other pitch that requires you to pay for it out of your pension or sign over your benefits. Learn more at the FTC's "Pension Advances: Not So Fast" webpage (https://www.consumer.ftc.gov/articles/0513-pension-advances-not-so-fast). The VA also warns against working with anyone who tries to persuade you to move assets around or who charges you for help filing a claim for pension or Aid & Attendance benefits (https://www.benefits.va.gov/PENSION/Pensionprograminfo.pdf). Learn more at the Federal Trade Commission's "Veterans' Pensions" webpage (https://www.consumer.ftc.gov/articles/0349-veterans-pensions).

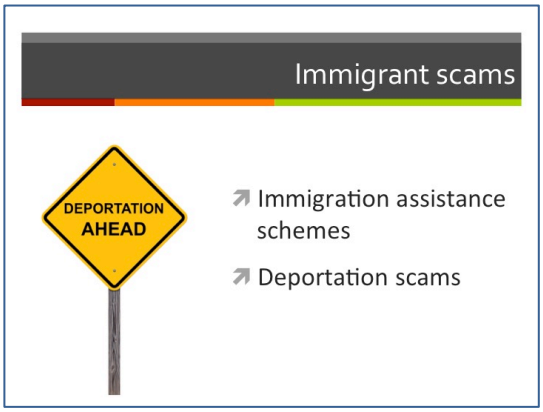
VA records/assistance scams: Someone attempts to charge you for military records that are available free or at a low cost directly through the VA or other agency. Or, they offer to assist you with filing for your VA benefits, for a fee.
Tip: Contact the VA or your service unit directly to request application forms or copies of the records you need, or visit https://www.archives.gov/. People accredited through the VA to provide assistance are not allowed to charge you for help completing and submitting VA paperwork. Find an adviser using the VA's online search tool (https://www.va.gov/ogc/apps/accreditation/index.asp) or contact your state Veterans Affairs office (https://www.va.gov/statedva.htm).

GI Bill schemes: Recruiters convince you to use your GI Bill benefits at their shady, sub-par for-profit school, and maybe even to take out expensive private student loans to cover the rest of the tuition and expenses. In other cases, you are enrolled in a low-cost correspondence course (rather than a traditional school) that isn't even covered by the GI Bill.
Tip: Before choosing a school or training program, visit the Know Before You Enroll website (http://knowbeforeyouenroll.org/). Consumer Action's *A Guide to Finding the Right Job Training School* (https://www.consumer-action.org/modules/articles/job_training_schools) presents the pros and cons of different education options and helps you vet schools and job training programs.

VA phishing attempts: Someone contacts you claiming to be with the VA and says that your personal data is needed to "update" your records, be considered for a job (through the Vets.gov career site), proceed with a benefits claim or for some other reason. Once you give up your information, the scammer steals your money or your identity.
Tip: The VA and related agencies will never ask you for your sensitive data by phone or email. If you get a call or message that you think might be legitimate, call the VA (800-827-1000), agency or business directly to verify.

→SLIDE #9

Go over slide notes.



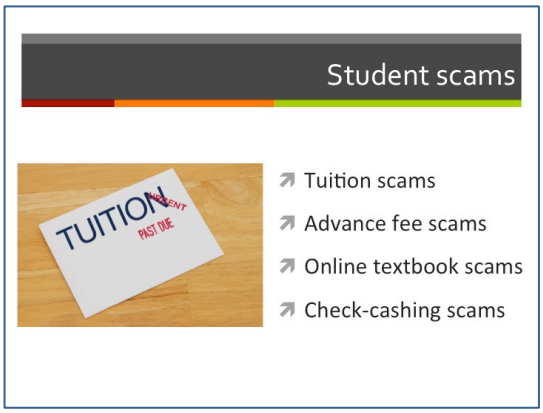
Slide notes:
The vast majority of scams targeting immigrants in the U.S. use either the promise of achieving the prey's desired immigration status or the threat of deportation to persuade him or her to give the scammer money or disclose personal information. These schemes have become more widespread as the U.S. political climate has changed and it has become easier to exploit immigrants' fears. In such an environment, it's important to verify claims and get assistance from qualified agencies and individuals. These are some of the most common types of scams perpetrated against immigrants.

Immigration assistance schemes: Someone claiming to have special expertise or influence charges you for help applying for a visa, renewing a green card, applying for citizenship, etc. In most cases, the fee is unnecessary because free assistance is available. In many cases, the "service" is worthless and may even do more harm than good. In some cases, the perpetrator takes your money and does nothing at all.
Tip: In the U.S., *notarios* are not lawyers and are not authorized to provide any legal services related to immigration. Get immigration assistance only from people authorized to provide it. Find an authorized immigration service provider at the U.S. Citizenship and Immigration Service (USCIS) website (https://www.uscis.gov/avoid-scams/find-legal-services). Get free forms at www.uscis.gov/forms or 800-870-3676, or visit a local U.S. Citizenship and Immigration Services (USCIS) office (https://www.uscis.gov/about-us/find-uscis-office/field-offices). USCIS will never ask you to pay an individual, wire money via Western Union, use PayPal for immigration fees or email you about receiving a visa. Get more tips from the USCIS (https://www.uscis.gov/avoid-scams) and the FTC (https://www.consumer.ftc.gov/articles/0141-scams-against-immigrants).

Deportation scams: The scammer threatens to arrest or deport you or your family members if you don't pay a fee. Sometimes he or she impersonates an immigration official or Homeland Security officer, other times a debt collector or the IRS—anyone who can make the threat of deportation convincing.
Tip: Immigration, Homeland Security and other agency officials will not call you, threaten you, demand payment or ask you to confirm personal information (such as passport number) that they should already have. If you believe a call or other communication could be legitimate, call back using the contact number you were given at the time of your visa application. Or find it on the legitimate agency's website.

→SLIDE #10

Go over slide notes.



Slide notes: Students can be attractive targets for scammers because they are easy to find (college campuses), have some money (from parents, student loans, part-time jobs, etc.), are away from home for the first time (so not under parents' watchful eyes) and are probably inexperienced with money management. The best protection for college students is to learn, before heading off to school, how to recognize and avoid scams.

Tuition scams: Someone claiming to be from the college registrar or other school office contacts you to say that your tuition is late and you'll be dropped from your classes if you don't make a payment immediately.
Tip: Contact the office the caller claims to represent at a number you find yourself and know is legitimate and ask what the status of your account is. If the original contact was legitimate, you can pay the office when you contact them.

Advance fee scams: Someone contacts you offering help to get a scholarship, complete your FAFSA (Free Application for Federal Student Aid) or get an internship. You pay the scammer's fee upfront but don't get the help or results you expected.
Tip: You can do all these things yourself at no cost (it's not called a **"**Free**"** Application for Federal Student Aid for nothing). However, if you are interested in paying for assistance or guidance, do some research on the company or individual first—verify legitimacy, check customer satisfaction ratings, compare prices, etc.—and get guidance from a counselor at the school you are, or will be, attending.

Online textbook scams: A website offers textbooks at "unbeatable" prices, but the books you order never arrive.
Tip: Don't do business with an online retailer until you have verified that the website and merchant are legitimate. Check online reviews and ratings, and ask around to find out if other students at your school have had a good experience. If you do buy, use a credit card so that you have recourse if your order is not fulfilled or the items you receive were misrepresented.

Check-cashing scams: Similar in most ways to other counterfeit check scams, this one is carried out by someone posing as a fellow student, perhaps claiming to have lost their ID/debit card or not having an account established yet. The scammer offers to let you keep a portion of the check in exchange for your cashing it. Their check later bounces and you're out the cash you gave them plus a returned check fee.
Tip: Simply don't deposit or cash a check from someone you don't know and trust.

PROTECTING YOURSELF FROM SCAMS (10 minutes)

Learning objective: Understand how to use the internet, publications and other consumer resources to recognize and avoid scams.

Key points (slides 11-13):

- The internet is a strong tool for identifying and avoiding scams.
- There are free publications that expose specific scams and help consumers develop the ability to spot a potential scam.
- There are a handful of practices that consumers can employ to avoid being scammed.

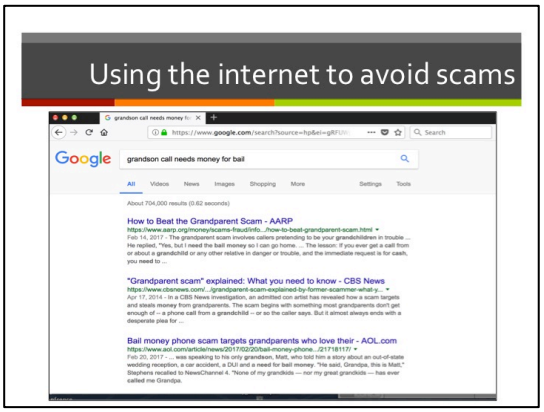
Questions to generate discussion:

- How do you use the internet to vet professionals, research products and services, check the validity of claims, etc.? How has the internet helped you make wise choices and avoid bad ones?
- What are some options for online research for someone who doesn't have access to the internet at home?
- Do you subscribe to any e-newsletters that help you stay abreast of the latest scams? If so, which ones? What do you like about them?

→SLIDE #11

Introduction: The internet has helped to level the playing field for consumers who used to be unable to verify a scammer's identity or story. Put to its full use, the internet can help foil a scammer's attempt to trick you out of your money or information.

Go over slide notes.



Slide notes: While the internet is the tool of choice for many scammers, it is also a strong tool for identifying and avoiding scams. Within minutes, a consumer with access to the internet can research an individual or company; verify a URL, phone number or address; check reviews and ratings; compare prices; and determine if a communication is questionable. Here are some ways to use the internet to protect yourself.

Check the validity of a threat, offer, claim or story. A simple online search can reveal a scam. For example, the two top search results for "grandson call needs money for bail" are "How to Beat the Grandparent Scam – AARP" and "'Grandparent scam' explained: What you need to know – CBS News." Do this type of search, using at least a couple of different combinations of key words, whenever you need to verify what a potential scammer tells you.

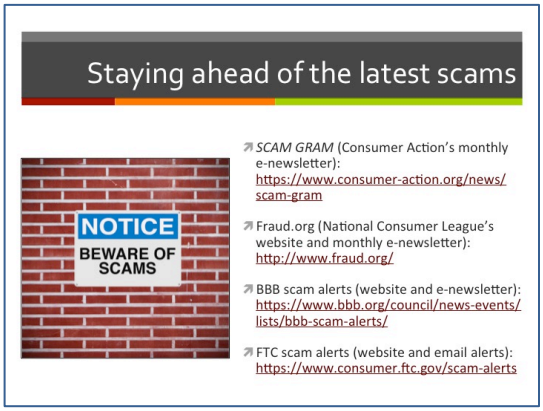
Research an individual or company. Type a name into the search bar of your browser and see what comes up (try it both with quotes around the name and without). Continue to dig until you are satisfied. If there are no results for your search, that could be a red flag that the individual or company name is made up. If you find the company or individual's website, check it for professionalism. Typos, fuzzy images, stock photos, missing information and limited pages (no privacy policy, terms of use, etc.) can be a sign that the site was put together hastily, perhaps because it is a scam. Check the site's registration data—the name under which the website was registered and when it was created—at WhoIs.net (www.whois.net). Learn more about checking a domain's registration at https://www.wikihow.com/Find-Out-Who-Registered-a-Domain.

Verify a company's web address, physical address and phone number. Rather than trust the contact information you are given by a possible scammer, find it online, at the company or agency's legitimate website. Be sure you have spelled the name correctly—misspellings can take you to spoofed (fake) sites. Check the URL of the site you visit to be sure it isn't an adulterated version of the correct address (for example, www.microsofthelp.com or www.micosoft.com instead of the correct www.microsoft.com).

Check ratings and reviews. Do a search for the name of the company or individual along with the word "ratings" or "reviews" to see what customers and complaint handling and rating services (such as the Better Business Bureau) have to say. Check Facebook to see if the company has a page and if there are customer comments on it. If a company doesn't have any online reviews or ratings, or if they are all glowing, you might be dealing with a scam. Learn how to recognize fake reviews from Money (http://time.com/money/4095258/fake-online-reviews-yelp-amazon-tripadvisor/) and How-To Geek (https://www.howtogeek.com/282802/how-to-spot-fake-reviews-on-amazon-yelp-and-other-sites/).

→SLIDE #12

Go over slide notes.



Slide notes: Scammers always seem to find new ways to find and trick their prey. Even consumers who consider themselves savvy can be caught off guard by a new twist on an old scam. The best way to avoid getting conned is to be aware of the latest scams making the rounds. That's easy to do thanks to a handful of newsletters and email alerts sent regularly by consumer protection groups and agencies to subscribers.

SCAM GRAM newsletter: SCAM GRAM is Consumer Action's monthly email alerting you to the dirtiest players in the world of tech fraud, credit card scams, ID theft and general con-artistry.

Sign up to receive the SCAM GRAM each month in your inbox (https://www.consumer-action.org/news/scam-gram).

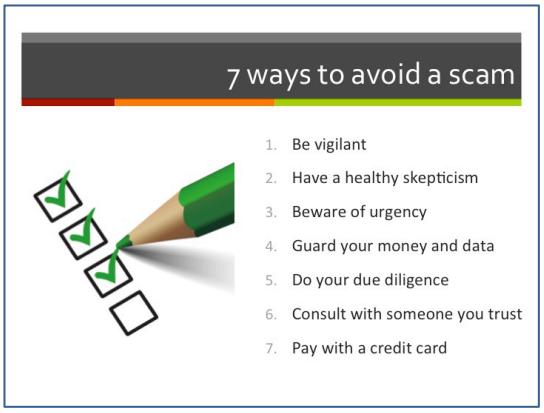
Fraud.org fraud alerts: Stay ahead of trending scams by signing up for Fraud.org monthly fraud alerts (http://www.fraud.org/). You can also visit the website anytime to read about the latest tricks and tactics (http://www.fraud.org/alerts).

Better Business Bureau (BBB) scam alerts: As the go-to for complaints against businesses, the BBB knows a thing or two about scams. The organization's Scam Tracker allows you to report a scam and read about other consumers' reported scams, all with the goal of foiling future attempts (https://www.bbb.org/scamtracker/us/).

Federal Trade Commission (FTC) scam alerts: Stay a step ahead with the latest information and practical tips from the nation's consumer protection agency. Browse FTC scam alerts by topic or by most recent (https://www.consumer.ftc.gov/scam-alerts), or sign up to have them sent directly to your inbox.

→SLIDE #13

Go over slide notes.



Slide notes:

1. *Be vigilant.* There are scammers and shady businesses around every corner, just waiting for their next victim. Keep your guard up.
2. *Maintain a healthy level of skepticism.* Scrutinize all unsolicited communications. If it sounds too good to be true, it almost certainly is.
3. *Beware of urgency.* Being rushed usually means someone doesn't want to give you time to do some research and make an informed decision.
4. *Guard your money and data.* If someone you don't know unexpectedly asks you for money or personal information, ignore them. Verify requests that might be legitimate *before* you act.
5. *Do your due diligence.* The internet is a great vetting tool. Use it to verify stories, names, phone numbers and other information you are given.
6. *Consult with someone you trust.* When faced with a request (or demand) for money, personal information or access, get a second opinion from someone savvy and trustworthy.
7. *Pay with a credit card.* While other types of payment cards offer some protections, credit cards offer the strongest consumer protections under federal law—the right to dispute a fraudulent transaction, for example, and a $50 limit on your liability for unauthorized charges—and payments are traceable.

"BAD ACTORS" EXERCISE (20 minutes)

Follow the instructions for this role-play exercise on page 23 of the lesson plan. Ask for volunteers to act out the scenarios. (Instructor's notes are on page 24.)

REPORTING A SCAM (10 minutes)

Learning objective: Know where to report various types of scams.

Key point (slide 14):

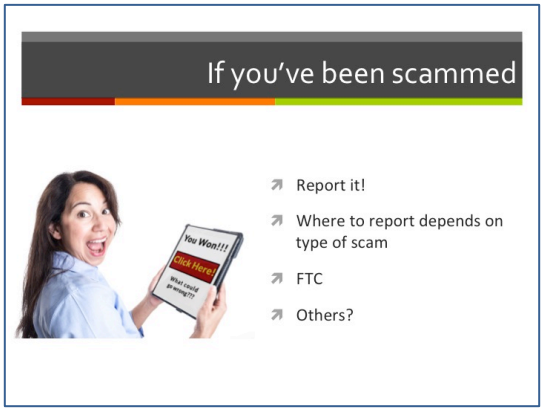
- If you are the victim of a scam, you should report it to one or more of the many agencies that accept consumer scam complaints.

Questions to generate discussion:

- Why go to the trouble of reporting a scam? What are some possible outcomes?
- Have you ever reported a scam? Were you satisfied with the outcome?

→SLIDE #14

Go over slide notes.



Slide notes: If you are the victim of a scam, you should report it. Where to report it depends on the type of scam. In virtually all cases, you should notify the Federal Trade Commission (https://www.ftccomplaintassistant.gov). The FTC collects information about current scams and frauds and directs it to law enforcement officials.

In most cases, you should also report it to your state attorney general (http://www.naag.org/). If the scam was a local job, notify your district attorney's office (https://www.usa.gov/state-consumer) as well. If you need a police report, contact local law enforcement.

If the scam was perpetrated via the internet, report it to the Internet Crime Complaint Center (IC3), an interagency website run by the National White Collar Crime Center and the FBI (https://www.ic3.gov/complaint/default.aspx).

If you believe it was an international scam, you can report it to eConsumer.gov (www.econsumer.gov), a site run by the International Consumer Protection and Enforcement Network (ICPEN), which is a partnership of 34 consumer protection agencies around the world.

If you received a scam letter or a fake check in the mail, report it to the United States Postal Inspection Service (https://ehome.uspis.gov/fcsexternal/default.aspx or 800-ASK-USPS).

IRS-related phishing attempts and other types of tax-related fraud should be reported to the Treasury Inspector General for Tax Administration (TIGTA) (https://www.treasury.gov/tigta/contact_report_scam.shtml or 800-366-4484).

If you are the victim of investment fraud, report it to one or more of the agencies that regulate the investment industry. This might include the Securities and Exchange Commission (www.sec.gov/complaint/select.shtml or 800-SEC-0330) and/or your state securities regulator (http://www.nasaa.org/about-us/contact-us/contact-your-regulator/). For reporting tips and additional contact information, visit the "Reporting Investment Fraud" page of SaveAndInvest.org (https://www.saveandinvest.org/protect-your-money-report-fraud/reporting-investment-fraud).

If the fraud was related to Medicare or Medicaid, visit the Centers for Medicare & Medicaid Services "Reporting Fraud" webpage for contact information: https://www.cms.gov/About-CMS/Components/CPI/CPIReportingFraud. If you received a suspicious call from someone alleging to be from the Social Security Administration (SSA), report it to the Office of the Inspector General (https://oig.ssa.gov/report or 800-269-0271).

Report credit and loan-related frauds, as well as scams related to money transfers, credit reports and other financial services, to the Consumer Financial Protection Bureau (https://www.consumerfinance.gov/complaint/ or 855-411-2372). Find out where else to report different types of financial scams at the "Complaints About Banks and Lenders" page of USA.gov (https://www.usa.gov/complaints-lender). For tips on reporting mortgage and lending fraud, visit the

"Reporting Mortgage and Lending Fraud" page of SaveAndInvest.org (https://www.saveandinvest.org/protect-your-money-report-fraud/reporting-mortgage-and-lending-fraud).

Notify your wireless service provider and/or your internet service provider of scam text, email and phone messages.

If you paid a scammer by credit card, dispute the charge with your card issuer. Contact your bank if you paid by debit card to see if you can stop payment or dispute the transaction. If you paid by prepaid card or gift card, contact the card issuer to find out if you have any recourse. If you paid via a third-party payment intermediary, such as PayPal or eBay, contact the company to see if you can dispute the transaction. If you paid the scammer via Western Union, call the company's fraud hotline (800-448-1492). If you used a different money transfer service, check its website for fraud reporting contact information.

If you're an identity theft victim, visit IdentityTheft.gov (www.identitytheft.gov) to report the theft and create a recovery plan (which will include placing a fraud alert on your credit reports and receiving a free copy from each of the three major credit reporting agencies).

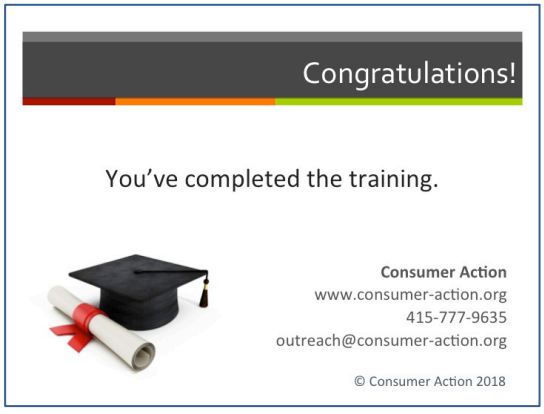
If you have low income and are the victim of a home equity, investment or similar financial scam, find local legal aid through the Legal Services Corporation website (https://www.lsc.gov/what-legal-aid/find-legal-aid). If you don't meet income guidelines, you can contact the National Association of Consumer Advocates (NACA) (https://www.consumeradvocates.org/) or a local bar association to find an attorney (https://www.americanbar.org/groups/legal_services/flh-home/flh-bar-directories-and-lawyer-finders.html).

QUESTIONS AND ANSWERS (10 minutes)

Preparation: Review the module publications. Open the floor to questions.

WRAP-UP AND EVALUATION (5 minutes)

→SLIDE #15



See page 25 of this lesson plan for the course evaluation form and instructions.

Thank participants for attending. Ask them to take a few minutes to fill out the evaluation form that is in their folders and leave it in a large envelope you provide or face down on a table at the front or back of the room. If you will be conducting other trainings at a future time, announce that now.

Gone phishing! (exercise)

Fill in the blanks from the choices at the bottom of the page to complete the following statements.

1) _____ is one of the oldest and most widely used methods of scammers to get you to reveal sensitive information that can be used to steal your money, identity or security.

2) Scammers will often use a promise or a _____ to get you to act.

3) Phishers _____ a legitimate business, government agency or other trusted individual or entity.

4) A _____ website looks legitimate but is created by a scammer to steal your information.

5) Phishers create _____ so that you respond before verifying or consulting someone.

6) You can't trust _____ or an _____.

7) In addition to email, phone and text, phishing messages are sometimes delivered via _____.

8) _____ is designed to encrypt your files so that you lose access to them unless you agree to pay the scammer.

9) Among other things, malware can steal your _____.

10) _____ refers to a fraudster installing malicious code on your computer that redirects you to a fraudulent website without your knowledge.

11) Don't click _____ or open _____ from unknown and unverified sources.

12) If you are asked for payment via a _____, it could be a scam.

13) _____ and bad _____ often are signs of a scam.

14) Financial institutions and other businesses will never ask you to disclose your _____.

15) If a federal agency _____ you unexpectedly, it might be a scam.

16) In addition to reporting phishing attempts to the company, agency or organization impersonated in the message, forward phishing emails to the _____, and file a complaint with the _____.

caller ID	links	threat	spoofed	gift card
credit card	urgency	social media	attachments	pharming
impersonate	password	email "From" field	phishing	FTC
typos	email "To" field	grammar	calls	friendly fraud
account number	ransomware	IC3	FCBA	contacts

Answer key: Gone phishing!

The correct answer is in bold, with details about the answer in italics at the end of the statement.

1) **Phishing** is one of the oldest and most widely used methods of scammers to get you to reveal sensitive information that can be used to steal your money, identity or security. *(In fact, phishing plays a role in many different scams. Recognizing and avoiding phishing attempts is key to protecting yourself.)*

2) Scammers will often use a promise or a **threat** to get you to act. *(With phishing, you're typically promised something enticing or threatened with an unwelcome consequence.)*

3) Phishers **impersonate** a legitimate business, government agency or other trusted individual or entity. *(By pretending to be a legitimate business, government agency or other trusted individual or entity, the scammer creates a believable situation where there is a need for your Social Security number, account number, password, birthdate or other sensitive personal information.)*

4) A **spoofed** website looks legitimate but is created by a scammer to steal your information. *(The legitimate-looking website tricks you into believing that the information you enter is secure.)*

5) Phishers create **urgency** so that you respond before verifying or consulting someone. (*Scammers know that if you have time to think, verify or consult someone, you will most likely realize it's a scam.)*

6) You can't trust **caller ID** or an **email "From" field**. *(Scammers routinely rig caller ID so that it looks like the call is coming from a recognized business, agency or neighbor, and they often forge the "From" address in email to look like it's from a trustworthy source.)*

7) In addition to email, phone and text, phishing messages are sometimes delivered via **social media**. *(Phishing messages can come via email, phone, text message or social media.)*

8) **Ransomware** is designed to encrypt your files so that you lose access to them unless you agree to pay the scammer. *(To avoid being at a scammers mercy, back up your files regularly and store important files—photos, etc.—in the cloud.)*

9) Among other things, malware can steal your **contacts**. *(Depending on the type of malware used, it could allow the scammer to access your files, track your online activity, record your keystrokes or steal your contacts. That's why you have to be wary even of messages sent to you by people you know; they could have had their contacts list stolen by a scammer.)*

10) **Pharming** refers to a fraudster installing malicious code on your computer that redirects you to a fraudulent website without your knowledge. *(If the website looks different from the last time you visited or its appearance is in any way "off," leave without entering any sensitive information.)*

11) Don't click **links** or open **attachments** from unknown and unverified sources. *(Links can take you to spoofed sites, and attachments can be infected with malware. Be cautious even with links and attachments sent from friends and other familiar sources, whose email address or contact list could have been hijacked.)*

12) If you are asked for payment via a **gift card**, it could be a scam. *(Scammers typically request payment in a form that is untraceable or difficult to cancel or recover, such as a wire transfer or a gift or prepaid card.)*

13) **Typos** and bad **grammar** often are signs of a scam. *(Typos, unusual capitalization, non-native English use, bad grammar and other errors in a communication supposedly coming from a well-known business or agency are an indication that it's probably coming from a scammer.)*

14) Financial institutions and other businesses will never ask you to disclose your **password**. *(If anyone asks for your password, beware.)*

15) If a federal agency **calls** you unexpectedly, it might be a scam. *(Federal agencies will rarely call you or ask you to confirm personal information by phone, and then typically only regarding a matter you're already aware of.)*

16) In addition to reporting phishing attempts to the company, agency or organization impersonated in the message, forward phishing emails to the **FTC**, and file a complaint with the **IC3**. *(Report phishing attempts to the company, agency or organization impersonated in the message. Also forward phishing emails to the Federal Trade Commission (FTC), and file a complaint with the Internet Crime Complaint Center (IC3).)*

Bad actors (exercise)

This exercise—named "Bad actors" in reference to the scammers portrayed—calls on participants to act out scam scenarios and critique the targeted consumer's response.

Each scenario requires at least two actors: the scammer and the consumer. If there are enough volunteers, two different actors can play the consumer, one acting out the wrong response and the other acting out the right one. The same actors can act out all the scenarios, or you can use different actors for each.

Provide the scenarios to the actor(s) playing the scammer. The scammer should make it a "hard sell." First, run through the scenario with the consumer falling for the scam. Then ask the non-acting participants what the consumer did wrong, what the red flags were, and what he or she should have done differently. Then have the actors run through the scenario a second time, this time with the consumer successfully evading the scam attempt. (Note: Use the "Common Scams" publication to create scenarios around other types of scams if they are more relevant to your group than the following options.)

1) The scammer, impersonating an IRS agent, calls and tells the taxpayer that s/he needs to verify his/her Social Security number and bank account information before the agency can process the taxpayer's refund.

2) The caller (scammer, or actual debt collector?), who appears to have some accurate details about the consumer and the debt, says the consumer owes $1,000 on a past-due medical bill and will be arrested if the payment isn't wired immediately.

3) In response to an eBay posting, the scammer meets with the seller of some Star Wars collectibles to purchase the set for $225 in cash on a Sunday morning. The scammer arrives at the meeting with a prewritten check for $275, saying s/he couldn't get cash because s/he lost his/her debit card and, since it's a Sunday, can't go into a branch. The scammer apologizes for the error, and says that the seller should give back $25 of the extra $50 and keep the other $25 "for your trouble."

4) The scammer, posing as a tech support agent, calls the consumer and says that the company has detected a virus on his/her computer but, fortunately, can fix it, either by being given remote access to the computer or by selling the required antivirus software download.

5) The scammer, pretending to be the target's grandchild (and explaining that his/her different voice is due to a broken nose), says that s/he caused an accident while in Mexico for spring break and needs $500 bail money because of the DUI charge. The scammer gives the grandparent the wiring instructions and implores him/her not to let any other family members know.

6) A "fundraiser" appears at the door asking for a donation in support of an organization or cause that appeals to the consumer. S/he explains that the organization doesn't take credit card donations because the charity wants to keep expenses low (i.e., they don't want to pay credit card transaction fees), but they *will* gladly take cash donations.

7) The representative of a "financial services" company encourages a veteran to allow the company to help him/her transfer assets into a trust, which will qualify him/her for the VA's Aid & Attendance benefit (for very low-income vets), worth about $2,000 per month. There is, of course, a "reasonable" fee for the financial advice, the establishment of the trust, and the transfer transaction.

Answer key: Bad Actors

The following are notes about each scenario that you can use to guide participants' advice to the actors, if necessary.

1) Statistically, most people file their tax return by the April due date, and most taxpayers get a refund, so scammers calling in March, April and May have good odds of reaching people who have already filed and are expecting a return—don't assume that if the caller gets that right, s/he is from the IRS. Also, the IRS will always contact you by mail first. If you haven't received a letter, be suspicious of a call or other communication claiming to be from the agency. And be suspicious if the person asks for personal data such as your Social Security or other account number, or your PIN or password. The taxpayer should hang up on the call. If s/he is concerned that it could be legitimate, s/he should call the U.S. Treasury Inspector General for Tax Administration (TIGTA) at 800-366-4484 to verify.

2) The consumer is faced with two issues: determining whether the caller is an imposter or a legitimate debt collector and, if a legitimate collector, how to proceed with the call. The fact that the caller knows that the consumer owes $1,000 on a past-due medical bill and has other accurate details about him/her and the debt doesn't make the call legitimate. That information could have been gotten from a stolen/hacked credit report. One red flag that the caller is a scammer is the threat of arrest if payment isn't made immediately (illegal under the Fair Debt Collection Practices Act). Another red flag is the specification to wire the money. Even if the caller is a legitimate debt collector, the debt might not be valid, so the consumer shouldn't discuss it or agree to pay anything without first receiving a mailed "validation notice."

3) Online sellers always have to beware of scammers. In this case, the scammer plans to take the merchandise as well as the $25 in cash that the seller hands over, leaving the seller without his/her merchandise ***or*** the money due for the purchase (when the check bounces), out an additional $25 in cash, and responsible for the non-sufficient funds (NSF) fee the bank will charge for the returned check. The seller, when faced with a check rather than the required cash, should call off the deal and walk away.

4) The consumer should assume that any unexpected call claiming to be aware of his/her computer problems is a scam and hang up.

5) As with other scams carried out by a caller demanding immediate payment, recipients should just hang up. If the grandparent is concerned about the person who is supposedly in trouble and in need of money, s/he should try to contact him or her directly, or verify with another family member or anyone else likely to know if the story is true (even if the scammer says not to).

6) The consumer should either say no or, if genuinely interested, ask for literature about the organization so that s/he can research it online through sites such as Charity Navigator (https://www.charitynavigator.org/) and Give.org (http://give.org/). (It's not enough to simply go to the website address included in the literature—it could be a bogus charity that built a website to support the scam.) If the consumer decides to donate, s/he should only donate by credit card—they are accepted by established charities and provide strong consumer protections if the charity turns out to be bogus.

7) The VA warns against working with anyone who tries to persuade you to move assets around in order to qualify for the Aid & Attendance benefit. Doing so means you will end up paying high fees for the advice and financial products, and you might also jeopardize your eligibility for Medicaid, lose access to your money for a long time or have to repay the benefits after an investigation. Veterans should not respond to such ads and should say no to "advisers" who promote such schemes.

Training evaluation:
Just say no to scams

Please help us improve future presentations by giving us your opinion of today's class. Circle the response that best reflects your feelings about each statement.

1. I feel better prepared to recognize and avoid a scam attempt.

Strongly agree Agree Disagree Strongly disagree

2. I feel better able to help others protect themselves from scams.

Strongly agree Agree Disagree Strongly disagree

3. I have learned about new agencies and resources for learning about and reporting scams.

Strongly agree Agree Disagree Strongly disagree

4. The instructor was well informed.

Strongly agree Agree Disagree Strongly disagree

5. The materials I received are easy to read and understand.

Strongly agree Agree Disagree Strongly disagree

6. I would like to attend another class like this.

Strongly agree Agree Disagree Strongly disagree

On a scale of 1 to 10 (10 being the best), how would you rate the training? _____

Please let us know how we could improve future trainings (use back, if necessary):

_____

_____

_____

_____

Thank you for attending!