**Volunteer Instructor Guide**

**Cybersecurity Basics**

**Instructor Outline: Cybersecurity Basics**

This document is designed for the instructor to use alongside the PowerPoint presentation. It includes a course overview, talking points, and activity instructions. Please note the PowerPoint slide numbers to help keep you on track.

**Workshop Description**

This in-person or virtual workshop is for those interested in online safety, including keeping their accounts and identities safe and protecting themselves from fraudsters and scams. It will build participants’ confidence when visiting websites, using text messaging and email, talking on the phone, and playing online games.

**Curriculum Track**

Basics

**Audience**

Adults from newly connected households and/or who are looking to build basic skills and confidence using technology

**Workshop Length**

60 minutes

**Training Method**

Volunteer, instructor-led

**Purpose**

In this workshop, you will learn about cybersecurity, including how to keep your accounts and identity safe online and protect yourself from online fraud and scams. A primary objective of the workshop is for learners to increase confidence in their ability to engage online while staying safe from scams and fraud.

**Equipment Requirements**

* In person: Projector and projection screen; internet-connected computers for instructor; laser pointer (recommended).
* Virtual: A web conferencing platform; computers for instructor and participants with internet connections.

**Instructor Software Requirements**

Computer that includes:

* PowerPoint
* Web browser (optional)

**Material Requirements**

* Instructor PowerPoint: Before the workshop, review the slides and update the following information:
  + Slide 1: Update instructor name, instructor affiliation (for example, AT&T employee, library staff member, community volunteer, etc.), and location name.
  + Slide 2: Be prepared to briefly introduce yourself.
  + In addition to updating the slides, please preview the PowerPoint presentation display on the instructor station before the workshop to correct any minor formatting issues that may occur due to variations in devices, operating systems, and application versions.
  + Slide 102: Insert name and date of next workshop if one is being offered.
* Instructor Guide (this document): Review the Instructor Guide and familiarize yourself with the workshop materials. The script, which starts on page 5 of this document, is also included in the Notes field of the PowerPoint presentation. The script includes the following information:
  + Slide # and Slide Title
  + On Slide Text. The text displayed on the slide.
  + Notes Section
    - Talking Points. The information you share with the learners. Some slides also include instructions on actions the instructor needs to take to display or highlight information on the slide at the appropriate time.
    - Instructor Note.Includes notes the instructor can use to help facilitate group conversations, actions you should take, etc.
    - Additional Details: Identifies text on the slide that may need to be updated before the workshop begins.
* Learner Handout
  + **For in-person workshop:** Print handouts for each learner and provide them before the workshop begins.
  + **For virtual workshop:** Provide link to the Learner Handout, either before the workshop as part of the registration confirmation or include in the online platform’s chat feature.
* Learner Activity Sheet
  + **For in-person workshop:** Print handouts for each learner and distribute before the workshop begins.
* Certificate of Completion: For the in-person workshop, print a certificate to hand out to each learner once the workshop is completed. For virtual learners, send them an electronic copy by email.
* Learner Survey and Instructor Survey: Links and QR codes are included on the presentation and learner activity sheets.
* Learner Name Tags: If you want to easily identify learners, make sure to bring name tag stickers or table tents. (Optional but highly recommended)
* Notepaper, pens, or pencils. (Optional)

**Learning Objectives**

At the end of the session, learners will be able to:

* + How to create a strong account password.
  + List at least three
    - types of online scams they may encounter online.
    - ways they can recognize if something is an online scam.
    - organizations to contact to report a scam.

**Before the Workshop Begins**

* In person:
  + Make sure the instructor computer is turned on and the Instructor PowerPoint works.
  + Test and troubleshoot the instructor’s computer well before the course begins to ensure it meets the technical requirements of the workshop.
  + Place learner materials at each computer. Learner materials include the Learner Activity Sheet and Learner Handout. You may also include paper (for learners to take notes) and pens or pencils. (Important note: For a classroom setup, the instructor may need to print the Learner Survey for participants to complete and hand in at the end of the workshop. The instructor will be responsible for entering the surveys into [digitalliteracy.att.com/learnersurvey](https://digitalliteracy.att.com/learnersurvey)
  + If using name tags, make sure they are easily accessible to learners and that you provide a marker or pen for learners to write their names.
  + Keep a registration list so you can identify who attended.
  + Learners will follow along with the demonstration and answer collectively as a group. Learners can also use the Activity Sheet to write down their answers.
  + Identify a “parking lot,” a place to track questions to be answered later in the workshop. Some suggested places for a parking lot are a whiteboard, flip chart, or notepad. Encourage learners to note the slide number and section as they “park” questions.
  + Print a certificate to hand out to each learner once the workshop is completed.
* Virtual:
  + A few days before the workshop, send instructions to participants about how to connect to the workshop. If possible, you may want to create a short video or document with step-by-step instructions (with images) to provide a basic overview of how to use the web conferencing tool to share with your participants.
  + Before the workshop, email participants the Learner Handout. During the workshop, resend the link through the web conferencing chat tool.
  + Keep a registration list so you can identify who attended.
  + Identify a virtual “parking lot,” which is a place for participants to ask questions later in the workshop. For your virtual parking lot, you may want to use the chat feature or the question feature of the web conferencing tool. Encourage learners to note the slide number and section as they “park” questions.

**Assessment Technique(s)**

Objective: Successful completion of activities

Ways to measure and identify learner success:

* Engagement: Participation in group conversations.
* Check for Understanding: Check for verbal and non-verbal cues to ensure the learner’s understanding before beginning a new section. Check-ins occur on Slides 20, 21, 46, 48, 51, 55, 60, and 81.
* Formal Evaluation: The learner completes a survey. The QR code to access the survey is available on the Learner Activity Handout and Slide 103. You may wish to print out the survey and manually enter the responses after the workshop.

**Instructor Presentation**

**The following section will take you step by step through the PowerPoint presentation slides and notes section. While reviewing this part of the guide, we suggest you open the PowerPoint presentation so you can become more familiar with the slides.**

**You will need to edit multiple slides of the presentation. You can also remove or edit slides to customize the workshop to your specific goals and audience.**

**Slide Number & Title.** Slide 1: Cybersecurity Basics Workshop.

**On Slide Text:**

* Cybersecurity Basics
* Instructor Name
* Instructor Affiliation
* Location Name

**Notes Section**

**Talking Points:** none

**Instructor Note:**none

**Additional Details:** Before the workshop, please update this slide with the appropriate information:

* Instructor name
* Instructor affiliation (for example, AT&T employee, library staff, community volunteer, and so on)
* Location name

Before the workshop, please review the Instructor Outline. It provides guidance on what to do to prepare for the workshop, how to conduct the workshop, and what you should do once the workshop ends.

**Slide Number & Title.** Slide 2: Welcome, New Learners!

**On Slide Text:**

Welcome! Today’s workshop is provided by AT&T and the Public Library Association*.*

**Notes Section**

**Talking Points:** Welcome! Today’s workshop is provided by AT&T and the Public Library Association*.* My name is **<your name here>** and I am **<brief description of yourself>**. Before we get started, here are a few housekeeping items: [Mention the items that are relevant to your workshop.]

* Where are the restrooms?
* Where are the emergency exits?
* When/how to ask questions. Point to the page number located on each slide for participants to write down along with the question.
* If you have a cell phone with you, please make sure to either turn it off or set to silent.
* Will there be a break?
* If the workshop is virtual include instructions on how learners can mute and unmute themselves.

**Instructor Note:** Include a thank-you to community collaborator if applicable.

**Additional Details:** none

**Workshop Introduction**

**Slide Number & Title.** Slide 3: Workshop Content Outline—Agenda (3 mins.)

**On Slide Text:** Today’s Agenda

* Introduction
* What is cybersecurity?
* Skill Building
* How to create safe and secure accounts and passwords
* Learn about the most common types of scams
* How to recognize the warning signs
* What to do when you recognize a scam
* How to report a scam
* Tips and Tricks
* Practice

**Notes Section**

**Talking Points:** In this workshop, you will learn about cybersecurity—in other words, keeping your accounts and identity safe online. We’ll work on building skills and confidence to keep you safe online.

This will include creating safe and secure accounts and passwords, identifying the most common types of scams, recognizing the warning signs, knowing how to respond when you suspect something is a scam, and reporting a scam.

You’ll also learn Tips and Tricks to protect yourself and avoid scams. And, you will have opportunities to Practice what you’ve learned.

Let’s get started!

**Instructor Note:**none

**Additional Details:** none

**Talking Points, Topics, and Activities (85 mins.)**

**Introduction – What is Cybersecurity?**

**Slide Number & Title.** Slide 4: Introduction

**On Slide Text:** **Cybersecurity:**

Personal data is not accessible to others.

Devices work properly and are free from **malware.**

**Notes Section**

**Talking Points:** Today we are going to talk about how to use the internet safely. This is also called Cybersecurity. Cybersecurity is how we protect and keep safe —our identity, our personal data, and our financial assets— when we’re online.

For people like you and me, cybersecurity means that 1) your personal data is only accessible to you or others you authorize and safe from those we do not want to have access to it, and that 2) our devices—laptops, desktop computers, smartphones, tablets, and gaming devices — work properly, are secure and free from malware like viruses.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 5: What is Malware?

**On Slide Text:** What is Malware?

**Notes Section**

* Also known as malicious software
* It is a virus created to infect a computing device.
* It tracks your online activities.

**Talking Points:** Malware, short for malicious software, is a virus created to harm a computing device. It can take many shapes—from viruses that infect your favorite devices to spyware and adware that tracks your online activities.

Fraudsters and scammers use malware to steal sensitive information, such as your identity, money from your accounts, or other information you do not want to share with others. Use caution when downloading software or clicking on links from sources you do not know – it could be malware.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 6: Online Activities

**On Slide Text:**

**Talking Points:** You can do a lot of great things online. Examples include

* Connect with family and friends
* Listen to music
* Watch a tv show or movie
* Attend a class
* Learn a new skill
* Pay bills
* Check bank statements
* Find a recipe
* Figure out how to repair something

But sometimes we may not feel safe when doing these activities.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 7: Feeling Safe Online: Discussion

**On Slide Text:** Have you ever felt unsafe doing something online?

Why did you feel unsafe, and what did you do to protect yourself?

**Talking Points:** Have you ever felt unsafe doing something online? Why did you feel unsafe, and what did you do to protect yourself?  
  
Examples of why people could feel unsafe include:

* I did not know the sender
* They were trying to pressure me into acting now
* It did not seem like I could trust them.
* They wanted information I did not want to share e.g. credit card number, username and password, Social Security Number.

What did you do to protect yourself? Examples include:

* I deleted the email or text messages
* I hung up on the caller
* I closed my browser window
* I called a friend or family member for help

**Instructor Note:**Ask the questions on the slide of attendees, have them share their thoughts. Or, you can ask the question, allow a moment for the attendees to think about it, and then discuss.

The conversation should be approximately 2-3 minutes.

**Additional Details:** none

**Personal Accounts**

**Slide Number & Title.** Slide 8: Personal Accounts

**On Slide Text:** 

**Notes Section**

**Talking Points:** Many websites and mobile apps allow you to create a personal account. Your account has a unique username and password. You will use this username and password to sign into a website or mobile app. Then, you will have access to your individual account information.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 9:Personal Accounts: Discussion

**On Slide Text:** What kinds of online accounts have you created?

**Notes Section**

**Talking Points:**

Possible kinds of accounts that attendees may discuss: email, social media, job search sites, schools, banks, credit cards, media and news platforms, video streaming sites, retail sites.

**Instructor Notes:** Facilitate a brief discussion with participants. What kind of accounts have you created?

The conversation should be approximately 2-3 minutes.

**Additional Notes:** none

**Slide Number & Title.** Slide 10: Personal Accounts

**On Slide Text:** At a public transit station.

**Notes Section**

**Talking Points:** A personal account is essential for things like email, where you want to have your own account that’s private to you. Many websites and mobile apps offer or sometimes require a personal account to use them.

A primary reason to create a personal account is so you can keep track of what you do on a website or app—watch streaming videos, apply for jobs, track purchases, and more. Some features of websites are available only if you’ve logged into your account. With an online account, you can pay bills for things like phones, rent or mortgage, and utilities. An online account is critical for things like bank accounts and other financial accounts. Why? So only you can access them.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 11: Strong Passwords: Discussion

**On Slide Text:**How do you come up with a password?

How do you make it strong and secure?

**Notes Section**

**Talking Points:**Most personal accounts require that you create a password to ensure that only you have access to the information in the account.

Good answers. Let's learn more on how we can create strong passwords.

**Instructor Note:**Facilitate a brief discussion with attendees— “How do you come up with a password?” “How do you make it strong and secure?”The conversation should be approximately 2-3 minutes.

**Additional Details:**none

**Slide Number & Title.** Slide 12: Common Requirements

**On Slide Text:** Can usually include:

* Numbers
* Uppercase and lowercase letters
* Symbols, such as punctuation marks

**Notes Section**

**Talking Points:** Most websites and mobile apps include password requirements on their signup forms. These requirements are either listed underneath the form or will display on the screen when the password you create does not meet the requirements.

*INSTRUCTOR NOTE:* Click enter to see the items in the bulleted list.

Passwords can usually include numbers, uppercase and lowercase letters, and symbols such as punctuation. If your first try isn’t acceptable, review the website or application requirements. They try adding a capital letter number, or symbol, or making the password longer.

In this example, the password must be at least eight characters long, and must contain at least one uppercase letter, one lowercase letter, and one number.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 13: Tips for Strong Passwords

**On Slide Text:**

* Don’t use **common words** like “password”
* Don’t include **personal information**
* Don’t use the **same password** on multiple accounts and sites
* Don’t share with others—keep them **private**

**Notes Section**

**Talking Points:** What makes a strong password? Here are some Dos and Don’ts.

*INSTRUCTOR NOTE:* Press enter to see the first bullet

Avoid weak passwords like “password” (the most commonly used password!) or “123456.”

*INSTRUCTOR NOTE:* Press enter to see the second bulletDon’t include personal information, such as your address or name.

*INSTRUCTOR NOTE:* Press enter to see the third bullet

Don’t use the same password on multiple accounts and websites.

*INSTRUCTOR NOTE:* Press enter to see the fourth bullet

Don’t share your password with others. Passwords are the secret key that unlocks your account. They should be kept private.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 14: Tips for Strong Passwords: Longer and Phrases

**On Slide Text:**  Make the password longer. Use short phrases that are easier to remember. “cowshelpmakecheese”

**Notes Section**

**Talking Points:** Do make the password longer. The best defense is length.

*INSTRUCTOR NOTE:* Press Enter to see the first bullet

Longer passwords don’t need to be complex and hard to remember.

*INSTRUCTOR NOTE:* Press Enter to see the second bullet

But we can make a long, secure password that’s easier to remember by using short phrases. An example might be “Cows help make cheese.”

Remember, many websites have requirements for passwords. These requirements are usually listed underneath the password field or identified once you click on the password field. They may require you to include uppercase and lowercase letters, numbers, and symbols.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 15: Keeping Track of Passwords

**On Slide Text:** 

**Notes Section**

**Talking Points:** Now that we’ve discussed creating a strong password, let’s talk about how we can keep track of our passwords.

You may have created a lot of accounts on many websites or mobile apps. Your passwords may be different on each site—and it’s more secure if they are—so it can be a challenge to remember them.

Let’s look at a few different approaches we might take to remembering our passwords.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 16: Notebook

**On Slide Text:** Store in a safe place.Instead of writing the actual password, write down something that helps you remember which password it is.

**Notes Section**

**Talking Points:**You could write your passwords down in a notebook. If you do this, make sure to store the notebook in a safe and secure place.

*INSTRUCTOR NOTE:* Press Enter to see the Tip

Instead of writing the actual password, write down something that helps you remember which password it is.

**Instructor Note:**none

**Additional Details:**none

**Slide Number & Title.** Slide 17: Password Software

**On Slide Text:** 

**Notes Section**

**Talking Points:** You may choose to use a secure password management mobile app or website that can help keep track of your passwords. Most password managers are available with a paid subscription. These programs are usually unlocked with a single master password, which allows you to access all your passwords when you need them. The apps will also generate passwords for you that are complex combinations of letters, numbers, and special characters.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 18: Phrase

**On Slide Text:** You can make your passwords longer and stronger by using a phrase. Example: “Cows help make cheese.”

**Notes Section**

**Talking Points:** Phrase – soon this will be the standard. You can make your passwords longer and stronger by using a phrase. Example: “Cows help make cheese.”

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 19: Activity 1

**On Slide Text:** Activity #1

**Notes Section**

**Talking Points:** In this lesson, we learned how to create strong passwords to protect our online accounts. Let’s practice what we learned.

Remember we will be discussing your answers, so please DO NOT use any real passwords.

**Instructor Note:**Point attendees to Activity 1a and 1b on the Activity Sheet.

**Additional Details:** none

**Slide Number & Title.** Slide 20: Activity #1a: Account Sign Up

**On Slide Text:** Using the password requirements in the Sign Up form above, create a strong password that meets the criteria.

**Notes Section**

**Talking Points:** Using the password requirements in the Sign Up form in 1a of the Learner Activity Sheet, create a strong password that meets the criteria. Remember we will be discussing your answers, so please DO NOT use any real passwords.

**Instructor Note:**After the attendees have time to complete the activity, ask them about the passwords they created.

**Additional Details:** none

**Slide Number & Title**. Slide 21: Slide 20: Activity #1b

**On Slide Text:** Use the information from the course on strong passwords to discuss the participant responses. Examples:

1. happybirthday
2. josephsmith

Passwords should be at least 12 characters long and contain one uppercase letter, one lowercase letter, one number, and one special character.

Remember: Longer passwords are stronger passwords.

1. 1234567890
2. password1

Passwords should be at least 12 characters long with no other character requirements. To make this a strong password, use a short phrase.

Remember: Longer passwords are stronger passwords.

**Notes Section**

**Talking Points:** Use the information from the course on strong passwords to discuss the participant responses. Examples:

1. happybirthday – H@PPyBirthD@y$0$
2. josephsmith – 212Joe!Smith212

Criteria: Passwords should be at least 12 characters long and contain one uppercase letter, one lowercase letter, one number, and one special character.

1. 1234567890 – onetwobuckleymyshoe
2. password1 – keepmypasswordsafe

Criteria: Passwords should be at least 12 characters long with no other character requirements. To make this a strong password, use a short phrase.

Remember: Longer passwords are stronger passwords.

**After learners complete Activity 1:** Great job, everyone! Before we move to the next section, do you have any questions?

**Instructor Note:**Review and address items in the “parking lot”.

**Additional Details:** For information about what the parking lot is, see the “Before the Workshop Begins” section of the Instructor Guide.

**Online Scams: Phishing and Social Engineering**

**Slide Number & Title.** Slide 22: Online Scams

**On Slide Text:**

**Notes Section**

**Talking Points:**In the last lesson, we learned that creating strong passwords is one step you can take to protect your information online.

There are bad actors out there trying to access your personal information. Let’s look at some common scams you may encounter.

**Instructor Note:**none

**Additional Details:**none

**Slide Number & Title.** Slide 23:Online Scams

**On Slide Text:**Phishing, Social Engineering

**Notes Section**

**Talking Points:**Online scams can take many forms. The most common types include phishing and social engineering.

You may encounter these scams on a website, in an email, text message, or phone call, in an online game, or even in a pop-up window on your computer.

**Instructor Note:**

**Additional Details:**

**Slide Number & Title.** Slide 24:Phishing

**On Slide Text:** Emails, Text messages, Social media profiles, Websites, Phone Calls

**Notes Section**

**Talking Points:**Phishing occurs when fraudsters or scammers use fake emails, text messages, social media profiles, websites, or phone calls to fish for sensitive information like passwords, Social Security Numbers, credit card and bank account details, or personal data. The scammers can use this information to gain access to your money or steal your identity.

**Instructor Note:**none

**Additional Details:**none

**Slide Number & Title.** Slide 25: Phishing Scams

**On Slide Text:**

* Try to win your trust
* Claim to be from a real person or organization
* Ask for your personal and/or financial information
* Steal your money or identify

**Notes Section**

**Talking Points:** These messages can look real, but when you dig deeper, you find it’s fake. Phishing scams try to win your trust, by pretending to be a trusted person or organization. The fraudster wants you to share personal information about yourself that you would not normally share with a stranger. The fraudster then uses this personal information to gain access to your finances or steal your identity.

Let’s explore some examples of phishing scams that you may experience when using your smartphone, computer, or tablet.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 26:Email Scams

**On Slide Text:** 

**Notes Section**

**Talking Points:** You may receive an email that pretends to be from someone you know. In this example, the email says it is from your employer’s helpdesk and asks you to log into a website to update your password.

*INSTRUCTOR NOTE:* Press ENTER to display the spelling errors.

If you look closely, you will notice the email includes misspellings.

In this example, a fraudster pretends to work at the same organization to access personal information. If you had filled out the form, the fraudster could have used your account to access your employer’s systems.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 27:Text Message Scam

**On Slide Text:** 

**Notes Section**

**Talking Points:** Fraudsters also use text messages to scam you. In this example, it appears a state agency is sending an urgent text message asking you to pay an unpaid toll immediately.

Like the email phishing example, text message scams try to trick people into sharing personal information. States don’t send texts to ask for toll payments. If you had clicked to pay the bill, you may have unwittingly provided your financial information to a fraudster.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 28: Phone Call Scam

**On Slide Text:** Who am I talking to?

**Notes Section**

**Talking Points:** You may also receive phone calls pretending to be from an official organization, like a government agency, bank, or insurance company, to gain your trust and access to your personal information.

For example, you might receive a phone call from someone who says they work at your health insurance company. They then ask for your personal information and credit card information so they can send you a medical device. If you had provided the information, the fraudster would have had personal information and your credit card number.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 29:Phone Call Scam: Caller ID Spoofs

**On Slide Text:** Beware! You can’t trust your Caller ID. The call is not from Support. It is a scammer pretending to be Support.

**Notes Section**

**Talking Points:** Beware! You can’t trust your Caller ID. Fraudsters can spoof Caller ID to make it appear that a trusted organization is making the call, even when it isn't.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 30:Social Media Scam

**On Slide Text:** 

**Notes Section**

**Talking Points:** There are also scammers on social media platforms. They try to trick you into sharing personal information by pretending to be an individual or organization. One scam occurs after you complain about a product or service on social media. The next time you log into your social media account, someone claiming to be from the company contacts you and promises to resolve your issue. They then ask for your password so they can fix the problem. Companies should not need your password to fix a problem.

tap the link on the screen.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 31:Free Wi-Fi Scams

**On Slide Text:** iPhone and Android

**Notes Section**

**Talking Points:** Not all free Wi-Fi networks are safe and secure. When visiting a coffee shop, restaurant, or lobby, ensure you are using the organization’s secure Wi-Fi and not a fake network set up by a scammer. Connecting to an unofficial Wi-Fi network allows the scammer to see and track everything you do online. If you log into your bank account or credit card portal, the scammer can view your login details and potentially access your accounts.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 32:Survey and Online Quiz Phishing Scams

**On Slide Text:** Don’t share personal information with online surveys and quizzes, such as your SSN, answers you have used for account security questions, etc.

**Notes Section**

**Talking Points:** Beware of surveys and online quizzes found in online ads, social media, mobile games, email, or text messages. Fraudsters can use surveys and quizzes to gather sensitive information about you, which they can later use to steal your identity or gain access to your bank account or credit card information. Don’t provide your usernames, passwords, Social Security number, credit card details, answers you have used for account security questions, or any other personal information used to answer online security questions. While the promise of a gift certificate or the chance to win a vacation can be enticing, it’s not worth the potential harm of sharing personal information.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title.** Slide 33:Online Gaming Scams

**On Slide Text:** Malware is a virus created to damage your computer and steal sensitive information you don't want to share.

**Notes Section**

**Talking Points:** Fraudsters will also use online or mobile games to access personal information. When you create a gaming account or communicate with other players, do not share private information – fraudsters can exploit that information to attempt to steal your identity.

*INSTRUCTOR NOTE:* Press ENTER to display pop-up advertisement.

Pop-up advertisements may appear within the game to promote a new game or application. If you click on the ad you may install malware software onto your device. Malware shares your personal information with a fraudster.

*INSTRUCTOR NOTE:* Press ENTER to display malware definition.

Remember, malware is a virus created to harm a computing device. Fraudsters and scammers use malware to steal sensitive information, such as your identity, money from your accounts, or other information you do not want to share with others. Use caution when downloading software or clicking on links from sources you do not know.

**Instructor Note:**none

**Additional Details:** none.

**Slide Number & Title.** Slide 34:CAPTCHA Malware Scam

**On Slide Text:**

**Notes Section**

**Talking Points:** Another malware scam involves the CAPTCHA verification tool. A CAPTCHA is a checkbox or puzzle that websites use to verify that the person using the website is a human and not a bot. However, some bad actors now use fraudulent CAPTCHAs to install malware on your computer. It starts out working just like a real CAPTCHA. You visit a website and are asked to click a checkbox that you are not a robot, type the letters you see on the screen into the textbox or select all of the pictures that match the prompt. The scam begins after you complete the first step.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title.** Slide 35:CAPTCHA Malware Scam (continued)

**On Slide Text:**

**Notes Section**

**Talking Points:** Another screen appears asking you to take an additional step to verify you are a human. When you complete this task, like pressing the Windows Key + R on your keyboard, it will download malware onto your device and try to install it. Valid CAPTCHAs will not ask you to take additional steps that require downloading applications onto your device.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title.** Slide 36:Social Engineering

**On Slide Text:** A fraudster tries to gain your trust by convincing you that they are someone they are not, to get personal information from you.

**Notes Section**

**Talking Points:** Social engineering is another common type of scam. It’s a new name for an old con-artist trick. In this scam, a fraudster tries to gain your trust by convincing you that they are someone they are not, to get personal information from you.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title.** Slide 37:Social Engineering: List

**On Slide Text:**

* Claim to be a family member or friend in trouble
* Pretend to be a company with a great offer
* Claim to be working on behalf of the government, organization, or collections.

**Notes Section**

**Talking Points:** For example, the person may claim to be a friend or family member in trouble, pretend to be a company with a great discount or offer, or work on behalf of a government agency, organization, or collection agency. These fraudsters can approach you by phone, email, text, or social media.

Let’s explore some examples of social engineering.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title.** Slide 38:Family or Grandparent Emergency Scam

**On Slide Text:** Fraudsters may impersonate a family member, like a grandchild, claiming a fake emergency, and ask you to transfer money to them as soon as possible!

**Notes Section**

**Talking Points:** Fraudsters may impersonate a family member, like a grandchild, in urgent need, claiming a fake emergency such as bail, medical expenses, a car accident, or a stolen credit card, and ask you to transfer money to them as soon as possible!

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title.** Slide 39:Romance Scam

**On Slide Text:** Fraudsters create fake online profiles on social media or dating apps. Over time, the criminal gains your trust and will try to trick the victim into giving them money and sharing personal information.

**Notes Section**

**Talking Points:** Beware of romance scams. Fraudsters create fictional personas with fake online profiles on social media or dating apps. Over time, the criminal gains your trust only to take advantage of the relationship, tricking the victim into giving them money and sharing personal information.

**Slide Number & Title.** Slide 40:Sender Pretends to Be Someone You Know

**On Slide Text:** Fraudsters send you

* emails
* text messages
* social media messages

**pretending** to be someone you know, like

* A co-worker
* police officer
* delivery person
* government representative

**Notes Section**

**Talking Points:** You may also be contacted by email, text message, or on social media by a person pretending to be someone you know, like a co-worker, police officer, delivery person, or government representative.

This text message claims to come from US Customs but uses a fraudulent US Postal Service link to try to get personal information from you.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 41: Job Scams

**On Slide Text:** Fraudsters can also pose as employers who are hiring but are using the hiring process to scam job seekers. They use the hiring process to gain your personal information and bank account details.

**Notes Section**

**Talking Points:** Fraudsters can also pose as employers who are hiring but are actually using the hiring process to scam job seekers. For example, a potential employer reaches out about a job. After a few emails, they offer you the position and send paperwork that requires your personal information, such as your Social Security Number and bank account details. Once you submit this paperwork, you never hear from them again, and they now have your personal information.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 42: Job Scam: Upfront Payment

**On Slide Text:** The new job requires an upfront payment for training or equipment. The employer promises to reimburse you once you begin, but after they receive your money, you never hear from them again.

**Notes Section**

**Talking Points:** Another employment scam involves offering jobs that require an upfront payment for training or equipment. The employer promises to reimburse you once you begin, but after they receive your money, you never hear from them again.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 43: Gathering High Level Information

**On Slide Text:**  A fraudster

* Wants to target high-ranking people within an organization or influential people in a community.
* Contacts lower-level staff, friends, or associates to gather information.
* Seeks access to sensitive data, such as personal or company financial information, passwords, trade secrets, or other confidential information that could harm the person or the organization.

**Notes Section**

**Talking Points:** This type of scam typically targets high-ranking people within an organization or influential people in a community. A fraudster will begin by contacting lower level staff members at a company, or by contacting friends or associates of someone of influence. During the contact, the fraudster will attempt to lure sensitive data, such as personal or company financial information, passwords, trade secrets, or other confidential information that could harm the organization.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title.** Slide 44: Fraudster Goals

**On Slide Text:** Fraudster Goals.

* Steal your money
* Collect passwords, credit card numbers and more
* Infect your computer with viruses or malware.

They do this by...

* Trying to win your trust
* Claiming to be from a real person or organization
* Asking for your personal and/or financial information
* Stealing your money or identify

**Notes Section**

**Talking Points:** No matter what form a scam takes, fraudsters usually have the same goals: to steal your money or collect information like your passwords or credit card numbers. Scams can also cause problems for your computer by infecting it with viruses or malware. Let’s see what you remember about the scams we covered today.

*INSTRUCTOR NOTE:* Press ENTER to display the section *They do this by…*

Fraudsters do this by trying to win your trust, by pretending to be a trusted person or organization. The fraudster wants you to share personal information about yourself that you would not normally share with a stranger and then uses this personal information to gain access to your finances or steal your identity.

**Instructor Note:**none

**Additional Details:**none

**Slide Number & Title.** Slide 45: Activity #2: Fraudster Goals

**On Slide Text:** Activity 2

**Notes Section**

**Talking Points:** In this lesson, we learned about common types of fraud and scams, including phishing and social engineering. We learned that we may encounter these scams while browsing a website, receiving a phone call, in an email, text message, online game, or even in a pop-up window on your computer.

Let’s practice what we learned.

**Instructor Note:** Point attendees to Activity 2 on Activity Sheet page 2.

**Additional Details:** none

**Slide Number & Title.** Slide 46:Activity 2 Question

**On Slide Text:** What do scammers want? Select the correct answer.

* To collect passwords and credit card numbers.
* To sell your information to make money.
* To get you to visit a website or download a file
* To get you to transfer them money.
* All of the above

**Notes Section**

**Talking Points:**Read the question and answers, and ask the learners to call out the answer.

**Answer:** The correct answer is all of the above. Knowing what scammers want can help you protect yourself from fraud and keep your accounts and devices safe from online scams.

**After learners complete Activity 2:** Great job, everyone! Before we move to the next section, do you have any questions?

**Instructor Note:**Review and address items in the “parking lot”.

**Additional Note:** For information about what the parking lot is, see the “Before the Workshop Begins” section of the Instructor Guide.

**Tips to Recognize Scams**

**Slide Number & Title.** Slide 47:Tips to Recognize Scams

**On Slide Text:**

**Notes Section**

**Talking Points:** In the previous lesson, we learned about common types of fraud and scams, including phishing and social engineering.

So how can you tell if something is a scam or fraud? Here are some tips that will help you identify common scams you may encounter while browsing a website, receiving a phone call, in an email, text message, online game, or even in a pop-up window on your computer.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 48:Have You Heard of the Person or Organization

**On Slide Text:** Have you heard of the person or organization?

**Notes Section**

**Talking Points:** Have you heard of the person or organization? A legitimate business will have their official logo, address, and contact information posted on their website.​Other questions to ask yourself include, have you heard of this business? Is there a logo for the business? Is there contact information? ​

INSTRUCTOR NOTE: Ask participants if they can find the logo? Click Enter to highlight the logo.

INSTRUCTOR NOTE: Ask participants if they can find the address and contact information. Click Enter to highlight the answer.

In this example, we are using the Public Library Association website. This is a good example of a legitimate business website. ​

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 49:Can You Tell Who It’s From?

**On Slide Text**: Can you tell who it’s from? Should be @irs.gov

If you can’t see the sender’s address you can

1. roll over the email name
2. tap on the email name on a mobile device,

to see the sender’s email address.

**Notes Section**

**Talking Points:** Can you tell who it's from? This email claims to be from the IRS. But if you look closely, you will notice the address is not from @irs.gov and was sent from someone you do not know. This is a sure sign of a phishing scam.

*INSTRUCTOR NOTE:* Press ENTER to display the instructions in the orange box.

If you can’t see the actual email address from the sender, you can roll over the email name, or tap on the email name on a mobile device, to see the sender’s email address.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 50:Is the Organization Legitimate?

**On Slide Text:** Is the organization legitimate?

**Notes Section**

**Talking Points:** Is the organization legitimate? Use caution when you're contacted by a charity on the phone, text, email or online. To learn more about a charity asking for money, check the BBB Wise Giving Alliance website to see reports and ratings about how charitable organizations spend donations.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 51: Does the Email Look Professional?

**On Slide Text:** Does the email look professional?

**Notes Section**

**Talking Points:** Is the message professional? Does the email look professional or are there a lot of mistakes? Let’s see if we can find the mistakes.

*INSTRUCTOR NOTE:* Encourage the participants to identify the errors.

*INSTRUCTOR NOTE:* Click enter to highlight the errors.

* Albert’s name is misspelled.
* Instead of addressing the recipient by name they use Adorable Member. A company would not address someone that way.
* The word account is misspelled in different ways throughout the document.
* The words renewal and hear are also misspelled.
* The word proceeded should be processed.

If the email is from a legitimate business, it wouldn’t include those mistakes.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 52: Do They Claim They Can Fix Your Device?

**On Slide Text:** Do they claim they can fix your device?

**Notes Section**

**Talking Points:** Do they claim that they can fix your computer? When you are on a website or playing an online game, a pop-up message may display that claims your computer is infected and that you should click on a link or call a number to fix it.

Remember, legitimate companies will never ask you to fix your computer this way.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 53:Are They Asking for Money or Information?

**On Slide Text:** Are they asking for money or information?

**Notes Section**

**Talking Points:** Are they asking for your money or information? In this email, the fraudster is asking for his credit card information. Fraudsters may claim that they need to verify or update your information. Some fraudsters will also ask you to wire them money or send a deposit, promising to pay you more in return.

**Instructor Note:**none

**Additional Notes:** none

**Slide Number & Title.** Slide 54:Are They Trying to Rush You into Quick Action?

**On Slide Text:** Are they trying to rush you into quick action?

**Notes Section**

**Talking Points:** Are they trying to rush you into a quick action before you have time to think about it? This message is trying to get you to ACT NOW so you don’t lose your pharmacy points. Fraudsters try to scare you into acting fast, threatening that something bad will happen, like an account will be closed or you will lose all of your points if you don’t act now. Or something good will happen if you act now! Take the time you need to verify that it is true!

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 55:Is It Too Good to Be True?

**On Slide Text:** Is it too good to be true?

**Notes Section**

**Talking Points:** What sounds "too good to be true" in this example?

*INSTRUCTOR NOTE:* Encourage the participants to answer the question.

In this example, the recipient is being offered a $1000 gift card.

Remember, if it sounds too good to be true, it probably is.

**Instructor Note:**none

**Additional Notes:** none

**Slide Number & Title.** Slide 56:Are They Asking You to Keep a Secret?

**On Slide Text:** Are they asking you to keep a secret?

**Notes Section**

**Talking Points:** Is the sender asking you to keep it secret? In this text, a fraudster claims to be a family member who needs help and does not want their parents to know.

Another variation on this scam is that the person claims they are using a friend’s phone.

Scammers try to pressure you into sending money or information before you have time to check if the emergency is real. If someone you know says they are in trouble, contact them using the information you have, not the contact information or link from the person who reaches out to you.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 57:Are They Eager to Connect Romantically?

**On Slide Text:** Are they eager to connect romantically?

**Notes Section**

**Talking Points:** Has someone tried to connect with you romantically online? You may have met them on a dating app or your favorite social media platform. It starts slow, but over time, the conversation becomes more personal. Then they start asking for money or gifts, or they need help with an unexpected bill, or they would love to come see you, but they need you to pay for the plane ticket. Scammers create fake profiles using stolen photos to build personal relationships.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 58:Is This the Official Organization?

**On Slide Text:** Is it the official organization?

**Notes Section**

**Talking Points:** Are you working with the organization you thought you were? Some organizations will provide the goods or service you requested but will charge large service fees – fees that you would not have paid if you had purchased from the original provider.

You may encounter this when searching for a product or service online. If you click one of the Sponsored links in the search results or on the advertisement on a webpage, it may not be the official organization but a reseller who charges you additional fees you would not have paid if you paid the organization directly.

If you are not sure if the link is an advertisement, look for the word SPONSORED in your search results. Sponsored indicates the link in the result list is a paid advertisement.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 59:Activity #3

**On Slide Text:** Activity #3

**Notes Section**

**Talking Points:** In this lesson, we learned how to identify scams while browsing a website, receiving a phone call, in an email, text message, online game, or even in a pop-up window on your computer.

Let’s practice what we learned.

**Instructor Note:**Point attendees to Activity 3 on the Activity Sheet, page 3.

**Additional Details:** none

**Slide Number & Title.** Slide 60:Activity #3

**On Slide Text:** Activity #3: How can you tell if a text message is a scam?

* Tries to rush you into an action
* Asks you for your information
* Too good to be true
* All of the above

**Notes Section**

*INSTRUCTOR NOTE:* After the attendees have time to complete the activity, review the question and ask the learners to call out the correct answers.

**Answer:** The correct answer is all of the above. There are a variety of ways to determine if a text message, website or email is a scam. Knowing how to identify a scam can help you protect yourself from fraud and keep your accounts and devices safe.

**After learners complete Activity 3:** Great job, everyone! Before we move to the next section, do you have any questions?

**Instructor Note:** Review and address items in the “parking lot”.

**Additional Details:** For information about what the parking lot is, see the “Before the Workshop Begins” section of the Instructor Guide.

**Dos and Don’ts to Avoid Scams**

**Slide Number & Title**. Slide 61: Dos and Don’ts to Avoid Scams

**On Slide Text:**

**Talking Points:** In the previous lesson, we learned about common types of fraud and scams, including phishing and social engineering.

Now that we have learned how to recognize common frauds and scams, let's explore what you should and should not do when you encounter a scam on a website, in an email, text message, or phone call. These tips can also be found in the Learner Handout.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 62: Don’t Give Out Personal Information

**On Slide Text:** Don’t give out personal information.

**Talking Points:** Don’t give out personal information to something that could be a scam. This includes name, email address, credit card number, or password.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 63: Don’t Share Your PIN, Password, or Passcode

**On Slide Text:** Don’t share your PIN, password, or passcode.

**Talking Points:** Never share the PIN, passwords, or passcodes associated with your accounts.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 64: Don’t Give Them Money

**On Slide Text:** Don’t give them money.

**Talking Points:** Do not send money, gift cards, prepaid debit cards, or transfer money to someone you have not met in person.

If you’re shopping on a social media marketplace or another local buy and sell marketplace, don’t send money before you see the item in person.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 65: Don’t Give in to the Pressure to Act Now!

**On Slide Text:** Don’t give in to the pressure to act now!

**Talking Points:** Don’t give in to the pressure to act now. Scammers try to create a sense of urgency so that you act quickly. Take the time you need to verify the request.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 66: Don’t Reply to or Engage with the Fraudster

**On Slide Text:** Don’t reply to or engage with the fraudster.

**Talking Points:** Don’t reply or engage with them. Doing so can notify the scammer that they’ve reached a real person, which can result in more scam emails, phone calls, or text messages.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 67: Don’t Click Any Links

**On Slide Text:** Don’t click any links.

**Talking Points:** Don’t click on any links in a scam email or text message. This can take you to untrustworthy websites.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 68: Don’t Provide Remote Access to Your Device

**On Slide Text:** Don’t provide remote access to your device.

**Talking Points:** Never give anyone you don’t trust access to your device. Just by installing software, you can give someone remote access to your device. This means that someone with remote access can control your device as if they were sitting in front of it. This would give them access to your personal information, allowing them to install malware or steal your data.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 69: Don’t Download Any Files or Attachments

**On Slide Text:** Don’t download any files or attachments.

**Talking Points:** Don’t download attachments from emails, text messages, or files on an untrustworthy website. They could contain viruses or malware that could harm your computer or collect your personal information.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 70: Do Take Time to Investigate the Request

**On Slide Text:**

**Talking Points:** If you think something might be a scam, check with a trusted person to verify if it's safe. If someone reports that a family member is in trouble, contact that person to check. If someone reports a problem with your bank account, contact your bank using information from their official website or bank statement – do not use the contact information or link from the person who contacts you.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 71: Do Put Email in Your Spam Folder

**On Slide Text:** Do put email in your spam folder**.**

**Talking Points:** Most email flagged as spam is automatically moved to a spam folder, so you don’t see it in the Inbox. This is an example of the spam folder in Gmail. If you do see a spam email in your Inbox, mark the item as spam. Avoid opening the message, clicking on any links, or viewing any pictures in the message.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 72: Do Look Up Information on Your Own

**On Slide Text:** Do look up information on your own.

**Talking Points:** Do confirm the contact information is correct by checking a statement you received in the mail or the official website of the company.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 73: Do Only Access Websites That Begin with HTTPS

**On Slide Text:** Do only access websites that begin with HTTPS.

**Talking Points:** Only click on links to websites that begin with HTTPS.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 74: Do Discuss with a Trusted Person

**On Slide Text:** Do discuss with a trusted person.

**Talking Points:** If you are unsure about the request you receive in a text, email, phone call, or online, talk to someone you trust, like a friend or family member. Scammers are trying to get you to act quickly – don’t let them rush you into making a quick decision.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 75: Do Register Your Phone Number with DoNotCall.gov.

**On Slide Text:** Do register your phone number with DoNotCall.gov.

**Talking Points:** Register your phone number with the National Do Not Call Registry and request that telemarketers not call you.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 76: Do Close Pop-Ups with ALT+F4

**On Slide Text:** Do close pop-ups with ALT+F4

**Talking Points:** When a pop-up window opens, don’t click on any buttons. Sometimes, even the X will not close a scam pop-up window and may trigger more pop-ups to open instead.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 77: Do Close Pop-Ups with ALT+F4 Continued

**On Slide Text:** Do close pop-ups with ALT+F4.

**Talking Points:** Do try using another method to close the pop-up window. One way to close it is to hold down the Alt key while you press F4 on a PC and Command-W on a Mac. This will close the window. If all else fails, restart your computer, or turn it off and back on again. This is better than being stuck inside a scam.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 78: Do Regularly Update and Patch Your Devices

**On Slide Text:** Do regularly update and patch your devices.

**Talking Points:** Do regularly update and patch your devices. Check with your device manufacturer to learn more about how to secure your device.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 79: Do Use Multi-Factor Authentication

**On Slide Text:** Do use multi-factor authentication.

**Talking Points:** Do use multi-factor authentication, which uses two methods to verify access to your account. It usually includes entering a username and password and one other method, which could be a code sent to your email or phone, or your fingerprint. Multi-factor authentication is not always available, but it is quickly becoming an option on websites and apps.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 80: Activity #4

**On Slide Text:** Activity #4

**Talking Points:** In this lesson, we explored what you should and should not do while browsing a website, receiving a phone call, email, or text message, playing an online game, or even in a pop-up window on your computer.

Let’s practice what we learned.

**Instructor Note:** Point attendees to Activity 4 on Activity Sheet page 3.

**Additional Details:** none

**Slide Number & Title**. Slide 81: Activity 4

**On Slide Text:** You receive an email that claims you have won a prize. You think it is spam? What should you do?

* Reply and tell the sender to stop emailing
* Click the link to visit the website to see if it’s untrustworthy
* Click “Unsubscribe”
* Put it in the spam folder or ignore it.

**Talking Points:**

*INSTRUCTOR NOTE:* Read the question and answers, and ask the learners to call out the answer.

**Answer:** The correct answer is **“**Put it in the spam folder or ignore it.”

*INSTRUCTOR NOTE:* Press ENTER to display the next question*.*

Why are the other answers not correct?

A possible answer for the first and third choices is that you should not let the fraudster know the email account is valid. If they realize someone is checking the email, they will keep contacting you.

Possible answer for the second choice. The link will most likely open a fraudulent website. They may try to trick you into installing malware on your device or try to get you to share personal information.

**After learners complete Activity 4:** Great job, everyone! Before we move to the next section, do you have any questions?

**Instructor Note:** Review and address items in the “parking lot”.

**Additional Details:** For information about what the parking lot is, see the “Before the Workshop Begins” section of the Instructor Guide.

**Have I Been Scammed?**

**Slide Number & Title**. Slide 82: Have I Been Scammed?

**On Slide Text:**

**Talking Points:** In the previous lesson, we learned what you should and should not do when encountering a scam. However, even if you remain vigilant, you may still fall for a scam. Let’s talk about how to identify if you have been scammed and how to report scams.

Here are some examples to help you identify if you’ve been scammed.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 83: Unexpected Transactions on Your Bank or Credit Card   
Statement

**On Slide Text:** Unexpected transactions on your bank or credit card   
statement.

**Talking Points:** You see transactions you did not make on your bank statement or credit report.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 84: The Item You Ordered Did Not Arrive

**On Slide Text:** The item you ordered did not arrive.

**Talking Points:** You purchased an item, but it did not arrive. When you try to report the issue to the seller, you do not get a response.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 85: Unsuccessful Account Login Warning.

**On Slide Text:** Unsuccessful account login warning.

**Talking Points:** You receive an email that there have been an unusual number of unsuccessful sign-in attempts for one of your accounts, but you have not tried to log in. This could mean someone is trying to access your account.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 86: You Can’t Log into Your Account

**On Slide Text:** You can’t log into your account.

**Talking Points:** You can no longer log into your account and are unable to reset the password; someone may have taken over your account.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 87: You Can’t Withdraw Money from Your Account

**On Slide Text:** You can’t withdraw money from your account.

**Talking Points:** You can’t withdraw money from your account, and when you log into your bank account, the balance is zero, or it has been closed.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 88: Person You Were Communicating with Disappears

**On Slide Text:** Person you were communicating with disappears.

**Talking Points:** Sometimes, a person may just disappear. You reach out to them via email, text, or social media, but they no longer respond, or you can’t locate their online profiles anymore.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 89: Signs of Malware on the Computer

**On Slide Text:** Signs of malware

* Pop-up ads
* Pop-up windows are hard to close
* New or unfamiliar toolbar icons
* Response is not as fast

**Talking Points:** You encounter one or more of these signs: Pop-up ads appear and are hard to close; new or unfamiliar toolbar icons appear on the screen; or your computer or mobile device is not responding as fast as it used to. Your device may be infected with malware.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 90: How to Report Scams

**On Slide Text:**

**Talking Points:** Online scams can originate anywhere in the world, making it very hard or even impossible to track down the fraudsters behind them. However, you can take a few actions if you identify or fall victim to a scam. The list can also be found on the Learner Handout.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 91: Contact the Organization

**On Slide Text:** Contact the organization.

**Talking Points:** If you encounter a phishing scam imitating an organization you know, you can contact that organization. But remember not to use the contact information in the suspicious email. Look up their information from a different source. For instance, if you receive a suspicious email claiming to be from the IRS, the website requests that you forward it to phishing@irs.gov.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 92: Contact Your Bank and Credit Card Companies

**On Slide Text:** Contact your bank and credit card companies.

**Talking Points:** If you notice some transactions on your bank account statement that you did not make, contact your bank immediately to report the problem!

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 93: Freeze Your Credit Report

**On Slide Text:** Freeze your credit report.

**Talking Points:** If you are a victim of identity theft, a data breach, or want to be extra cautious, you can freeze your credit report to prevent someone else from applying for credit cards or loans under your name.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 94: Change Your Password.

**On Slide Text:** Change your password.

**Talking Points:** If you receive an email that someone is trying to access your account, you may want to change your password. If you give your password to a scammer or you think someone may have access to your password through a data breach, unsecured internet hotspot, malware, or phishing attempt, change your password.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 95: File a Complaint with the FTC

**On Slide Text:** File a complaint. https://reportfraud.ftc.gov

**Talking Points:** If you have been scammed, there are multiple ways to report an incident. You can file official complaints with the Federal Trade Commission by visiting their website at reportfraud.ftc.gov,

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 96: File a Complaint with the Internet Crime Complaint Center

**On Slide Text:** File a complaint. https://www.ic3.gov

**Talking Points:** or the Federal Bureau of Investigation's Internet Crime Complaint Center at www.ic3.gov,

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 97: File a Complaint with the State’s Attorney General

**On Slide Text:** File a complaint. https://usa.gov/state-attorney-general

**Talking Points:** or your state’s attorney general. You can find your state’s attorney general contact information at usa.gov/state-attorney-general

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 98: Report Suspicious Activity to Your Phone and Internet Service Provider

**On Slide Text:** Report suspicious activity to your phone and internet service provider.  
**Stay Alert: Protect Yourself from Scams**

* Free Mobile Security with the AT&T ActiveArmor® App – Available to AT&T and non-AT&T customers. Download the free app to:

✔ Block and filter spam calls and texts

✔ Get alerts when companies have a data breach

✔ Device security to protect your phone and your personal data on it

* Report Suspicious Activity
  + For AT&T Internet Service Customers: Forward suspicious emails or other activity related to AT&T to [abuse@att.net](mailto:abuse@att.net).
  + For AT&T Wireless (Cell Phone) Customers: Block and report spam calls in the the AT&T ActiveArmor® App

**DISCLAIMER:** If AT&T is not your internet or wireless service provider, please contact your provider for guidance on reporting suspicious activity and available security resources.

Some mobile security features—such as Caller ID, Spam Text Protection, and Auto Fraud Risk Call Blocking—are only available to AT&T wireless customers. These rely on AT&T’s network-level protections and are not accessible to users on other carriers.

**Talking Points:** You can report suspicious phone calls, texts, or online scams to your telephone company or internet service provider.

Stay Alert: Protect Yourself from Scams

Be cautious of unexpected phone calls, texts, or emails asking for your personal, account, or credit card information. AT&T will never request sensitive details through these channels.

Get free mobile security with the AT&T ActiveArmor® App which is available to AT&T and non-AT&T customers. Download the free app to:

✔ Block and filter spam calls and texts

✔ Get alerts when companies have a data breach

✔ Device security to protect your phone and your personal data on it

To report Suspicious Activity

* + For AT&T Internet Service Customers: Forward suspicious emails or other activity related to AT&T to [abuse@att.net](mailto:abuse@att.net).
  + For AT&T Wireless (Cell Phone) Customers: Block and report spam calls in the the AT&T ActiveArmor® App

**DISCLAIMER:** If AT&T is not your internet or wireless service provider, please contact your provider for guidance on reporting suspicious activity and available security resources.

Some mobile security features—such as Caller ID, Spam Text Protection, and Auto Fraud Risk Call Blocking—are only available to AT&T wireless customers. These rely on AT&T’s network-level protections and are not accessible to users on other carriers.

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 99: If Your Identity Was Stolen Contact IdentifyTheft.gov

**On Slide Text:** If your identity was stolen contact IdentifyTheft.gov. https://IdentifyTheft.gov.

**Talking Points:** If your identity was stolen, you suspect someone may have stolen your identity, or your information was exposed in a data breach, check the IdentifyTheft.gov website to explore your options, report the theft, and create a recovery plan

**Instructor Note:** none

**Additional Details:** none

**Slide Number & Title**. Slide 100: Questions

**On Slide Text:**

**Talking Points:** Do you have any questions before we wrap up today’s workshop?

**Instructor Note:** Review and address items in the “parking lot”.

**Additional Details:** For information about what the parking lot is, see the “Before the Workshop Begins” section of the Instructor Guide.

**Slide Number & Title**. Slide 101: Congratulations, Learners!

**On Slide Text:** Congratulations, learners! Today you:

* learned about cybersecurity.
* built skills to:
  + make passwords strong and memorable.
  + create safe and secure accounts and passwords.
  + identify the most common types of scams.
  + recognize and avoid online scams.
  + report a scam.
* discovered useful tips to help you stay safe online.

**Talking Points:** Congratulations, learners! Today you:

* learned about cybersecurity.
* built skills to:
  + make passwords strong and memorable.
  + create safe and secure accounts and passwords.
  + identify the most common types of scams.
  + recognize and avoid online scams.
  + report a scam.
* discovered useful tips to help you stay safe online

**Instructor Note:**Provide each learner with a Certificate of Completion.

**Additional Details:** none

**Slide Number & Title.** Slide 102: Additional Training Online.

**On Slide Text:** Today’s training is provided by AT&T   
and the Public Library Association.   
Visit https://digitalliteracy.att.com/   
for more courses and to build confidence using technology.

**Notes Section**

**Talking Points:**

**Instructor Note:**Highlight the <https://digitalliteracy.att.com> and <https://www.digitallearn.org/> websites as resources for additional virtual online courses.

**Additional Details:** none

**Slide Number & Title.** 103: Learner Survey.

**On Slide Text:** Please be sure to complete the learner survey.   
Visit: **digitalliteracy.att.com/learnersurvey**  
or   
Scan the QR code here:

The QR code is also on the Activity Sheet.   
  
We appreciate your feedback and participation!

**Notes Section**

**Talking Points:** Please be sure to complete the learner survey.   
Visit **digitalliteracy.att.com/learnersurvey**  
or   
Scan the QR code

The link and code are also located on the Activity Sheet.

**Instructor Note:**none

**Additional Details:** none

**Slide Number & Title.** Slide 104: **Thank You!**

**On Slide Text:**Questions? Thank you for coming!

**Notes Section**

**Talking Points:**

**Instructor Note:**Close out the session by following these steps:

* (If applicable): Mention future AT&T and PLA digital learning workshops planned for the location and/or community.
* Ask if there are any other final questions and answer any outstanding ones that may have been missed in the parking lot sections*.*
* “Thanks again to AT&T and the PLA for this workshop. We appreciate all our participants for coming and we encourage you to keep learning!”
* The instructor will be responsible for entering the paper survey responses into [digitalliteracy.att.com/[learnersurveylearnersurvey](https://learnersurvey)](https://digitalliteracy.att.com/learnersurvey)

**Important Note to Instructor:**   
**Please complete the Impact Survey for this workshop by visiting:**

**digitalliteracy.att.com/impactsurvey or scan the QR code:**



**Thank you!**