Cybersecurity Basics Training Workshop

Instructor Outline: Cybersecurity

This document is designed to be used by the instructor alongside the PowerPoint presentation and/or projected live demonstration. It includes a course overview, talking points, and instructions for the activities. Please note the slide number notations to help keep you on track.

Workshop Description

This in-person or virtual workshop is for those who are interested in safety online and want to protect themselves from fraudsters and scams. It will build participants' confidence when they are visiting websites, creating passwords, and responding to email.

Curriculum Track

Basics

Audience

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

Workshop Length

60–90 minutes

Training Method

Volunteer Instructor-led, hands-on

Purpose

In this workshop you will introduce newly connected computer and internet users to basic safety when they visit websites, create passwords, and receive email and other communication from potential fraudsters. 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; computers for instructor and participants with internet connections; laser pointer (recommended).

For classroom-only settings (no participant computers), instructor will project a live demonstration and engage participants by talking through the activities and performing interactive tasks in a group discussion format.

Virtual: A web conferencing platform; computers for instructor and participants with internet connections.

Software Requirements

Computer capable of running a PowerPoint presentation with a web browser, preferably Google Chrome.

Material Requirements

- Notepaper, pens, or pencils
- Instructor PowerPoint: Before the workshop, review the slides and update the following information:
    - Verify which web browser you will be using during the workshop and how to launch the browser from desktop.
    - Slide 1: Update instructor name, instructor affiliation (for example, library staff, community volunteer, and so on), location name, and insert the organization's logo.
    - Slide 2: Be prepared to give a brief introduction about yourself.
    - Slide 57: Insert name and date of next workshop if one is being offered.
- Instructor Outline (this document): Review the Instructor Outline and familiarize yourself with the workshop materials.
- Learner Handout
    - For in-person workshop: Print handouts for each attendee and provide them to learners before the workshop begins.
    - For virtual workshop: Provide link to the Learner Handout, either before the workshop as part of their registration confirmation or in the online platform's chat feature.
- Learner Activity Worksheet
    - For in-person workshop: Print handouts for each attendee and provide to the attendee before the workshop begins.

    - For virtual workshop: Ask the questions listed on the Activity Sheet during the workshop and encourage attendees to share their answer via chat or use the internal polling tool if available within the web conferencing tool.
- Certificate of Completion: For the in-person workshop, print a certificate to hand out to each attendee once the workshop is completed. For virtual attendees, send them an electronic copy via email.
- Attendee Name Tags: If you want to easily identify attendees, make sure to bring name tag stickers or table tents.

Learning Objectives

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

- Identify a secure website (i.e. a website that's safe to create an account on).
- Employ two tips from the workshop to create a strong password that is easy to remember.
- Identify key factors in an email message that indicate a scam.

Before Workshop Begins

- In person:
    - Make sure all computers are turned on and ready for attendees to use. (See the previous note about classroom settings, in the "Equipment Requirements" section.)
    - Place attendee materials at each computer. Attendee materials include the Learner Activity Sheet and Learner Handout. You may also want to provide paper (for attendees to take notes) and pens or pencils.
    - If using name tags make sure they are easily accessible to attendees and that you provide a marker or pen for attendees to write their name.
    - A registration list so you can identify who attended.
    - Review the computer before the course and see which web browser is installed and how to launch it from the computer.
    - Identify a "parking lot," which is 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.
- Virtual:
    - 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.

- Send a link before the workshop to the learner materials. These include the Learner Activity Sheet and 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 and a way for you to easily track the questions to be answered 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)

Successful completion of activities

Instructor Presentation

Slide 1: Cybersecurity Basics. Show workshop title slide.

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.

Today's workshop is provided by AT&T and the Public Library Association.

INSTRUCTOR NOTE: Include thank-you to community collaborator if applicable

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?

Slide 2: Workshop Content Outline—Agenda (3 mins.)

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. This will include:

- Recognizing secure websites
- Making your account passwords strong and memorable, and
- Recognizing common scams

As we go, you'll learn **Tips and Tricks** for strong passwords and avoiding scams. And, you will have opportunities to Practice what you've learned.

Let's get started!

Slide 3: Why do we need to be concerned about safety when we're online?

INSTRUCTOR NOTE: Ask attendees the question on the slide. Lead a brief discussion on safety, then proceed to the information. Or you can ask the question, allow a moment for the attendees to think about it, and proceed to the information.

Enter for bullet 1:

When we surf the web, create personal accounts on websites, and use email, we share personal information that we want to keep private. This includes credit card information, bank information, personal health information, and more. We need to keep this information safe and private.

Enter for bullet 2:

Unfortunately, fraudsters will sometimes try to gain access to this information. They may try to gain access to your personal accounts through guessing your passwords, getting you to send them information, or persuading you to install software on your computer or device that allows them to access your information.

Slide 4: What is Cybersecurity?
Cybersecurity is all about the safety of information—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 that 2) our devices—laptops, desktop computers, mobile phones, tablets—work properly and are free from malware. Malware is malicious software that can take many shapes – from viruses that infect your favorite devices to spyware and adware that track your online activities.

Slide 5: Secure Websites.

Let's begin by talking about secure websites. Why does a website need to be secure? If you're going to enter personal information, you want to keep your information safe.

INSTRUCTOR NOTE: Ask the question on the slide of attendees, have them share their thoughts, then proceed to the bullet. Or, you can ask the question, allow a moment for the attendees to think about it, and proceed to the bullet.

Slide 6: Secure Websites. There are two things to look for when you visit a website:

1) a padlock icon next to the address bar, and

2) the website address begins with HTTPS.

ENTER for larger image and badge:

If the website has one or both, the website is secure. That means it's safe to browse without being tracked, and it's safe to create an account and share personal information.

In many modern browsers, the website address may not show the beginning of the URL unless you double-click the address. Remember, if you can't see the HTTPS, be sure you can see the padlock icon.

Slide 7: Secure Websites. If the website does not have a padlock icon, it is not secure. If the website address does not begin with HTTPS, but instead uses HTTP without the S, the site is not secure.

ENTER for larger image and badge

Most modern browsers will show some kind of warning to help you determine whether the site is secure. In this example, the browser shows an exclamation point to draw your attention. If you don't see the padlock, use a different website if possible.

Slide 8: Personal Accounts.

INSTRUCTOR NOTE: Facilitate a brief discussion with participants. Have you created an online account? What kind of accounts have you created? Why would someone create an account on a website?

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

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 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 they are only accessible to you.

Enter for bullet 1

You create a personal account so that your information is **only accessible to you.**

Slide 9: Secure Websites.

INSTRUCTOR NOTE: Tie information on personal accounts with the importance of secure websites. Reiterate the information on secure websites.

This is why secure websites are important—so your data is protected. It's important to keep your account secure on any website. If someone gains access to one of your online accounts, your personal information could potentially be used to access other accounts as well. Or your account could even be used by hackers and fraudsters to commit crimes.

INSTRUCTOR NOTE: Before moving to Activity 1, review "parking lot" questions. If there are no questions in the parking lot, ask the attendees if they have any questions before you move to Activity 1.

Slide 10: Activity 1—Secure Websites.

INSTRUCTOR NOTE: Point attendees to Activity 1 on Activity Sheet page 1.

If learners are on computers, encourage attendees to select a website they might use—for shopping, banking, social media, and so on. Participants go to the website and complete the activity questions. Facilitate a brief discussion. What sites did they visit? Were they secure? How did they know?

If there are no computers, ask participants for a few websites they might want to use for shopping, banking, social media, and so on. Go to the websites they mention and ask attendees to share how they can tell it's secure. Facilitate a brief discussion.

Slide 11: Activity 1 Debrief.

INSTRUCTOR NOTE: Use slide to debrief the activity or as a guide for yourself if you are doing a demonstration.

Suggested secure sites for instructor to demo:

- *www.digitalleearn.com*
- *google.com*
- *nypl.org*

Answers to Questions:

1. Padlock icon *–(instructor—point out the padlock in your example.)*

2. https:// visible in address bar or if you double-click the address bar *(instructor —please demonstrate if the https:// is not visible).*

Slide 12: Strong Passwords.

When we create personal accounts on websites, it's important to make sure our account passwords are as strong as possible.

Let's continue our discussion of online safety with a look at strong passwords. When we create personal accounts on websites, it's important to make sure our account passwords are as strong as possible.

Slide 13: 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?"

INSTRUCTOR NOTE: It's important to be strengths-based and not to shame attendees for any approaches they use.

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

Slide 14: Strong Passwords.

Most websites have requirements for passwords on their signup forms. The requirements are usually listed underneath the form. The requirements may not show until your password has failed their requirements.

ENTER for bulleted list:

Passwords can usually include numbers, uppercase and lowercase letters, and symbols like punctuation. If your first try isn't accepted, review the website's requirements. Try adding a capital letter, number, or symbol, or make the password longer.

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

Slide 15: Tips for Strong Passwords.

What makes a strong password? Here are some Dos and Don'ts.

ENTER for bullet 1 Avoid weak passwords like 'password' (the most commonly used password!) or '123456'.

ENTER for bullet 2 Don't include personal information like your address or name.

ENTER for bullet 3 Don't use the same password on multiple accounts and websites.

ENTER for bullet 4 Don't share your password with others. Passwords are the secret key that unlocks your account. They should be kept private.

Slide 16: Tips for Strong Passwords

Do make the password longer. The best defense is length.

ENTER for image:

Longer passwords don't need to be complex and hard to remember. We may be used to creating long, complicated passwords that are hard to remember.

ENTER for bullet 2:

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.

Slide 17: Keeping Track of Passwords

INSTRUCTOR NOTE: How do you remember your passwords? Facilitate a brief discussion.

It's important to be strengths-based and not to shame. Some of this discussion may have already come up in the Strong Passwords section. Previous attendee comments can be brought in here if appropriate.

Now that we've discussed creating a strong password, let's talk about how we can keep track of our passwords.

If you've used the internet for a while, you may create 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.

ENTER for numbered list:

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

Slide 18: Item 1: Notebook.

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

ENTER for Tips:

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

Slide 19: Item 2: Password Software.

You may choose to use a secure password management mobile app or website that can help keep track of your passwords. These programs are usually unlocked with a single master password and then allow you to access all your passwords when you need them. The apps also will generate passwords for you that are complex combinations of letters, numbers, and special characters.

Slide 20: Item 3: Phrase.

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

Slide 21: Strong and Memorable Passwords. – Activity 2

INSTRUCTOR NOTE: Point attendees to Activity 2a and 2b on Activity Sheet pages 2 and 3.

Let attendees know that we will be discussing what they come up with, so they shouldn't use any real passwords. The exercise is to practice using the methods we just went over—using phrases and combinations. When attendees have completed the activities, facilitate a discussion on what people came up with using the next two slides.

Slide 22: Activity 2a Debrief.

INSTRUCTOR NOTE: Use slide to debrief the activity or as a guide for yourself if you are doing a demonstration.

Slide 23: Activity 2b Debrief

INSTRUCTOR NOTE: *Use the slide to debrief the activity or as a guide for yourself if you are doing a demonstration.*

Use the information from the course on strong passwords to discuss the participant responses. Examples you might use if you need to provide them:

1. happybirthday – H@PPyBirthD@y0
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.

3. 1234567890 – onetwobuckleymyshoe
4. 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 a phrase.

Remember: Longer passwords are stronger passwords.

Slide 24: Online Fraud and Scams.

Let's continue our discussion of online safety with a look at online fraud and scams. When we started the workshop today, we discussed that cybersecurity is all about the safety of information—our identity, our personal data, and our financial assets—when we're online.

As we discussed, cybersecurity means that 1) your personal data is only accessible to you or others you authorize, and that 2) your devices—laptops, desktop computers, mobile phones, tablets—work properly and are free from malware.

INSTRUCTOR NOTE: In case a definition of malware is needed: Malware is malicious software that can take many shapes—from viruses that infect your favorite devices to spyware and adware that track your online activities.

While we can do our best to keep safe by using secure websites and strong passwords for our accounts, we also need to be aware of various online scams, where people try to swindle our information from us. Let's shift to talk about different ways that people with bad intent try to get access to your personal information and financial accounts. In other words, online fraud and scams. We'll see how to recognize a scam, and how to protect yourself when you see a scam.

Slide 25: Online Fraud and Scams.

Some of the most common types include phishing and social engineering. You may encounter these scams on a website, in an email or text message, or even in a pop-up window on your computer.

Slide 26: Phishing.

Let's begin by talking about phishing, which is a common type of scam. Phishing is when scammers use fake emails or text messages to "fish" for information.

These fake messages can look real, but link to fake websites. The website may look like a trusted, well-known company, organization or government agency, but it's all a trick to get your information—such as Social Security number or bank and credit card account numbers.

Slide 27: Phishing.

A fake email can also be used to infect your computer with malicious software (referred to as malware) or a virus as soon as you open the email. Malware is a tool fraudsters use that can take many shapes. For example, malware can lead to viruses that infect your computer or spyware that tracks your online activities.

Slide 28: Social Engineering.

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 they are someone they are not, in order to get personal information from you.

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 claim to be working on behalf of a government agency, organization or collection agency. These fraudsters can approach you by phone, email, text or social media.

Slide 29: Online Fraud and Scams.

INSTRUCTOR NOTE: Facilitate a brief discussion with attendees.

- What are some examples of phishing and social engineering you've experienced?
- How can you stay safe from fraudsters?

INSTRUCTOR NOTE: Ask for a few examples, and then move to the next slide.

Slide 30: Tips to Recognize Scams.

Here are some things to think about when you review scam emails and other phishing attempts.

We'll look at these one by one, and this list is also in your Learner Handout.

- Have you heard of the person or organization before?
- Can you tell who the email message is from?
- Does the email have mistakes?
- Are they asking for your information?
- Are they trying to rush you into a quick action?
- Is it too good to be true?

Slide 31: Have you heard of the person or organization?

INSTRUCTOR NOTE: Please begin by asking the question on the slide of the participants: ***Have you heard of the person or organization?***

A legitimate business will have their official logo, address, and contact information should be posted on their website. Have you heard of this business? Is there a logo for the business? Is there contact information?

This is a good example of a legitimate business website.

Slide 32: Can you tell who the email message is from?

INSTRUCTOR NOTE: Please begin by asking the question on the slide of the participants: ***Can you tell who the email is from?***

This example claims to be from PayPal. What is the sender's email address? Does it match?

The email address doesn't match and does not appear to be from PayPal. This is a sure sign of a phishing scam.

Slide 33: Are they asking for your information?

INSTRUCTOR NOTE: Please begin by asking the question on the slide of the participants: ***Are they asking for your information?***

Are they asking for credit card information or other personal 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.

In this example . . .

- the email is asking for the recipient to confirm their identity.
- the email is asking the recipient to log in using the button, to provide documentation.

Slide 34: Does the email have mistakes?

INSTRUCTOR NOTE: Please begin by asking the question on the slide of the participants: **Does the email look professional or are there a lot of mistakes?**

Can you identify mistakes in this email? In this example, . . .

- the word "account" is misspelled in different ways throughout the email.
- the word "suspicious" is misspelled.
- there is a grammar error: "please confirming provide the documents."
- there is an extra space between "asked" and "to" in the first paragraph.

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

Slide 35: Are they trying to rush you into a quick action?

INSTRUCTOR NOTE: Please begin by asking the question on the slide of the participants: ***Are they trying to rush you into a quick action before taking the time to think about it?***

What "alarming phrases or words" is the fraudster using to give urgency to the request?

In this example:

- the email is creating urgency by suggesting they've been trying to reach you.
- the message includes: "expiring soon" related to the gift card.

Some fraudsters try to scare you into acting fast. They threaten that something bad will happen, like an account will be closed. Other fraudsters will promise something good, but only if you respond right away.

Slide 36: Is it too good to be true?

INSTRUCTOR NOTE: Please begin by asking the question on the slide of the participants: ***Is it too good to be true, like winning the prize for a contest that you don't remember entering?***

What sounds "too good to be true" in this example?

In this example, the recipient is being offered a $750 gift card.

If it sounds too good to be true, it probably is.

Slide 37: Activity #3—Online Fraud and Scams

INSTRUCTOR NOTE: Point attendees to Activity 3 on Activity Sheet. When attendees have completed the activity, facilitate a discussion on what people came up with.

Slide 38: Activity Debrief.

INSTRUCTOR NOTE: Use slide to debrief the activity or as a guide for yourself if you are doing a demonstration.

Things that indicate a scam include . . . *(Point out each answer on the slide to review with learners.)*

- the sender email is not from the pharmacy. Also, it includes an excessive number of letters and numbers, unlike most business email addresses.
- the email includes extra spaces between words in lines 1, 3, and 4.
- the email includes grammar mistakes: "accounts coming in from palpability of account so the Pharmacy suspends the account service . . ."
- the email includes an attachment.

Slide 39: Dos and Don'ts to Avoid Scams.

Here are some tips to stay safe when it comes to online scams. We'll look at these one by one, and this list is also in your Learner Handout.

Slide 40: Don't give any personal information.

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

Slide 41: Don't reply to or engage with the fraudster.

Don't reply to or engage with them. This can notify the scammer that they've reached a real person, which can result in more scam emails.

Slide 42 – Don't click on any links or buttons.

Don't click on any links or buttons in a scam email. This can take you to untrustworthy websites.

Slide 43: Don't download any files or attachments.

Don't download any email attachments or files on an untrustworthy website. They could contain viruses or malware that could harm your computer or collect your personal information.

Slide 44: Do be skeptical.

Do be skeptical. If you think something may be a scam, it probably is.

Slide 45: Do read emails carefully.

Remember to read emails and text messages carefully, checking to make sure you know the sender. Apply the other tips we presented to determine if something is a scam.

Slide 46: Do look up information on your own.

Do look up contact information, details about a company, or your account information on your own. Go directly to the company website or to your own account information to check. Don't go to any website through the scam email.

Slide 47: Activity #4.

In this last activity, we will practice what we've covered and see what everyone has learned.

INSTRUCTOR NOTE: Walk through the following slides and encourage learners to provide answers as a group.

INSTRUCTOR NOTE: You don't need to refer to the Learner Activity sheet for this one.

Slide 48: How do you know a website is secure?

Answer: The web address begins with HTTPS and there is a padlock icon showing.

Sites that begin with HTTPS and a padlock are websites that are secure and will protect your password information.

Slide 49: Which of these passwords is the most secure?

Answer: cowshelpmakecheese

Longer passwords make stronger passwords. It's important not to use personal information or anything too easy to guess for your password.

Slide 50: Which is the best option to remember your password?

Answer: Notebook stored in a safe place.

The safest option of these three is to write the password in a notebook that is stored in a safe and secure location. A sticky note on your computer can easily be seen by others. Using your first and last name is easily guessed by someone who wants to get into your accounts.

Slide 51: What are three things that indicate a scam?

Answers:

- You don't know who the email is from.
- You never signed up for pharmacy points.
- The message has grammatical errors.
- The message is trying to rush you into an action.
- The message is telling you you'll lose something if you don't act.
- The message includes a link that may lead you to a nefarious website or may lead you to download malicious software.

Slide 52: What are three things that indicate a scam?

Answers:

- The message doesn't include your name, only "Adorable Member."
- "Adorable Member" is not what we might call "professional" for this kind of correspondence.
- You never signed up for tech support.
- The message has grammatical errors.
- The message is telling you that you've spent money you didn't and is trying to get you to react.

Slide 53: You've received an email telling you you've won a prize. You think it's a scam. What should you do?

Answer: Put it in your Spam folder or ignore it

Engaging the sender can result in getting more spam. Clicking on any link in a scam email can result in getting more spam and lead to unsafe websites.

Slide 54: Questions

INSTRUCTOR NOTE: Ask if there are any other final questions and answer any outstanding ones that may have been missed in the parking lot sections.

Slide 55: Congratulations

Today you . . .

- learned about cybersecurity.
- built skills to
    - recognize a secure website.
    - make passwords strong and memorable.
    - recognize and avoid online scams.
- learned useful tips to help you stay safe online.

*INSTRUCTOR NOTE: Provide attendees with Certificate of Completion***.**

Slide 56: DigitalLearn Courses.

INSTRUCTOR NOTE: Point the learners to additional courses available online at the website in the slide.

Slide 57: Thank You.

Thanks again to AT&T and PLA for this workshop. We appreciate all our participants for coming and we encourage you to keep learning!