Storyboard

Preventing Phishing Attacks

Module Title: Preventing Phishing Attacks

Target Audience: All employees within the company's email domain

Outline:

- Welcome
- Navigation
- Objectives
- What is Phishing?
    - Types of Phishing Attacks
    - Successful Attacks
    - Knowledge Check – Objective #1
- Identify a Phish
    - Mismatched URLs
    - Poor Grammar/Spelling
    - Unofficial Contact
    - Urgent Language
    - Knowledge Check – Objective #2
- Best Practices
    - Email Address
    - Online Posts
    - Passwords
    - Attachments
    - Domain
- Quiz
    - Learning Objectives #1–3
- Summary
- Congratulations

Learning Level: Knowledge & Understand

Learning Objectives:

1. Classify types of phishing attacks.
2. Analyze potential security threats.
3. Identify best practices for preventing malware.

Seat Time: 30 minute

Font:
Articulate Light

Color Palette

Module Resources/References:

- Stay Safe from Cyber Attacks Infographic

Media and Audio:

- Audio files that pair with this storyboard will use AI voiceover from WellSaid Labs
- Voiceover Script
- Audio Files

Directions: Each table will indicate the corresponding slide number and course menu title in the top row. The columns will include details of how the slide will be visually laid out, the voiceover script, the text that will be included on the slide and any possible animations or learner interactions.

Layers will be indicated with a letter after the slide number (1.1.A) and colored purple (as shown in table below).

Quiz Questions will be colored blue (as shown in table below).

🟥	Slide
🟪	Layer
🟦	Quiz Question

Reviewer notes should be added in the last column of each table for the corresponding slide/layer/quiz question. While providing feedback in the last column, please use yellow highlight to reference any in-line text edits. Reviewers should focus on content accuracy and scenarios.

Slide 1.1 / Menu Title: Welcome				
Narration / Voiceover:	Slide Text:	Visual Display:	Animation/ Interaction:	Reviewer Notes
Welcome to Preventing Phishing Attacks. This course is designed to stop the number one cyber security threat called Phishing attacks. All employees within our domain will learn how to identify types of Phishing attacks and to prevent them.	[Slide Title] **Preventing Phishing Attacks** [Directions] Click the START button to begin this course. Click the NAVIGATION button for a navigation tutorial.	Background picture of a person with a device. Large banner with title and navigation buttons at bottom.	Start button will take the learner to 1.3. Navigation button will take the learner to 1.2.	

Last updated: 5/25/2023

If you are familiar with the course navigation player, click the Start button to begin. If you would like some guidance with navigating the course, click the Navigation button. When you're ready, let's get started.	[Buttons] Start Navigation	Custom start and Navigation buttons.		

Slide 1.2 / Menu Title: Navigation

Narration / Voiceover:	Slide Text:	Visual Display:	Animation /Interaction:	Reviewer Notes
Please take a moment to review the course player so you feel comfortable navigating through the course. If you know your way around, you may proceed to the next slide. If you'd like to go backward or forward in the course, click the previous or next buttons. To adjust the volume, click the volume icon. Use the seekbar at any time to review a portion of the slide. You can also pause the player. Click the same button again to resume play. Revisit a slide by using the menu on the left. Finally, select resources for additional resources.	[Slide Title] **Navigation** [Directions] Use these options to navigate the course [Captions] Next Previous Accessibility Volume Replay Seekbar Play/Pause Menu Resources	Background Image: A screenshot of the welcome screen. Caption bubbles with labels point to player features	Caption bubbles with text labels will fade in timed with their reference in the audio. When clicked, each bubble will display information about the navigation tool.	

Click the next button now to begin the course.				

Slide 1.3 / Menu Title: Objectives

Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Cybercrime has become increasingly powerful to enable criminals to launch attacks to steal personal and private information. Phishing attacks are currently the number one cyber threat to organizations. Let's learn how to keep your information safe from cyber attacks. By the time we finish, you'll learn how to classify types of Phishing attacks, analyze potential security threats, and identify best practices for preventing malware.	[Slide Title] **Learning Objectives** Classify types of Phishing attacks. Analyze potential security threats. Identify best practices for preventing malware.	Title at the top. In the middle of the screen will be a cell phone. The objective will appear as text messages on the cellphone screen.	The objective will fade in a float up, timed with the audio.	

Slide 2.1 / Menu Title: What is Phishing

Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Phishing is an online scam where criminals send fraudulent email messages,	[Slide Title] **What is Phishing?**	Background image:	Scrolling text, floating up on the screen times with audio.	

appearing legitimate. The email contains links or attachments that trick recipients into entering confidential information such as account numbers, or passwords, into fake websites, or infect their computers with malware. The most successful and dangerous of all the cyber attacks is phishing.	Phishing is an online scam where criminals send fraudulent email messages, appearing legitimate. The email contains links or attachments that trick recipients into entering confidential information such as… account numbers.. passwords.. into fake websites, or infect their computers with malware.	semi transparent of someone working on a computer Lage text scrolling up in white Key words bolded in red color: online scam, email messages, links or attachment, account numbers, websites, fake, infect.	This slide will auto advance to 2.2.	

Slide 2.2 / Menu Title: Types of Phishing Attacks				
Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
There are several different types of Phishing attacks to look out for. They all have the same purpose – to steal your personal details. Click on each type to learn more information.	[Slide Title] **Types of Phishing Attacks.** Be aware there are several different types of phishing attacks. [Directions]	Title at the top. Additional text directly below the title. Large icon of a desktop computer with buttons to left.	Buttons to slide layers with fly in from the left. When each button is clicked, it will reveal the corresponding slide layer. The buttons will have visited states to	

	Click on each type to learn more information. [Buttons] Spear Phishing Vishing Smiching Clone Phishing Whaling	Directions will be in a blue box at the bottom of the slide.	indicate to the learner that they have already clicked on that item. The next button will be disabled until the learner visits every layer.	

Slide 2.2.A / LAYER: Spear Layer *(Hidden from menu)*				
Narration / Voiceover:	Layer Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Spear Phishing is a targeted attempt to steal sensitive information, typically focusing on a specific individual or organization. These types of attacks use personalized facts in order to appear legitimate. Generally, cybercriminals turn to social media and company sites to research their victims.	Spear Phishing ● targeted attempt to steal sensitive information ● use personal facts to appear legitimate ● cyber criminals use social media and company websites to find out information about their victims	Slide base layer will be displayed (2.2) The Layer text will appear inside the computer icon.	The learner will be restricted from clicking on other buttons until the audio completes.	

Slide 2.2.B / LAYER: Vishing Layer *(Hidden from menu)*				
Narration / Voiceover:	Layer Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Vishing is a phone scam, and has the most human interaction of all the phishing attacks. The fraudsters deceive victims by creating a sense of urgency to divulge sensitive information. Calls are often made through a spoofed ID, so it looks like a trustworthy source.	Vishing ● create a sense of urgency ● try to get victims to divulge sensitive information ● phone scam often made through a spoofed ID to look trustworthy	Slide base layer will be displayed (2.2) The Layer text will appear inside the computer icon.	The learner will be restricted from clicking on other buttons until the audio completes.	

Slide 2.2.C / LAYER: Smishing Layer *(Hidden from menu)*				
Narration / Voiceover:	Layer Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Smishing is a type of phishing that uses text (SMS) messages, as opposed to emails, to target victims. Fraudsters send a text message to an individual, usually calling for the individual to act.	Smishing ● text (SMS) messages ● asks the victim to click on a link ● requests a PIN number	Slide base layer will be displayed (2.2) The Layer text will appear inside the computer icon.	The learner will be restricted from clicking on other buttons until the audio completes.	

Slide 2.2.D / LAYER: Clone Phishing Layer *(Hidden from menu)*				
Narration / Voiceover:	Layer Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
In Clone Phishing, a legitimate and previously delivered email message is used to create an identical email with malicious content. The cloned email will appear to come from the original sender and will contain malicious links or attachments.	Clone Phishing ● uses a legitimate and previously delivered email message ● contains malicious links or attachments ● appears to come from original sender	Slide base layer will be displayed (2.2) The Layer text will appear inside the computer icon.	The learner will be restricted from clicking on other buttons until the audio completes.	

Slide 2.2.E / LAYER: Whaling Layer *(Hidden from menu)*				
Narration / Voiceover:	Layer Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
A Whaling attack is an attempt to steal sensitive information from senior-level management. Whaling emails contain highly personalized information about the target or organization, so they are more difficult to detect.	Whaling ● attempt to steal sensitive information from senior-level management. ● contains highly personalized information ● most difficult to detect	Slide base layer will be displayed (2.2) The Layer text will appear inside the computer icon.	The learner will be restricted from clicking on other buttons until the audio completes.	

Slide 2.3 / Menu Title: Successful Attacks				
Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Cyber attacks have been far more frequent and advanced than ever seen before.The cost of a phishing attack can be grave depending on the scope of the attack. Phishing attacks are gaining momentum because they are easy to set up, rewarding, and pose little risk to cybercriminals. Click on each icon to reveal the effects of a successful attack.	[Slide Title] **Successful Attack Results** What are the results of a successful attack? [Directions] Click on each type for more information. Icon text: Identity Theft Malware/Ransomware Installation Loss of sensitive information Data sold to Criminals Financial Loss Access to Company Systems	Title across the top of the slide. Six identical shapes with individual icons in the center will be positioned to the left half of the slide. The icons will represent the text that is revealed. There will be an image of a criminal on the right.	The icons will be a click to reveal interaction. The next button will advance the learner to slide 2.4.	

Slide 2.4 / Menu Title: Knowledge Check / Learning Objective #1				
Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Let's check what you have learned so far. Which of the following are types of Phishing attacks? Select all that apply, then select submit.	[Slide Title] **Knowledge Check** Which of the following are types of Phishing attacks? Select all that apply, then select submit. –Data Sold to Criminals –Identity Theft –Spearing (Correct) –Smishing (Correct) –Vishing (Correct) Answer Responses: Correct – That's right! Those are all types of Phishing attacks. Incorrect –Incorrect. Vishing, Smishing, and Spearing are all types of Phishing Attacks. Try Again –That is incorrect. Please try again.	Title across the top. A banner is a lighter color under the title with the question. Multiple answer checkboxes under the question.	The learner will receive immediate feedback on their answer.	

Slide 3.1 / Menu Title: Identifying a Phish				
Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Now that you know the types of Phishing that happens, let's learn how to spot a potential attack. There are things you can be on the lookout for to identify a Phish. Mismatched URLs, Poor grammar or spelling, unofficial contact, and urgent language. Select each type to learn more.	[Slide Title] **Identifying a Phish** There are things you can be on the lookout for to identify a Phish… Mismatched URLs Poor Grammar or Spelling Unofficial Contact Urgent Language [Directions] Select each option to learn more.	Title across the top of the slide. Directions in a blue box at the bottom. In the center each option will be in Red text with a semi transparent banner behind it.	The text will float up similarly to slide 2.1. Each text option will be a button to take the learner to its corresponding slide. The buttons will have a hover state to glow. The buttons will have a visited state to indicate to the learner that they have already viewed the information. The next button will be disabled until all of the options have been visited.	

Slide 3.2 / Menu Title: Mismatch URLs *(Hidden from menu)*				
Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
When receiving any email of any kid, NEVER click on any link before checking the validity of the URL. One way to do this is to hover your cursor over the	[Slide Title] **Mismatched URLs**	The title will be across the top of the slide.	The next and previous buttons will take the learner back to slide 3.1.	

URL link but DO NOT CLICK on it. A window should appear to show you the URL address. If it does not match where it is intended to go, it is most likely fraudulent. Click next to continue.	Never click on any link before checking the validity of the URL. Hover your cursor over the IRL link. DO NOT CLICK If the IRL does not match the intended address, it is most likely fraudulent.	The text box with a white border will be on the left. An icon of a computer screen with a screenshot of a real email will be to the right. The email will be a gif of an actual email being opened and the mouse hovering over a link. The mismatched link will appear on the screen in a larger box.	The text will fade in timed with the audio.	

Slide 3.3 / Menu Title: Poor Grammar/Spelling *(Hidden from menu)*				
Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Be aware that many phishing emails will contain misspelled words and use poor grammar. Reputable companies will not send emails with common mistakes so look out for errors.	[Slide Title] **Poor Grammar of Spelling** Many Phishing emails will contain misspelled words and use poor grammar. Look for common errors.	The title will be across the top of the slide. The text box with a white border will be on the left. An icon of a computer screen with a screenshot of a real email will be to the right. The email will contain errors.	The next and previous buttons will take the learner back to slide 3.1. The text will fade in by paragraph. Using a motion path, a magnifying glass will hover over some of the errors in the email.	

Last updated: 5/25/2023

Slide 3.4 / Menu Title: Unofficial Contact *(Hidden from menu)*

Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Reputable companies will never randomly ask for account numbers, pins, or passwords. Whether you receive a text or email, always verify the sender's complete emails, phone number and other contact information. If you do not recognize the sender, or did not initiate the correspondence, do not respond or click on any links.	[Slide Title] **Unofficial Contact** Reputable companies will never randomly ask for account numbers, pins, or passwords. Always verify the sender's complete emails, phone number and other contact information. If you do not recognize the sender, or did not initiate the correspondence, do not respond or click on any links.	The title will be across the top of the slide. The text box with a white border will be on the left. An icon of a cell phone with a screenshot of a real text on the screen will be to the right. The sender's name and "PIN" will be highlighted.	The next and previous buttons will take the learner back to slide 3.1. The text will fade in by paragraph. The highlighted text will be timed with the audio.	

Slide 3.5 / Menu Title: Urgent Language *(Hidden from menu)*

Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Cyber criminals sometimes use fear or urgency to pressure you to take action quickly. They will also pretend to be a common service because more	[Slide Title] **Urgent Language** Cyber criminals sometimes use fear or	The title will be across the top of the slide.	The next and previous buttons will take the learner back to slide 3.1.	

people will act immediately to avoid losing access. If this happens, do not respond or click on any links.	urgency to pressure you to take action quickly. They will also pretend to be a common service because more people will act immediately to avoid losing access.	The text box with a white border will be on the left. An icon of a cell phone with a screenshot of a real text on the screen will be to the right. The urgent language and sender will be highlighted.	The text will fade in by paragraph. The highlighted text will be timed with the audio.	

Slide 3.6 / Menu Title: Knowledge Check / Learning Objective #2

Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Let's check what you have learned so far. How can you identify that you are receiving a Phishing attack message? Select all that apply, then select submit.	[Slide Title] **Knowledge Check** How can you identify that you are receiving a Phishing attack message? Select all that apply, then select submit. -You have a weird feeling about the message.	Title across the top. A banner is a lighter color under the title with the question. Multiple answer checkboxes under the question.	The learner will receive immediate feedback on their answer.	

	–The sender is requesting your pin or password. (Correct) –The email address does not match the sender.(Correct) –The message contains pictures. –The message contains threats if you don’t act immediately.(Correct) Answer Responses: Correct – That's right! Those are all types of Phishing attacks. Incorrect –Incorrect. Requesting pins/passwords, threats, and the email not matching the sender are all signs the message might be an attack. Try Again –That is incorrect. Please try again.			

Slide 4.1 / Menu Title: Best Practices				
Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
There are many things we can do to prevent Phishing. Follow	[Slide Title] **Best Practices**	Title across the top of the slide.	Accordion Interaction	

these tips to avoid becoming the next victim of a cyber attack. Select each option from left to right, starting with Email Address.	Follow these tips to avoid being the victim of malware… [Directions] Select each option to learn more. [Buttons] Email Address Attachments Passwords Online Posts Domain	The directions in a blue box above the accordion. The accordion buttons are in tall columns to the left in different colors. The slide will start with the text on the screen and fade with the audio.	When each button is clicked, it will reveal the corresponding slide layer. It will look as if the button is moving across the screen like an accordion. The next button will be disabled until the learner visits every layer and the entire accordion is open. The beginning text will fade with the audio.	

Slide 4.1.A / LAYER: Email Layer *(Hidden from menu)*

Narration / Voiceover:	Layer Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
When receiving an email, always look at the email address, not just the sender's name.Cyber criminals will often use a company member's real name to trick you into thinking the email is legitimate. Always check the email address, paying special attention to the domain.	**Look at the EMAIL address, not just the sender.** ● Criminals will use a company member's name ● Always check the email address ● Look at the Domain name	The layer button will move to the right. A picture will be at the top and the text underneath. The text will be in a slightly lighter color than the rest of the layer. The text will be black.	The layer button will slide to the right.	

Slide 4.1.B / LAYER: Attachments Layer *(Hidden from menu)*				
Narration / Voiceover:	Layer Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Never click a link or open attachments in an email. This is the number one way malware and ransomware is installed onto your computer. Go to the source of the email if you have questions about the validity of the URL or attachment.	**Never click a link or open attachments.** ● Number one cause of malware ● Contact the source	The layer button will move to the right. A picture will be at the top and the text underneath. The text will be in a slightly lighter color than the rest of the layer. The text will be black.	The layer button will slide to the right.	

Slide 4.1.C / LAYER: Passwords Layer *(Hidden from menu)*				
Narration / Voiceover:	Layer Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Be sure to create strong passwords for all of your accounts.The best passwords do not include words, have a mix of numbers, letters, and symbols, and are at least 8 characters in length. It is VERY important that your bank account password should	**Create strong passwords for all accounts.** ● Do not include real words ● Your bank account password should ALWAYS be entirely	The layer button will move to the right. A picture will be at the top and the text underneath. The text will be in a slightly lighter color	The layer button will slide to the right.	

ALWAYS be entirely different from any other password. Also, enable two-step verification on accounts whenever possible.	different from any other password - Enable two-step verification on accounts	than the rest of the layer. The text will be black.		

Slide 4.1.D / LAYER: Online Posts Layer *(Hidden from menu)*				
Narration / Voiceover:	Layer Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Be careful when posting to social media online. Never give away too much personal information or divulge common security question answers such as your mother’s maiden name, first car model, or town where you grew up. It is important to enable privacy options and restrict public access to personal accounts on social media as well.	**Be careful with online posts.** - Never give away too much personal information online - Never divulge common security question answers online - Enable privacy options and restrict public access to personal accounts	The layer button will move to the right. A picture will be at the top and the text underneath. The text will be in a slightly lighter color than the rest of the layer. The text will be black.	The layer button will slide to the right.	

Slide 4.1..E / LAYER: Domain Layer *(Hidden from menu)*				
Narration / Voiceover:	Layer Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Any time you receive an email from someone at your company, check the domain in their email address. It is easy for a cyber criminal to use a real company member's name as their contact. Always verify the domain is accurate. The domain is located after the at symbol.	**For internal emails, check the domain in their email address.** ● Cyber criminal use a real company member's name as their contact ● Always verify the domain is accurate	The layer button will move to the right. A picture will be at the top and the text underneath. The text will be in a slightly lighter color than the rest of the layer. The text will be black.	The layer button will slide to the right.	

Slide 4.2 / Menu Title: Quiz Intro				
Narration / Voiceover:	Slide Text:	Visual Display:	Animation/Interaction:	Reviewer Notes
It's time for your assessment. You'll answer 5 questions. You must earn 80% to pass. Click Next to begin the quiz.	[Slide Title] **Graded Quiz** **5 Questions** **80% to pass** [Directions] Click NEXT to begin the quiz.	Background image: Semi transparent picture of someone on their computer.	The text will fade in timed with the audio.	

Last updated: 5/25/2023

Slide 4.3 / Menu Title: Quiz Question 1 *(Hidden from menu)* / Learning Objective #3				
Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
NA	[Slide Title] **Quiz** [Multiple Selection Question] Select all of the ways you can spot a Phishing Attack. Then select submit.	Title across the top. A banner is a lighter color under the title with the question. Image of a desktop computer in the center. Multiple answer checkboxes inside the computer icon.	*No immediate feedback.*	

Slide 4.4 / Menu Title: Quiz Question 2 *(Hidden from menu)* / Learning Objective #1				
Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
NA	[Slide Title] **Quiz** [Matching Question] Match the type of Phishing attack with its definition. Then select submit.	Title across the top. A banner is a lighter color under the title with the question. Matching boxes underneath the question.	*No immediate feedback.*	

Slide 4.5 / Menu Title: Quiz Question 3 *(Hidden from menu)* / Learning Objective #2				
Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
NA	[Slide Title] **Quiz** [Scenario Question] Scenario 1 You receive this text message from a subscription you use daily. You are afraid you might lose your access if you don't respond immediately. What is the best action to take? Select the correct answer, then select submit. ● Respond with your PIN number so you don't lose access ● Don't respond. Call the company to verify your account access. ● Click on the link and see what the next steps are.	Title across the top. A banner is a lighter color under the title with the question. Multiple answers are underneath. An image of a cell phone is to the left.	*No immediate feedback.*	

Last updated: 5/25/2023

Slide 4.6 / Menu Title: Quiz Question 4 *(Hidden from menu)* / Learning Objective #2

Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
NA	[Slide Title] **Quiz** [Question] Scenario 2 You receive an email from what appears to be your boss. You don't want to get in trouble for not following her request. What do you do? Select the correct answer, then select submit. ● Immediately call her to confirm the email is legitimate. ● Follow the request in the email to avoid any reprimand from your boss. ● Email back to see if it is really her.	Title across the top. A banner is a lighter color under the title with the question. Multiple answers are underneath. An image of a computer is to the left.	*No immediate feedback.*	

Slide 4.7 / Menu Title: Quiz Question 5 *(Hidden from menu)* / Learning Objective #3				
Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
NA	[Slide Title] **Quiz** [Question] Select all of the ways you can stay protected from potential malware. Then select submit. ● Check the email of a sender, not just their contact name. ● Verify the URL of a link in an email by hovering over it. ● Copy and paste any URL from an email in a new tab to verify it. ● Enable privacy restrictions on social media accounts. ● Use familiar words or phrases for your passwords.	Title across the top. A banner is a lighter color under the title with the question. Multiple answer checkboxes inside the computer icon.	*No immediate feedback.*	

Slide 4.8 / Menu Title: Quiz Results				
Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
NA	[Slide Title] **Quiz Results** Your Score Passing Score: 80%	Background image: Semi transparent picture of someone on their computer.	*This is the base layer.* *All interaction will be on the slide layers depending on the learner's score.*	

Slide 4.8.A / LAYER: SUCCESS *(Hidden from menu)*				
Narration / Voiceover:	Layer Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Thank you for taking the quiz. Congratulations! You passed. You can review your results by clicking on the review quiz button. If you are satisfied with your results and ready to move on, please click on the continue button.	Nice job, you passed! [Buttons} Review Quiz Continue	Slide base layer will be displayed (4.8)	*A passing score will show this layer with the learners score.* *The Review Quiz will take the learner back through the questions.* *The Continue button will advance to slide 4.9.*	

Last updated: 5/25/2023

Slide 4.8.B / LAYER: FAILURE *(Hidden from menu)*				
Narration / Voiceover:	Layer Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Thank you for taking the quiz. Unfortunately, you did not pass. You can review your results by clicking on the review quiz button. When you are ready to try again, please click on the retake quiz button.	Sorry, you didn't pass. [Buttons} Retake Quiz Review Quiz	Slide base layer will be displayed (4.8)	*A failing score will show this layer with the learners score.* *The Review Quiz button will take the learner back through the questions.* *The Retake Quiz button will bring the learner to the beginning of the quiz, slide 4.3.*	

Slide 4.9 / Menu Title: Summary				
Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
You should now be able to classify types of Phishing attacks, analyze potential security threats, and identify best practices for preventing malware.	[Slide Title] **Summary** You should now be able to: Classify types of Phishing attacks Analyze potential security threats identify best practices for preventing malware	The title will be across the top. The text will be directly below. The three objectives will be shown in the center of the screen with a different color background.	*The text will fade in timed with audio.* *The slide will auto advance to slide 4.10.*	

Last updated: 5/25/2023

Slide 4.10 / Menu Title: Congratulations				
Narration / Voiceover:	Slide Text:	Visual Display:	Animation / Interaction:	Reviewer Notes
Congratulations on completing the Preventing Phishing Attack course. Now you have the knowledge you need to keep your personal and private information safe. You will be able to spot threats before replying, clicking links, or opening attachments. We thank you for helping our company stay safe.	[Slide Title] **Congratulations!** [Directions] Click the COMPLETE button to exit this course. [Button] Complete	Background picture of a person with a device. Large banner with title and button at the bottom similar to Welcome slide. Custom Complete button.	*The text will fade in timed with audio.* *The Complete button will exit the course.*	

Last updated: 5/25/2023