STORYBOARD

Module Title: Think Before You Click: Identifying and Reporting Phishing E-mails

Target Audience: All new employees as part of onboarding. Employees are generally college graduates that are familiar with email and technology.

Learning Objectives:

Terminal LOs:

1. Explain the purpose of phishing emails and their potential impact on individuals and organizations.
2. Identify common characteristics of phishing emails.
3. Evaluate the validity of links and sender addresses to determine whether an email is legitimate.
4. Respond appropriately to suspicious emails.

Seat Time: 30 minutes

Outline:

- Welcome
- Navigation
- Workplace Scenario
- Phishing at Work
- Course Overview
- What is Phishing
- Phishing in the Workplace
- Knowledge Check
- Consequences of Phishing
- Preventing Damage from Phishing
- Characteristics of Phishing
    - Suspicious Language
    - Urgency
    - Unusual Requests
- Knowledge Check
- Evaluation of Emails
    - Link Verification
    - Email Verification

- Reacting to Suspicious Emails
- Reporting Suspicious Emails
- Simulated vs. Real Phishing
- Summary
- Introduction to Quiz
- Congratulations

Font: Segoe UI
Segoe UI Bold - Major Headings
Segoe UI Semibold

Color Palette:



Global Comments: ***(optional)***

- Texts generally have a 0.5 second fade
- Slide titles are in all caps with a gray color font (#6B7280)
- In lieu of white background, use a background rectangle in light gray color (#F2F4F7)
- Unless otherwise specified, hide the next button on each slide until the audio ends and the learner has clicked on all required objects
- Informational text that does not need to be on-screen is noted in brackets, [ ].

Slide: 1.1 / Menu Title: Welcome			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Use a scrolling video as a background that is related to email and phishing attempts.	[Slide Title] Think Before You Click [slide subheading] Preventing Phishing Attacks [Buttons] Navigation Start	Welcome to Think Before You Click: Preventing Phishing Attacks. In this training you'll see how everyday emails can lead to real security breaches — and how to recognize and report them before damage is done. Select Navigation to review the controls, or choose Start to begin the training.	The subheading, Start and Navigation buttons will fade in timed with the VO reference The Start button will jump to slide 1.3 The Navigation button will jump to slide 1.2

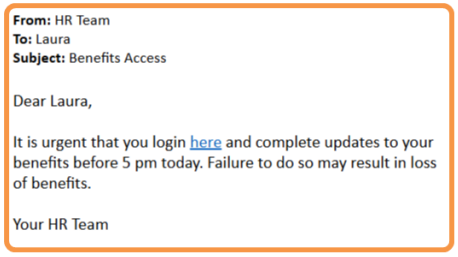
Slide: 1.2 / Menu Title: Course Navigation			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Player shows Menu on the left. Background image is screenshot of home page with previous and next buttons visible. Caption bubbles with labels point to player features	[Slide Title] Navigation [Captions] Next Previous Volume Replay Seekbar Play/Pause	Take a few minutes to become familiar with the navigation features of the player. Click next to advance to the next slide or previous to return to the previous slide. Click the Full Screen icon to enlarge the slide. Use the volume icon to control the sound.	Caption bubbles are timed to appear when introduced in VO. Next button is visible.

	Menu Full Screen Playback Speed	You can speed up or slow down the playback speed using this feature. You can replay the entire slide by clicking here or use the seek bar to find the specific portion of the slide you'd like to revisit. Use this button to pause or play the slide and finally, Revisit a slide by using the menu resource on the left. Click Next to begin the course	

Slide: 1.3 / Menu Title: Workplace Scenario			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
A woman avatar (Laura) is on the left side of the screen. She is happy facing forward. The remainder of the slide is an image of an office background.	[Slide Title] WORKPLACE SCENARIO	Phishing emails don't always seem obviously suspicious and they're often timed to catch you off guard, like when you're busy, distracted, or about to log off for the day. Let's take a look at what happens to Laura, Director of HR, late on a Friday afternoon.	The slide automatically advances to the next slide when the media completes.

Slide: 1.4 / Menu Title:			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**

Slide begins with same female avatar and office background as in previous slide. Male avatar fades on right side of screen. Female avatar has three poses. • Happy facing forward pose • Turn to male avatar pose • Concerned pose Male avatar has two poses. • Happy facing forward • Pointing to watch	[Slide Title] WORKPLACE SCENARIO [Male avatar caption] We're heading out to eat now. You coming? [Female avatar caption] Be there in a sec - one last email check [Male avatar] [3] Don't take too long	[Male avatar] [1] We're heading out to eat now. You coming? [Female avatar] [2] Be there in a sec - one last email check [Male avatar] [3] Don't take too long [Female avatar] [4] What is this?	Male avatar fades in on right side of screen. Female avatar turns to look at male when she first speaks. Male avatar points at watch as he says 'don't take too long. Zoom into female avatar as her expression changes to concern.' Slide auto advances when the timeline ends on this slide.

Slide: 1.5 / Menu Title:			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Zoomed region of previous slide is visible with shape muting colors. An email is prominent on the screen.	[Slide Title] WORKPLACE SCENARIO  **From:** HR Team **To:** Laura **Subject:** Benefits Access Dear Laura, It is urgent that you login here and complete updates to your benefits before 5 pm today. Failure to do so may result in loss of benefits. Your HR Team	Laura receives the following email.	Next button is hidden when timeline starts. Next button is visible once media completes on this slide.

Slide: 1.6 / Menu Title:			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Question is at top of slide. Three boxes with statements below the question. The middle box is the correct answer.	[Slide Title] WORKPLACE SCENARIO How should Laura respond to the email? [Box 1] Ignore the email. It is late on a Friday and she can deal with it on Monday. [Box 2 Correct] Report the email to IT as a suspected phishing attempt. [Box 3] Click on the link and enter information to prevent losing benefits.	How should Laura respond to the email? Select the button of the best response.	Question fades in as timeline starts. Boxes appear once VO completes reading the question. Hover states exist for boxes. Once clicked, the box says Incorrect or Correct. Learner is restricted from selecting a box until VO ends. Audio plays on separate layers once a box is selected [see below]

Slide: 1.6.a / Menu Title:			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Layer is the same as base layer - just audio playing once button 1 is selected.		Incorrect If Laura ignores the email she risks allowing a colleague to engage with the suspicious email.	Hide this layer when media completes.

Slide: 1.6.b / Menu Title:			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Layer is the same as base layer - just audio playing once button 2 is selected.		CORRECT Laura should report the email to IT as a suspected phishing attempt before she heads out.	Jump to next slide when media completes.

Slide: 1.6.c			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Layer is the same as base layer - just audio playing once button 3 is selected.		Incorrect The email contains characteristics of phishing emails and clicking on the link could pose a variety of risks.	Hide layer when media completes.

Slide: 1.7 / Menu Title: Phishing at Work			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Slide begins with a gray background and the same image of the email Laura received in slide 1.5 Three boxes with text appear later.	[Slide Title] PHISHING AT WORK [Box 1] Phishing emails are designed to look routine and urgent [Box 2] Security breaches often begin with a single click	If Laura had clicked on the link in the email she would likely have put her company's information at risk. As you'll learn in this training, phishing emails are designed to look routine and urgent. Security breaches often begin	The email fades in as slide begins. Aligned to VO, the email fades out. Three boxes with text appear aligned to VO. Advance to next slide when timeline ends on this slide.

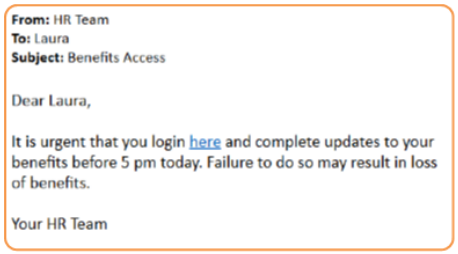
	[Box 3] Security breaches often begin with a single click Learning how to recognize and report emails protects you and your organization.	with a single click on a seemingly routine message. Learning how to recognize and report suspicious emails protects you and your organization.	

Slide: 1.8 / Menu Title: Course Overview			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Heading is present at top of slide Gray bar is present under heading. Four bullet points with phrases are present underneath the heading and bar.	[Slide Title] COURSE OVERVIEW [Heading] In this course, you'll learn how to: [Bullet 1] Explain the purpose of phishing emails and their potential impact on individuals and organizations. [Bullet 2] Identify common characteristics of phishing emails. [Bullet 3] Evaluate the validity of links and sender addresses to determine whether an email is legitimate. [Bullet 4] Respond appropriately to suspicious emails.	In this course, you'll discover ways to prevent against attempted phishing by learning how to: explain the purpose of phishing emails and their potential impact on individuals and organizations. Identify common characteristics of phishing emails. evaluate the validity of links and sender addresses to determine whether an email is legitimate, and Respond appropriately to suspicious emails Click Next when you are ready and let's get started	Heading fades in as slide begins. Four bullet points and statements fade in timed to VO.

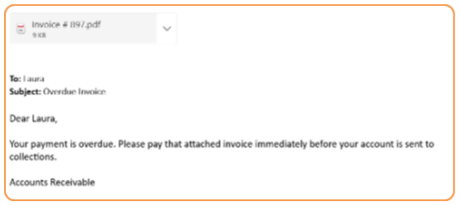
Slide: 1.9 / Menu Title: What is Phishing	**LO:** Explain the purpose of phishing emails and their potential

		impact on individuals and organizations.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Image on right of a computer screen with visual indicators suggesting a potential phishing attempt. Text box on left side of slide	[Slide Title] WHAT IS PHISHING [Text box] **Phishing**: when a trusted source is impersonated to gain access to sensitive information.	To start this course, let's clarify what we mean by phishing. Phishing occurs when someone impersonates a trusted source to gain access to sensitive information. In the workplace, these attempts most commonly arrive through email.	The picture fades in as the slide starts. Text box fades in when VO defines phishing.

Slide: 1.10 / Menu Title: Phishing in the Workplace		**LO:** Explain the purpose of phishing emails and their potential impact on individuals and organizations.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
A large rectangle is present. Inside the rectangle is an image of a desktop with a computer open and email on laptop screen, Three tabs (as part of a click to reveal) exist horizontally across the top of the rectangle.	[Slide Title] PHISHING IN THE WORKPLACE [Heading Text] Phishing emails in the workplace often contain links, attachments, or QR codes. [Box 1] Links [Box 2] Attachments [Box 3] QR Codes	To gain access to sensitive information, phishing emails in the workplace often contain links, attachments, or QR codes. Click on each tab to learn more. Then click next to proceed.	Learner is prevented from clicking on a button until the VO completes. This slide requires the learner to click 3 buttons. Each button takes them to a separate layer on this slide. Each button has a hover and visited state. Next button is hidden until the state of all three boxes is visited.

Slide: 1.10a /		**LO:** Explain the purpose of phishing emails and their potential impact on individuals and organizations.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
The base layer is present, but the image of the desktop and computer is hidden. Text and a sample email are present inside the large rectangle. The buttons remain at the top.	[Slide Title] PHISHING AT WORK Phishing emails may contain links that send recipients to fake websites designed to mimic legitimate pages.  **From:** HR Team **To:** Laura **Subject:** Benefits Access Dear Laura, It is urgent that you login here and complete updates to your benefits before 5 pm today. Failure to do so may result in loss of benefits. Your HR Team	Phishing emails may contain links that send recipients to fake websites designed to mimic legitimate pages. When account information is entered on these fake sites, attackers can capture credentials and use them to access email accounts, internal systems, or cloud-based tools. Once inside, hackers may steal data, impersonate employees, or launch additional attacks across the organization.	Clicking on the links button brings up this layer. User is prevented from clicking on other tabs until VO completes. A circle fades in to highlight the link in the email - aligned to VO.

Slide: 1.10.b		**LO:** Explain the purpose of phishing emails and their potential impact on individuals and organizations.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
The base layer is present, but the image of the desktop and computer is hidden. Text and a sample email are present inside the large rectangle. The buttons remain at the top.	[Slide Title] PHISHING AT WORK Phishing emails may contain malicious attachments that install malware on a computer.	Phishing emails may contain malicious attachments that install malware on a computer. Some types of malware can record keystrokes, allowing attackers to capture usernames, passwords, and other sensitive information without the user's	Clicking the attachments button brings up this layer. Learners are prevented from clicking on other tabs until VO completes. A circle fades in to highlight the attachment in the email - aligned

		knowledge. Other malware, such as ransomware, can lock or encrypt systems, preventing employees from accessing files and applications needed to perform their work.	to VO

Slide: 1.10c		**LO:** Explain the purpose of phishing emails and their potential impact on individuals and organizations.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
The base layer is present, but the image of the desktop and computer is hidden. Text and a sample email are present inside the large rectangle. The buttons remain at the top.	[Slide Title] PHISHING AT WORK Phishing emails can also contain QR codes that direct you to a fake website. 	Increasingly, phishing emails contain QR codes that direct you to a fake website, where attackers try to obtain sensitive login information. The use of QR codes is increasing because they obscure the actual destination of the link, making it harder for users and security tools to identify malicious websites.	Clicking the QR button brings up this layer. Learners are prevented from clicking on other tabs until VO completes. A circle fades in to highlight the QR code in the email - aligned to VO

Slide: 1.11 / Menu Title: Knowledge Check		**LO:** Explain the purpose of phishing emails and their potential impact on individuals and organizations.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
The question is at the top of the screen with four rectangular buttons.	[Slide Title] KNOWLEDGE CHECK	Before continuing on, let's pause for a moment and check your understanding of what you've	Learners cannot click on a button until VO completes. Learners have two attempts.

	Which of the following are likely to be found in a phishing email in the workplace? Select all that apply. [Box 1 - correct] QR Codes [Box 2 - correct] Links [Box 3- correct] Attachments [Box 4] Employee Signatures	learned so far. Select all options that are commonly found in phishing emails. Then click submit to check your answers.	Use a convert to freeform to create this KC and create customized feedback layers.

Slide: 1.11.a			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Correct layer. A rectangle with text is present along with a continue button. The base layer is present, but the answer buttons are hidden.	[Box with text] Correct. Phishing emails in the workplace often contain QR codes, links, and/or attachments. [Custom Button] Continue	Correct. Phishing emails in the workplace often contain QR codes, links, and/or attachments. Click Continue to proceed.	Learners click on a custom continue button to continue to slide 12.

Slide: 1.11.b			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Incorrect layer	[Text Box]	Incorrect.	Learners click on a custom continue button to continue to

At the top of the slide is a box with text. A screenshot of the knowledge check question with the correct answers selected is visible. A custom continue button is also present.	Incorrect. Review the correct answers below.	QR codes, links, and attachments are all likely to be found in phishing attempts in the workplace. Click Continue to proceed.	slide 12

Slide: 1.11.c			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Try again layer. A rectangle with text is present along with a custom try again button. The base layer is present, but the answer buttons are hidden.	[Box] Incorrect. Try Again. [Custom button] Try again	Incorrect. Click Try Again to try answering the question again.	Try Again button hides the layer Change state of answer choices on base layer to normal.

Slide:1.12 / Menu Title: Consequences of Phishing		**LO:** Explain the purpose of phishing emails and their potential impact on individuals and organizations.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Five vertical bars in an accordion configuration are on the left side of the screen. A picture of a distressed man in an office is visible to the right of the accordion configuration.	[Slide Title] CONSEQUENCES OF PHISHING [Accordion Box 1] Financial Loss [Accordion Box 2]	Now that you understand the purpose of phishing attacks, let's take a closer look at the consequences of a successful attack. Select each tab to explore the	Learners are prevented from clicking on a box until VO ends. Next button is hidden until the states of each accordion (or vertical) box are visited.

Two additional text boxes appear later and are across the image of the man.	Reputational Damage [Accordion Box 3] Data Compromise [Accordion Box 4] Privacy Breach [Accordion Box 5] Business Disruption [Direction Text box 1] Select each tab to explore the different impacts. [Direction Text box 2] When you're finished with a tab, use the X button to close it.	different impacts. When you're finished with a tab, use the X button to close it.	Accordion boxes have hover and visited states. Clicking on an accordion box brings up that layer. Each direction box fades in separately timed to VO. Directions boxes fade out together as VO ends.

Slide: 1.12.a			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Financial Loss layer Most base layer images are hidden. The ones that remain are the slide title text and the Financial Loss Button The other four accordion buttons are recreated on this layer, but are not clickable. An image of a person at a computer in distress is present. Text is on top of the image.	[Slide Title] CONSEQUENCES OF PHISHING [Informational Text} Financial losses can happen from: theft of account information and funds approval of fraudulent invoices Example: Facebook and Google paid over $100 million in fraudulent invoices [Accordion Box 2]	Financial losses from phishing attacks can occur when attackers gain access to account information - allowing them to send funds to other accounts. Phishing attacks can also lead to the approval and payment of fake invoices. One notorious example of financial losses from phishing attacks occurred in 2013-2015 when attackers sent fake invoices to Facebook and Google. These fraudulent invoices were	Learner is prevented from clicking on the base layer accordion buttons that remain active. Learner is prevented from clicking on the X until the VO ends. Clicking the X closes the layer. As the layer opens, the four accordion boxes next to Financial loss slide open along a motion path. The image and text with X

An X is in the upper right hand corner.	Reputational Damage [Accordion Box 3] Data Compromise [Accordion Box 4] Privacy Breach [Accordion Box 5] Business Disruption	approved and paid, resulting in total losses exceeding $100 million.	appears. When learner clicks on X the accordion boxes close and the learner returns to the base layer. The four accordion boxes on the layer do not have hover or visited states.

Slide: 1.12.b			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Reputational Damage Most base layer images are hidden. The ones that remain are the slide title text and the Financial Loss and Reputational Damage buttons. The other three accordion buttons are recreated on this layer, but are not clickable. An image of a computer screen with down arrows is present. Text is on top of the image. An X is in the upper right hand corner.	[Slide Title] CONSEQUENCES OF PHISHING [Informational Text} Reputational damage can occur from: public notification of compromised data loss of customer trust Example: Payment information exposed for more than 40 million Target customers. [Accordion Box 3] Data Compromise [Accordion Box 4] Privacy Breach [Accordion Box 5]	Successful phishing attacks can also damage a company's reputation. Companies must provide notification to their customers after a data breach, which can lead to loss of customer trust when a company is perceived to not take security seriously. For example, following a fishing attack on Target in 2013, attackers gained access to credit card information for more than 40 million customers. Target notified affected customers, and the incident significantly damaged customer trust and the company’s reputation.	Same as 12.a, but the three accordion boxes next to Reputational Damage slide open along a motion path.

	Business Disruption		

Slide: 1.12.c			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Data Compromise layer Most base layer images are hidden. The ones that remain are the slide title text and the Financial Loss, Reputational Damage, and Data Compromise The other two accordion buttons are recreated on this layer, but are not clickable. An image of a computer screen with various pieces of data is visible. Text is on top of the image. An X is in the upper right hand corner.	[Slide Title] CONSEQUENCES OF PHISHING [Informational Text} Phishing attacks can result in the exposure of: proprietary data and information intellectual property or confidential business data Example: Attack at Sony Pictures Entertainment led to exposure of unreleased films and confidential information [Accordion Box 4] Privacy Breach [Accordion Box 5] Business Disruption	Successful phishing attacks compromise company data. This can include the loss or exposure of proprietary data and information as well as the exposure of intellectual property or confidential business data One notorious example happened when Sony Pictures was attacked and unreleased movies as well as other confidential information was exposed.	Same as 12.a, but the three accordion boxes next to Data Compromise slide open along a motion path.

Slide: 1.12.d			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Privacy Breach layer Most base layer images are hidden. The ones that remain are	[Slide Title] CONSEQUENCES OF PHISHING	Successful phishing attacks can also expose sensitive customer information. This information can include	Same as 12.a, but the one accordion box next to Privacy Beach slides open along a motion path.

the slide title text and the Financial Loss, Reputational Damage, Data Compromise and Privacy Breach The other accordion button is recreated on this layer, but is not clickable. A unique image of a computer screen with different pieces of data is visible. Text is on top of the image. An X is in the upper right hand corner.	[Informational Text} Attacks can expose sensitive customer information: Social Security numbers, bank account information and passwords leads to identity theft and other forms of fraud Example: Healthcare company attack resulted in the exposure of information for over 100,000 patients [Accordion Box 5] Business Disruption	Social Security numbers, bank account information, and passwords. This unauthorized access to customer personal data can lead to identity theft and other forms of fraud. In 2020, phishing attacks were successful on two employees at a healthcare company. The result was the exposure of information for over 100,000 patients.	

Slide: 1.12.e			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Privacy Breach layer Most base layer images are hidden. The ones that remain are the slide title text and all the accordion buttons. An image with a closed sign in the window of a business is visible. Text is on top of the image. An X is in the upper right hand corner.	[Slide Title] CONSEQUENCES OF PHISHING [Informational Text} Successful attacks can result in: disruption or slowdown of business processes. Example Attack on Colonial Pipeline disrupted fuel delivery across many parts of the country	Successful phishing attacks can also result in the disruption or shutdown of business. For example, in 2021, a phishing email compromised employee credentials at Colonial Pipeline, enabling a ransomware attack. Pipeline operations were shut down to contain the damage, disrupting fuel delivery across large parts of the United States. Colonial Pipeline ultimately paid a ransom to resume normal	Learner is prevented from clicking on the base layer accordion buttons that remain active. Learner is prevented from clicking on the X until the VO ends. Clicking the X closes the layer. The image and text with X appears.

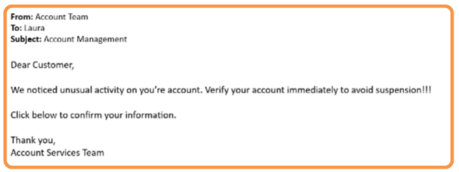
		operation	

Slide: 1.13 / Menu Title: Preventing Damage From Phishing		**LO:** Identify common characteristics of phishing emails.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
When slide appears, an image of colleagues looking at a computer screen appears. Information text is on the left side of the screen	[Slide Title] PREVENTING DAMAGE FROM PHISHING [Informational Box] Most phishing attempts can be identified and stopped before damage occurs.	Although a single phishing email can lead to serious consequences, most attempts can be identified and stopped—especially when everyone stays alert. In the next section, you'll learn the common characteristics of phishing emails and how to recognize them before any information is shared.	The informational text appears aligned to the VO. Picture fades in on right side of screen as slide appears..

Slide: 1.14 Characteristics of Phishing Emails		**LO:** Identify common characteristics of phishing emails.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Image of an email icon on lower ⅔ of the slide. Three buttons across the middle of the email image.	[Slide Title] CHARACTERISTICS OF PHISHING EMAILS [Line of text at top] Click each button to learn more. [Button 1] Suspicious Language [Button 2] Urgency [Button 3] Unusual Requests	Phishing emails often contain one or more of the following characteristics: suspicious language, a sense of urgency, and unusual requests. Click on each button to learn more about each of these characteristics.	Learner is prevented from clicking on each button until VO is complete. Next button is hidden until all three buttons have been visited. Clicking on the Next button brings up slide 1.18. Suspicious Language button - slide 15 Unusual Requests button - slide 16

			Urgency button- Slide 17 Line of text and buttons fade in as slide starts. Each button has a visited and hover state. Clicking on a button brings up a new slide [in a branching scenario]. An orange rectangle highlights each button in a clock animation as the VO names each button.

Slide: 1.15 Suspicious Language		**LO:** Identify common characteristics of phishing emails.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Light gray background on slide. Lines of text at the top. Rounded box in branded colors with text. Image of email with border.	[Slide Title] SUSPICIOUS LANGUAGE [Line text] Signs of suspicious language include: • Inconsistent formatting • Misspelled words • Phrases that don't' sound quite right [Box of text] Click the email to investigate suspicious language.	Suspicious language is common in most phishing emails and includes language that seems unusual or unprofessional. Watch for signs of suspicious language, such as: inconsistent formatting, misspelled words, or phrases that don't sound quite right. Legitimate organizations typically use clear, professional language and carefully review messages before sending them. Click the email to investigate suspicious language.	Learner is prevented from clicking until VO is complete. Lines of text fade in aligned to VO. Box of text and email image fade in together as aligned in VO. Next button is hidden (trigger on next layer), but takes to slide 1.14 once available Clicking on email brings up zoomed in layer.

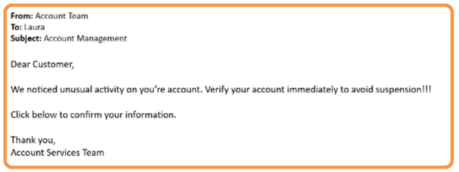
Slide: 1.15.a [zoomed in layer]			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Everything in base layer except for gray background and title is hidden. Line text is near the top of the slide. A larger image of the email from the base layer is present.	[Slide Title] SUSPICIOUS LANGUAGE [Line text] Click on the two parts of the email that have unusual or unprofessional language.	Take a moment to read the email and find two instances of suspicious language. Click each instance of suspicious language in the email. After identifying both, select Next.	Learner is prevented from clicking on the email until the VO completes. Transparent shapes cover the following three words/phrases in the email. • You're • !!! • Thank you, Account Services Team Next button is hidden until learner clicks on the boxes over the correct phrases (you're and !!!). Each shape has a visited state. The first two (correct answers) have a green check in the visited state. The last shape has a red x in the visited state. All images, shapes, and text fade in as slide starts. Clicking on each shape brings up a new layer.

Slide: 1.15.b [you're layer]			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Clicking on the shape around "you're" brings up this layer. The email from the base layer is visible. An orange circle surrounds the word you're in the email. Lines of text are at the top	[Slide Title] [Slide Title] SUSPICIOUS LANGUAGE [Lines of text] Correct! The email confused your and you're.	Correct! Grammar errors - like incorrectly using you're and your - can signal a phishing attempt.	The circle and lines of text fade in as the slide appears. The zoomed in layer is shown when the media completes on this layer.

Slide: 1.15.c [!!! layer]			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Clicking on the shape around "!!!" brings up this layer. The email from the base layer is visible. An orange circle surrounds the !!! in the email. Lines of text are at the top	[Slide Title] [Slide Title] SUSPICIOUS LANGUAGE [Lines of text] Correct! The email contained excessive punctuation.	Correct! Excessive punctuation — like multiple exclamation points —can signal an unprofessional or suspicious email.	The circle and lines of text fade in as the slide appears. The zoomed in layer is shown when the media completes on this layer.

Slide: 1.15.d [Closing layer]			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Clicking on the shape around the	[Slide Title]	While this closing is generic, it	

email closing brings up this layer. The email from the base layer is visible. Lines of text are at the top	SUSPICIOUS LANGUAGE [Lines of text] Incorrect! The closing is not suspicious or unprofessional.	does not clearly indicate suspicious or unprofessional language. Try again.	The zoomed in layer is shown when the media completes on this layer.

Slide: 1.16 Unusual Requests		**LO:** Identify common characteristics of phishing emails.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Light gray background on slide. Lines of text at the top. Rounded box in branded colors with text. Image of email with border.	[Slide Title] UNUSUAL REQUESTS [Line text] Unusual requests include: • sharing of sensitive information like Social Security numbers, passwords, and account information • Instructions that don't follow typical processes. [Box of text] Click the email to investigate unusual requests. [Image of e-mail]  **From:** Account Team **To:** Laura **Subject:** Account Management Dear Customer, We noticed unusual activity on you're account. Verify your account immediately to avoid suspension!!! Click below to confirm your information. Thank you, Account Services Team	Phishing emails often contain unusual requests like sharing of sensitive information like Social Security numbers, passwords, and account information as well as instructions that don't follow typical processes Legitimate organizations never request sensitive information via email and instead use secure portals, internal systems, or in-person verification. Click the email to practice spotting unusual requests.	Learner is prevented from clicking until VO is complete. Lines of text fade in aligned to VO. Box of text and email image fade in together as aligned in VO. Next button is hidden (trigger on next layer), but takes to slide 1.14 once available Clicking on email brings up zoomed in layer.

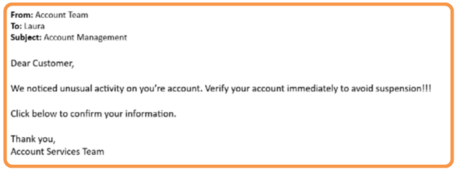
Slide: 1.16.a [zoomed in layer]			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Everything in base layer except for gray background and title is hidden. Line text is near the top of the slide. A larger image of the email from the base layer is present.	[Slide Title] Unusual Requests [Line text] Click on the part of the email that contains an unusual request.	Take a moment to read the email and try to find one unusual request. Click on the part of the email that contains the unusual request. After checking your answer, select Next.	Learner is prevented from clicking on the email until the VO completes. Transparent shapes cover the following phrases: • We are updating our system • Please reply to this email with your username and password. Next button is hidden until learner clicks on the box covering the correct phrase (Please reply to this email with your username and password.). Each shape has a visited state. The correct answer has a green check in the visited state. The incorrect answer has a red x in the visited state. All images and text fade in as slide starts. Clicking on each shape brings up a new layer.

Slide: 1.16.b [Updating System layer]			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Clicking on the shape around	[Slide Title]	Incorrect. Although the phrasing	The lines of text fade in as the

“updating systems" brings up this layer. The email from the base layer is visible. Lines of text are at the top	UNUSUAL REQUESTS [Lines of text] Incorrect! Companies may update systems periodically.	is generic, companies may periodically update systems.	slide appears. The zoomed in layer is shown when the media completes on this layer.

Slide: 1.16.c [Reply to email layer]			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Clicking on the shape around “Please reply to this email with your username and password." brings up this layer. The email from the base layer is visible. An orange circle surrounds the ‘Please reply to this email with your username and password’ in the email. Lines of text are at the top	[Slide Title] UNUSUAL REQUESTS Correct! Legitimate corporations will never ask for your username and password in an email.	Correct! Legitimate corporations will NEVER ask for any account or password information in an email.	Learner is prevented from clicking on the slide. The circle and lines of text fade in as the slide appears. The zoomed in layer is shown when the media completes on this layer.

Slide: 1.17 Urgency			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Light gray background on slide. Lines of text at the top. Rounded box in branded colors with text.	[Slide Title] URGENCY [Line text] Common signs of urgency include:	Most phishing emails create a sense of urgency to generate panic and cause the recipient to act hastily. Common signs of false urgency in phishing emails include	Learner is prevented from clicking until VO is complete. Lines of text fade in aligned to VO. Box of text and email image fade

Image of email with border.	• requests for immediate action • threats of consequences • pressure to act quickly [Box of text] Click the email to investigate signs of urgency. [Image of e-mail]  **From:** Account Team **To:** Laura **Subject:** Account Management Dear Customer, We noticed unusual activity on you're account. Verify your account immediately to avoid suspension!!! Click below to confirm your information. Thank you, Account Services Team	requests for immediate action threats of consequences, which results in pressure to act quickly. Legitimate organizations rarely demand immediate action without allowing time for verification. Click the email to practice spotting urgency.	in together as aligned in VO. Next button is hidden (trigger on next layer), but takes to slide 1.14 once available Clicking on email brings up zoomed in layer.

Slide: 1.17.a [zoomed in layer]			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Everything in base layer except for gray background and title is hidden. Line text is near the top of the slide. A larger image of the email from the base layer is present.	[Slide Title] Urgency [Line text] Click on the two parts of the email intended to create urgency.	Take a moment to read the email and try to find two instances of language intended to create urgency. Click on each part of the email meant to cause the recipient to panic and act quickly. After identifying both and checking your answers, select Next.	Learner is prevented from clicking on the email until the VO completes. Transparent shapes cover the following phrases: • Dear Laura • immediately • 24 hours will result in suspension. Next button is hidden until the learner clicks on the boxes covering the correct phrase (immediately and 24 hours will result in suspension). Each shape has a visited state. The correct answers have a

			green check in the visited state. The incorrect answer has a red x in the visited state. All images and text fade in as slide starts. Clicking on each shape brings up a new layer.

Slide: 1.17.b [Immediately]			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Clicking on the shape around “immediately" brings up this layer. The email from the base layer is visible. An orange circle surrounds ‘immediately’ in the email. Lines of text are at the top.	Correct! *Immediately* generates a sense of urgency.	Correct! Words like "immediately" create urgency and can cause someone to act hastily.	Learner is prevented from clicking on the slide. The lines of text and circle fade in as the slide appears. The zoomed in layer is shown when the media completes on this layer.

Slide: 1.17.c [Suspension]			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Clicking on the shape around “suspension" brings up this layer. The email from the base layer is visible. An orange circle surrounds ‘suspension’	Correct! Fear of account closure generates urgency.	Correct! Fear of account suspension creates urgency and can cause someone to act quickly.	Learner is prevented from clicking on the slide. The circle and lines of text fade in as the slide appears. The zoomed in layer is shown when the media completes on this layer.

Lines of text are at the top			

Slide: 1.17d [Dear Laura]			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Clicking on the shape around “Dear Laura" brings up this layer. The email from the base layer is visible. Lines of text are at the top	Incorrect! The opening does not create a sense of urgency.	Incorrect. This opening does not create a sense of urgency. Try again.	Learner is prevented from clicking on the slide. The lines of text fade in as the slide appears. The zoomed in layer is shown when the media completes on this layer.

Slide: 1.18 Knowledge Check		**LO:** Identify common characteristics of phishing emails.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Slide title is present along with gray background. Line text is at the top. Cards (with phrases) are stacked on top of each other in the right hand corner. Two large boxes are present on the slide.	[Slide Title] Knowledge Check [Lines of text] Drag each phrase to the correct box. [Box 1] Phishing [Box 2] Not Phishing [phrase cards] • Let me know if you have any questions. [not phishing]	Now it’s your turn to put your knowledge to the test. Review each phrase in the box at the top of the slide and decide whether it is phishing or not phishing. Drag each example to the correct category. Then click submit.	The phrase cards fade in. The drag and drop answers are submitted when the user clicks submit. Delay feedback until all answers are submitted. Learner is given 2 attempts.

	• Please review the meeting notes from today's team call when you have a chance. [not phishing] • Please review the attached agenda for tomorrow's meeting.[not phishing] • Failure to respond immediately will result in account closure. [phishing] • Reply with your Social Security number. [phishing] • Kindly do the needful [phishing]		

Slide: 1.18a [Correct]			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Submitting correct answers brings up this layer. The base layer shows through with only the cover and the lines of text hidden. Line text at the top Button in the lower right hand corner.	[Lines of text] Correct [Button] Continue	Great job! You correctly determined whether or not phrases were suspected phishing attempts. Click Continue to proceed.	Clicking on "Continue" jumps to slide 1.19

Slide: 1.18b [Incorrect]	

Visual / Display:	Slide Text:	Narration / Voiceover:	Animation / Interaction:
Submitting incorrect answers twice brings up this layer. The Phishing and Not Phishing boxes are present with the correct green phrases in the boxes. Line text at the top Button in the lower right hand corner.	[Lines of text] Incorrect. Review the correct answers below. Then click Continue. [Button] Continue [Drag and Drop] Phishing Kindly do the needful Reply with your Social Security number Failure to respond immediately will result in account closure. Not Phishing Let me know if you have any questions. Please review the meeting notes from today's team call when you have a chance. Please review the attached agenda for tomorrow's meeting	Incorrect. Review the correct answers and then click continue.	Clicking on continue returns to KC.

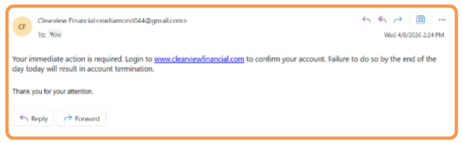
Slide: 1.18c [Try again]		**LO:** Identify common characteristics of phishing emails.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Submitting incorrect answers once brings up this layer. Line text at the top The base layer shows through	[Lines of text] Incorrect. Try Again [Button] Continue	Incorrect. Review your answers and try again.	Clicking on continue returns learner to KC.

with only the cover and the lines of text hidden. Line text at the top Button in the lower right hand corner. r.			

Slide: 1.19 Characteristics of Phishing Emails		**LO:** Identify common characteristics of phishing emails.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Image on right of two laptops on counter with people's hands visible in a working environment. Text on left side of slide	[Lines of text] Characteristics of Phishing Emails [Body Text] In the next section, you'll learn how to safely evaluate the legitimacy of emails.	Once you've identified an email as suspicious - whether from suspicious language, a false sense of urgency, or unusual requests - further action is needed. In the next section, you'll learn how to safely evaluate the legitimacy of emails.	Body text fades in aligned to audio. Photo fades in as slide starts.

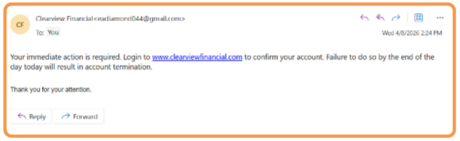
Slide: 1.20 Evaluating Suspicious Emails		**LO:** Evaluate the validity of links and sender addresses to determine whether an email is legitimate	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Text at top of slide. An image of a computer screen with Gmail logo visible is present on the screen.	[Lines of text] Evaluating Suspicious Emails [Body Text] Suspicious emails can be	Suspicious emails can be evaluated without engaging, or clicking, on anything in the email. Click on each of the tabs below to learn more.	Body text fades in aligned to audio. Photo fades in as slide starts.

Two buttons on the image.	evaluated without clicking the email. Click on each tab to learn more. [Button} Email Address Link Verification		Next button is hidden when slide starts. Next button is visible when the state of both buttons is visited. Learner is prevented from clicking on the buttons until audio stops. The buttons are part of a branching scenario. Email button takes to slide 1.23; link verification button takes to slide 1.21

Slide: 1.21 Link Verification		**LO:** Evaluate the validity of links and sender addresses to determine whether an email is legitimate	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Text at top of slide. Transparent box around the web address in the email. This will act as a popup via a hover state.  	[Slide Title] Link Verification [Hover text] www.notarealwebsite.com	The text in links can be manipulated, so always confirm the true URL before clicking. Hover over the link to preview the actual destination.	Next button is hidden when slide starts. Learner cannot click on the slide until the narration is over. Set next button to jump to slide 1.20 [layer will activate next button] Box has a hover state. Show layer link (below) when the box is in the hover state.

Slide: 1.21a [Link]	**LO:** Evaluate the validity of links and sender addresses to determine whether an email is legitimate

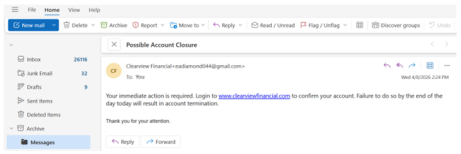
Visual / Display:	Slide Text:	Narration / Voiceover:	Animation / Interaction:
Base layer shows through. A text box appears in the bottom portion of the slide.	[Lines of text] The actual web address does not match the title of the link.	The actual URL the link directs to does not match what is shown in the message. This is a clear sign of a phishing attempt.	Change state of next button to normal when the timeline ends on this layer. Next button returns learner to 1.20.

Slide: 1.22 Email Verification		**LO:** Evaluate the validity of links and sender addresses to determine whether an email is legitimate	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Text at top of slide. Transparent box around the email address of the message. This will act as a popup via a hover state.  	[Slide title] Email Verification [Hover text] eadiamond044@gmail.com	The sender names on emails can be easily altered, so an email may appear to come from a trusted source even when it does not. One easy way to spot a phishing attempt is to check that the sender name of an email matches the domain the message was actually sent from. To do this, simply hover over the sender's name to reveal the full domain of the email.	Next button is hidden when slide starts. Learner cannot click on the slide until the narration is over. Set next button to jump to slide 1.20 [layer will activate next button] Box has a hover state. Show layer link (below) when the box is in the hover state.

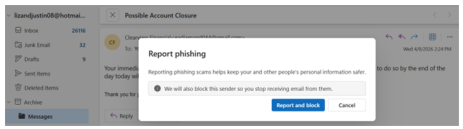
Slide: 1.22a [Address]		**LO:** Evaluate the validity of links and sender addresses to determine whether an email is legitimate	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Base layer shows through. A text box appears in the bottom portion of the slide.	[Lines of text] Although the sender name is Clearview Financial, the email address is associated with a gmail	Although the sender name is Clearview Financial, the email is coming from a gmail account. This suggests a phishing attempt	Change state of next button to normal when the timeline ends on this layer. Next button returns learner to slide 1.20.

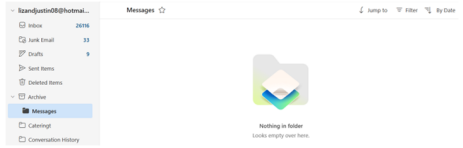
	account.	because the sender name and domain do not match.	

Slide: 1.23 Responding to Suspicious Emails		**LO:** Respond appropriately to suspicious emails.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Side title at top Heading text with orange outline surrounding the text. Remainder of slide has lines of text on left side and an image of a business person working late at night is on the right side.	[Slide Title] Responding to Suspicious Emails [Heading Text] Report ALL suspicious emails to the IT team immediately! [Lines of text] The IT department can: • block similar senders or domains • remove the email from other in boxes, and • strengthen security filters to prevent future attacks.	Once you've identified an email as suspicious, report it to the IT team immediately. Do not hesitate, do not forward to a colleague or friend. Just report the email. The IT team reviews reported emails and, if it's deemed malicious, the team can: block similar senders or domains, remove the email from other inboxes, and strengthen security filters to prevent future attacks.	Heading text and photo fade in. The orange outline appears with a wheel animation. The lines of text appear aligned to VO. State of next button is set to hidden. Next button appears when VO ends.

Slide: 1.24 Responding to Suspicious Emails		**LO:** Respond appropriately to suspicious emails.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Side title at top  	[Slide Title] Responding to Suspicious Emails	Once you've identified a suspicious email, the next step is to report it.	Learner is prevented from clicking until VO ends. Hotspot present around the word report. Next button is deactivated. Clicking on hotspot brings up

An orange outline around the word report animates in and out timed with the audio.			layer report and block.

Slide: 1.24a [Report and block layer]		**LO:** Respond appropriately to suspicious emails.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Slide title at top shows through from base layer. 	[Slide Title] Responding to Suspicious Emails	After clicking on Report, a pop-up will appear - allowing you to confirm you want to report the email. Take a moment to review the message. Then, click Report and Block to continue.	Learner is prevented from clicking until VO ends. Hotspot over“Report and block.” Clicking on hotspot brings up the confirmation layer.

Slide: 1.24b [Confirmation layer]		**LO:** Respond appropriately to suspicious emails.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Side title at top shows through from base layer. This screenshot is present with a text box below it. 	[Slide Title] Responding to Suspicious Emails [Box Text] Sender blocked [an x is present in the upper right hand corner]	Confirmation will appear letting you know the email has been reported, and the sender is now blocked - protecting you and your organization from future threats. Click the X to close the message and continue.	Learner is prevented from clicking until VO ends. Hotspot present on the ”x” in the upper right hand corner. . Clicking on hotspot jumps to next slide

Slide: 1.25 Simulated vs Real Phishing		**LO:** Respond appropriately to suspicious emails.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Side title at top Two texts boxes with title headings side by side and same size [looks like a table format] An orange box surrounds each one of the text boxes. Line of text at the bottom of the slide	[Slide Title] Simulated vs. Real Phishing [Table text box 1 - Normal State] Simulated Phishing [title] Sent by IT Used for training Image of a check mark with a check mark. [Table text box 1 - Chosen State] Simulated Phishing [title] Reporting simulated emails: ● allows IT to evaluate training ● prevents additional training ● provides practice [Table text box 2 - Normal State] Real Phishing - [title] External attack Designed to steal information Image of an email with a phishing hook. [Table text box 2 - Chosen State] Real Phishing - [title] Reporting phishing emails: ● allows quick investigations ● blocks the sender or link ● prevents others engaging [Line of text]	In addition to actual phishing emails, the IT department periodically sends simulated phishing emails. Simulated phishing emails are sent by IT and used for training purposes. Real phishing emails are sent by attackers outside the organization with the intention of stealing information. Click on each of the boxes to learn the importance of reporting both of these types of emails.	Learner is prevented from clicking until VO ends. Orange boxes around Simulated phishing and Real Phishing animate with a wheel, timed to voiceover. Clicking on Simulated Phishing box brings a chosen state and causes audio on layer A to play. Clicking on Real Phishing box brings up a chosen state and causes audio on layer B to play. Once the text boxes of Simulated Phishing and Real Phishing are set to chosen, the audio on layer C will play automatically. The next button will return to normal when the audio on layer C completes.

	Always follow the same process. Report. Don't click. A danger/warning sign is present		

Slide: 1.25a		**LO:** Respond appropriately to suspicious emails.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Base layer remains	Base layer remains	Reporting simulated phishing emails helps IT teams evaluate training effectiveness and identify areas where additional support may be needed. Accurately reporting simulated emails also prevents additional follow-up training that may be assigned if you fail to report a simulated attack. Practicing with simulated phishing emails also builds awareness and confidence, helping you better recognize and respond to real phishing attempts before any harm occurs.	Learner is prevented from clicking on the other text box. Hide the layer when audio completes Set state of text box to chosen when layer completes.

Slide: 1.25b		**LO:** Respond appropriately to suspicious emails.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Base layer remains	Base layer remains	Phishing emails are often sent to multiple employees. When one person reports a phishing email, security teams can quickly investigate, block the sender or link, and prevent colleagues from	Learner is prevented from clicking on the other text box. Hide the layer when audio completes

		clicking on the same message. Early reporting helps stop attacks before they spread. Simply ignoring or deleting the email prevents these security measures from taking place.	Set state of text box to chosen when layer completes.

Slide: 1.25c		**LO:** Respond appropriately to suspicious emails.	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Base layer remains	Base layer remains	Regardless of the type of email - simulated or real - the response is the same. Report the email, Do not click!	Show this layer when the state of all the rectangles is chosen. State of next button is normal when VO completes.

Slide: 1.26 Summary			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Side title at top Heading text with bullets listed below it. Text box with two shading colors at bottom.	[Slide Title] Summary [Heading text and bullets] Throughout this course you: • Identified the purpose and impact of phishing emails • Recognized common phishing characteristics • Evaluated links and sender information • Learned how and why to report suspicious emails	Throughout this course, you learned how to identify the purpose and impact of phishing emails as well as recognize the common characteristics of phishing, including suspicious language, urgency, and unusual requests. You also practiced evaluating links and sender information to determine their legitimacy, And finally, you learned how and why to report suspicious emails	Text appears aligned with VO. Jump to next slide when timeline ends.

	[Text box text] Remember! Report Don't Click.	to help protect your organization. Remember! when in doubt, report. Don't Click.	

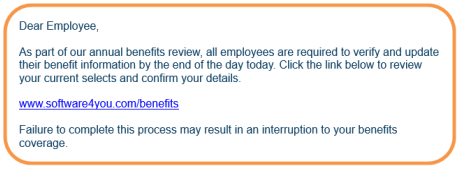
Slide: 1.27 Final Graded Quiz			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Side title at top Picture of laptop with code and hands visible. One text box in the middle. Custom button.	[Slide Title] Final Graded Quiz [Text box] Four Questions 75% to pass [Custom button] Start Quiz	You're ready for the final quiz. You'll answer four questions and need a score of 75 percent to pass. Select Start Quiz when you're ready.	Custom Start Quiz button fades in aligned to the VO.

Slide: 1.28 - [choose many]			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Question heading at top of slide. Question text Six text boxes with answer choices below.	[Slide Title] Question 1 [Question] An employee clicks a link in an email that appears to come from a trusted vendor. The link leads to a fake login page, and the employee enters their company credentials. Which of the following could be potential consequences of this phishing attack? Select all that		Hover and selected states for answer choices

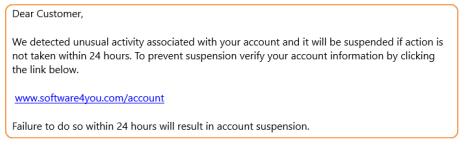
	apply. [Answer Choices - green indicates correct] Faster system performance Exposure of private or sensitive information. Disruption or shutdown of business processes. Improved employee efficiency. Reputational damage to the organization. Financial losses.		

Slide: 1.29 -[choose many]			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Question heading at top of slide. Question text Four text boxes with answer choices below.	[Slide Title] Question 2 [Question] You receive an email that claims to be from a trusted company. The email contains several unusual sentences. Which of the following sentences in the email could indicate that it is a phishing attempt? Select all that apply. [Answer choices - green indicates correct]		Hover and selected states for answer choices

	Please review the attached agenda before tomorrow's meeting. Immediate action is required to prevent your account from being suspended. Verify your account by replying with your password and Social Security number. Your invoice has been processed successfully.		

Slide: 1.30 - [choose many]			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Question heading at top of slide. Question text [email image]  Four text boxes with answer choices below.	[Slide Title] Question 3 [Question] You receive the following email. Which of the following should you do? Select all that apply.. Image of email [Answer choices - green indicates correct] Hover over the link to see where it really leads. Click on the link to see if it takes you to a valid website. Review the actual sender email address. Reply to the email to get more		Hover and selected states for answer choices

	information.		

Slide: 1.31 - [pick one]			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Question heading at top of slide. Question text [email image]  Four text boxes with answer choices below.	[Slide Title] Question 4 [Question] You receive the following email. When hovering over the link you discover it directs to www.notarealwebsite.com. Which of the following steps should you take? Image of email [Answer choices - green indicates correct] Reply to the email asking for more information. Click the link to determine if the email is valid. Report the email using the phishing tool. Forward the email to a colleague to get their opinion.		Hover and selected states for answer choices.

Slide: 1.31 - Quiz Results			
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Slide Title	[Slide Title] Quiz Results		Layers add specific information Disable Next and Previous

Text	[Text] Your Score Passing score 75%		buttons.

Slide: 1.31a [passing]		**LO:**	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Slide Title from base layer visible. Green circle with white check mark. Text directly below the check mark. Text from base layer present with learner score shown in middle. Another line of text. Two custom buttons present at the bottom of the slide.	[Slide Title] Quiz Results [First line of text] Nice job; you passed! [Second line of text] Click Review to see your results or click Continue to move on. [Custom buttons] Review quiz Continue	Great job, you passed the quiz! Click review to see your results or click Continue to proceed.	Percentage learner scored correctly populates. Clicking Review quiz allows learner to review responses. Click Continue allows learner to advance to next slide.

Slide: 1.31b [failure]		**LO:**	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Slide Title from base layer visible. Red circle with white x. Text directly below the check mark.	[Slide Title] Quiz Results [First line of text] Sorry, you didn't pass.	Sorry, you didn't pass. Click Review to see your results for each question. Click Retake Quiz to try again.	Percentage learner scored correctly populates. Clicking Review quiz allows learner to review responses.

Text from base layer present with learner score shown in middle. Another line of text. Two custom buttons present at the bottom of the slide.	[Second line of text] Click Review to see your results. Click Retake Quiz to try again. [Custom buttons] Review quiz Retake quiz		Clicking Retake quiz allows learner to retake the quiz.

Slide: 1.32 Congratulations		**LO:**	
Visual / Display:	**Slide Text:**	**Narration / Voiceover:**	**Animation / Interaction:**
Slide title. Background office/computer image. Large rectangle in middle with the following: Line of text Green circle with white checkmark Second line of text Custom button	[Slide title] Congratulations! [line of text] You've successfully completed the Preventing Phishing Attacks Training [Custom button] Exit Course	Congratulations! You've successfully completed the preventing phishing attacks training and you're now ready to recognize and report suspicious emails. Remember: If it seems suspicious, report it! Don't click! Click Exit Course to finish.	Clicking on the exit course button closes the course. Disable the next button.