Storyboard

Title: Cybersecurity Awareness: Recognizing and Preventing Phishing Attacks

Slide #	Slide Text	Visuals / Layout	Narration / VO / Audio	Interaction/Animation
1	**Welcome!** Cybersecurity Awareness: Recognizing and Preventing Phishing Attacks	Company-branded intro screen with lock icon and circuit design background	"Welcome to your cybersecurity awareness course. In the next few minutes, you'll learn how to spot and stop phishing attacks before they become a threat."	Fade-in animation for elements. Start button to proceed (click to continue).
2	**What is Phishing?** Phishing is a fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity.	Side-by-side layout: text on left, image of phishing email on right	"Phishing is one of the most common cyber threats. These emails try to trick you into clicking a malicious link or giving up your information." **What could happen if I fall for a phishing attack?** ● You could lose access to your email, bank accounts, or work systems. ● Attackers might steal your identity, money, or data. ● One small mistake can lead to big consequences, like being locked out of	"Build" animation: text appears in sync with narration. Hover-over hotspots on an email image to reveal info tips (e.g., “Look at the sender address”).

			accounts or compromising your employer's systems. **2. How common is phishing, and am I really a target?** ● Phishing is the #1 cause of data breaches globally. ● It targets **everyone**—not just tech professionals. Attackers often rely on casting a wide net, and all it takes is one person to click. ● With social engineering, attackers may use personal info (from social media, for example) to craft highly convincing messages. **3. What's at risk for my company, family, or community?** ● A successful phishing attack at work can lead to massive data breaches, financial loss, reputational damage, and regulatory consequences.	

			• In your personal life, your friends or family members could also be targeted if a hacker gains access to your email or social media. • In critical sectors (like healthcare or government), phishing can disrupt vital services and put public safety at risk.	
3	**Common Red Flags** - Spelling/grammar errors - Urgent tone - Suspicious links - Spoofed email addresses	Icons or screenshots illustrating each red flag	"Be on the lookout for these warning signs. Even small mistakes can reveal a big scam." **Spelling/Grammar Errors** Phishing messages often contain awkward phrasing, typos, or grammar mistakes because they're written quickly or by non-native speakers. These errors are a red flag that the message may not come from a professional or legitimate source. **Urgent Tone** Scammers try to create panic or pressure—like saying your	Click-to-reveal: learner clicks each red flag icon to reveal example and explanation. Subtle slide-in animations for icons.

			account will be locked or you'll miss a delivery—so you'll act quickly without thinking. If a message feels rushed or threatening, slow down and double-check its legitimacy. **Suspicious Links** Phishing emails usually include links that lead to fake websites designed to steal your information. Hover over any link (without clicking) to preview where it actually goes—if it looks strange or unrelated to the sender, don't trust it. **Spoofed Email Addresses** Attackers often disguise their email addresses to look like they're from a trusted source, such as your bank or IT department. Always check the full email address—small changes (like "micros0ft.com" instead of "microsoft.com") can signal a scam.	

4	**Interactive Activity** Drag the red flags onto the email	Interactive mock email with clickable items	[No voiceover; feedback appears after each drop]	Drag-and-drop interaction: learner matches each red flag to a part of the email (e.g., suspicious link, odd greeting). Instant feedback appears after each correct drop.
5	**Scenario** You receive this email from your 'IT department' asking to reset your password. What do you do?	Branching scenario: clickable choices	"Your response matters. Choose how you'd react in this situation."	Branching scenario: learner chooses a response (e.g., click link, report it, delete it). Each path has a short feedback popup or mini consequence. Returns to the main path after feedback.
6	**How to Report a Phishing Email** Use the 'Report Phishing' button in Outlook or forward to IT	Screenshot of Outlook reporting process	"If you suspect phishing, don't click anything. Report it immediately using your company's reporting tools."	Guided walkthrough: a fake Outlook interface with clickable hotspot on the "Report" button. Tooltip text when hovered over. Use pulse animation to highlight the button.
7	**Quick Recap** ✅ What phishing is ✅ Red flags ✅ What to do	Icons or animation of checklist items	"Let's recap what you've learned so far."	Wipe-in animation of each checklist item. Use a progress meter or animated ticks to reinforce completion.
8	**Knowledge Check** Which of these is a sign of phishing?	Multiple-choice quiz	[No VO; onscreen feedback]	MCQ interaction: learner selects an answer and gets instant visual feedback (✔️ or ❌ with brief

				explanation). Use subtle bounce animation on a correct answer.
9	**Thank You!** Download your Phishing Detection Checklist	End screen with download link	"Thanks for keeping your company safe! Download your checklist and keep it close."	Download button links to job aid PDF. Fade-in animation on screen elements. Include an optional restart course or exit button.