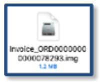
Data Security Awareness Training
STORYBOARD

Slide #	Title	Onscreen Text	Slide Images
1.1	Title	Data Security Awareness Training	Timer and headphones icons indicating the training will take 8-10 minutes and employs sound
1.2	Introduction	1) Since COVID-19, the US FBI reported a 300% increase in reported cybercrimes. The total cost for cybercrime committed globally will reach $6 trillion in 2021. 2) Cybercriminals and hackers will infiltrate your company through your weakest link … … which is almost never in the IT department. 3) 95% of cybersecurity breaches are due to human error. Human intelligence and comprehension are the best defense against cyber attacks. 4) This is where you come in. Begin.	Stats on cybercrime are superimposed on video of data flying through space while tense music plays, building anticipation. Final words invite the learner to be part of the solution and begin the training.
2.1	Learning Objectives	At the end of this experience, you will be able to: 1) Define and recognize a phishing attempt 2) Identify 2 ways hackers gain access to company data 3) Name 3 actions you must take to keep your mobile devices safe	Each objective floats up from the bottom. Background video and sound of static.
2.2	Story Setup 1	This is ABC Company. The company is unknowingly being targeted by Hacker X.	Image of office building, image of Hacker X Music
2.3	Story Setup 2	This is Chris, a new employee at ABC Company. Chris works in the accounts payable department, where he'll spend some days in the office and some days working from home. He's been issued a company laptop, smart phone, and tablet.	Image of Chris, video of busy office, video of working from home, equipment graphics (laptop, smart phone, and tablet) Music

2.4	Consequences	If ABC Company suffers a data breach, the results could be catastrophic: Loss of customer trust Ruined business reputation Financial losses Regulatory fines Falling share prices Disclosure of trade secrets	Image of ABC Company slowly fades out and is replaced by a pile of smoldering rubble as each consequence is revealed above. Music
2.5	Mission	Your Mission: Help Chris navigate his first week, and keep Hacker X from using him to gain access to ABC Company's sensitive corporate data.	Ominous faded image of Hacker X Button: I'm ready! Music
3.1	Email	Chris receives a lot of emails from ABC Company vendors and suppliers. On his third day, this message arrives.	This is phishing attempt 1: bogus order confirmation with link to invoice Image of the email. Sound of timer ticking.
3.2	Decision	What should Chris do? Click one of the icons below to select.	 Open the attachment to review the invoice details. Scrutinize the email for red flags.
3.3	Open attachment (only appears if user selects open attachment)	- HelpDesk. - Hey, it's Chris in Accounts Payable. I just clicked on an email attachment, and my laptop crashed. - The whole network went down. I think we've been hacked!	Hacker X appears (image), video of system meltdown plays, image of Chris reacting, then image of Chris phoning IT HelpDesk, sound of phone ringing. Captions with dialog.
3.3.1	Open attachment (continued) Result layer	Oh no! Hacker X successfully tricked Chris into installing malware on the company network using a technique called "phishing." Click the icon to learn more. Want to turn back the clock and try again?	Smug Hacker X video, clock image. When user clicks on the clock, hands spin in reverse, taking the learner back to slide 3.2. Click to learn more icon opens job aid on phishing.

3.4	Scrutinize 1 (only appears if user selects scrutinize)	Voiceover of Chris thinking aloud: *Hmmmm… Why is this email addressed to some generic “Recipients,” instead of to “Accounts Payable”?* *And that’s funny, … the sender’s email address doesn’t match up with the name of the company the invoice is supposedly from!* *And look! The order number on the attached invoice doesn’t even match the order confirmation number in the body of the email!* *I smell a hacker, and there’s no way I’m clicking on that attachment!*	Image of Chris scrutinizing image of the email and gesturing. Zooms in on each “red flag” element as the voiceover mentions it and draws a red circle around it.
3.5	Scrutinize 2 (only appears if user selects scrutinize)	Voiceover of Chris thinking aloud: *But before I report this email to IT, … maybe I should go ahead and call the 800 number from the email, … just make sure it’s not legit. Wait a minute! … … The phone number has an extra digit! Yup, it’s definitely a scam.*	Images of Chris scrutinizing image of the email and gesturing. Zooms in on last “red flag” element and draws a red circle around it.
3.5.1	Scrutinize 2 Result layer	Nice work! Hacker X was unable to trick Chris into installing malware on the company network using a technique called ”phishing.”	Image of Chris holding a stop sign. Click to learn more icon opens job aid on phishing.
4.1	Software update	The next day, Chris gets a pop-up message on his tablet. He’s really busy, as usual. What should he do?	Buttons: Install Update or Ignore
4.1.1	Software update “Install Update” result layer	That’s right! It’s important to keep all systems and software up to date on all devices. Hackers will infiltrate through security flaws, which are constantly being discovered and patched by software developers. If you don’t install the update, you don’t get the patch, and your device remains vulnerable to attack.	Green checkmark image. Click to learn more icon opens Equifax data breach story layer.

Data Security Awareness Training
STORYBOARD

4.1.2	Software update "Ignore Update" result layer	Incorrect! It's important to keep all systems and software up to date on all devices. Hackers will infiltrate through security flaws, which are constantly being discovered and patched by software developers. If you don't install the update, you don't get the patch, and your device remains vulnerable to attack.	Red X image. Click to learn more icon opens Equifax data breach story layer.
4.2	Software update conclusion	Chris makes a quick call to the HelpDesk to verify the update is legit, then installs it. Dialog captions: *Thanks for checking, Chris!* *And remember to use strong passwords and always keep your devices locked when unattended. Great job!*	Image of Chris talking on the phone. Click to learn more icon opens job aid about password hygiene.
5.1	Final Assessment intro	Great job helping Chris get through his first week! Now it's your turn. You must answer 3 out of 4 of the following questions correctly in order to pass the final assessment.	Video and music from the training intro plays in the background to mark the transition from instruction to assessment. Begin button
5.2	Question 1	What should you do if you receive this email? Radio button choices: Follow instructions and fill out the form OR Delete it because it's a phishing scam	Image of phishing email posing as an urgent request from the IT HelpDesk at ABC Company, requiring the recipient to enter their password. Mousing over the sender reveals the actual hacker address.
5.3	Question 2	What are the 6 warning signs of a phishing email? (Drag and drop a red flag next to each.) Tries to sell you something Poor grammar/spelling Strange sender address Urgent call to action Contains a threat if you don't act Requests sensitive information Contains an attachment or a link	6 red flag icons

5.4	Question 3	Which of these actions are mandatory for keeping your mobile devices safe from hackers? (choose all that apply)	3 checkboxes
5.5	Question 4	A strong password is safe to use on multiple accounts.	2 radio buttons: True / False
5.6	Assessment Results	Score	Pass/fail and option to try again, review, or submit score
6.1	Summary	Now that you have completed the training: You know that hackers will try to exploit both human weakness and technology weakness. You know what phishing is and how to recognize and deflect it. And you know how to keep your mobile devices safe from hackers. CONGRATULATIONS You are no longer a bystander, but part of the solution!	Background image of hacker
6.2	Conclusion	Thank you for taking the Data Security Awareness Training	Image of Chris holding a sign that says “Employees are the first line of defense against cyber crime.” Image of Hacker X appears, then fades out to drum beat. Credits MLD Logo