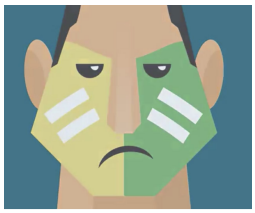
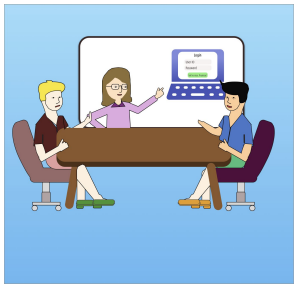
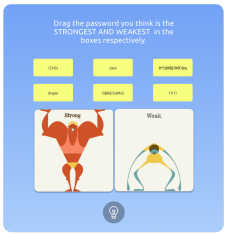
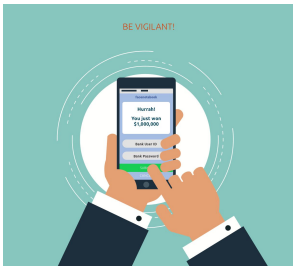
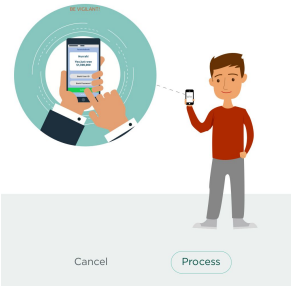
Course Outline

Section	Content	Storyboard Notes
Hook into materials	Email re Security Training is sent to employees. It contains a funny gif, is humorous and relatable in delivery. It is tailored to the personalities of the individuals at the company in order to lull them into a false sense of security. The email contains a hyper-link that directs them to a fake login page. The fake login phishes their information, shows them a scary page and then redirects them into the training where they are met with the message “Careful what you click”. **Objectives:** 1. Get folks to navigate to the training. 2. Demonstrate how easy it is to get phished. 3. Demonstrate the consequences of not being wary of security vulnerabilities.	
1-minute intro video	Animated video begins with a melodramatic TED Talk-like speech delivered by Sad Steve who begins the module with a cautionary tale. Steve explains that he was a victim of multiple security breaches due to his own poor internet security practices. When speech concludes, “Continue” button appears in bottom right-hand corner to advance to Module 1.	

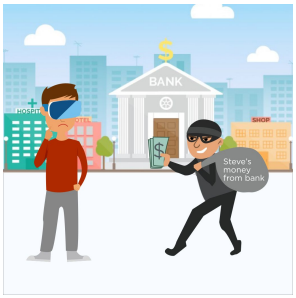
Module 1: Password security	**Learning Objective:** Given a reliable password crafting strategy, employees will be able to create a strong password containing at least 13 characters to secure all personal and corporate devices.
	
	Instructional Strategies:
	- Animation:“Steve” floating head in top left corner explains content
	- Graphics: slide onto screen to accompany voice over:
	  - the value of a strong password
	  - vulnerabilities if one fails to craft a
		

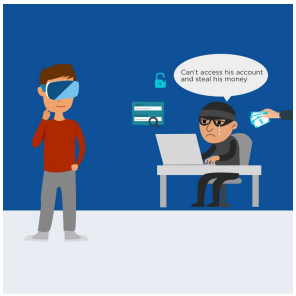
	strong pw (w/ Steve's real-world examples) - how to create a strong password - Examples and non-examples - Clickable "Now You Try!" button appears after voice over instruction. **Assessments**: - Drag-and-drop activity asking students to sort passwords into strong vs. weak using criteria discussed (perhaps include a "?" button that students can roll over which pops open criteria as a reminder) - Practice writing a password with a sample sentence using the strategy taught. (For example: "It is a beautiful day to take a brief walk around the lake!" becomes "1i@Bd2taWAtL!" - Create your own secure password with a sentence of your own. Once entered, the tool will rate the level of security of your attempt. Practice until barometer reaches 100% secure.	 
Module 2: Phishing attacks	**Learning Objective**: Given a definition and examples of phishing attacks, students will be able to recognize and avoid phishing attempts on their own e-mail and mobile platforms with 100% accuracy. **Instructional Strategies:** - <u>Animation</u>: "Steve" floating head in top left corner explains content - <u>Graphics:</u> slide onto screen to accompany voice over: - Define phishing via email and phone - Define two-factor authentication - Examples and non-examples - Clickable "Now You Try!" button appears after voice over instruction. **Assessment:** - At a mock desk, students will see both an inbox with unread e-mails (some already present, some that appear in real time) and an animated cell phone. They must	

	correctly “mark as spam” all phishing attempts in their inbox. Phone calls must be answered, but students are expected to correctly identify any phishing attempts. Each call must be responded to with the appropriate response, selected via multiple choice. Roll-over “?” will provide students with an aide reminding them about tips to identify phishing attempts.	

Module 3: Privacy settings	**Learning Objective**: Given a step-by-step tutorial on adjusting one’s privacy settings, students will be able to assess and (if necessary) adjust their own web browser and mobile privacy settings to ensure the security of sensitive digital information 100% of the time.
	
	Instructional Strategies:
	- Animation: “Steve” floating head explains the importance of adjusting web browser privacy settings:
	  - Importance of safe browsing/incognito/cookies management
	- Demonstration: Segue to a demonstration that mirrors the web browser that employees use will show step-by-step where to click and what settings to adjust.
	  - Animated “Steve” floating head in top left corner provides voice over throughout demo
	- Simulation Practice: on a screen that looks exactly like employee web browser, student will need to adjust privacy settings just like demo page. After a few seconds an animated prompt will tell student what to click next. When finished “Continue” button will turn live.
	- Animation: “Steve” floating head explains the importance of adjusting mobile app privacy settings:
	  - GPS and Bluetooth vulnerabilities
	  - Screen lock w/ pin of touch ID
	  - Data backup
	- Demonstration: Segue to a
		

	demonstration that mirrors the company mobile phone will show step-by-step where to click and what settings to adjust. - Animated "Steve" floating head in top left corner provides voice over throughout demo - <u>Simulation Practice</u>: on a screen that looks exactly like employee mobile, student will need to adjust app settings, screen lock, and GPS/Bluetooth enable just like demo page. After a few seconds an animated prompt will tell student what to click next. When finished "Now You Try!" button turns live. **Assessment:** - Students see a screen with web browser and mobile phone interface identical to simulation. They must complete all steps to adjust privacy/security settings as during the simulation--this time without an animated prompt. Once completed, "Continue" button turns live. "Hint" button can be pressed as many times as needed for students who get stuck on a step.	
Module 4: Physical assets	**Learning Objective**: Given a catalog of best practices, students will be able to protect personal and corporate physical assets. **Instructional Strategies:** - <u>Animation</u>: "Steve" floating head explains the importance of protecting physical assets. - <u>Graphics:</u> slide onto screen to accompany voice over: - Place case on phone - Ensure password protection on mobile and screensaver - Risks of unauthorized personnel - Lock up electronics when away from desk - Protect sensitive personal information (both for self and for clients)	 

	Assessment:
	- Students see a mock employee desk with several glowing red exclamation points sizzling at various points:
	  - An email open with sensitive client information
	  - A post-it note with a password scrawled on it
	  - A phone with no case
	  - Same phone with no screen lock enabled (glowing as if recently pinged)
	  - A man glancing at vacant desk office without a guest badge
	  - An tablet charging (vs. locked up)
	- Student must resolve all exclamation points. Clicking on each point asks students to diagnose what is wrong and how to fix it in a multiple-choice format.
	- When all is resolved, "Test Your Knowledge" button appears, taking students to summative assessment.
		

Summative assessment	Begin with a voice over from Steve explaining how glad he is that you now have this information because when he was at his lowest point just a year ago, he thought he'd never recover. Students then see… Sad Steve is slumped in front of his desktop computer at work. On his screen, we see: - A pop-up informing him that he's the "Lucky Winner!"--indicating that he's clicked on a phishing attempt - An alert indicating that there has been a possible attempt to access his account and that he review his privacy settings - An unread email with the subject line "Fraud Alert" And, around his office we see: - A post-it with his passwords written out - A document with sensitive client information (SSN, DOB, etc.) nearly	

	slipping off of his desk as if forgotten (or perhaps in his wastebin?). - A smartphone with no password protection setup On each of these problems is a clickable icon that will take the student to an activity asking them to help Steve fix this issue using the skills learned in Modules 1-4. As each problem is resolved, Steve becomes visibly happier! For students who need a reminder, a "?" button will direct them back to an information page (the same video/VO from the module? An outline or transcript of the module lesson?) that will remind them how to solve this particular problem.	

Interactive Techniques

Element	**Design Description**
Animated Video	Cartoon will be static and every page will be animated by using principle. Animations are accompanied by voiceovers to aid both visual and aural learners.
Clickable buttons	There are two types of icon buttons. One is secure password icon button, the other is not secure password icon button.
Drag-and-drop	During drag and drop to create the password, student can ask chatbot about whether their password is secure or not. Chatbot will give "add special sign, for example"@" sign in password".
Roll-over content	Every page will be animated by using principle.
Virtual simulations	When student clicks "cancel" button, Steve wears VR headset and sees hacker who can't access his computer and is very sad. When student clicks "process" button, Steve wears VR headset and sees hacker who has accessed his computer and steals his money.

Metrics Tracking

Content is created in SCORM to be presented via an LMS. Through use of an LMS the following will be tracked:

Item tracked	**Purpose**
# of people who click through to the redirect from the signup email.	Track engagement.
# of people who enter login details (plus those login details).	Measure staff susceptibility to phishing attacks pre-training.
# of people who begin the course materials	Track engagement through measuring # of signups vs # of folks who completed the training.
# of minutes participants spend on the course materials	Track engagement with materials.
# of failed attempts during assessments throughout	Track if delivery is effective or if reinforcement is needed.
Results of summative assessment	Track retention.
Learner satisfaction	CSAT score entered at the end of training to guage learners' enjoyment of the materials.
# & Names of participants in completed lessons	Ensure we accurately track completion to cover security compliance requirements.
# of participants & names of those who enter details as part of second phishing email	Track efficacy of the training through practical application.

Success Metrics

Success Rate	

100%	Employees will complete the information security elearning module.
90%	Minimum score that employees must earn on the elearning module summative assessment activity to advance to the “completion” screen.
80%	Employees will create passwords that IT department is unable to break.
80%	Employees will correctly identify a simulated phishing attempt and mark the email as spam.
99%	Employees will avoid clicking on any links in a phishing attempt.

Security Training Instructional Design Brief

Amy, Laura, Liz, Harsha, Rachel, & Sasha

AKA Steve's Saviors

Appendix

Presentation talking points:

Creative process
- Began with a brainstorm & metrics
- Worked out learning objectives from content
- Brainstormed interactions that would be engaging but match content
- Drafted course outline
- Sketched illustrations
- Wireframed content
- Finalized illustrations
- Finalized Demo & Design sheet.

Instructional Design Focus
- Interactivity
- Engagement
    - Human aspect & building rapport
    - Using new technologies
- Compliance
- Tracking & Metrics
- Self-led online content because it is catered toward 500+ employees

Content
- Focus on what's relevant & useful

Concept Sketch # 1
Concept Sketch # 1
Concept Sketch # 2
Concept Sketch # 3

Concept Illustration # 1

Concept Sketch # **4**

Concept sketch #5
Concept sketch #6

Concept Sketch #3.1
Concept sketch #4.1
Concept sketch #7
Concept sketch #7.1
Concept Sketch # 1
Concept Sketch # 2