Rise and Soar Aeronautics:

Cybersecurity Refresher eLearning

Subject	Topics to Include
Business Purpose	• Provide a mid-year refresher course on basic cybersecurity protocols. • Over time, employees have been negligent in some areas and the training will provide a reminder. • There has been a 30% increase of employees clicking on malicious links. This training will underscore the importance of being vigilant. • Additionally, there has been an observed number of unattended computers that have not been locked down while the employee is away from his or her desk.
Target Audience	• All employees with computer access.
Training Time	20 minutes

Training Recommendation	• 1 e-Learning course (Rise)
	  ○ eLearning will not require employees to come in during when they aren't scheduled. They can take the course at any time within a given time-frame as the content and desired outcomes are a priority
	  ○ It allows the learner to proceed at their own pace and review material as needed.
	• Post eLearning: Track occurrences of malicious links clicks

Deliverables	• 1 storyboard outlining the module
	• 1 e-Learning course
	  ○ Developed in Articulate Rise
	  ○ Includes two interactive scenarios as knowledge checks
	  ○ Assessment (80% to pass)

Learning Objectives	At the end of this course, the learner will be able to: • Identify situations where potential breaches may happen • Create a strong password • Implement protocols if you suspect a breach

	• Explain how our IT department can help you

Training Outline	**Introduction**
	• Overview with reasoning for training
	• Objectives
	• Course modules
	  ○ Brief Overview
	  ○ Be Smart
	  ○ Don't Be a Fish
	  ○ Be Secure
	  ○ Test Your Cybersecurity Awareness
	  ○ End of Course
	(Very) Brief Overview
	• Open with quote: It takes 20 years to build a reputation and few minutes of cyberincident to ruin it. –Stephane Nappo
	• Carousel with corresponding images to the topics
	  ○ Who's responsible for cybersecurity?
	  ○ Cybercrime is not new.
	  ○ First antivirus software.
	Be Smart
	• Quote: Cybercrime is the greatest threat to every company in the world. –Ginni Romety
	• Basic summary of IT combined in the same department as Cybersecurity
	• 3 benefit of IT
	  ○ Communicate: malicious link? Let them know
	  ○ Training
	  ○ IT and Cybersecurity (reporting to one is reporting to both)
	• Knowledge check MC
	  ○ Which of the following is NOT one of the ways IT can or should help you?
	  ○ Must get it correct before continuing.
	Don't Be a Phish
	• Statistic: Phishing attacks account for 90% of data breaches.
	• Think before you click: questions to consider before posting images from work—even if sharing isn't malicious.
	  ○ Does it [the pic you want to send] contain intellectual property or other sensitive/proprietary info in the background?
	  ○ Is the link you're about to click from someone you trust and is it normal for them to send a link without explanation?

	o Are you sure it's from that person? • Explain "phishing." • What can you the employee do to prevent such an attack? • What do you do if you've clicked on a corrupted/malicious link? • Knowledge Check **Scenario**: Austin is working late and accustomed to his project manager sending him emails at all hours. o Austin receives an email from PM with a link and no explanation. Does he open it? o Branching choices. If he makes the correct choice the knowledge check is over. o If incorrect, it branches to what should he do now? • Learner cannot go onto next module until they select the correct response in the scenario. **Be Secure** • Quote: We discovered in our research that inside threats are not viewed as seriously as external threats, like a cyberattack. But when companies had an insider threat, in general, they were muchmore costly than external incidents. This was largely because the insider that is smart has the skills to hide the crime, for months, for years, sometimes forever. –Dr. Larry Ponemon. • Reminder that if it's on a computer, it's vulnerable to attack. • Statistic: 36% of all data breaches were caused by malicious employees. • What can you do to make RSA more secure? o Passwords: make them strong; characteristics of strong one (10 characters, combo letters, numbers, caps and lowercase, special symbols) o Firewalls: use them and keep them up-to-date o Limit Access: don't stay logged in when away from your computer—even if clients or 3rd parties aren't in office o Secure Devices: install updates in a timely manner, use VPN when not on company network • Knowledge Check Branching **Scenario**: o Three questions the head of IT asks: ▪ Per IT's email, have you updated your computer yet?

	• If answered incorrectly, this one leads to another branch and the question: When do you plan on installing the update? • When answered correctly, it'll take the learner back to the main scenario and the other two questions. ▪ What should you do when you leave your desk? ▪ What other measures are you taking to prevent data breaches? • Learner must get the scenario correct to continue to the next lesson. **Assessment** • Variety of multiple choice questions referencing material • 80% correct to pass (If only 6 questions can it be 100% to pass?) **End of course** • Congratulations for passing • Summary • References for course content
Evaluation Plan	• Track occurrences of malicious link clicks. • Periodic desk checks to make sure all unattended computers have a lock screen on or are powered off.