Phishing Attacks Design Document

Business Purpose	User error counts for 95% of the successful email phishing scams. When a successful phishing scam provides a hacker with access to a business network, sensitive data can be compromised. The goal of this training would be to for all employees who utilize the company's email system to understand how to spot a phishing email and utilize security systems on their accounts to prevent cyber attacks. This should reduce the number of IT support tickets related to hacked accounts and data breaches.
Target Audience	All employees who have been with company for at least one year and who utilize the company's email and network systems. This will be a part of the onboarding process for new hires.
Training Time	30-45 minute eLearning course
Training Recommendation	e-Learning is the best delivery method for this particular training; users can access the training via work-issued computers when they have free time. This is also a money-saving delivery method for the company since it does not require a paid in-person instructor. This course will provide real life scenarios as well as interactive components to test employees' ability to identify phishing emails. Administrators and managers should complete this training first since they are often the people who have access to secure data. By completing the training before the employees they directly supervise, they can support their employees and have an understanding of the time commitment and follow-up that may be needed in order to achieve compliance. The IT staff should be available for individual assistance if needed by the learner once the training is complete.
Deliverables	• 1 storyboard outlining the phishing attack training course • 1 eLearning module, developed in Articulate Storyline with voiceover narration
Learning Objectives	After completing this course, the learning will be able to: • Define social engineering phishing attacks • Identify three different types of phishing attacks • Distinguish between the types of multifactor authentication • Identify behaviors that can make them more likely to fall for phishing attacks
Training Outline	**Introduction** • Welcome • Navigation • Objectives **Topic: Social Engineering** • Psychological manipulation of human weaknesses that cyber criminals exploit when designing phishing attacks ○ Fear

- Sextortion emails
- Desire
  - Email scams that manipulate a victim's desire for money. Usually an announcement of a random lottery drawing or free gift card
- Empathy
  - Emails that appear to come from a relative or colleague. These often appear legitimate and rely on the victim wanting to be helpful

Topic: Types of Socially Engineered Phishing Attacks

- The three common types of phishing email attacks will be explained and an example of each will be included
  - Phishing
    - The most generic type. It is not personalized so that it can be sent to a large group of random people in the hopes that someone will fall for it. Usually these email contain malicious links that result in the victim inadvertently providing the hacker with personal and/or financial data.
  - Spear Phishing
    - Customized for a specific group of people, such as employees at a business, school, or other organization. This type of phishing scam can appear, at first glance, to be sent from a co-worker or someone the potential victim has a business relationship with. Like phishing scams, these emails often contain malicious links or requests to provide personal and/or financial information.
  - Whaling
    - This type of phishing scam targets whoever is at the top of an organization. The most common types of whaling scams are sent from an anonymous source who claims to have compromising information that will e detrimental to the career and/or personal life of the intended victim. Whaling attacks go after these specific types of victims because they often make the most money and have the most to lose so are more likely to pay the demands of the cyber attacker.
- **Topic: Multifactor Authentication**
  - Security settings that the user can utilize to protect their accounts and data.
    - Challenge Questions
      - Least secure type of MFA. Will provide examples of good and bad questions.
    - Possession Factors
      - Utilizes a second device for user to verify account ownership. Will provide

scenarios/examples of possession factor authentication.

- Biometrics
  - Considered most secure MFA method. Users authenticate with their physical person. Will provide examples of this type of MFA that most people use every day.

Knowledge Check

- A knowledge check will be placed here to test the learner's understanding of the types of phishing scams as well as MFA before moving on to the last topic. Users will receive feedback after each question and have the opportunity to review and retake as desired.

- **Topic: User Behaviors**
  - Will discuss four user behaviors that can contribute to the success or failure of phishing scams
    - Slow down-- people who are in a hurry or feeling rushed make mistakes. Will provide example of type of language that makes the potential victim feel like a response is urgently needed.
    - Impulsive – Question the legitimacy of an email before clicking on the link to claim the gift card from a supposedly random drawing.
    - Check Links – The most commonly fallen-for phishing attacks are those with malicious links. Will provide methods for how to identify a fake link.
    - Go directly to website – Cyber criminals who are looking for direct access to financial accounts will create emails that appear to come from financial institutions or the IRS. Reminders that those institutions will never ask for personal info via email. Users should always go directly to those websites by typing in the address of the financial institution or government agency.

Assessment

- A five-question graded assessment will test the learner over the course objectives. A passing score of 80% is required. Users will have unlimited opportunities to pass the assessment with the opportunity for review if the quiz is not passed.

Conclusion

- This slide will congratulate the user for successful completion of the course.

Assessment Plan	• **Knowledge Check**
	  ○ Placed after Topics 1 & 2 to confirm learner understands those two sections before moving on. Learner will receive feedback after each question and will have the opportunity to both review and take the KC a 2nd time.
	• **Final Assessment**
	  ○ 80% passing on e-learning module assessment via a 5-question quiz. Learner will have the opportunity to review assessment after completion.

Evaluation of Success	**IT dept should see a marked decline in help desk tickets requesting password resets due to breached accounts almost immediately. Data should be analyzed to identify employees who successfully completed training but who file password reset tickets due to a successful phishing attack so a remediation training plan can be put in place.**