

Cybersecurity and Email Safety 101 – AD&S Solutions

Design Document

Cybersecurity and Email Safety 101 – AD&S Solutions

Design Document

<i>Business Purpose</i>	AD&S Solutions is a global e-commerce company that deals with a substantial amount of email communications on a daily basis. AD&S has seen a 20% increase in data breaches over the last six months due to employees falling for phishing scams and clicking on malicious links. Many employees have reported that they were unaware that they had fallen victim to a phishing attack. Those that were aware did not know the company's reporting procedures. The goal is to: • Reduce the number of data breaches by 15% by the end of Q4 • Provide awareness and strategies to identify phishing emails, malicious links, and social engineering attempts • Provide information on the reporting procedures at AD&S Solutions • Train the learner how to detect phishing scams, how to take preventative measures, and how to be more vigilant about following reporting procedures
<i>Target Audience</i>	• All new employees at AD&S Solutions that have computer access will complete this new comprehensive cybersecurity training during onboarding • All current employees that have computer access will be required to take this course as a refresher training within one month. • All managers and supervisors will be required to complete the training. • All employees will be able to take it on their own time on a company computer
<i>Training Time</i>	• This training is the first training out of multiple cybersecurity courses • The training will be approximately 20 minutes
<i>Training Recommendation</i>	• 1 e-Learning course: ◦ This is the best format for this training since AD&S Solutions is a global e-commerce company that has employees working in a variety of settings (office, hybrid, remote) in numerous locations worldwide. This will also ensure learners are able to complete the training in their own time.

Cybersecurity and Email Safety 101 – AD&S Solutions

Design Document

	- o The training will use a variety of formats to encourage the learner’s engagement including multiple interactions, knowledge checks, and real-life scenario-based learning. - o Final assessment will measure the learner’s understanding of the material. The assessment will use a variety of methods (multiple choice, drag and drop, listing steps in sequential order, and multiple response answers).
<i>Deliverables</i>	● 1 e-Learning course: - o Developed in Articulate Rise - o Includes two real-life scenarios with avatars - o Final evaluation
<i>Learning Objectives</i>	● Define common cybersecurity threats ● Identify suspicious email practices ● Determine effective prevention measures ● List reporting procedures if you expect a breach
<i>Training Outline</i>	● Introduction and Overview ● Hook Interaction about alarming statistics ● Common Threats - o Define: ▪ Phishing ▪ Malware ▪ Social Engineering - o Information attackers obtain ▪ Login information ▪ Financial information ▪ PII (personal identifiable information) - o Consequences to an attack ● Knowledge check to match the definitions to the correct words (phishing, malware, and social engineering) ● Identifying Suspicious Emails - o Short mini email Scenario 1 ▪ Identify 9 red flags ▪ Provide 9 questions to ask yourself - o 3 best actions to take if you come across a suspicious email: ▪ Be cautious ▪ Click safely ▪ Report it

Cybersecurity and Email Safety 101 – AD&S Solutions

Design Document

	- o Scenario 2 with avatar ▪ Learner will be given a scenario where they have to practice identifying potential phishing attempts ● Prevention and Security Measures - o Use secure WiFi connection - o Update software immediately - o Enable security measures - o Create strong passwords ▪ List strong password requirements ● Knowledge check about prevention and security measures ● Reporting Procedures - o Report to IT department immediately - o Change your password - o Scan your system for malware - o Scenario 3 with avatar ▪ Learner will be given a scenario where they have to practice the necessary steps if they (or a coworker) fall victim to a phishing attack ● Assessment ● Conclusion - o Summary - o Congratulations
<i>Assessment Plan</i>	● 5 assessment questions will be included in the course ● Learner must score 80% to successfully complete the course ● Learner will be given immediate feedback ● Results will be given