Information Security Awareness Training Program

I. Purpose

The University of North Alabama (UNA) administration takes protecting the University, its intellectual property and any personal or confidential information extremely seriously. To help protect these interests, an information security awareness training program is being provided. This program is intended to set the training standards for all employees at the University of North Alabama, including, but not limited to: university administration; faculty (including full-time, part-time and adjunct); full-time, part-time, and temporary staff; and student employees all of whom are provided service or information by access to university information systems. The success of the University's security awareness training program depends on the ability of all users to work toward a common goal of protecting the University's information and related technical resources.

II. Scope

This program refers to all University information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and communication devices owned, leased, operated, or contracted by the University. This includes networking devices and infrastructure, personal digital devices, telephones, wireless devices, personal computers and any associated peripherals (external hard drives, USB flash drives, campus networked shared drives, etc.), and software, regardless of whether used for administration, research, teaching or other purposes. It is the intent of this program to help users be aware of actions they can take to better protect the University's information as well as their personal information. These actions include, but are not limited to: proper password usage, data backup, proper antivirus protection, reporting any suspected incidents or violations of security policy, and following rules established to avoid social engineering attacks.

III. Requirements

All employees referenced in paragraph I above will be required to participate in annual online training (the current cycle occurs during each Spring semester). This training consists of informational videos designed to provide insight and instruction regarding information security. Additionally, all new employees must complete the training within two weeks of their initial hire date. Training may vary year-to-year based on current trends. Failure to complete the annual training is subject to disciplinary actions as defined in the enforcement section of this document. In addition to annual training, UNA will provide supplemental information on various relevant topics. Training completion and results will be maintained for each employee. Finally, the individuals referenced above in paragraph I are included in quarterly phishing campaigns. These campaigns are designed to reinforce knowledge learned from annual training as well as other supplemental sources by producing phishing e-mails. Should an individual inappropriate acknowledge or interact with a phishing test e-mail, additional training materials are supplied to help increase knowledge and close gaps in knowledge to prevent actual phishing success.

IV. Access

Each user will receive an email with a username and temporary password. This email will provide all the necessary information to access the training. The following link can be used to access the training - https://training.knowbe4.com.

V. Enforcement

Any employee who fails to complete the required training will be subject to removal of access to University systems until such requirements have been met. Also, new employees will be denied access to University systems until such requirements have been met.

Frequently Asked Questions (FAQ)

1. **What is the purpose of the training?**

   In today's information age, it is essential that users be equipped with knowledge and skills that will allow some protection. As a University, we are concerned with protecting all our assets, including electronic assets. It is the hope that this training will increase employee awareness and security knowledge to help protect both UNA's and (possibly) each person's personal assets.

2. **Why was KnowBe4's training selected?**

   KnowBe4 is a market leader in information security training and is ranked each year by Gartner as one of the best training platforms. KnowBe4 training provides up-to-date knowledge and useful techniques in today's every changing world. KnowBe4 produces a number of new, updated training modules each year as well as when significant events occur. Finally, KnowBe4 employs Kevin Mitnick as its Chief Hacking Officer. In the 1990s, Kevin Mitnick was marked on the FBI's most wanted list and arrested for hacking several organizations. Now, Kevin uses his knowledge and skills to teach others the pitfalls and issues within information security. Kevin discusses techniques uses by today's criminals and teaches individuals how to protect themselves against such attacks.

3. **Why Annual Training?**

   Both technology and threats to technology change constantly. To ensure our employees are kept informed and aware of the latest changes, UNA has decided to require this training annually. Currently, the training cycle runs during each Spring semester.

4. **What if I receive an e-mail that looks suspicious?**

   If you receive an e-mail that looks suspicious, review the content for signs of a phishing attempt. This includes misspellings, immediately required actions, suspicious/incorrect links, etc. If you have any questions, report the e-mail and the ITS team will help review it. Each UNA e-mail account is equipped with a Phish Alert button to allow the reporting of a potential phishing attempt. Finally, you can forward the e-mail to infosec@una.edu and the ITS team will help evaluate the e-mail and provide instructions for next steps.

5. **Who manages the program at UNA?**

   This program is designed to be an awareness program for all employees of the University. The Information Technology Services (ITS) department manages the day-to-day functionality as well as the implementation of the program.

6. **Who has to take the training?**

   It is the ultimate goal that all employees (including student workers) take and maintain security awareness via this program. Currently, all full-time and temporary employees are required to take the training. Additionally, part-time, adjunct, and student employees who require access to sensitive data or experience security-related issues are required to complete training.

7. **Where can I find more information regarding this training as well as other security topics?**

For more information regarding security issues, training, concerns, or questions, please contact the Office of Information Technology Services via e-mail at infosec@una.edu, call 256.765.4865 during normal business hours, or visit the ITS department's website at http://www.una.edu/its/technology-security/index.html at any time.