KENTUCKY WESLEYAN COLLEGE
Policy & Procedure Manual

Phish Testing and Training Policy

Approval: Cabinet
Policy Type: College
Policy Owner: Information Services and Resources
Responsible Office: Information Services and Resources
Revision History
Approval Date: 08/07/2018
Modified:
Next Review: 08/2021

---

1. Purpose

1.1 This policy establishes guidelines for conducting email phish testing and end-user training. The intent of the policy is to improve the ability of computer end-users to detect possible malicious emails and possible malicious web sites. The goal is to minimize security risks to all College data. According to independent research conducted by the Ponemon Institute, for 2017 the global average cost of a data breach is up 6.4 percent over the previous year to $3.86 million. The average cost for each lost or stolen record containing sensitive and confidential information also increased by 4.8 percent year over year to $148; the cost to higher education is $111 per record. The Cabinet have agreed that safeguarding the College’s assets is a worthwhile objective. For all of us, one of the most critical assets we can protect is the information that is entrusted to us by prospective and current students, alumni, and all the College employees. Learning how not to be prey to data thieves is not something we want to leave to chance or to a “learn by doing” approach.

2. Scope

2.1 Applies to all faculty and staff with an active Kentucky Wesleyan College email account (any email address ending with @kwc.edu)

3. Definitions

3.1 Phishing – The fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

3.2 Phishing Test – An electronic communication embedded with code that simulates an attempt to obtain sensitive information.

3.3 Failed Phishing Test – Occurs when an end user responds to a phishing test by clicking on a simulated malicious link, attachment, or replying to the electronic communication.

3.4 Passed Phishing Test – Occurs when an end user does not fail the phishing test and notifies IT of a possible phish attack.

4. Policy

4.1 It is the policy of Kentucky Wesleyan College to take all possible measures to ensure the security and integrity of all data -including personal, sensitive information- which the College owns or processes as part of the College's daily business needs. These measures include the use of network and application detection and monitoring software as well as end-user phish testing software.

5. Procedures

5.1 Information Services will oversee the College's Phish Testing and Training program. The Technology Support Supervisor will be responsible for the operational requirements of the program.

5.2 Phish testing will be randomly conducted on a bi-monthly basis. Test recipients will be selected from all active staff and faculty email accounts. If it is determined (through industry based research and ongoing participation in industry communities) there is a specific, active phishing threat, an unscheduled phish test will be conducted. Participants will be from those employees whose job function relates to the specific, active phish threat.

5.3 The following groups will be used to classify all participant test results:

a. Failed Phishing test

b. Passed Phishing test

c. Non-Participation

5.4 For all test participants that pass the phishing test, no further action will be required. This group will receive an email informing them of the successful test results.

5.5 For all non-participants – this is the group that did not open the phishing email – no further action will be required. This group will be invited and encouraged to complete a Phishing Awareness Training session. This group will receive an email link for the training session.

5.6 For all test participants that failed the phishing test, successful completion of a Phishing Awareness Training session will be required. When a phishing test is failed, the participant's computer screen immediately displays a "failed test" message and informs the participant they will be receiving a link for Phishing Awareness Training in an email within the next 24 hours. Training must be successfully completed within 4 weeks of the failed test date.

6. Enforcement

The required training that results from a failed phishing test is not a punitive action; instead, the training is designed to help improve cyber-security awareness. According to a study sponsored by KnowBe4, a leading Phish Testing software vendor, 91% of security breaches start with a phish and that end-user susceptibility to a phishing email drops almost 20% after a company runs just one phish simulation.

6.1 If a failed test participant has not begun Phishing Awareness Training within two weeks of the failed test, at the end of the second week of inactivity, an email reminder will be sent to the individual indicating that

a. Training needs to be started.

b. Training must be successfully completed within 4 weeks of the failed testing date.

c. If training is not successfully completed within 4 weeks of the failed testing date, the individual’s College network account will be disabled until training is completed.

d. The individual’s immediate supervisor will be copied on the email.

6.2 If a failed test participant has not begun Phishing Awareness Training within three weeks of the failed test, at the end of the third week of inactivity, an email reminder will be sent to the individual indicating that

a. Training needs to be started.

b. Training must be successfully completed within 4 weeks of the failed testing date.

c. If training is not successfully completed within 4 weeks of the failed testing date, the

individual’s College network account will be disabled until training is completed.

d. The individual’s immediate supervisor will be copied on the email.

6.3 If a failed test participant has not successfully completed Phishing Awareness Training within four weeks of the failed test date, the individual’s College network account will be disabled until training is completed.