UCF UNIVERSITY OF CENTRAL FLORIDA

PROTOCOL TITLE:

Improving Cybersecurity Culture in the Workplace: A Study of Training Practices and Perceptions

PRINCIPAL INVESTIGATOR:

James Henderson; Patricia Montoya; Maxwell Stolarenko
Modeling and Simulation M.S. Program

VERSION NUMBER/DATE:

1.0

REVISION HISTORY

Revision #	**Version Date**	**Summary of Changes**	**Consent Change?**

Table of Contents

1.0 Study Summary

Study Title	*Improving Cybersecurity Culture in the Workplace: A Study of Training Practices and Perceptions*
Study Design	*The study will take participants with an average level of technology competency and have them view a cybersecurity training module for phishing prevention. Participants will then engage in a short interactive game that exposes them to real world examples of phishing emails to decipher if they are genuine emails or not. Subjects then take a short questionnaire to collect demographic as well as personal feeling and attitudes towards the training they went through.*
Primary Objective	*This study will evaluate which aspects of existing cybersecurity training programs for teaching phishing prevention techniques can affect a learner's perceived ease of use and perceived usefulness of cybersecurity.*
Secondary Objective(s)	*This study will also propose potential modifications to existing cybersecurity training programs that generate more positive feelings of perceived ease of use and perceived usefulness towards cybersecurity as a whole.*
Study Population	*Adults with an average level of computer literacy (enough years of experience working in a profession that requires occasionally accessing emails.*
Sample Size	*10-15 total sample size*
Study Duration for individual participants	*30-40 minutes*
Study Specific Abbreviations/ Definitions	*Perceived Usefulness (PU)* *Perceived Ease of Use (PEoU)*

2.0 Objectives*

2.1 The objective of this study is to carefully review a real world example of a workplace cybersecurity training program in terms of employee perceptions regarding their usefulness. The research study aims to extensively investigate how current cybersecurity training programs generate perceptions of usefulness and ease of use within the users it trains, and the role these perceptions have in the development of training courses, the key aspects of phishing prevention training that affect the users' overall attitudes and behaviors. The study also aims to propose potential alterations to existing phishing prevention training modules based on user perception reports obtained through surveys.

- *This study aims to identify aspects of cybersecurity training programs that influence ease of use.*
- *This study will allow researchers to identify which challenges a technology user may face when engaging with phishing training.*
- *This study will serve as the groundwork for providing recommendations to improve the design and delivery of training methods to enhance effectiveness.*
- *This study will aid in the identification of which aspects of phishing prevention training influence an employees' attitudes and behaviors.*

2.2 For this study, two primary research questions were proposed. The first research question seeks to answer how employees perceive the usefulness of cybersecurity training within their workplace and what factors influence their perceptions. The second research question of the study seeks to understand which specific aspects of cybersecurity training employees find the most valuable and why.

3.0 Background*

3.1

- *Cybersecurity refers to the practice of protecting computer systems and networks from unauthorized access that can lead to theft, damage, and other forms of cyber-attacks. The defense against cyber-attacks starts with training the personnel who engage with any network-connected system. Cybersecurity training covers a wide spectrum of topics from the principles of information security, cyber threat intelligence for future mitigation, vulnerability management, incident response and the compliance of standards. The intent of cybersecurity training is to improve the knowledge, skills, and awareness of individuals to enhance their ability to detect, prevent, and respond to a cyber threat (de Bruijn, 2017; Paulsen, 2012).*

Modern cybersecurity training involves different approaches such as simulations, virtual environments, and awareness of best practices with the most common implantation being online training (Leah, 2021). The online-training approach is a cost-effective and flexible method for providing individuals with access to a wide range of videos, reading passages, and interactive modules structured to test a user's ability to detect and respond to a cyber threat. The flexibility of online training affords a self-paced learning environment that can be accessed from any location. Regular training and assessment can ensure an individual's skills are meeting a given standard to identify and protect against cyber threats.

- *Cybersecurity is an umbrella term encompassing a wide range of terms surrounding attacks and the means to prevent them, one of which being phishing attacks. A phishing attack is a form of social engineering online where a malicious agent attempts to steal the personal information of users while acting under the guise of an official group or company. The term "phishing" is still a broad term that varies in use based on its intended target and the medium it takes place in. The most common form a phishing attack takes on is as an email targeting as many people as it can, known simply as an email phishing attack. This technique sends out vague emails in hopes of getting even a few users to fall for it. Standard email phishing attacks may target every student at a university, for example. In contrast, phishing attacks that target a smaller, more select group of individuals that share similar positions of authority at an organization is known as spear phishing. Spear phishing attempts may target the financial office of a university. Finally there are phishing attacks that target a single individual with high importance, known as whaling. Whaling attempts may target the head administrator of a university. While email phishing is the most prevalent method, phishing can appear across several other mediums, including SMS, phone calls, online games, and search engines (Al-Daeef et al., 2017).*

- *Due to the significant risks imposed from phishing threats, it is imperative that any user online, whether online for business, education, or personal reasons should be properly equipped and trained for possible cyber risks they may encounter. Al-Daeef et al. (2017) wrote that the most effective defensive strategies against phishing attacks include technical and non-technical preventive strategies in which technical tools and non-technical skills are adopted to reduce falling prey to a potential attack. The technical standalone applications and in-browser extensions exist as tools to automatically detect, warn of, and block access to phishing links but do so with varying levels of effectiveness. As such, the human needs to* *be trained to accurately detect instances of attempted phishing to avoid uncontested reliance of their technical strategies. To reinforce the effectiveness of individuals' non-technical prevention skills, training methodologies are often employed to help raise awareness of the existence of phishing attacks and properly recognize the signs to differentiate a phishing email from a real one. Cybersecurity training for phishing emails can be administered in several ways including slide-like presentations, videos/embedded videos, modular training, computer-based simulations, virtual machine environments, classroom teaching, and much more (Jampen et al., 2020). Of particular note are the phishing email demonstrations as these directly pertain to the current study. Unlike other training methods, phishing email evaluations can be sent on a per user basis with varying levels of difficulty depending on the individuals' past behaviors. This can allow for multiple parameter modifications across each person, including the time between training intervals, the degree of accuracy of the phishing email versus a real one, the relevancy of the content within the email, and the difficulty of its fraudulent characteristics (Jampen et al., 2020).*

- *A n often overlooked aspect of non-technical prevention of phishing attacks are the attitudes an individual develops for the training strategies or content, or their perceived usefulness of the training. Perceived usefulness is an individual's subjective opinion of how much they feel a technique or technology is actually beneficial to them, which can play a crucial part in knowledge acquisition and retention (Abbasi et al., 2016). Past research had demonstrated that users who did not perceive tools meant for mitigating phishing threats as useful would fall victim much more likely to real phishing attempts through both emails and websites alike, often ignoring warnings from the system and relying solely on their intuition instead. In contrast, users that did perceive anti-phishing tools to be helpful were much more careful with their actions with each website they visited. These individuals would frequently hesitate to click anything suspicious and would often wait for the assistive tool to inform them if anything they were viewing was malicious or not. (Abbasi et al., 2016). Bouts of intuition reliance over the several different techniques to train and detect phishing attacks showed that users that perceived the usefulness of the protective tools to instead place their trust in their own abilities, often resulting in over-confidence in their likelihood to correctly identify genuine phishing attacks (Jampen et al., 2020). Users with a low perceived usefulness towards a technique or technology may find it more of a hinderance than an aid and may ignore what it says to do or even actively do the opposite.*

- *The other half to a user's acceptance towards a training technique beyond their perceived usefulness is their perceived ease of use of the training content itself. Perceived ease of use is an individual's subjective opinion regarding the difficulty of a cybersecurity training. This perceived ease of use can present itself based on the difficulty of the training content such as how easily identifiable the phishing email is, the difficulty navigating through the training content if the email training is in learning modules, and the general amount of time the user has to divert away to perform the training task. (Reeves et al., 2021). This perceived ease of use can also be the inverse as the lack of difficulty, as the lack of a challenge may not make the training content challenging enough to feel cognitively engaging. A phishing training that is too easy to complete may not only underwhelm the learner, but it may also habituate improper techniques for recognizing phishing emails. (Reeves et al., 2021). People may feel cybersecurity fatigue from both ends of the difficulty spectrum. If the content is too easy they may become dismissive to the need to continue training any further than what they already know as it is no longer challenging enough to retain any useful information. If the training content is too hard then they might develop defeatist attitudes towards the training as they know they will complete the assessment incorrectly and be subject to even further training (Reeves et al., 2021).*

3.2 No preliminary data was obtained for this study as no existing data was found with the literature gaps in mind.

3.3 While there was extensive research on phishing practices, phishing training, tools to prevent phishing, and perceived usefulness & perceived ease of use with cybersecurity training, there exists no literature that ties all of these concepts together in a presentable form. The perceived usefulness research pertained to the use of the technical side of phishing prevention but leaves a desirable gap for the perceived usefulness of non-technical prevention techniques. Similarly, the research on the perceived ease of use was not limited to merely phishing training but rather a multitude of cybersecurity concepts to generate cyber fatigue. With this in mind, this review demonstrates that the examined literature leaves much to uncover for the human side of phishing training by further researching perceived usefulness and perceived ease of use of phishing training specifically.

4.0 Study Endpoints*

NA

5.0 Study Intervention/Investigational Agent

NA

6.0 Procedures Involved*

6.1 The study will examine a user's general response towards online cybersecurity training programs based on their perceived ease of use and perceived usefulness of the course content. Participants will be provided with an informed consent form at the beginning of the study that details the structural format of the remainder of the study. Participants will be instructed to follow the instructions on the provided laptop in the lab room and to complete the cybersecurity training module on phishing prevention. The module features text, videos, and brief demonstrations that the participant will need to manually click through over the course of its duration. After completing the training course, the research team member will instruct the participant to begin the other module on the training program's main page to start an interactive game on the laptop. The interactive game will prompt the participant to determine if the following examples of emails are phishing attempts or genuine harmless emails. Each response the participant selects will include immediate feedback regarding their accuracy. Lastly, there will be a questionnaire with Qualtrics to obtain demographic information as well as general feelings and attitudes towards the training course they just completed. The study will conclude with a debriefing segment by the research team member explaining the purpose of the study.

6.2 For this study:

- *Participants will be introduced to the study which will include a verbal explanation from the research team members and a consent form for participants to read through (5 minutes)*
- *Participants will go through the cybersecurity training course on the provided laptop (12 minutes).*
- *Participants will begin an interactive game to test their abilities to differentiate phishing emails from real emails (8 minutes)*
- *Participants will be given a demographic and self-report evaluation of the training module they just took (10 minutes)*
- *Participant will be debriefed by the research team member of the nature of the study and handed a debriefing form (3 minutes)*

6.3 The primary instrument used in this study will be a standard laptop capable of accessing the Internet for the purpose of working through a cybersecurity training module and completing a questionnaire. No other devices with a higher required authorization are required.

Data will be solely gathered and stored through the UCF survey system Qualtrics.

- *Documents necessary for the study:*
    - *Demographics and Perceived Usefulness/Ease of User Questionnaire*
    - *Study Consent Form (HRP-502 CONSENT.pdf)*
    - *Introduction and Debriefing Form (introanddebrief.pdf)*

6.4 Data necessary for the study that will be collected during participant trials includes general emotional responses and personal beliefs and perceptions towards how they interpret cybersecurity training courses to be useful to learn from and easy to use. Such data will be obtained through a survey the research team developed through the UCF Qualtrics system. Survey questions are presented on a 5-point scale to quantify emotional responses and perceptions towards cybersecurity. The study will also be looking at open-ended user responses that are coded based on common patters, themes, and concepts..

7.0 Data and Specimen Banking*

NA

8.0 Sharing of Results with Subjects*

NA

9.0 Study Timelines*

9.1 The entire study for a single participant should take approximately 30-40 minutes to complete. In that time period, the participant will be constantly engaged in different tasks. The primary goal of the study is to obtain survey data, so the time it takes for each participant to reach the survey would take approximately 25 minutes, while the survey itself would take 5-10 minutes.

- *The time needed to enroll at least 15 participants should be completed within 3-4 weeks after the request is put out. The time needed to enroll at most 30 participants should be completed withing 1-2 months after the request is put out.*

10.0 Inclusion and Exclusion Criteria*

10.1 Any participant that applies via recruitment requests through word of mouth or email will be enrolled into the study as a subject. An initial screening test will not be required for the sake of this study due to the commonplace practices needed to operate a laptop. However, the research team members reserve the right to end the study for an early withdrawal if they determine that the participant's performance does not fit the study's inclusion criteria.

10.2

Criteria for inclusive eligibility include:

- *Participant is an adult ages 18 and up.*
- *Participant knows how to operate computers at a basic to intermediate level of performance.*
- *Participant has an email address they regularly visit.*
- *Participant knows how to open and navigate through their emails.*
- *Participant is currently working or has worked in a profession that requires them to routinely check their emails.*

Criteria for excluding participants from the study include:

- *Participants are unable to operate a computer or similar device.*
- *Participants who do not have an email address or knowledge to navigate through one.*
- *Participants come from high technology professions (i.e., I.T., computer science, cybersecurity).*

11.0 Vulnerable Populations*

NA

12.0 Local Number of Subjects

12.1 A desired total of 30 participants will be recruited through word of mouth, email, and bulletin advertisements.

12.2 The study will stop accepting new participant enrollment requests after gathering a sample size of 30 individuals, however the study needs at minimum 15 participants to begin statistical analysis.

13.0 Recruitment Methods

13.1 A desired total of 30 participants will be recruited through word of mouth and bulletin advertisements across the Partnership II and Partnership III buildings at the Modeling and Simulation department of UCF's Research Park.

13.2 Participants will be recruited based on a combination of accessibility and relevancy to the research team members. For this criteria, the best candidates for the study are the other classmates taking the course this study was created for as well as any other students or faculty within the Modeling and Simulation department at UCF. With this, participants will primarily consist of individuals coming from backgrounds with varying levels of computer literacy *but will nonetheless operate computers and view emails on a frequent basis.*

13.3 *NA*

13.4 *NA*

13.5 *Participants will be compensated for their time working through the study with a $5 gift card. Gift cards will be provided during the debriefing period of the study. Due to the short duration nature of the study, participants that withdraw early from the study will not receive any compensation.*

14.0 Withdrawal of Subjects*

14.1 *Participants are free to withdraw from the study at any time. Participants will be withdrawn from the study without consent if:*

- *Participants is under the age of 18 years old.*
- *Participants are overqualified by working in computer science professions*
- *Participants lacks a clear understanding of how to perform basic tasks on computers.*
- *Participants had reported in the demographic survey that they have not worked in a career requiring computer use in the past.*

14.2 *In the event a participant meets one of our exclusion criteria, proper orderly termination procedures of the participant will follow. The research coordinator will thank the subject for their time and explain the reason for the necessary withdrawal. The research team members will still provide the participant with proper debriefing procedures as well as answer any questions they have.*

14.3 *Subjects are free to withdraw at any point during the study. Partial data collected from the terminated subject will not be considered for evaluative review alongside other participant's data due to the incomplete nature. The UCF Qualtrics tool allows for the omission of individual responses.*

15.0 Risks to Subjects*

NA

16.0 Potential Benefits to Subjects*

16.1 *Participants in the study may develop a greater appreciation for cybersecurity practices and behaviors, specifically how to properly spot a phishing attack in the future.*

16.2 *No other direct benefits are expected for our participants to gain.*

17.0 Data Management* and Confidentiality

17.1 The study will stop taking new participants after a sample size of 30 but will begin statistical analysis once obtaining survey data from at least 15 participants. A exploratory factor analysis will be used as the first type of data management to better understand which underlying factors of our phishing training modules best contribute to our understanding of perceived usefulness and ease of use. We then intend to implement linear regression analysis to examine the relationship between the participants' demographic characteristics and their perceived usefulness and perceived ease of use responses to the provided phishing training modules. Necessary steps and procedures will be taken by the research team to ensure the safe handling of collected data obtained from participants in the study.

- *The research team members will all be properly acquainted with the relevant CITI training protocols and requirements that teach how to ethically collect, store, and use collected data. If CITI training certification has not been renewed in the past two years then the research team member will be required to renew their certificate.*
- *Data acquired from the study will require proper authorization to access and evaluate. Authorization will only be given to the research team members as well as the faculty member overseeing operations of the study as a whole. Additional protections will be put in place that can only be circumvented by individuals granted appropriate authorization.*
- *Participant survey responses will be automatically recorded in UCF's Qualtrics system that can only be accessed by the student account that created the survey. The student account is password protected and is the account of one of the research team members. Database copies and statistical analysis files of the surveyed data will be housed on the computers of each research team member, all of which are password protected.*
- *While not required, some participants may feel the need to physically sign their informed consent forms at the start of the study. These consent forms will be safely locked with a key within a filing cabinet of one of the research team members.*
- *UCF's Qualtrics system will automatically generate an ID to attach each participant's survey responses to rather than needing each participant to provide their name. These identifiers cannot be used to trace a participant's*

information back to them as contextual information like names or place of work will not be recorded.

- *Data will be safely stored for five years after collection after which point the data will be automatically discarded to ensure privacy for the affected participants.*

17.2 As survey responses will serve as the primary source of data for this study, statistical procedures will be implemented for quality control of said data. Specifically, Cronbach's alpha will be called upon during SPSS analysis to examine the reliability of the chosen survey questions and to determine if the wording of a survey question must be restructured..

18.0 Provisions to Monitor the Data to Ensure the Safety of Subjects*

NA

19.0 Provisions to Protect the Privacy Interests of Subjects

19.1 Participants use a survey developed by the research team to answer demographic questions relating to age and years of experience. The participant's raw data will not be displayed anywhere public, nor can their responses be traced back to specific persons. Names and other sensitive data will not be collected at any point during the study.

19.2 Participants are given an informed consent form at the beginning of the study detailing the nature and purpose of the study as well as the structural layout of the remainder of the study. The researcher and the consent form will both explain that they are free to withdraw from the study at any point they feel uncomfortable. At the end of the study, participants will be given a verbal debriefing as well as a written form of the debriefing as physical proof. In the debriefing, the researchers will assure the participant that all information recorded during the trial will remain anonymous and will not be arranged in any way that could trace information back to specific individuals. Finally the researcher will tell the participant that they can be contacted via the number on the informed consent form at any point to answer any questions they may have.

19.3 The research team members are the only individuals permitted to access raw collected data of the participating subjects. Participant information will not be shared with anyone outside of the research team and will be carefully handled by the research team's members to ensure safety and privacy of any sensitive data.

20.0 Compensation for Research-Related Injury

NA

21.0 Economic Burden to Subjects

NA

22.0 Consent Process

22.1

- *Upon arriving to the testing site of the study, the research team will provide each participant with a physical copy of an informed consent form detailing the contents of the study and a verbal summarization of the consent form from the researchers. Participants may ask any questions they have before giving their consent.*
- *While an informed consent form will be provided to each participant, the study presents less than minimal risk to all parties involved and thus qualifies to the right to forgo the need for a signed copy of the informed consent form for each participant.*
- *Following the main component of the study, participants will be provided both a verbal debriefing from the researcher as well as a physical debriefing form. The form contains a phone number for participants to ask the researchers further questions after the trial is completed.*

23.0 Process to Document Consent in Writing

NA

24.0 Setting

24.1

- *The research team will identify and recruit fellow cohorts and faculty members from the UCF Modeling and Simulation department as potential subjects for the study.*
- *This study's primary testing location will be in room 233 of the Modeling and Simulation Partnership III building at the UCF Research Park. The testing location will operate during any hours of the day when no other parties occupy the room.*

25.0 Resources Available

25.1 Experiment sessions are planned to run for 30-40 minutes per participant. Modeling and Simulation graduate students will be conducting the study but will be overseen by Dr. Joseph Kider in the Modeling and Simulation Practicum.

- *All three research team members are currently in the Modeling and Simulation M.S. graduate program and are knowledgeable in conducting research with human participants.*
- *The three research team members are up to date with current CITI training regulations to demonstrate competency with human-oriented research protocols.*

26.0 Multi-Site Research*

NA