

2023

Comparing Phishing Training and Campaign Methods for Mitigating Malicious Emails in Organizations

Jackie Christopher Scott
Nova Southeastern University, cto2011@ymail.com

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd

 Part of the [Computer Sciences Commons](#)

Share Feedback About This Item

NSUWorks Citation

Jackie Christopher Scott. 2023. *Comparing Phishing Training and Campaign Methods for Mitigating Malicious Emails in Organizations*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Computing and Engineering. (1186)
https://nsuworks.nova.edu/gscis_etd/1186.

This Dissertation is brought to you by the College of Computing and Engineering at NSUWorks. It has been accepted for inclusion in CCE Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

Comparing Phishing Training and Campaign Methods for Mitigating
Malicious Emails in Organizations

By

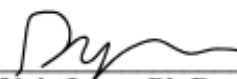
Jackie Christopher Scott

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Cybersecurity Management

College of Computing and Engineering
Nova Southeastern University

2023

**We hereby certify that this dissertation, submitted by Jackie Scott
Conforms to acceptable standards and is fully adequate in scope
And quality to fulfill the dissertation requirements for the degree s
of Doctor of Philosophy.**




Yair Levy, Ph.D.
Chairperson of Dissertation Committee

8/29/23
Date



Wei Li, Ph.D.
Dissertation Committee Member


8/29/23
Date



Ajoy Kumar, Ph.D.
Dissertation Committee Member

8/29/23
Date

Approved:



Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

8/29/23
Date

**College of Computing and Engineering
Nova Southeastern University**

2023

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial fulfillment of the Requirements for the Degree of Doctor of Philosophy

Comparing Phishing Training and Campaign Methods for Mitigating Malicious Emails in Organizations

By

Jackie Christopher Scott

August 2023

Although there have been numerous technological advancements in the last several years, there continues to be a real threat as it pertains to social engineering, especially phishing, spear-phishing, and Business Email Compromise (BEC). While the technologies to protect corporate employees and network borders have gotten better, there are still human elements to consider. No technology can protect an organization completely, so it is imperative that end users are provided with the most up-to-date and relevant Security Education, Training, and Awareness (SETA). Phishing, spear-phishing, and BEC are three primary vehicles used by attackers to infiltrate corporate networks and manipulate end users into providing them with valuable company information. Many times, this information can be used to hack the network for ransom or impersonate employees so that the attacker can steal money from the company. Analysis of successful attacks show not only a lack of technology adoption by many organizations, but also the end user's susceptibility to attacks. One of the primary mediums in which attackers enjoy success is through business email. This dissertation study was aimed at researching several phishing mitigation methods, including phishing training and campaign methods, as well as any human characteristics which create a successful cyberattack through business email. Phase 1 of this study validated the approach and measures through 27 cybersecurity experts' opinions. Phase 2 was a pilot study that produced a procedure for data collection and analysis and gathered 172 data points across three groups containing 86 users. Phase 3, the main study, used the established data approach and gathered 1,104 data points across three groups containing 552 users. The results of the experiments were analyzed using Analysis of Variance (ANOVA) and Analysis of Covariance (ANCOVA) to address the research questions. Several significant findings are documented, including results that showed there were no statistical differences in phishing training methods. This study indicates that current training methods, such as annual awareness or continuous customized training appear to provide little to no added value compared to no training at all. In addition, this study indicates that phishing campaign methods have a significant impact on phishing success, specifically a Red Team campaign. Lastly, recommendations for future research and opinions for industry stakeholders on ways to strengthen their cybersecurity posture are provided.

Acknowledgments

Completing my Ph.D. has been an outstanding experience; one filled with many learnings that I can apply to my life and any future journeys I undertake. Earning this degree has been a personal goal of mine for over 20 years. I view the completion of the Ph.D. as a Maslow's Hierarchy of Needs "self-actualization" achievement more than anything else, as it's something I have truly done for myself, to prove that I can complete this educational pinnacle.

I would like to sincerely thank my wife Amanda for allowing me the time and effort to complete this portion of my education that I so desperately wanted to finish. Without her encouragement and support, this would have never been possible. All the nights and weekends needed to accomplish this feat were no doubt inconvenient, but she always supported me in everything I have taken on, and she is by far, the best thing to ever happen in my life. Someone whom I share everything with and take an equal partnership in everything we aspire to do.

I would like to thank our four adult children, Morgan, Amanda Eva, Matthew, and Victoria. I also want to provide some advice; that you are never too old to learn and to continue to achieve your dreams. Never settle for what today is, but rather continue to aspire for what tomorrow can bring. Never give up on what you want in life, never stop learning, and never settle.

I would also like to thank my mother, Joyce Scott, for always supporting me, and above all, always encouraging me to do whatever I wanted in life. She provided a drive and desire to achieve in me that continues to burn, and although I am completing this chapter, there are several things left to do. In her eyes, I can do anything I set my mind to, and I still work to ensure I prove her right every day. She also taught me that a person's character is more valuable than anything else, and to treat everyone with courtesy, kindness, and respect. Do unto others as you would have them do unto you.

Last, I would like to thank my dissertation chair, Dr. Yair Levy, who has been an incredible professor, mentor, and sponsor throughout my entire NSU career. He is undoubtedly one of the brightest individuals I have ever met, and demands excellence in every assignment, project, or paper. With his guidance, I feel I am well-prepared for all the chapters to come in my career. I would also like to thank the rest of my dissertation committee, Dr. Wei Li and Dr. Ajoy Kumar. It has been amazing to go through this process with such talented individuals. Thank you all from the bottom of my heart for investing in me.

Table of Contents

Abstract	ii
Acknowledgements	iii
Table of Contents	iv
List of Tables	vi
List of Figures	vii

Chapters

1. Introduction	1
Background	1
Problem Statement	2
Dissertation Goal	6
Research Questions	7
Relevance and Significance	9
Relevance	9
Significance	10
Barriers and Issues	10
Limitations and Delimitations	11
Limitations	11
Delimitations	11
Definition of Terms	12
Summary	13
2. Review of Literature	15
Introduction	15
Social Engineering	16
Phishing	17
Spear-phishing	21
Business Email Compromise	23
Security Education, Training, and Awareness	26
SETA in Organizations	26
General public personal knowledge	28
Phishing Mitigation Methods	31
COTS email security software	31
Ethical Hacker or Red Team	33
Intrusion Detection and Prevention Systems	36
Summary of What is Known and Unknown	39
3. Methodology	41
Overview of Research Design	41
Measures	43
Instrument Development	44
SMEs Instrument	44
Organizational End User Instrument	45

Data Analysis	45	
Phase I	45	
Phase II	46	
Phase III	47	
Population and Sample	49	
4. Results	50	
Overview	50	
Phase I – Cybersecurity SME survey feedback	51	
Phase I - RQ1 & RQ2	52	
Phase II – Pilot Study	56	
Data Collection	56	
Data Analysis	57	
Phase III – Main Study	59	
Data Collection	59	
Data Analysis	61	
Summary	67	
5. Conclusions, Implications, Recommendations, and Summary		71
Conclusions	71	
Discussions	72	
Implications	73	
Recommendations and Future Research	74	
Summary	75	
Appendices	80	
A. IRB Exception Approval	80	
B. Example of SME Panel Survey Introduction	81	
C. Example of SME Survey	82	
D. Organizational End User Instrument	91	
E. Example of Participant Invitation Email	92	
References	93	

List of Tables

Tables

1. Summary of Phishing	20
2. Summary of Spear-phishing	23
3. Summary of Business Email Compromise	26
4. Summary of SETA in Organizations	28
5. Summary of General Public Personal Knowledge	31
6. Summary of COTS Email Security Software	33
7. Summary of Ethical Hacker or Red Team	35
8. Summary of Intrusion Detection and Prevention Systems	38
9. Summary of Research Phases	50
10. Summary of SME Demographics	52
11. SME % Agreement for Six End User Negative Response Actions	53
12. SME % Agreement for Phishing Campaign Methods	55
13. One-way ANOVA Output for RQ3 Using Pilot Data	57
14. One-way ANOVA output for RQ4 Using Pilot Data	58
15. One-way ANOVA Output for RQ3	61
16. Tukey HSD Output for RQ3	
17. One-way ANOVA Output for RQ4	62
18. ANVOVA Output for RQ5	63
19. Average Click Rates Across Training Groups	
20. Summary of SME Demographics for RQ6 & RQ7	64
21. ANCOVA Output for RQ6 with Demographics Control	66

List of Figures

Figures

1. Social Engineering Categories 18
2. Social Engineering Attack Types 18
3. Business Email Compromise Categories 25
4. Overview of the Research Design Process 42
5. Randomized Quasi-Experimental Design 43
6. SME % Agreement for Six End User Negative Response Actions 54
7. SME % Agreement for Phishing Campaign Method 55

Chapter 1

Introduction

Background

The role of Information Security (ISec) continues to be the first line of defense in guarding Personally Identifiable Information (PII) of the end users of modern Information Systems (IS) (Ho, 2018). As the focus on email threats continue to strengthen from attackers, it is imperative to research the success factors of these attacks so that steps can be taken to guard against email sabotage, financial ransom, email compromise and hacking (Costantino et al., 2018). Salahdine and Kaabouch (2019) stated that social engineering, specifically phishing and Business Email Compromise (BEC) campaigns, are on the rise and it is critical to understand the factors behind it and the impact to Intellectual Property (IP). While the research on social engineering goes back to the mid-1990s, the research on specific phishing and BEC topics, outcomes, and mitigations is starting to gain momentum in academia as it is a serious threat to IP. According to D'Qrill and Hendricks (2018), it seems that social engineering is an inescapable threat to organizations in highly competitive markets, or in fact, any market where profit margins are low. Social engineering itself is not always done for hacking purposes, rather can merely be done to lure end users to a webpage, advertisement, or store to facilitate purchases. Bullee et al. (2017) set out to explore the psychological effects of spear phishing in organizations by conducting an experiment where emails

were addressed in a personalized manner. Their findings indicated a significantly higher chance of success through personalization versus generic emails, further enforcing the role end users play in social engineering attacks.

There have been a variety of research studies related to the education of the end user, as well as the level of ISec awareness training they have been exposed to.

Volkamer et al. (2016) indicated that improved detection can be attained by focusing the end users attention on the address bar where the Uniform Resource Locator (URL) is displayed. In doing so, the end user can often detect an invalid URL, web address, or domain and avoid compromise (Volkamer et al., 2016). Similar research studies indicated that fear-based emails, such as an account error or tax lien notice, are also particularly effective in luring unsuspecting end users (Harrison et al., 2016). Social engineering, including phishing, are now an even larger threat as end users continue the prevalence of mobile devices and applications. Jain and Gupta (2017) declared that nowadays mobile devices are more popular and seem to be a perfect target for malicious attacks like mobile phishing. Thus, this study aims to analyze the various forms of phishing mitigation methods to determine their role in malicious email circumvention.

Problem Statement

The research problem that this study will address is the continued growth of cyberattacks targeting businesses via email to impersonate the corporate end user for stealing money or assets from organizations (FBI, 2019). Further, lack of cybersecurity knowledge and skills contribute to the enablement of up to 95% of cybersecurity threats, which lead to significant financial loss to businesses (Carlton & Levy, 2015). The Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) stated

successful cybercrime attacks were responsible for \$4.2 billion in financial losses in 2020, in the United States (US) alone (FBI IC3, 2020). Phishing is one type of social engineering, which is defined as a scalable act of deception whereby impersonation is used to obtain information from the target (Lastdrager, 2014). These attacks have become increasingly more sophisticated with attackers using very customized business emails to lure corporate end users to trust and act on them (Kotson & Shultz, 2015). The FBI (2017) stated that modern email cyberattacks are more sophisticated than ever and pose a very real threat to global organizations of every size. These attacks have long been used to acquire sensitive information through email messages that seem to be trusted and valid to the corporate end users' (Thakur et al., 2015). According to Furnell et al. (2019), the most common attacks involve manipulating corporate end users for financial gain. This activity is so common in recent years the FBI (2017) created five pillars of BEC scams that still require research including Chief Executive Officer (CEO) fraud, attorney or executive impersonation, account compromise, data theft, and the bogus invoice scheme.

The origin of phishing, BEC, and other forms of social engineering, has roots in the Rational Choice theory (Cornish & Clark, 1987), which is based on a mindful assessment of the value of performing a certain task (i.e. cost vs. benefit or risk vs. reward). Cialdini (2009) introduced a theory that outlined six principles of persuasion: social proof, authority, reciprocation, consistency, liking, and scarcity. Effectively, all the Cialdini (2009) principles support the reasons behind the acts of social engineering and deception. Even though Security Education, Training, and Awareness (SETA) programs continue to mature, according to the FBI (2019), the global financial impact of successful

phishing and BEC breaches is well over \$85 billion. In addition, Verizon (2020) stated that 86% of all data breaches were financially motivated.

Miranda (2018) suggested that the continued evolution of SETA can further protect organizations against phishing attacks. With these threats growing each day, it is critical that SETA continues to evolve because the more educated the end user, the less likely the phishing attack will result in success (Mihaela, 2020). Kolouch (2018) stated, unlike a traditional phishing attack, that BEC is usually targeted at a specific corporate end user within an organization. In the case of BEC, the bad actor prepares for the attack very meticulously and works to obtain the most information possible about the victim before commencement. Further, Kolouch (2018) stated this premeditation and analysis of the end user helps these email campaigns slip through cybersecurity filters and evade many other tactics such as whitelisting. Bullee et al. (2017) stated that personalization makes it extremely hard for end users to recognize that an email is not from a trusted source. Greitzer et al. (2014) identified that additional research is needed on both the organizational security practices and the human factors that contribute to the success of data breach through malicious business emails. Stembert et al. (2015) concluded that as email attacks become more sophisticated, it is up to the end user to detect and report suspicious emails to cybersecurity teams.

Aviv (2019) suggested that while there had been significant research completed around end user characteristics that lead to BEC attacks, there was sparse research on end user detection skills. Wilkerson et al. (2017) stated that the continued growth of attacks was a key indicator that current research methodologies were not sufficient, and that further research is needed in this domain. In addition, Zweighaft (2017) found that

current regulation in the industry, as well as the lack of security training were additional factors impacting end users' ability to detect BEC. Stembert et al. (2015) found that the increasingly complex nature of cybersecurity email attacks warrants more studies focused on the users' ability to detect these threats. Ernst and Young (2015) indicated that the top reason for corporate security breaches via social engineering was the end users' carelessness and lack of mitigation methods, such as various phishing training and phishing campaign methods. While SETA has been widely researched (Alnatheer, 2015), its effectiveness when deployed alongside multiple phishing campaign methods has not.

Techopedia (2017) defined a Commercial-Off-The-Shelf (COTS) product as computer hardware or software tailored for specific uses, such as email security, and made available to the public. These products are designed to be readily available, user friendly, and do not require any customizations. A COTS email security software vendor (Proofpoint, 2021) stated that impostor emails are purpose-built to impersonate someone the user trusts and tricks them into sending money or personal information. COTS email security software can provide an integrated, holistic solution that addresses the attackers' tactics, provides visibility into malicious activities and user behavior, as well as automates detection and threat response. In addition, for companies to further prepare for BEC attacks, it is suggested that organizations may employ an ethical hacker or Red Team approach by consistently simulating attacks, as to raise the level of awareness of the employees about social engineering threats (Mirian, 2019). Considering this context, it is evident that the creation of new technology is moving faster than the cybersecurity industry can implement (Mihaela, 2020). As a result of this slow implementation, there continues to be a rise in social engineering attacks such as BEC (FBI, 2019) from end

user negative response actions (opening malicious email, opening attachments, clicking on malicious links, etc). However, despite significant development of anti-cybercrime technology, one of the most significant vulnerabilities continues to be the end users themselves (Mihaela, 2020). Therefore, further research is needed to understand modern phishing training and campaign methods, and their role in mitigating malicious emails in organizations.

Dissertation Goal

The main goal of this research study was to compare phishing training methods (annual industry-standard awareness training and continuous customized social engineering SETA program) and phishing campaign methods (industry-standard phishing campaign and a Red Team phishing campaign) and their role in mitigating simulated phishing attempts in organizations. The SETA platform utilized was KnowBe4 (<https://www.knowbe4.com>) to create both phishing training methods. KnowBe4 was used to create one of the phishing campaigns, and the other was created by a Red Team during penetration testing. KnowBe4 also acted as the single instrument for gathering data on the success of malicious email when delivered to the corporate end users. The secondary goal of this research study was to assess any statistical mean differences between the two types of training and campaign methods and their impact on phishing mitigation when controlled by five demographic factors. According to Information Systems Audit and Control Association (ISACA) (2015), enterprises that provide security awareness training do not seem to be benefiting from a comparable decrease in successful cyberattacks. Further, Mihaela (2020) warned that corporate end user' cybersecurity knowledge is only as good as their last training.

According to Tversky and Kahneman (1972), cognitive biases are systematic errors of thinking or rationality in judgment that influence the perception of the world and decision-making ability. These mental shortcuts increase efficiency by enabling end users to make quick decisions without the need to thoroughly analyze a situation. Instead of constantly becoming paralyzed by the process of mental examination each time a decision is made, the end user can rely on these unconscious automatic responses to help expedite things, only engaging in heavier mental processing when necessary. However, cognitive biases can also distort thinking and perception, ultimately leading to inaccurate judgments and poor decisions (Tversky & Kahneman, 1972). These poor decisions can also manifest themselves in negative end user response actions related to corporate email. Examples of negative end user response actions can include opening suspicious emails, clicking on links in suspicious emails, downloading content from clicked links, forwarding suspicious emails, or divulging sensitive data requested. Sometimes these unconscious automatic responses can prove detrimental to an organization's security, and potentially lead to a breach.

Research Questions

The seven research questions this study addressed are:

RQ1: What are the approved components of the experimental procedures for the phishing training and campaign methods according to cybersecurity SMEs?

RQ2: What level of validity of the experimental procedures the phishing training and campaign methods is sufficient according to cybersecurity SMEs?

RQ3: Are there any statistically significant mean differences between the use of *an annual industry-standard phishing training, continuous customized social*

engineering focused training, and a control group without training, on end users' negative response to malicious emails?

RQ4: Are there any statistically significant mean differences between the use of *an industry-standard phishing campaign and a Red Team phishing campaign* on end users' negative response to malicious emails?

RQ5: Are there any statistically significant mean differences between *the phishing training methods* (an annual industry-standard phishing awareness training vs. continuous customized social engineering focused training vs. no training - control) and *the phishing campaign methods* (industry-standard phishing campaign vs. Red Team phishing campaign) on end users' negative response to malicious emails?

RQ6: Are there any statistically significant mean differences between the use of *an annual industry-standard phishing training, continuous customized social engineering focused training, and a control group without training, on end users' negative response to malicious emails, when controlled for participants': (a) age, (b) gender, (c) job role, (d) location (clinic vs. admin), and (e) years of job experience?*

RQ7: Are there any statistically significant mean differences between the use of *an industry-standard phishing campaign and a Red Team phishing campaign* on end users' negative response to malicious emails, when controlled for participants': (a) age, (b) gender, (c) job role, (d) location (clinic vs. admin), and (e) years of job experience?

Relevance and Significance

Relevance

This research study is relevant as it seeks to improve the understanding of phishing mitigation methods and their impact on malicious emails in organizations. Phishing continues to be the number one type of social engineering, with over 90% of all data breaches starting as a phish and may be increasing by as much as 400% per year (FBI, 2021). Nearly 50% of senior IT leaders say that phishing is their primary concern because of weaknesses in their processes, policies, and IT security infrastructure. Additionally, the impact of phishing is evident, with 60% of security leaders stating their organization has lost data, 52% experienced credential compromise, and 47% contended with ransomware, all due to a successful phish (Cybertalk, 2022). The cost to the organization from a successful phishing attack is also skyrocketing. IBM (2021) reported phishing to be the second most expensive attack vector, costing organizations on average \$4.65 million.

While the cost and likelihood of phishing attacks continue to increase, only 60% of organizations offer a formal cybersecurity education for their end users. Similar to corporate email phishing, end users are also experiencing this threat in their personal lives. According to the Swiss Cyber Institute (2021), social media users are also in danger of phishing attacks on all major platforms. As an example, LinkedIn phishing messages accounted for 47% of all social media phishing attempts. The understanding and knowledge regarding phishing mitigation methods are critically important, making the relevance of this research study substantial.

Significance

This research study is significant in several ways. This study will enhance existing research regarding phishing, more specifically the comparison of multiple phishing mitigation methods. While phishing attacks continue to grow, there are many statistics in place, however, limited number of research studies on the effectiveness of modern mitigation methods exist. In the review of the literature in this area, it appears that little is known about the effectiveness of two types of phishing campaigns. In addition, it appears that limited research studies exist regarding the effectiveness of the two training methods when measured against the campaign methods. According to Mihaela (2020), despite the significant development of anti-cybercrime technology, the most significant cybersecurity vulnerability continues to be the end user.

Phishing remains the number one threat to organizations and is consistently used by attackers to deliver malicious URLs, malware, and other nefarious payloads. According to Crowdstrike (2022), there has also been a shift to “hands-on-keyboard” activity and 62% of attacks were non-malware, meaning that traditional anti-virus and anti-malware tools would not detect the attack. With every organization’s dependency on email, coupled with the fact that over three billion phishing emails are sent every day around the globe (Earthweb, 2022), there is still a need to continue researching phishing mitigation methods. Therefore, the significance of this research study is substantial.

Barriers and Issues

There are several potential barriers to this research study regarding the creation and execution of a meaningful experiment for phishing training and campaign methods. The first potential barrier is the validation of existing phishing mitigation methods (training and campaign) utilizing cybersecurity SMEs via the Delphi method. A potential barrier exists if the right SME panel is not chosen, and the cybersecurity experts are not

appropriately versed in specific Red Team campaign methods. A second potential barrier to this study is gaining Institutional Review Board (IRB) approval to use human subjects in the execution of this experimental research. A third potential barrier to this study is the use of the corporate production environment to ensure the simulation testing is consistent with real-world scenarios and corporate end users.

Limitations and Delimitations

Limitations

A limitation of this study is related to employee classification, as there is a broad mix of hourly, salaried, professional, and credentialed roles within the company. This wide range of employee background, education, certification, etc. may be a limitation of this study as all employees are not of equal standing or positions. In addition, employees from recently acquired healthcare offices are likely less knowledgeable or aware of cybersecurity threats than those in a corporate environment. Lastly, this study was conducted in a Dental Services Organization (DSO), which historically has less stringent privacy practices than other healthcare organizations such as medical primary or specialty care offices, urgent care clinics, or hospitals.

Delimitations

This study was limited to research participants from a medium-sized, privately held, healthcare company. The sample population for this study are a mix of “admin” employees who centrally support the enterprise, and “clinic” employees who engage in direct patient care at various offices around the country. As all healthcare organizations are governed by the Health Information Portability and Accountability Act (HIPAA) guidelines, there may be differences in statistical findings between a healthcare versus non-healthcare organization.

Definition of Terms

The following represents the definition of terms:

Business Email Compromise (BEC) – Email attacks that are responsible for exceptionally large financial losses for organizations around the world every year (FBI, 2017).

Commercial-Off-The-Shelf (COTS) – Computer hardware or software tailored for specific uses, such as email security, and made available to the public for commercial use (Techopedia, 2017).

Cyberattack – Any fraudulent task conducted by an individual or group to a computer information system or network (Jain et al., 2017).

Delphi Expert Methodology – “The Delphi methodology has been found to effectively utilize a group communication process to refine measures based on the input of an expert panel” (Ramim & Lichvar, 2014, p.43).

Negative End User Response Actions – Corporate end user unconscious response to suspicious email which puts organization at risk of breach. Follows cognitive bias theory (Tversky & Kahneman, 1972).

Phishing – “Email based cyberattack aimed at acquiring sensitive information from the target using malicious software, hyperlinks, or fraudulent online websites” (Osugwu & Chukwudebe, 2015, p. 91).

Red Team - Group of internal IT employees or outside vendors used to simulate the actions of those who are malicious or adversarial, with a focus on exposing vulnerabilities (Techtarget, 2021)

Security Education, Training, and Awareness Programs (SETA) – Organizational

learning used to empower employees by increasing their knowledge and awareness and increasing skillsets (Albrechtsen, 2007).

Spear-phishing – “Email based cyberattacks that are customized and targeted toward specific individuals and organizations to obtain confidential information that is used for fraudulent purposes” (Osuagwu & Chukwudebe, 2015, p. 91).

Social Engineering – Defined as “a scalable act of deception whereby impersonation is used to obtain information from the target” (Lastdrager, 2014, p. 8).

Summary

Phishing campaigns have become increasingly common to most organizational end users, accounting for some of the most successful breaches in the last decade.

Phishing is the entry point for bad actors, whether to perform a ransom attack, hold data hostage, or perform one of the five BEC schemes. This activity is so common and successful, that the FBI IC3 (2022) reported worldwide losses of BEC to be over \$43 billion inclusive of all 50 states and 117 countries in 2021. These social engineering methods are continuing to become more complex over time, as organizations work to shore up their security awareness training programs and phishing mitigation methods. Despite the focus within organizations on phishing, finding the right combination of training programs and campaign methods has been a challenge.

This study added to the field of knowledge by measuring two different phishing training programs against two different phishing campaign methods. In addition to these measurements, and their impact on malicious emails, there were several demographic indicators and vulnerability action types measured. Vulnerability action type was measured based on end user negative response actions, such as opening an email, double-

clicking an attachment, clicking a hyperlink, data input, etc. All campaigns were measured using the same industry-standard SETA platform (KnowBe4) as the instrument. As this study was conducted in a production environment, using organizational employees, the opportunity for finding the right combination of phishing mitigation methods is possible. The findings from this study can be used within any organization to further help mitigate successful phishing attacks.

Chapter 2

Review of the Literature

Introduction

In this chapter, a literature review was conducted to provide a theoretical foundation for this research study focused on phishing mitigation methods. Based on the overall increase in cyberattacks, and the many high-profile ransomware and data theft cases over the last several years, phishing mitigation remains a primary goal in every organization. Most current statistics state that over 90% of successful cyberattacks and breaches begin as a phishing. With every organization's dependency on email, coupled with the fact that over three billion phishing emails are sent every day around the globe (Earthweb, 2022), it appears there is a need to continue researching phishing mitigation methods.

Although social engineering research has been present since the 1990s, it appears that there is still a considerable gap in knowledge around malicious phishing emails and how to protect against them. Cross and Gillet (2020) found even today there exists a large gap in knowledge of non-technical and human elements as it relates to social engineering. As such, it appears that phishing is only getting worse, with the US leading the way in negative financial impact. According to Mimecast (2022), there are well over a trillion phishing emails sent around the globe each year. In addition, the impact of these nefarious emails on organizations is astounding, with 47% resulting in account

compromise, and 49% resulting in malware infection. Review of the phishing literature also uncovered that, although SETA is effective at training employees, this knowledge is only as good as the last training session. Humans tend to quickly forget the lessons learned regarding the seriousness of phishing and nefarious emails, and require constant training and reminding (Mihaela, 2020).

The outcome of the literature review intends to add to the existing body of knowledge regarding social engineering, specifically phishing, spear-phishing, and BEC. In addition, the role that SETA plays in controlling a company's exposure to these risks is also explored. While SETA is imperative to any company's IT Security posture, it is important that the content, timeliness, and re-training of employees are taken into consideration. Lastly, the review of literature focused on phishing mitigation methods. While it is impossible to control every employee, organizations must deploy tools, software, and processes that provide technical means to protect the company and environment. These mitigation methods can include some or all of the following: deploying COTS email security software; building an internal team or contracting with a vendor to perform Red Team services (ethical hacking); and lastly, deploying a modern Intrusion Detection and Prevention System (IDPS) on the outside borders of the company network.

Social Engineering

In this section of the literature review, a systematic review of the literature was conducted on the evolution of social engineering, as well as the three specific types of social engineering most applicable to corporate email threats. According to Flores and Ekstedt (2016), there continues to be a gap in understanding the multiple types as it

relates to corporate email risk and cyberattacks. Greitzer et al. (2014) identified that additional research is needed on both the organizational security practices and the human factors that contribute to the success of data breaches through malicious business emails. According to Salahdine and Kaabouch (2019), social engineering attacks can be classified into three different categories: technical-based; social-based; and, physical-based (See Figure 1).

Figure 1

Social Engineering Categories



There are several social engineering attack types (see Figure 2), although this review is focused on three technical-based types: phishing, spear-phishing, and BEC.

Figure 2

Social Engineering Attack Types



Phishing

One of the most mature and prevalent forms of social engineering is broadly distributed phishing emails. These attacks utilize malicious messages that seem to be from a known or reputable source, however, they trick the target into action aimed at obtaining personal or banking information from either individuals or corporate employees (Thakur et al., 2015). While the perception of phishing is mostly negative, some forms of phishing have been used for years as a sales tool to establish leads (D'Qrill & Hendricks, 2018). This very effective form of social engineering has matured through the years and has been found to be even more effective if the email message is personalized or relatable in some way (Harrison et al., 2016). Several studies of phishing email campaigns have noted nearly a 50% chance of success if the attacker can connect with the target on a personal level.

While there have been many advancements in SETA deployed in organizations, there remains a high risk to employees. According to Mihaela (2020), despite the significant development of anti-cybercrime technology, the most significant security vulnerability continues to be the end user. Research by Volkamer et al. (2016) concluded that prompting or alerting a user of possible nefarious activity can significantly decrease the success of a phishing attack either via email or malicious URL. As malicious URLs are oftentimes part of phishing attacks, several research studies have focused on newer advances in technology, such as Machine Learning (ML) algorithms and Natural Language Processing (NLP) to identify them. In addition, Krishna et al. (2020) developed an approach for reading the URL and automatically dissecting it to detect if it appears malicious. They also found that the most effective way to identify the nefarious code was to deploy the dissection logic to the client side of the workstation.

Phishing remains the number one threat to organizations and is consistently used by attackers to deliver malicious URLs, malware, and other nefarious payloads.

According to Crowdstrike (2022), there has also been a shift to “hands-on-keyboard” activity and 62% of attacks were non-malware, meaning that traditional anti-virus and anti-malware tools would not detect the attack. In addition, since phishing is so effective and efficient, it has significantly reduced the time an attacker needs to move laterally through the target’s corporate network. In 2018, the average time to move laterally by an attacker was registered at nine hours and 42 minutes, and in 2021, that time has been drastically reduced to one hour and 38 minutes (Crowdstrike, 2022).

Table 1

Summary of Phishing

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
D’Qrill & Hendricks, 2018	Conceptual analysis		Deliberate phishing as a sales tactic	Phishing as a sales tool can be beneficial for the market if the equilibrium between phishermen and honest salesmen is not breached
Harrison et al., 2016	Experimental study	194 student subjects	Assessing user detection of phishing	47% of targets divulged their private information on fake online webpages. Phishing success was highly predicted by personalizing messages and low attention to email elements

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Jain & Gupta, 2017	Empirical study of phishing websites	Dataset of 2,141 phishing and 1,918 legitimate websites	ML engine using random forest algorithm	Identified 19 features of phishing websites. Using the ML engine, the authors achieved 99.09% positive detection of phishing websites
Kotson & Shultz, 2015	Empirical study of phishing emails	596 emails sent to 274 individuals	Phishing email identification methods	All emails sent to institutions disguised as job applications with attachments. The authors were successful in building an NLP engine that could identify phishing attachments with a high degree of statistical certainty
Krishna et al., 2020	Literature review		Approaches for identifying malicious URLs	Deployment of tools to client-side personal computers is the most effective way to detect phishing URLs. Using intelligent code to dissect the URL lexical and host-based features shows promise

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Volkamer et al., 2016	Empirical study of phishing and pruned URLs	411 participants; 16 websites	User awareness of address bar and use of pruned URLs	Significant improvement of phishing URL identification through providing hint to check the address bar and the use of URL pruning. Authors found 46% of participants did not check URL unprompted

Spear-phishing

An advanced form of phishing attacks are spear-phishing attacks, where more customized campaigns on targets are conducted by utilizing social engineering methods which make it difficult for both security systems and end users to detect (Laszka et al., 2016). Spear-phishing is successful because the target is often researched for weeks or months to ensure a personalized phishing email can be delivered. Bullee et al. (2017) concluded that by personalizing the first sentence, or opening phrase, of an email, the attacker had a much better chance of success.

According to TrendMicro (2022), spear-phishing is a phishing method that targets specific individuals or groups within an organization. It is a potent variant of phishing, a malicious tactic that uses emails, social media, instant messaging, and other platforms to get users to divulge personal information or perform actions that cause network compromise, data loss, or financial loss. While phishing tactics may rely on shotgun

methods that deliver mass emails to random individuals, spear-phishing focuses on specific targets and involves prior research. A typical spear-phishing attack includes an email and attachment where the email includes information specific to the target, including the target's name and rank within the company. This social engineering tactic boosts the chances that the victim will carry out all the actions necessary for infection, including opening the email and the included attachment. Spear-phishing is generally a precursor to BEC if the attacker is successful. Phishing and spear-phishing have their roots in the criminology Rational Choice theory (Cornish & Clark, 1987), which is based on a mindful assessment of the value of performing a certain task.

Although spear-phishing is hard to defend against, there are some basic precautions to take in defense. Being wary of unsolicited or unexpected emails, especially those that call for urgency. Common themes are generally involving an employee's boss or another executive that needs the target to take some action quickly. Always verify with the person involved through a different means of communication, such as a telephone call or face-to-face conversation to ensure the requests are valid.

Table 2

Summary of Spear-phishing

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Bullee et al., 2017	Empirical study of spear phishing emails	593 corporate employees	How opening phrase influences spear phishing	19% of employees in sample provided personally identifiable information (PII), compared to 29% when the first sentence of the email was personalized to the victim

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Lastdrager, 2014	Theoretical		Create common definition of phishing	Analyzed key concepts and components in literature to derive a new, comprehensive definition of phishing
Salahdine & Kaabouch, 2019	Literature review		Identification of current knowledge of spear phishing and other forms of social engineering	Updated knowledge of all forms of social engineering attacks. Suggestions of prevention and mitigation techniques reviewed, compared, and documented
Stembert et al., 2015	Qualitative study	24 participants	End user detection and response to spear phishing	Created a combination of warnings, blocking, educational messages, and reporting to aid end users with spear phishing identification

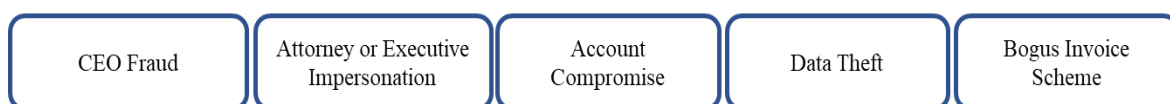
Business Email Compromise

BEC continues to be an ever-present threat to organizations around the world. The FBI IC3 (2021) reported that this type of social engineering shows no signs of slowing down. It is reported that in 2021, there were 19,954 complaints of BEC with an adjusted loss of nearly \$2.4 billion in the US alone. FBI IC3 (2022) reported worldwide losses of BEC to be over \$43 billion inclusive of all 50 states and 117 countries. While no

industries or business sectors are immune to BEC, the most targeted are Healthcare, Industrial or Engineering, Manufacturing, and lastly Technology. While phishing and spear-phishing are generally used for network infiltration, BEC is most often used for financial crimes and the exfiltration of dollars from an organization. This activity is so common in recent years the FBI (2017) created five pillars of BEC scams that still require research including Chief Executive Officer (CEO) fraud, attorney or executive impersonation, account compromise, data theft, and the bogus invoice scheme (See Figure 3).

Figure 3

Business Email Compromise Categories



In the recent past, there have been several scholarly journal studies written on BEC and have contributed much to the body of knowledge. Aviv (2019) found that there was a measurable deficit in the corporate end users detection skills, and created a way to measure this defect, and built a training module to address future education. In addition to end user detection there are also several studies that have explored how to detect BEC from a technical perspective. Nisha et al. (2021) published a case study to help support this effort by identifying techniques bad actors use to facilitate BEC, as well as several mitigations and countermeasures for organizations to enact. Lastly, Simpson and Moore (2020) found that small financial thefts are much less successful than larger ones in the hundreds of thousands of dollars. There was also empirical evidence suggesting that the transfer of these thefts to international accounts was more successful than domestic

transfers, which further suggests that continued research of BEC and mitigation methods are warranted.

Table 3

Summary of Business Email Compromise

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Aviv, 2019	Empirical	45 corporate end users	Online surveys and BEC detection mobile app	Developed a measure of BEC detection skills and a BEC awareness training module for corporate end users
Cross & Gillet, 2020	Literature review		Review of literature related to BEC through time of publication	Highlights gap in knowledge that still remains for non-technical, human elements of BEC
Nisha et al., 2021	Case Study		BEC techniques and detection methodologies	Detailed findings related to the media and techniques used by bad actors. In addition, several preventions, and countermeasures for organizations
Simpson & Moore, 2020	Empirical analysis of BEC thefts	7,925 BEC thefts	Data provided for nine months in 2017 via the FBI IC3 database	Small thefts from BEC succeed less often than larger dollars ranges. Additionally, transfers of money to international banks succeed more often than domestic US transfers

Security Education, Training, and Awareness (SETA)

SETA in Organizations

While several types of social engineering continue to be an issue for organizations, the global focus on ransomware has taken center stage. Over the last several years there have been hundreds of high-profile cases where billions of dollars have been extorted, and most start with a successful phishing attack. According to CrowdStrike (2022) there has been an 82% increase in ransomware attacks leading to data leakage. In 2020 there were 1,474 cases of data leakage reported, skyrocketing to 2,686 cases in 2021. Attackers are getting much better at ransom, and one of the primary ways for organizations to fight back is to better prepare employees through a comprehensive SETA program.

According to Bada and Nurse (2019), Small-to-Medium-sized Businesses (SMBs) continue to struggle with SETA and were able to deliver a program for SMBs to follow for cybersecurity awareness. In addition to SMBs, the healthcare industry also continues to struggle with cyberattacks as noted in a recent literature review (Nifakos et al., 2021). According to the review by Nifakos et al. (2021), clinicians in healthcare environments continue to struggle with cyber-related training and education while requiring continuous assistance and reminders of the threats. Outside of healthcare, many other business sectors struggle with SETA programs, and oftentimes fall victim to bad actors. Schweigert and Johnson (2021) found in a recent study of 8200 corporate employees that on average the organization can expect up to 27% of its employees will fall victim to phishing and that the role of SETA cannot be overstated.

Despite a focus on SETA in organizations for annual awareness training, it is imperative that ongoing training, such as monthly internally engineered phishing campaigns are implemented to continuously remind and teach the enterprise. In addition, it is important to understand the technical solutions required to protect the corporate network and solutions to stop attacks before they infiltrate the environment. Priestman et al. (2019) suggested that as much as three percent of all traffic coming from the internet is nefarious. Based on these facts, organizations must do everything necessary to defend their networks with robust firewalls, firewall rules, and state-of-the-art cybersecurity applications and tools.

Table 4

Summary of SETA in Organizations

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Bada & Nurse, 2019	Theoretical		SETA for small-to-medium-sized businesses and enterprises (SMB/SME)	Delivered high level program for SMB/SMEs to follow for cybersecurity awareness and training
Miranda, 2018	Conceptual		Implementing phishing awareness in organizations	Delivered comprehensive program for implementing phishing training and phishing detection and response. Also, an approach to follow for management buy-in.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Nifakos et al., 2021	Literature review		Human factors influence on cybersecurity in healthcare	Synthesis of 70 articles on cybersecurity in healthcare environments. Suggested approach for promotion of SETA, as well as need to adapt cyber hygiene practices among clinical professionals
Priestman et al., 2019	Empirical study of emails	18,871 threat messages	Third party cybersecurity firm conducting vulnerability testing via email	Finding suggests that two to three percent of emails and internet traffic are suspicious. Emphasized need for robust firewalls, cybersecurity infrastructure, IT policies and staff training
Schweigert & Johnson, 2021	Empirical study of emails	8200 corporate employees	PhishMe software used to send phishing emails	Organizations on average can expect that 27% of its employees will fall victim to phishing attacks. Companies have to create SETA programs for phishing awareness

General Public Personal Knowledge

Outside of the corporate environment and the struggles employees have distinguishing threats, those same problems are transferred to personal lives online. With every industry moving to a nearly complete online, self-service presence, it is necessary

for the general public to be aware of cyber threats. These threats transcend everything done online, from social media interactions, to online banking, to online shopping, and more. In a recent survey of adult online users, Ricci et al. (2019) found that nearly every respondent had anxiety and fear over their personal safety online, and most welcomed adult cyber education courses. Additionally, Hamid and Dali (2019) found that environment significantly influences the personal values of individuals, as well as the level of risk-taking online. The conclusion was that level of experience, skills, and self-efficacy have a significant impact on risky behavior.

While in most contexts SETA in organizations is understood, having these skills and applying them to personal behavior is critical to prevent from being a victim. Chou et al. (2021) found that mindless response and mindful interpretation can occur at the same time. From a personal email perspective, this means the end user needs to focus on identifying the influence inside the message to gauge its safety. This concept can be transferred to other online experiences as well. Feng et al. (2019) produced an online user analysis model to assess the risk by collecting personal information and online social behaviors to predict the probability of attack. Knowing what constitutes risky behavior online and presenting that to the general public can prevent end users from falling victim to scams. For all the media coverage of cyberattacks, there continues to be a disbelief that it will happen in a personal setting. Mihaela (2020) found that despite known risks, and significant coverage of cyberattacks in the media, individuals are still falling for the same exploits. Legacy cybersecurity issues continue to remain, with the top three incidents being phishing, malware, and malicious URLs. The keys to protection lie in personal SETA and remaining vigilant of these ever-present dangers.

Table 5*Summary of SETA General Public Personal Knowledge*

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Chou et al., 2021	Quantitative	273 university students	Post-phishing simulation survey administered across two universities	Research found that mindless response and mindful interpretation can happen simultaneously. One practical implication is to refocus SETA on identifying the influence inside the message to gauge phishing
Feng et al., 2019	Empirical study of social network information	4,536 social network users	Algorithm created to extract five features for classification	Study produced a novel user analysis model to assess the user's risk. This model collects user personal information and social behaviors online to predict probability of attack
Hamid & Dali, 2019	Empirical study	396 professional workers	Online survey (Google doc)	Environment significantly influences the personal values of the employee. Skills, experience, and self-efficacy have significant impact to the behavior of the employee

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Mihaela, 2020	Qualitative	20 cybersecurity reports	University databases and online professional websites	Legacy cybersecurity issues continue to remain, with the top three incidents being phishing, malware, and malicious URLs
Ricci et al., 2019	Empirical study	233 participants	Online survey regarding adult cyber-education	Most respondents expressed anxiety regarding their personal safety online. 77% favored seminars of one to one and a half hours in length to educate themselves

Phishing Mitigation Methods

Commercial-Off-The-Shelf Email Security Software

Although there are several types of phishing mitigation methods, this literature review focused on three. Proofpoint (2021) stated that impostor emails are purpose-built to impersonate someone the user trusts and tricks them into sending money or personal information. COTS email security software can provide an integrated, holistic solution that addresses the attackers' tactics, provides visibility into malicious activities and user behavior, as well as automates detection and threat response. According to Mimecast (2022), there are well over a trillion phishing emails sent around the globe each year, which makes it imperative that every organization deploy a COTS email security solution.

While COTS email security software has been around for many years, recently the technologies have improved vastly. Alabdan (2020) found increasing numbers of COTS tools that have now integrated newer ML algorithms and NLP features to make the products more effective. In addition, Fortino et al. (2020) proclaimed that in the last few years major COTS vendors have increased investment in “security by design” architectures to further protect customer data and strengthen their security posture. Some COTS email security vendors, as well as mainstream cybersecurity mitigation vendors, have even started providing a guarantee with their products, where they reimburse for any cyberattack up to a certain dollar threshold.

In line with utilizing the newest technologies, vendors such as Mimecast, Proofpoint, Microsoft and others offer additional features which can significantly protect against nefarious external emails. One modern approach is to enable Domain-based Message Authentication, Reporting, and Conformance (DMARC) on the platform. DMARC uses two other technologies, DomainKeys Identified Mail (DKIM), and Sender Policy Framework (SPF) in conjunction with the enterprise Domain Name System (DNS) to protect the company. DKIM and SPF are email authentication methods designed to detect forged sender addresses in email, a technique often used in phishing attacks. These methods allow the receiver to check that an email claimed to have come from a specific domain was indeed authorized by the owner of that domain. Although the advances in COTS email security software are increasing, there are no perfect solutions, and the end user is responsible for the last action.

Table 6

Summary of COTS Email Security Software

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Alabdan, 2020	Literature review		Review current approaches used during phishing attacks	Research found support for using NLP, ML, and COTS tools to prevent phishing attacks
Fortino et al., 2020	Case study		Investigation of commercial Internet of Things (IoT) platforms and their security design	Since 2020, most major COTS IoT platforms have increased investment in “security by design” architecture to protect customer data and further strengthen their security posture
Humayan et al., 2022	Literature review		Comprehensive review of software as a service (SaaS) security software	Identification of 75 security issues and 44 best practices from scientific studies. 55 security issues and 47 best practices from grey studies

Ethical Hacker or Red Team

The second phishing mitigation method included in the literature review is that of ethical hacking or red teaming. According to Scott (2021), a red team is a group of experts deployed within an organization to identify vulnerabilities and threats by adopting the perspective of an adversary. Red teaming developed out of wargaming exercises used in the military and was first used extensively in the government intelligence sectors (Zenko, 2015). In the private sector, as large organizations became

aware that they were static targets for hackers whose methods and motives were poorly understood, red teaming methods found a natural home in cybersecurity. Red teams of cybersecurity professionals, either engaged as consultants or an internal team of specialists, conduct penetration testing to probe for weaknesses in an organization's protective systems.

Based on the continued growth of cybersecurity threats, many organizations have moved to this approach to ensure they know where the weaknesses are, and to quickly improve their overall security posture. Miran (2019) engaged the services of 27 red teaming vendors and found they were able to produce sophisticated, persistent, and personalized attacks that were incredibly insightful to the organization. Additionally, Pradeep and Sakthivel (2020), realizing the importance of deploying an ethical hacker program, created a framework for deploying this methodology within organizations. Their case study also identified and documented the different stages of hacking and preventative measures to deploy (Pradeep & Sakthivel, 2020). Further, Gandhi et al. (2022) researched the importance of ethical hackers in an organization by classifying the types of hackers and how to guard against them. As with most cybersecurity concepts, the last few years have seen a marked improvement in red teaming, including the automation of the methodology. Red teams are focused on offensive measures, whereas blue teams try to defend against them. Yoo et al. (2020) created an adversary emulation framework to automate both red and blue team processes to constantly monitor for potential issues in the enterprise.

Table 7

Summary of Ethical Hacker or Red Team

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Gandhi et al., 2022	Conceptual		Visibility into the types of hackers	Importance of ethical hackers in organizations to find IT Security vulnerabilities before the bad actors do
Mirian, 2019	Empirical study of hacking services	27 hack-for-hire vendors	Assess the value of contracting with hack-for-hire services	Hack-for-hire services were shown to produce sophisticated, persistent, and personalized attacks that couple bypass 2-factor authentication via phishing
Pradeep & Sakhivel, 2020	Case study		Create a framework for ethical hacking	Importance of deploying an ethical hacker program. Also identified the different stages of hacking and preventative measures
Scott, 2021	Experimental	Three example teams	How to apply red teaming methodologies	Regulators in the financial sector are now expecting approaches for managing both financial and non-financial risk. Red teaming can play a key part of the organization's protection and compliance strategy

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Yoo et al., 2020	Experimental	Eight attack and two defense techniques	Automation of red and blue team emulations	Creation of adversary emulation framework to automate red and blue team algorithms to constantly monitor for cyber issues

Intrusion Detection and Prevention Systems

The last phishing mitigation method included in this literature review is IDPS. IDPS have become increasingly more sophisticated and complex due to ever-present threats and malicious activity on worldwide networks. The outcome of the Bul'ajoul et al. (2019) research exposed that, despite this sophistication, even modern IDPS have many flaws, particularly in high-speed environments. To highly enhance the protection of the environment, it is suggested that a novel Quality of Service (QoS) architecture be erected to increase the IDPS effectiveness (Bul'ajoul et al., 2019). Even through the lens of modern Software Defined Networks (SDN) which assist in increasing the cybersecurity posture, Ali et al. (2020), suggested building a three-tier IDPS to validate the transaction from a user, packet, and flow perspective.

According to Khraisat et al. (2019), the continuous evolution of malicious software (malware) also continues to be a challenge to the design principles of IDPS. These attacks often come in the form of unidentified or obfuscated transactions, making evasion techniques more challenging for the industry. As a result, many countries, including the US have seen a significant impact from zero-day attacks. Further,

the popularity of mobile devices has created yet another challenge for the industry.

Ribero et al. (2020), suggested the best approach for mobile security is to create a host based IDPS, and were able to prove this local IDPS could detect the difference between normal and malicious activity. IDPS must continue to evolve with technology, regardless of which medium, be it traditional, mobile, internet or big data systems.

According to Samson (2020), an IDPS identifies potential threats based upon built-in rules and profiles. These rules can work in a couple of different ways, including looking for signatures or anomalies. A signature based IDPS is looking for instances of known attacks. After a piece of malware or other malicious content has been identified and analyzed, unique features are extracted from it to create a fingerprint of that attack. Signature-based detection systems compare all traffic, files, activity, etc. to a database of signatures. If a match is found, the IDPS knows that the content is part of an attack. Anomaly-based detection systems take a different approach to identify malicious content. Instead of fingerprinting known attacks, they build a model of “normal” behavior for a particular system. After this model is built, the IDPS can look for anything that does not match its model (an anomaly). If the model is well-trained, any anomalies are attacks. Many IDPS systems combine both signature and anomaly detection (hybrid model). The reason for this is that the two approaches have complementary strengths and weaknesses.

Table 8

Summary of Intrusion Detection and Prevention Systems

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Ali & Yousef, 2020	Conceptual		Built a three-tier IDPS to reduce effect of intruders	The software-defined three-tier IDPS shows better efficiency in terms of detection rate, failure rate, precision, accuracy, relay throughput, and traffic load
Bul'ajoul et al., 2019	Experimental		Improving network intrusion detection and prevention systems (NIDPS) in high-speed environments	Created a Quality of Service (QoS) architecture allowing Snort to process packets at 8gb/sec. This new architecture solved one of the long-standing issues of packet inspection in high-speed environments
Kraisat et al., 2019	Literature review		Taxonomy changes and recent research in anomaly and signature-based IDS	After a detailed survey of new IDPS approaches, it has been found that there exists a need for newer and more comprehensive data sets for ML algorithms

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Ribeiro et al., 2020	Empirical study	15 test data sets, each containing 600 examples	Building a host-based Android IDPS	Created a novel IDPS called HIDROID. This autonomous app runs on an Android device and is not reliant on a remote server. Testing showed great promise that this app is very accurate in determining infected vs. benign code

Summary of what is Known and Unknown

A literature review of social engineering, SETA, and phishing mitigation methods in the cybersecurity research field has been conducted to provide a foundation for this research study. While many studies have focused on types of social engineering, phishing continues to be the number one cause of successful cyberattacks in organizations. The FBI (2021) stated over 90% of all data breaches start as a phish and may be increasing by as much as 400% per year. Phishing success and the negative impact to organizations is widely publicized and known, however, this research study will focus on what is unknown in this field. What is unknown, as it relates to successful phishing email attacks in organizations, is the impact that various forms of phishing training programs coupled with various phishing campaign methods have on phishing mitigation. Another mitigation method, IDPS, was also discussed as part of the literature review, however, the focus of this study was contained within the corporate email environment and not the

external network. This study addressed a current gap in the body of knowledge as it relates to phishing attacks and how to effectively mitigate them in an organizational environment.

Chapter 3

Methodology

Overview of the Research Design

This experimental research targeted the difference between phishing training methods and phishing campaign methods when controlled by multiple factors. Figure 4 illustrates the research design this study leveraged (Levy & Ellis, 2011). In Phase 1, this study developed a baseline measure between training and campaign results leveraging an expert panel of cybersecurity professionals utilizing the Delphi method. The expert panel consisted of 50 cybersecurity SMEs to conduct the review. The Delphi method is a demonstrated technique in the field of information systems in the development of the experiment with SMEs (Ramim & Lichvar, 2014). Once the measurement instrument was validated, Phase 2 of this study included a randomized participant sample selection of 30 business professionals for each quasi-experiment (Figure 5). Furthermore, Phase 2 of this study created a baseline, or top-tier level, experiment without any prevailing controls. Last, Phase 3 of this study further expanded on phishing training methods versus phishing campaign methods results but was controlled by demographic indicators and vulnerability action types to quantify any statistically significant differences.

Figure 4

Overview of the Research Design Process

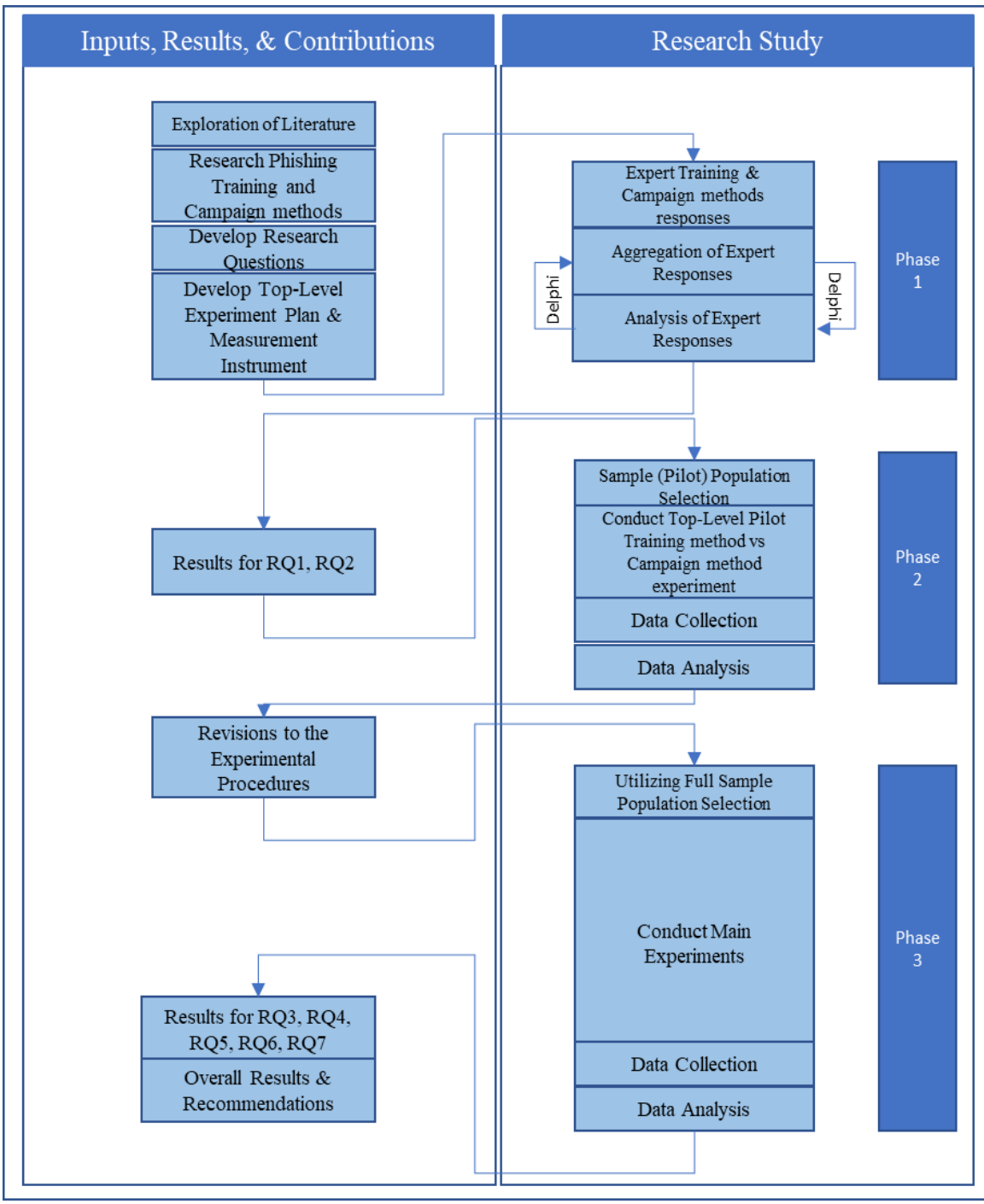


Figure 5
Randomized Quasi-Experimental Design

		Phishing Campaign Method	
		Industry-standard phishing campaign	Red Team phishing campaign
Phishing Training Method	An annual industry-standard phishing awareness training	30 end user random sample for pilot study	30 end user random sample for pilot study
	Continuous customized social engineering focused training	30 end user random sample for pilot study	30 end user random sample for pilot study
	No training - Control	30 end user random sample for pilot study	30 end user random sample for pilot study

Measures

There continues to be a lack of research around social engineering email attacks within organizations as well as a gap in the examination of an organization's professional end user behavior (Flores & Ekstedt, 2016). Therefore, this study evaluated the results of phishing training methods versus phishing campaign methods by using organization professionals who extensively use business email. The participants were randomly chosen based on demographic characteristics to ensure that the data collected is a solid representation of the population. A random sample method was utilized to ensure equal probability of being selected and as well ensuring that the sample is generalizable to the population (Creswell, 2014). While Phase 2 utilized 30 targeted end users for the pilot

study, Phase 3 incorporated 200 targeted unique organizational end users in the main study. The results of each simulated phishing email campaign were measured by KnowBe4 using six-actual performance metrics. The instrument was assessed utilizing cybersecurity SMEs via the Delphi process. The Delphi method is an effective approach to achieving an expert panel consensus in designing or validating a measurement instrument (Ramim & Lichvar, 2014).

The specific end user negative response actions or vulnerability types measured during Phase 2 and Phase 3 were: 1) non-identification, 2) clicking/opening, 3) replying/forwarding, 4) opening attachments, 5) enabling macros, as well as 6) data entry. In addition, further measurements based on demographic indicators were assessed for both training programs and campaign methods. During the events, each end user received a unique email from the different campaign methods to ensure no duplication. As no campaign emails were duplicated, the results were more effectively assessed.

Instruments

SMEs Instrument

The 50 targeted cybersecurity SMEs were recruited through many different methods, including social media (Facebook, LinkedIn, etc.), as well as word of mouth and personal network facilitation. Appendix B shows the recruitment letter that was sent to each cybersecurity SME via email in order to facilitate their participation after IRB approval is achieved. Once the SME panel was finalized, each person received a link to the “Cybersecurity SME Survey” (Appendix C) using the Google Forms ® platform. Ultimately this survey confirmed the approved components of the experimental procedures, as well as validated their use as part of the research experiments. The

outcome of the SMEs instrument results was used to positively confirm RQ1 and RQ2 of this research study.

Organizational End User Instrument

This study leveraged a commercially available COTS platform that provided reporting as to the behavior of the end user (Appendix D). During phishing campaigns, the negative response actions related to the vulnerability types were logged for every email and every end user in that specific campaign. This industry-standard reporting platform (KnowBe4) provided a detailed analysis of the campaign, regardless of method (industry-standard or Red Team), so the IT leadership may understand which phishing campaigns are most effective. Once the campaign was completed, the platform offers an overall “phish-prone” percentage for that specific campaign, but also provides the detailed actions each end user did or did not perform. While the overall score of the campaign is continuous (percentage) data, the details of each end users negative response actions are binary or discrete (pass/fail), allowing for further detailed analysis. Based on the overall output, the IT leadership can determine which campaigns are more successful at phishing the organizations’ population. The data provided from the platform provided insights that helped inform the continuous customized and annual SETA training programs.

Data Analysis

Phase I

Quantitative data collection methods were used in Phase 1 for the collection of cybersecurity SMEs inputs with validation of current phishing mitigation methods, as well as phishing training and campaign methods. The specific data collection method was

a short survey sent by email to the selected SMEs. According to Kost and Correa da Rosa (2018), a shorter survey instrument holds the potential to dramatically improve the response rate as opposed to a longer survey. This shortened survey was created utilizing a 7-point Likert scale to achieve a more granular and accurate response from the SMEs. The 7-point Likert scale was used for non-demographic questions and will rate agreement from (1) Strongly Disagree through (7) Strongly Agree.

The Delphi methodology was used to ensure the reliability and validity of the instrument utilized for this research study. This methodology is oftentimes used to summarize the agreement between the SME group as to the applicability of the measurement instrument. Walker and Selfe (1996) stated that a 70% agreement in the survey questions by respondents was an acceptable rate to validate the instrument and move forward with this study. Provided the result of the survey is 70% or more agreement, a consensus was achieved. Therefore, using the inputs from the cybersecurity SMEs provided the needed validation for the first two RQs:

RQ1: What are the approved components of the experimental procedures for the phishing training and campaign methods according to cybersecurity SMEs?

RQ2: What level of validity of the experimental procedures for the phishing training and campaign methods is sufficient according to cybersecurity SMEs?

Phase II

Phase 2 consisted of a pilot study with randomized participants grouped into one of two developed treatments (Industry-standard and Red Team) as well as a control group (no training). Pilot data was collected, and data analysis performed using ANOVA. The

experiment was revised per the preliminary data analysis and the results aided in adjusting the research measures to ensure internal validity. This study utilized the linear statistical models to address the research questions utilizing SPSS® Statistics™ version 28. The statistical analysis one-way ANOVA was used to assess significant mean differences between variables being studied (Sekaran & Bougie, 2016).

Phase III

Phase 3 incorporated the findings from the pilot study in Phase 2 and used this information to perform the main study. All data gathered on the population came from a System Administrator on the Chief Technology Officers (CTO) team. In addition, all needed information to codify and analyze the data was provided by this separate team. All data to answer demographic questions as part of RQ6 and RQ7 was provided by the team based on the employee ID of the participants. All end user participants were required to provide consent in email (Appendix E) to be considered for the research study. No PII was provided during data collection for the experiments per IRB guidelines.

The main study was inclusive of all phishing training program types, as well as both phishing campaign methods. All measurements were analyzed to determine if any statistically significant differences exist. A summary of research by phase and analysis method is described below (Table 9). Knowledge gained from the pilot and main study experiments were used to answer all of the RQs, with RQ6 and RQ7 controlled for multiple demographic indicators:

RQ3: Are there any statistically significant mean differences between the use of an annual industry-standard phishing training, continuous customized social

engineering focused training, and a control group without training, on end users' negative response to malicious emails?

RQ4: Are there any statistically significant mean differences between the use of an industry-standard phishing campaign and a Red Team phishing campaign on end users' negative response to malicious emails?

RQ5: Are there any statistically significant mean differences between the phishing training methods (an annual industry-standard phishing awareness training vs. continuous customized social engineering focused training vs. no training - control) and the phishing campaign methods (industry-standard phishing campaign vs. Red Team phishing campaign) on end users' negative response to malicious emails?

RQ6: Are there any statistically significant mean differences between the use of an annual industry-standard phishing training, continuous customized social engineering focused training, and a control group without training, on end users' negative response to malicious emails, when controlled for participants': (a) age, (b) gender, (c) job role, (d) location (clinic vs. admin), and (e) years of job experience?

RQ7: Are there any statistically significant mean differences between the use of an industry-standard phishing campaign and a Red Team phishing campaign on end users' negative response to malicious emails, when controlled for participants': (a) age, (b) gender, (c) job role, (d) location (clinic vs. admin), and (e) years of job experience?

Table 9*Summary of Research Phases*

Research Question	Phase	Proposed Sample	Methodology	Analysis
RQ1	Phase I	50 SMEs	Delphi	Consensus via means
RQ2	Phase I	50 SMEs	Delphi	Consensus via means
RQ3	Phase II Phase III	30 users (x3) 200 users (x3)	Qualitative measure	ANOVA
RQ4	Phase III	30 users (x3) 200 users (x3)	Qualitative measure	ANOVA
RQ5	Phase III	200 users (x3)	Qualitative measure	ANCOVA
RQ6	Phase III	200 users (x3)	Qualitative measure	ANCOVA
RQ7	Phase III	200 users (x3)	Qualitative measure	ANCOVA

Population and Sample

This study evaluated the results of two phishing training programs versus two phishing campaign methods by using corporate professionals who extensively use email. The participants were chosen based on demographic characteristics to ensure that the data collected is a solid representation of the population. A random sample method was utilized to ensure an equal probability of being selected and as well as ensuring that the sample is generalizable to the population (Creswell, 2014). The population was representative of the organization's 5,000 associates with a proper mix of positions within the organization.

Chapter 4

Results

Overview

The results of the data collection and analysis for this research study are presented in this chapter. The research study results were completed in three phases (Delphi SME Survey, Pilot Study, and Main Study), where the details of each of the phases are presented in the order in which they were conducted. Phase 1 consisted of a Cybersecurity SME survey with data collection utilizing the Delphi method. The primary reasons for the survey were to provide expert opinion on the significance phishing still plays in the current threat environment, and to gauge agreement on the six negative response actions being measured by the instrument. The results of Phase 1 address RQ1 and RQ2. Phase 2 details the results of the pilot experimental study which utilized three randomly selected groups of 30 targeted organizational end users based on the type of phishing training they received (no training, continuous customized training, or annual industry-standard training). The data collected in the pilot study was used to confirm the experimental approach was successful and the quality of the data was adequate to move to the main study (Phase 3). Phase 3 details the results of the main experimental study which utilized three randomly selected groups of 200 targeted organizational end users, again based on the type of phishing training they received. Phase 2 and Phase 3 address

RQ3, RQ4, and RQ5, while Phase 3 addresses RQ6 and RQ7 which are controlled for five demographic variables.

Phase I – Cybersecurity SME survey feedback

RQ1 and RQ2 were answered through a survey instrument during the first phase of this research study. Participation in the Cybersecurity SME survey was facilitated by sending an email invitation to 50 potential candidates within the network of work, school, and personal acquaintances, with a goal of 25 respondents. Of the 50 potential candidates, 27 cybersecurity SMEs completed the survey over a period of about three weeks. Table 10 provides the descriptive statistics for the 27 respondents. The SMEs represented a variety of different and diverse current job roles/positions including cybersecurity analyst (3.7%), cybersecurity consultant (22.2%), cybersecurity instructor/professor (14.8%), middle management (14.8%), senior management (25.9%), and owner/executive/c-level (18.5%). The years of experience for the SME group also varied, with one to five (11.1%), six to 10 (18.5%), 11 to 15 (25.9%), 16 to 20 (7.4%), and the largest group 20 or more years (37.0%). The entire SME group was employed full-time (100%) with most participants (74%) over 40 years of age. Of the group of 27 respondents, a large majority (85.2%) were male, with female making up the remainder (14.8%). There were large discrepancies in the number of cybersecurity certifications ranging from none (37.0%), one (25.9%), two (11.1%), three (14.8%), and four or more (11.1%). Lastly, the SME group had a high level of education, with all but two having a bachelors degree (33.3%), masters degree (29.6%), or doctoral degree (29.6%).

Table 10

Summary of SME Demographics (N=27)

Demographic Item	Results	N	%
Current Position			
	Analyst	1	3.7%
	Consultant	6	22.2%
	Instructor/Professor	4	14.8%
	Middle Mgt	4	14.8%
	Owner/Exec/C-level	5	18.5%
	Senior Mgt	7	25.9%
Years of Experience			
	1-5 years	3	11.1%
	6-10 years	5	18.5%
	11-15 years	7	25.9%
	16-20 years	2	7.4%
	20+ years	10	37.0%
Employment			
	Full-time	27	100%
Age Range			
	21-30	1	3.7%
	31-40	6	22.2%
	41-50	10	37.0%
	51-60	9	33.3%
	61-67	1	3.7%
Gender			
	Female	4	14.8%
	Male	23	85.2%
Cyber Certifications			
	None	10	37.0%
	One	7	25.9%
	Two	3	11.1%
	Three	4	14.8%
	Four or more	3	11.1%
Level of Education			
	High School	1	3.7%
	Associates Degree	1	3.7%
	Bachelors Degree	9	33.3%
	Masters Degree	8	29.6%
	Doctoral Degree	8	29.6%

Phase I – RQ1 & RQ2

In addition to the demographics above, the cybersecurity SME group also provided inputs to answer both RQ1 and RQ2. The survey answers provided positive

feedback on both the approved components and the level of validity of the experiment based on Delphi consensus thresholds. In general, Delphi consensus thresholds range from 51% to 100%, however a 75% or greater score is standard and, therefore, is an acceptable threshold for decision making (Dupuis et al., 2016). For RQ1, the SME panel was asked to rate the six “end user negative response actions” used to score the experiment (Table 11 and Figure 6), as well as the two different campaigns methods that were to be used in both the pilot and main studies (Table 12).

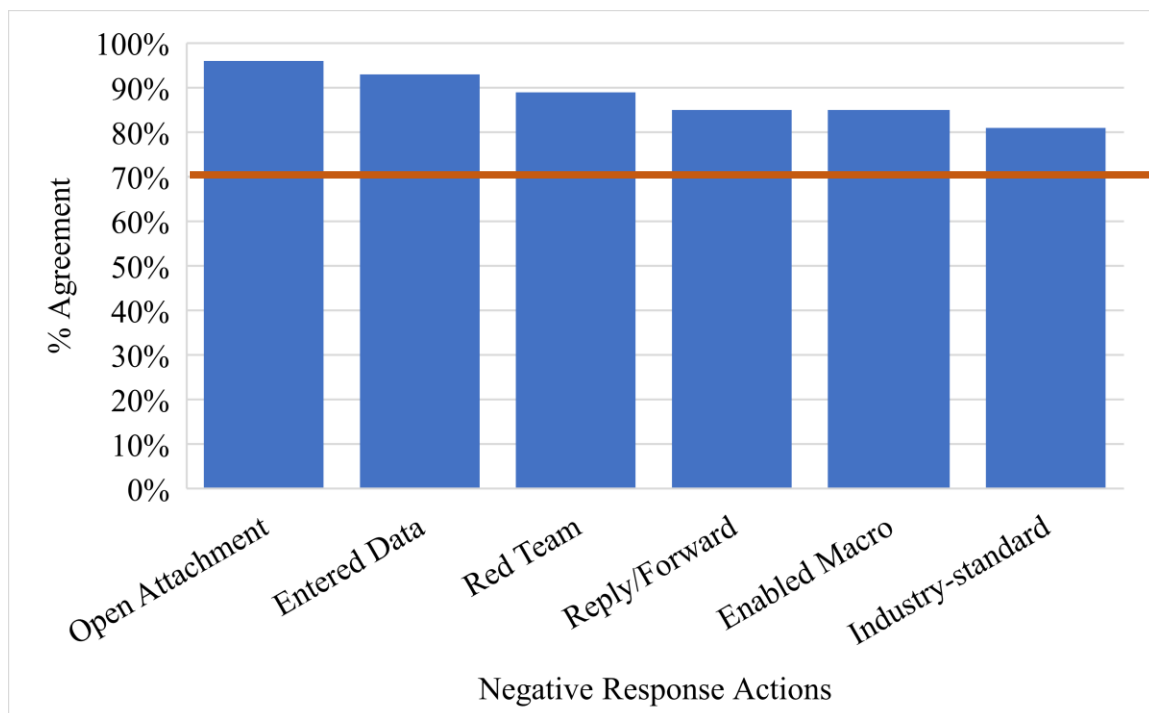
Table 11

SME % Agreement for Six End User Negative Response Actions (N=27)

Negative Response Action	Average	St.Dev	% Agreement
Not Reported	5.93	1.2066	85%
Opened	6.04	1.2855	89%
Reply/Forward	5.74	1.5589	85%
Open Attachment	6.52	0.9352	96%
Enabled Macro	6.11	1.6718	85%
Entered Data	6.30	1.1373	93%

Figure 6

SME % Agreement for Six End User Negative Response Actions (N=27)



For each of the six end user negative response actions, the SME respondents were asked to rate the action types based on the level of agreement of these measures as components of the users' negative response to the phishing campaign. A 7-point Likert scale was used with one being the least agreement and seven being the most. Based on the SMEs answers, and high percent agreement to the components, approval to move forward was gained with total percent agreement between 85% and 96% on all measures. Another set of questions was used to gauge the agreement on the two phishing campaigns to be employed (Industry-standard and Red Team). Table 12 and Figure 7 shows the high percent agreement of these components as well, Industry-standard (81%) and Red Team (89%).

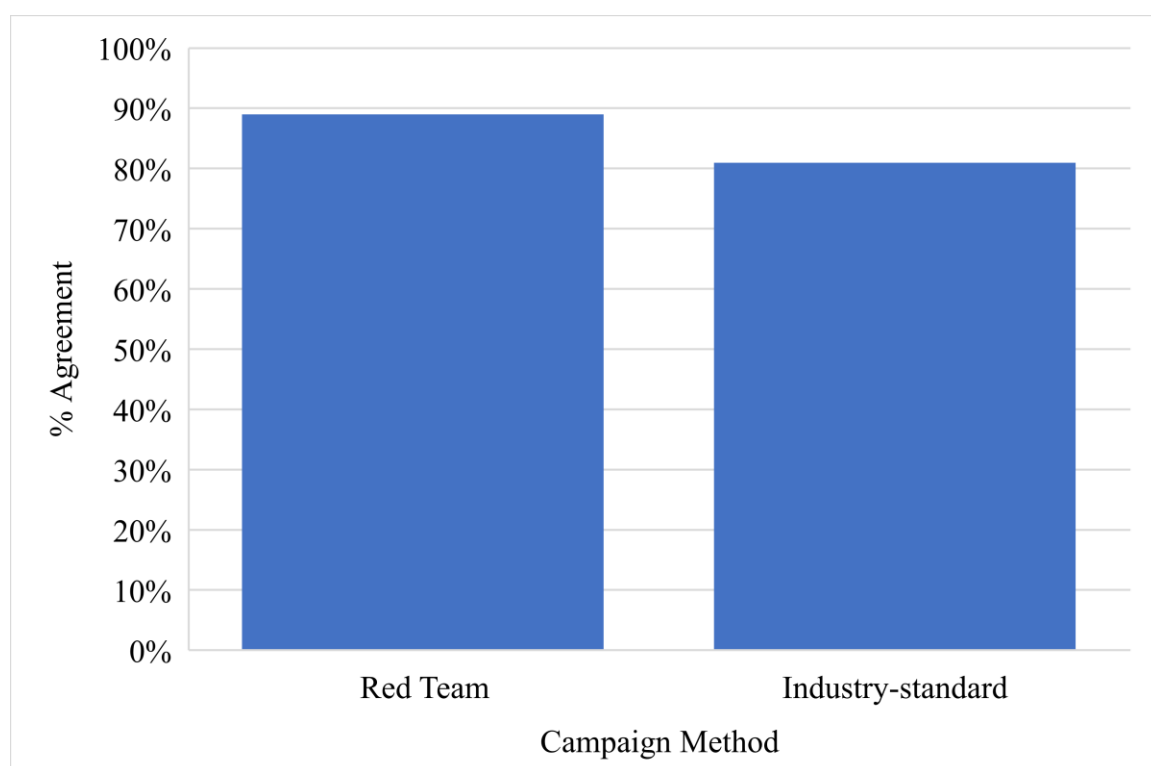
Table 12

SME % Agreement for Phishing Campaign Methods (N=27)

	Industry-standard	Red Team
Averages	5.44	5.85
Stand Dev	1.7172	1.6572
% Agreement	81%	89%

Figure 7

SME % Agreement for Phishing Campaign Methods (N=27)



In addition to the approval of the experiments components (RQ1), the SME respondents were asked to provide feedback on the validity of the overall experiment and the significance of phishing overall in the world of cybersecurity (RQ2). Based on the responses regarding the SMEs level of knowledge around phishing and phishing campaigns (96% agreement) coupled with the direct question about the “significance of phishing today” (also 96% agreement) showed clear support of the measures. With RQ1

and RQ2 successfully answered and approved, the Phase 2 pilot data collection process was followed.

Phase II – Pilot Study

Data Collection

The pilot study was conducted to confirm the ability to acquire the needed data for the main study, as well as to test the procedures in which the data was collected. In this phase, a random selection of three distinct groups of organizational end users were chosen to test and confirm the process. First, a group of 30 unique organizational end users were selected who were new to the organization and had not been exposed to any previous phishing training from the company. Second, a separate group of 30 unique organizational end users were selected to receive an annual, industry-standard phishing training of 30 minutes. Last, a separate group of 30 unique organizational end users were selected to receive customized, continuous phishing training, consisting of eight short videos of less than five minutes in length.

Once the three pilot groups were chosen, they were sent an email (Appendix E) to provide insight into this study and give them an opportunity to either consent (yes) or to dismiss (no) themselves. This initial recruitment process lasted for one week to provide the organization end user an opportunity to respond. The results for the pilot groups showed only a 3-6% opt out rate. For the no training group of 30, only two users responded no to participating in this study. For the annual training group of 30, as well as the continuous customized group of 30, only one person from each group declined.

With the three pilot groups set, the following week began the phishing training phase. By design, the no training group received no training as part of this study to ensure

an appropriate control group. The annual training group was provided with a link through their business email to complete the 30-minute annual phishing awareness training within four weeks. The continuous customized group received two short videos to their business email each week for four weeks, for a total of eight short video training courses. The completion status for both the annual group and the continuous customized group were tracked to ensure the completion of the courses.

After the 4-week training phase of the data collection process, the phishing campaigns commenced. Each week for two weeks, all three groups were phished twice a week by both phishing campaign methods (Industry-standard and Red Team). The data for all phishing campaigns was collected with the KnowBe4 platform to get a real-time view into the effectiveness of each campaign. The KnowBe4 platform was able to collect data on all six negative end user responses by providing a count of clicks for each action. Overall, this produced the needed data to further analyze the effectiveness of the phishing training methods, as well as the phishing campaign methods. The pilot data upon completion consisted of two sets of 86 responses (No training 28, Annual 29, Continuous 29) for 172 discrete responses to analyze. During the pilot data collection phase, there were no demographic indicators captured. To further confirm the data collection process was accurate, an analysis of the pilot data was completed to test the results for RQ3 and RQ4.

Data Analysis

Using SPSS® Statistics™ version 28, data collected from the pilot study was loaded and analyzed to test two of the research questions. To answer RQ3, if any statistically significant mean differences exist between the three types of organizational

end user phishing training (No Training, Annual, Continuous Customized) and the six negative end user response actions, an ANOVA was used to test for significant differences between groups. Table 13 shows the output of the one-way ANOVA to determine any mean differences.

Table 13

One-way ANOVA Output for RQ3 Using Pilot Data (N=172)

Negative Response Action	Sum of Squares	df	Mean Square	F	Sig.
Not Reported	.822	2	.411	1.151	.319
Opened	.166	2	.083	.109	.897
Reply/Forward	.012	2	.006	1.036	.357
Open Attachment	.000	2	.000	N/A	N/A
Enabled Macro	2.080	2	1.040	1.766	.174
Entered Data	1.825	2	.913	.746	.476

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Based on the output of the ANOVA, there appear to be no statistically significant mean differences between the phishing training method and the six negative response actions (p values above 0.05, see Table 13). This result would indicate that the training method is overall not an important factor in determining negative end user response actions.

To answer RQ4, if any statistically significant mean differences exist between the two types of phishing campaigns (Industry-standard and Red Team) and the six negative end user response actions, an ANOVA was used to test for significant differences between groups. Table 14 shows the output of the one-way ANOVA to determine any mean differences.

Table 14

One-way ANOVA Output for RQ4 Using Pilot Data (N=172)

Negative Response Action	Sum of Squares	df	Mean Square	F	Sig.
Not Reported	2.814	1	2.814	8.195	.005*
Opened	11.256	1	11.256	16.146	<.001***
Reply/Forward	.006	1	.006	1.000	.319
Open Attachment	.000	1	.000	N/A	N/A
Enabled Macro	3.930	1	3.930	6.840	.010*
Entered Data	7.535	1	7.535	6.375	.012*

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Based on the output of the ANOVA, there appears to be several statistically significant mean differences between phishing campaign method and the six negative end user response actions. The mean differences for Not Reported ($F(1,171) = 8.195$, $p = .005$), Opened ($F(1,171) = 16.146$, $p < .001$), Enabled Macro ($F(1,171) = 6.840$, $p = .010$), and Entered Data ($F(1,171) = 6.375$, $p = .012$) are all statistically significant. This result indicates the way the phishing campaign method is conducted has a significant impact on end user negative response actions. With the data collection and analysis process confirmed accurate, the research moved on to the main study to formally answer RQ3, RQ4, RQ5 with the larger main study dataset, and RQ6 and RQ7 with demographic data.

Phase III – Main Study

Data Collection

Like the pilot, in this phase, a random selection of three distinct groups of organizational end users were chosen to create the main study dataset. First, a group of 200 unique organizational end users were selected who were new to the organization and had not been exposed to any previous phishing training from the company. Second, a separate group of 200 unique organizational end users were selected to receive an annual, industry-standard phishing training of 30 minutes. Last, a separate group of 200 unique

organizational end users were selected to receive customized, continuous phishing training, consisting of eight short videos of less than five minutes in length.

Once the three main study groups were chosen, they were sent an email (Appendix E) to provide insight into this study and give them an opportunity to either consent (yes) or to dismiss (no) themselves. As with the pilot, this initial recruitment process lasted for one week to provide the organization end user an opportunity to respond. The results for the main study groups showed only a 7-9% opt out rate. For the no training group of 200, 17 users responded no to participating in this study. For the annual training group of 200, 15 users responded no to participating in this study, and for the continuous customized group of 200, 16 users declined.

With the three main study groups set, the following week began the phishing training phase. By design, the no training group received no training as part of this study to ensure an appropriate control group. The annual training group was provided with a link through their business email to complete the 30-minute annual phishing awareness training within four weeks. The continuous customized group received two short videos to their business email each week for four weeks, for a total of eight short video training courses. The completion status for both the annual group and the continuous customized group were tracked to ensure the completion of the courses.

After the 4-week training phase of the data collection process, the phishing campaigns commenced. Each week for two weeks, all three groups were phished twice a week by both phishing campaign methods (Industry-standard and Red Team). The data for all phishing campaigns was collected with the KnowBe4 platform to get a real-time view into the effectiveness of each campaign. The KnowBe4 platform was able to collect

data on all six negative end user responses by providing a count of clicks for each action. Overall, this process produced the main study data needed to further analyze the effectiveness of the phishing training methods, as well as the phishing campaign methods. The main study data upon completion consisted of two sets of 552 responses (No training 183, Annual 185, Continuous 184) for 1,104 discrete responses to analyze. During the main study, in addition to the six negative response actions, there were five demographic indicators collected.

Data Analysis

Using SPSS® Statistics™ version 28, data collected from the main study was loaded and analyzed to answer research questions RQ3, RQ4, and RQ5. To answer RQ3, if any statistically significant mean differences exist between the three types of organizational end user phishing training (No Training, Annual, Continuous Customized) and the six negative end user response actions, an ANOVA was used to test for significant differences between groups. Table 15 shows the output of the one-way ANOVA to determine any mean differences.

Table 15

One-way ANOVA Output for RQ3 (N=1104)

Negative Response Action	Sum of Squares	df	Mean Square	F	Sig.
Not Reported	2.270	2	1.135	1.266	.282
Opened	19.211	2	9.605	4.722	.009**
Reply/Forward	.002	2	.001	.121	.886
Open Attachment	.000	2	.000	N/A	N/A
Enabled Macro	1.516	2	.758	2.697	.068
Entered Data	1.770	2	.885	1.180	.308

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Based on the ANOVA results there is one statistically significant mean difference between the phishing training method and one of the six negative end user response actions. Opened ($F(2,1103) = 4.722, p = .009$) appears to be significant and warrants further analysis and investigation. Using the Tukey HSD output for multiple comparisons (Table 16), there is a statistically significant difference between training Group 2 (Annual) and training Group 3 (Continuous Customized) as it relates to an end user opening a phishing email ($p < 0.5$, see Table 15).

Table 16

Tukey HSD Output for RQ3 (Opened)

Dep Var	(I)Train Grp	(J)Train Grp	Mean Diff (I-J)	Std. Error	Sig.	Lower Bound	Upper Bound
Opened	1	2	-.244	.105	.053	-.49	.00
		3	.061	.105	.832	-.19	.31
	2	1	.244	.105	.053	.00	.49
		3	.305	.105	.011*	.06	.55
	3	1	-.061	.105	.832	-.31	.19
		2	-.305	.105	.011*	-.55	-.06

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

To answer RQ4, if any statistically significant mean differences exist between the two types of phishing campaigns (Industry-standard and Red Team) and the six negative end user response actions, an ANOVA was used to test for significant differences between groups. Table 17 shows the output of the one-way ANOVA to determine any mean differences.

Table 17

One-way ANOVA Output for RQ4 (N=1104)

Negative Response Action	Sum of Squares	df	Mean Square	F	Sig.
Not Reported	208.696	1	208.696	294.620	<.001***
Opened	315.308	1	315.308	178.780	<.001***
Reply/Forward	.058	1	.058	8.103	.005**
Open Attachment	.000	1	.000	N/A	N/A
Enabled Macro	.110	1	.110	.389	.533
Entered Data	21.204	1	21.204	28.970	<.001***

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Based on the output of the ANOVA, there appears to be several statistically significant mean differences between phishing campaign method and the six negative end user response actions. The mean differences for Not Reported ($F(1,1103) = 294.620$, $p < .001$), Opened ($F(1,1103) = 178.780$, $p < .001$), Reply/Forward ($F(1,1103) = 8.103$, $p = .005$), and Entered Data ($F(1,1103) = 28.970$, $p < .001$) are all statistically significant. This result indicates the way the phishing campaign method is delivered (Industry-standard vs. Red Team) has a significant impact on end user negative response actions. Both pilot and main study data results for RQ4 are consistent and statistically significant.

To answer RQ5, if any statistically significant mean differences exist between the phishing training methods (No training, Annual, Continuous Customized) and the phishing campaign methods (Industry-standard and Red Team) on the six negative end user response actions, an ANCOVA was used to test for significant differences between groups using training method and campaign method as covariates. Table 18 shows the output of the ANCOVA to determine any mean differences.

Table 18

ANCOVA Output for RQ5 (N=1104)

Method	Type III Sum of Squares	df	Mean Square	F	Sig.
Training Group	.688	1	.688	.390	.532
Campaign Method	315.308	1	315.308	178.681	<.001***

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Based on the output of the Tests of Between-Subjects Effects ANCOVA, there appears to be a statistically significant mean difference between phishing training group and phishing campaign. The mean differences for Campaign Method ($F(1,1103) = 178.681$, $p = < .001$) shows that overall, the campaign method is most important as it relates to phishing success for the six negative end user response actions measured. To take this a step further, all the data from each phishing campaign was summarized to show click rates by each training method. Table 19 shows that across all three training groups, the Red Team campaign method was the most successful in getting end users to take a negative action.

Table 19

Average Click Rates Across Training Groups

# Users	Oppts	Total Oppts	# Clicks	Click %	Train Grp	Campaign Type
183	4	732	213	29.10	No Train	Industry Std
183	4	732	268	36.61	No Train	Red Team
185	4	740	263	35.54	Annual	Industry Std
185	4	740	419	56.62	Annual	Red Team
184	4	736	225	30.57	Continuous	Industry Std
184	4	736	274	37.23	Continuous	Red Team
				31.74	Avg %	Industry Std
				43.49	Avg %	Red Team

Given the statistically significant findings of the ANCOVA, and the average click rates across training groups, the use of the Red Team method for phishing campaigns appears more effective than Industry-standard. In addition, it seems this holds true no matter the type of training method the end user receives.

To answer RQ6 and RQ7 there were five demographic indicators added to the main study dataset. The demographic indicators the final two RQs were controlled for are: (a) age, (b) gender, (c) job role, (d) location (clinic vs. admin), and (e) years of job experience. Table 20 provides a summary of the 552 individuals that were a part of the main study.

Table 20

Summary of End User Demographics for RQ6 & RQ7 (N=552)

Demographic Item	Results	N	%
Age	21-30	72	13.04%
	31-40	138	25.00%
	41-50	148	26.81%
	51-60	130	23.55%
	61-70	62	11.23%
	71+	2	0.36%
Gender	Female	464	84.06%
	Male	88	15.94%
Job Role	Accounting	29	5.25%
	Arclaims	4	0.72%
	Business Support	5	0.91%
	Call Center	16	2.90%
	Central Billing	43	7.79%
	Claims	10	1.81%
	Dental Assistant	5	0.91%
	Finance	26	4.71%
	Human Resources	18	3.26%
	Hygienist	6	1.09%
	Information Technology	27	4.89%
	Lab Technician	1	0.18%
	Legal	2	0.36%
	Marketing	16	2.90%
Mergers & Acquisitions	8	1.45%	

	Office Mgr	262	47.46%
	Operations Mgt	16	2.90%
	Patient Service Rep	11	1.99%
	Real Estate	4	0.72%
	Recruitment	21	3.80%
	Regional Mgr	21	3.80%
	Treatment Coordinator	1	0.18%
Location	Admin	224	40.57%
	Clinic	328	59.42%
Years of Experience	1-5	307	55.62%
	6-10	106	19.20%
	11-15	46	8.33%
	16-20	30	5.43%
	21-25	24	4.35%
	26-30	16	2.90%
	31+	23	4.17%

To answer RQ6, if any statistically significant mean differences exist between the phishing training methods (No training, Annual, Continuous Customized) and the six negative end user response actions when controlled for the five demographic indicators. An ANCOVA was used to test significant differences between groups using the demographic indicators as covariates. Table 21 shows the output of the ANCOVA to determine any mean differences.

Table 21

ANCOVA Output for RQ6 with Demographic Control (N=1104)

Demographic Variable	Type III Sum of Squares	df	Mean Square	F	Sig.
Age	.049	1	.049	.074	.785
Gender	2.026	1	2.026	3.045	.081
Job Role	1.789	1	1.789	2.689	.101
Location	.007	1	.007	.011	.917
YoE	1.169	1	1.169	1.757	.185

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Given the results of the ANCOVA there appears no statistically significant mean differences for phishing training group on the six negative end user response actions when controlled for demographic indicators.

To answer RQ7, if any statistically significant mean differences exist between the phishing campaign methods (Industry-standard vs Red Team) and the six negative end user response actions when controlled for the five demographic indicators. An ANCOVA was used to test significant differences between groups using the demographic indicators as covariates. Table 22 shows the output of the ANCOVA to determine any mean differences.

Table 22

ANCOVA Output for RQ7 with Demographic Control (N=1104)

Demographic Variable	Type III Sum of Squares	df	Mean Square	F	Sig.
Age	.056	1	.056	.429	.513
Gender	.009	1	.009	.069	.793
Job Role	.116	1	.116	.900	.343
Location	.008	1	.008	.063	.802
YoE	.001	1	.001	.004	.948

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Given the results of the ANCOVA there appears no statistically significant mean differences for phishing campaign method on the six negative end user response actions when controlled for demographic indicators.

Summary

In this chapter, the results of the research study were presented in the sequence in which this study was performed. There were three phases as part of this research study

that were utilized to address the seven research questions. The first section discussed Phase 1 of this research study that included utilizing cybersecurity SMEs via the Delphi process to confirm the approved components and the level of validity of the research study. A consensus was reached on all measurements (six negative end user response actions) and methods, and this study was approved to move forward. The cybersecurity SME survey results were used to answer RQ1 and RQ2.

In Phase 2, the pilot study, a 7-week process for randomly selecting organizational end user training groups was created. This formal process allowed one week for the potential participants to consent to this study. Following this was a 4-week training cycle for each of the three phishing training groups (No training, Annual training, and Continuous Customized training). The last part of the process consisted of a 2-week phishing campaign, in which each participant was phished twice a week by both phishing campaign methods (Industry-standard and Red Team). The result of the 7-week process was a clean and accurate dataset produced by the KnowBe4 platform to analyze. The pilot group data included 172 unique data points and was used in mock testing of two research questions (RQ3 and RQ4) utilizing an ANOVA to gauge statistical significance. The pilot study output for RQ3 found no statistically significant mean differences between the three phishing training methods and their effect on end users negative response actions. However, RQ4 testing found several statistically significant mean differences between the two phishing campaign methods and their effect on end users negative response actions. Having qualified the data collection and analysis procedure and process with the pilot group, it was approved to move forward and replicate for the main study.

In Phase 3, the main study, the same 7-week process was utilized to randomly select a larger set of organizational end users to participate. With the pilot study, three training groups of 30 were defined, however, the main study was significantly larger by utilizing three groups of 200. The result at the end of the data collection process was 1,104 unique data points, which were used to formally answer RQ3, RQ4, and RQ5. For the main study, demographic indicators were also attached to the organizational end user record to provide answers to RQ6 and RQ7. An ANOVA test was utilized to produce findings for RQ3 and RQ4. There was a slight difference in the output for RQ3, assuming due to a much larger dataset and more accuracy of calculations for the main study. In the pilot, there were no statistically significant mean differences recorded for RQ3, however, in the main study there was one statistically significant difference noted. Overall, it is clear from both phases that there is very little significance in the way end users are trained, as no training was essentially equal to annual and continuous customized training. RQ4 output was consistent with the pilot test, in that several (four) statistically significant mean differences exist between the phishing training method and the six negative end user response actions. RQ5 utilized both an ANCOVA and an average click rate chart to provide answers. Utilizing the ANCOVA with both the phishing training method and the phishing campaign method as covariates, it was determined again that there is a statistically significant mean difference for phishing campaign method. In addition, the average click rate chart showed end user click rates overall are higher for the Red Team phishing campaign method. RQ6 and RQ7 were both addressed utilizing an ANCOVA controlling the results by the five demographic indicators. The results of both tests revealed there are no statistically significant mean differences for phishing training

method, or phishing campaign method, when controlled for demographics. Further thoughts on the conclusions of this study, implications for future research and overall summary are provided in Chapter 5.

Chapter 5

Conclusions, Discussions, Implications, Recommendations, and Summary

Conclusions

Phishing continues to be the number one type of social engineering, with over 90% of all data breaches starting as a phish and may be increasing by as much as 400% per year (FBI, 2021). Nearly 50% of senior IT leaders say that phishing is their primary concern because of weaknesses in their processes, policies, and IT security infrastructure. Additionally, the impact of phishing is evident, with 60% of security leaders stating their organization has lost data, 52% experienced credential compromise, and 47% contended with ransomware, all due to a successful phish (Cybertalk, 2022). The cost to the organization from a successful phishing attack is also skyrocketing. IBM (2021) reported phishing to be the second most expensive attack vector, costing impacted organizations on average \$4.65 million per event. Therefore, the main goal of this research study was to assess if there are any significant differences between phishing training methods and phishing campaign methods as it relates to organizational end users. This research study successfully achieved the goal of answering seven research questions with a three-phased approach. First, a cybersecurity SME survey utilizing the Delphi method was used to validate the measure instrument and approve the validity of the experiment. Second, the pilot phase utilized three unique groups of 30 organizational end users to formalize a process for data collection and analysis and used 172 data points for preliminary testing.

Lastly, the main study, using the established process and procedure from the pilot, collected 1,104 data points from three groups of 200 organizational end users to finalize the analysis.

Discussions

The first result of this research study was the validation from cybersecurity SMEs that the measurement system was approved by consensus. In addition, consensus was also gained for the six negative end user response actions that were used as primary measures in the research study. Furthermore, the second result of this research study was agreement overall on the phishing campaign methods as both valid and relevant for the experiment. The third result indicated that overall, there is little statistical significance in the phishing training methods employed, and that in essence phishing training is not a deterrent for a successful attack on organizational end users. The fourth result, which adds significant value to the body of knowledge, indicated that phishing campaign methods provide a statistically significant impact. Furthermore, while this research study indicated statistical significance for campaign methods overall, given further analysis it was noted that the Red Team campaign method was most effective in this experiment. The fifth result, which also adds significant value to the body of knowledge, further indicated there is a statistical difference in phishing campaign methods when compared directly to phishing training methods. The sixth result indicated no statistically significant mean differences in phishing training methods when controlled for age, gender, job role, location, and years of job experience. Similarly, the seventh result indicated no statistically significant mean differences in phishing campaign methods when controlled for age, gender, job role, location, and years of job experience.

Overall, the main research study culminated with a group of 552 organizational end users who were provided one of three types of phishing training, and then subsequently phished in parallel using both an industry-standard campaign as well as a contracted Red Team campaign. In total, there were 1,104 discrete click events captured across the six negative end user response actions. Using the data captured in real-time by an industry recognized platform as the user is clicking provides a significant level of accuracy and provided an increased level of validity of the outcomes.

Implications

The findings of this research study significantly contributed to the body of knowledge and have several implications for providing both researchers and practitioners additional insight into mitigating phishing attacks. The indication that phishing training methods have little effect overall on end user negative response actions should imply that new ways of training should be developed. Business email users need to be trained in some fashion that is unique when compared to the current industry methods. Annual training, and even continuous customized training, are still delivered in video format and are easily dismissed. Despite indications that an end user has successfully completed a module or video really has little meaning today. An implication from this study should be to rethink how organizational end users are trained and find a new dynamic approach that is more efficient and effective. SETA is critical to ensure the user population is aware of the risks, but modernization of the approach and delivery methods is imperative.

The indication that phishing campaign methods are statistically significant should imply that organizations must continue phishing campaigns, but also learn from the results and act. This study indicates that a vended Red Team campaign was most

effective in phishing the end user population. While not every organization is large enough to support an internal Red Team, it is imperative this method is utilized, even on a contract or third-party vendor basis.

The Red Team approach is to utilize a well-trained, dedicated team of ethical hackers that know how to expose vulnerabilities. Not only within an organizations network, but in business email as well. These teams are trained to trick end users in email, and are trained to gain entry into networks, but doing so in a purposeful way can lead to great advances. By utilizing a Red Team, an organization can then document the exposures and enact programs to address their vulnerabilities. Utilization of a Red Team for phishing should not be a one-time event, rather, a continuous process where the organization continuously learns of its exposure and is constantly investing in a better IT security posture. The Red Team success is largely due to the approach taken by the team. As an example, the team does extensive research on the targeted end users to really understand how to approach the phishing campaign. The Red Team will research individual's social media pages, friends, family members, clubs, organizations, and anything they can to derive current intelligence. Ultimately this is the reason for the Red Team approach success, the phishing campaign is personalized, targeted, and uses up-to-date information on the end user.

Recommendations and Future Research

This research study was to compare phishing training and campaign methods and their role in mitigating malicious emails in organizations. While the goals of this research study were met, there are many areas for expansion and additional future research in the phishing training and campaign method domains. The implications above also lead to

recommendations on how to continuously improve this process. As stated, the IT security industry needs to rethink current ways of training end users, and their overall effectiveness. With so many current advances in Machine Learning (ML) and Artificial Intelligence (AI) there stands to be a great opportunity to address this issue. By combining legacy training methods with modern advances in behavioral technology, there must be a better way to deliver and assess the impacts and effectiveness of phishing training. In addition, these learnings can be carried over into all forms of training within an organization (Human Resources, Compliance, etc).

Future research in this area should include more modern training methods instead of the legacy training courses and modules that have been around for decades. In addition to modern training, the use of different phishing campaign platforms or services should be explored to analyze which are most effective at phishing the organizations end users. The best phishing campaigns will lead to increased learning of an organization's deficiencies and allow for remediation. This research study was conducted in a medium-sized, privately held, healthcare company. The composition of the organization is typical for a healthcare company that has offices distributed nationally, however, there is a very high employee turnover rate. In Chapter 4, I note that 55.62% of the organization has been employed by the company for five years or less. There may be future research done on a more mature, more stable employee base to see if there may be some correlation to the higher vulnerability rates. In addition, being a privately held company, there has historically been less investment in IT security processes, tools, procedures, and training. There may be some differences in outcomes based on company size, stability, and IT

security posture. Lastly, as this was a healthcare company, there may be more learnings from other industries or verticals which operate in non-healthcare mediums.

Summary

This dissertation study has addressed the research problem of the growing cyberattacks targeting businesses via email. With every organization's dependency on email, coupled with the fact that over three billion phishing emails are sent every day around the globe (Earthweb, 2022), there is still a need to continue researching phishing mitigation methods. While IT security technology, processes, and tools continue to evolve, organizations continue to struggle with the human element and the reality that most breaches start with a phish. To positively impact this trend, it is imperative that we rethink how organizations end users are trained, and how we can continuously measure vulnerabilities. Attackers have continued to evolve their skills of social engineering by researching targets at a very detailed level. Whatever they cannot get from the target directly, they simply search and scrape through public records, social media accounts, and even friends or family's information hoping to get enough intelligence for a successful phishing attack. This methodology is also employed by Red Team ethical hackers, but instead of malicious intent, the information is used to help mitigate the exposure or vulnerability. It is imperative that organizations understand there is always risk, and that social engineers and other hackers never take a day off. Employing a methodology, like a Red Team, to always test your organization is one of the keys to maintaining a superior IT security posture.

In Phase 1, cybersecurity SMEs were utilized to review and validate the phishing training methods, the phishing campaign methods, and the six end user negative response

action measures. This phase used the Delphi methodology to ensure reliability and validity measurement instrument that was being used for this study. This phase was used to answer the first two research questions as follows:

RQ1: What are the approved components of the experimental procedures for the phishing training and campaign methods according to cybersecurity SMEs?

RQ2: What level of validity of the experimental procedures the phishing training and campaign methods is sufficient according to cybersecurity SMEs?

Phase 2 of this research study was a pilot to create a process and procedure for data collection and analysis of the phishing data from organizational end users, as well as use the pilot data as a preliminary test for RQ3 and RQ4. The next two research questions utilized the statistical model ANOVA as follows:

RQ3: Are there any statistically significant mean differences between the use of *an annual industry-standard phishing training, continuous customized social engineering focused training, and a control group without training*, on end users' negative response to malicious emails?

RQ4: Are there any statistically significant mean differences between the use of *an industry-standard phishing campaign and a Red Team phishing campaign* on end users' negative response to malicious emails?

The preliminary results indicated that there were no statistically significant mean differences between phishing training method on end user negative response actions. However, the results indicated that there were several statistically significant mean differences between phishing campaign method on end user negative response actions.

Phase 3 of this research study was a main study with a significantly larger dataset to analyze. RQ3 and RQ4 utilized the ANOVA, while RQ5, RQ6, and RQ7 utilized the ANCOVA. The main study data was used to answer all of the following RQs:

RQ3: Are there any statistically significant mean differences between the use of *an annual industry-standard phishing training, continuous customized social engineering focused training, and a control group without training*, on end users' negative response to malicious emails?

RQ4: Are there any statistically significant mean differences between the use of *an industry-standard phishing campaign and a Red Team phishing campaign* on end users' negative response to malicious emails?

RQ5: Are there any statistically significant mean differences between *the phishing training methods* (an annual industry-standard phishing awareness training vs. continuous customized social engineering focused training vs. no training - control) and *the phishing campaign methods* (industry-standard phishing campaign vs. Red Team phishing campaign) on end users' negative response to malicious emails?

RQ6: Are there any statistically significant mean differences between the use of *an annual industry-standard phishing training, continuous customized social engineering focused training, and a control group without training*, on end users' negative response to malicious emails, when controlled for participants': (a) age, (b) gender, (c) job role, (d) location (clinic vs. admin), and (e) years of job experience?

RQ7: Are there any statistically significant mean differences between the use of *an industry-standard phishing campaign* and *a Red Team phishing campaign* on end users' negative response to malicious emails, when controlled for participants': (a) age, (b) gender, (c) job role, (d) location (clinic vs. admin), and (e) years of job experience?

The results supported what had been discovered with the pilot data set during preliminary testing. There were no statistically significant mean differences as it relates to phishing training methods, however, there were several statistically significant mean differences for phishing campaign methods. When further investigating the main study data down to the click level, it was discovered of the phishing campaign methods, the Red Team campaign had a higher average click rate and was more likely to successfully phish the end user.

In conclusion, this research makes several contributions to the body of knowledge, including that the effectiveness of phishing training methods lacks significant effects for the end user. In this study, in essence any training is of equal value to no training. In addition, there are significant effects on end user negative response actions as it relates to phishing campaign methods. Continued exploration of various types of phishing campaigns could continue to add to the body of knowledge. In this study, however, the best campaign was delivered through a contracted Red Team and was shown to be more effective than the industry-standard campaign method. As phishing continues to increase in its imperative organizations invest in the best methods to guard against these attacks. The conclusions from this research and insights gained are transferrable to all business sectors within any size organization.

Appendix A

Institutional Review Board Exemption Letter



MEMORANDUM

To: Jackie Scott
College of Engineering and Computing

From: Ling Wang, Ph.D.
College Representative, College of Engineering and Computing

Date: January 10, 2023

Subject: IRB Exempt Initial Approval Memo

TITLE: Comparing Phishing Training and Campaign Methods for Mitigating Malicious Emails in Corporations– NSU IRB Protocol Number 2022-552

Dear Principal Investigator,

Your submission has been reviewed and Exempted by your IRB College Representative or their Alternate on **January 10, 2023**. You may proceed with your study.

Please Note: Exempt studies do not require approval stamped documents. If your study site requires stamped copies of consent forms, recruiting materials, etc., contact the IRB Office.

Level of Review: Exempt

Type of Approval: Initial Approval

Exempt Review Category: Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies

Post-Approval Monitoring: The IRB Office conducts post-approval review and monitoring of all studies involving human participants under the purview of the NSU IRB. The Post-Approval Monitor may randomly select any active study for a Not-for-Cause Evaluation.

Annual Status of Research Update: You are required to notify the IRB Office annually if your

Appendix B

Expert Recruitment Email

Dear Information Security Subject Matter Expert (SME),

I am conducting a research study that focuses on comparing phishing mitigation methods, specifically two phishing training methods and two phishing campaign methods, for my dissertation work. I am a PhD candidate in Cybersecurity Management at the College of Computing and Engineering of Nova Southeastern University. My dissertation is chaired by Dr. Yair Levy and this work is part of the Levy CyLab. (<http://CyLab.nova.edu/>). My research study is seeking to compare multiple phishing mitigation methods and their impact on malicious email in organizations. The experiment that I am seeking assistance with is aimed at comparing these phishing mitigation methods in a 2x3 quasi-experimental format measured on six specific end user negative response actions and vulnerability types. A secondary outcome of this experiment is to measure the samples based on several demographic factors.

By participating in this research study, you agree and understand that your responses are voluntary. All responses are anonymous and no personally identifiable information will be collected or traced back to anyone. Of course, you may stop your participation at any time. If you agree to participate, please reply to this email with your approval. As a token of appreciation for your IT security expert contribution to this research study you will receive a \$10 Amazon digital gift card to your email address upon completing the survey required to initiate this research study.

Thank you in advance for your consideration. I appreciate your assistance and contribution to this research study. If you wish to receive the findings of this study, feel free to contact me via email and I will be more than happy to provide you with the information about the academic research publication resulting from this study.

Best Regards,

Jackie (Chris) Scott, PhD Candidate in Cybersecurity Management

Nova Southeastern University

Email: js5065@mynsu.nova.edu

Appendix C

Cybersecurity SME Survey

Cybersecurity SME Survey

Dear Information Security Subject Matter Expert (SME),

I am conducting a research study that focuses on comparing phishing mitigation methods, specifically two phishing training methods and two phishing campaign methods, for my dissertation work. I am a PhD candidate in Cybersecurity Management at the College of Computing and Engineering of Nova Southeastern University. My dissertation is chaired by Dr. Yair Levy and this work is part of the Levy CyLab. (<http://CyLab.nova.edu/>). My research study is seeking to compare multiple phishing mitigation methods and their impact on malicious email in organizations. The experiment that I am seeking assistance with is aimed at comparing these phishing mitigation methods in a 2x3 quasi-experimental format measured on six specific end user negative response actions and vulnerability types. A secondary outcome of this experiment is to measure the samples based on several demographic factors.

By participating in this research study, you agree and understand that your responses are voluntary. All responses are anonymous and no personally identifiable information will be collected or traced back to anyone. Of course, you may stop your participation at any time. If you agree to participate, please reply to this email with your approval. As a token of appreciation for your IT security expert contribution to this research study you will receive a \$10 Amazon digital gift card to your email address upon completing the survey required to initiate this research study.

Thank you in advance for your consideration. I appreciate your assistance and contribution to this research study. If you wish to receive the findings of the study, feel free to contact me via email and I will be more than happy to provide you with the information about the academic research publication resulting from this study.


Best Regards,

Jackie (Chris) Scott, PhD Candidate in Cybersecurity Management

Nova Southeastern University

Email: js5065@mynsu.nova.edu

⋮

1. Which of the following best describes your current job level?  Multiple choice ▾

Owner/Executive/C-level ✕

Senior Management ✕



Middle Management ✕

Analyst ✕

Consultant ✕

Instructor/Professor ✕

Add option or [add "Other"](#)

  | Required ⋮

2. How many years of experience do you have in information security? *

Less than 1 year

1-3 years

4-5 years

6-10 years

5. What is your age group? *

- 18-20
- 21-30
- 31-40
- 41-50
- 51-60
- 61-67
- Above 67

6. What Gender do you identify as? *

- Male
- Female
- Prefer not to say
- Other...

7. How many Cybersecurity certifications do you have? *

- None
- One
- Two
- Three
- Four or more

8. What Cybersecurity certifications do you currently hold? (If more than one, use a comma to separate them) *

Short answer text

9. What is your Education Level? *

- High School
- Associates Degree
- Bachelors Degree
- Masters Degree
- Doctoral Degree

14. Please rate your level of agreement that the following two (2) phishing campaign methods (A & B) are relevant for this phishing experiment. *

A. Industry-standard phishing campaign

	1	2	3	4	5	6	7	
Strongly Disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly Agree

B. Red Team phishing campaign *

	1	2	3	4	5	6	7	
Strongly Disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly Agree

15. Are there any other phishing training or campaign methods that you feel should be included in this phishing mitigation experiment?

Short answer text

Appendix D

Organizational End User Instrument

Campaign: Beginner Phishing

Every two weeks from category: Production

Overview Users

130 Recipients	93.1% 121 Delivered	24.8% 30 Opened	22.3% 27 Clicked	2.5% 3 Replied	6.6% 8 Attachment Opened	0% 0 Macro Enabled	0% 0 Data Entered	15.7% 19 Reported	6.9% 9 Bounced
--------------------------	----------------------------------	------------------------------	-------------------------------	-----------------------------	--	------------------------------------	-----------------------------------	--------------------------------	-----------------------------

[Bulk Update](#) [Download CSV](#)

⚙ This Phishing Security Test	
Status	Closed
Phish-prone %	31.4%
Recipients	130
Failures	38

Appendix E

Example of Participant Invitation Email

Associates of Dental Care Alliance (DCA) have the unique opportunity to participate in a cybersecurity study focused on social engineering, more specifically various phishing mitigation methods. The learnings from this research will help organizations better understand how phishing may be mitigated, and how best to train the organization's end users.

This study is being performed by a Ph.D. candidate in Cybersecurity Management at the College of Engineering and Computing of Nova Southeastern University. This dissertation is chaired by Dr. Yair Levy, and this work is part of the Levy CyLab Projects (<http://CyLab.nova.edu/>). **Participation consent from you is needed for the dissertation study to be academically compliant.**

This study will not require any work from you, rather just your action to click on the voting buttons above. "Yes", means you consent to participate in this study, and "No" means you would prefer not to participate. By participating in this research study, you agree and understand that your responses are voluntary. All responses are anonymous and no Personally Identifiable Information (PII) will be collected as part of this study. You may choose at any time to rescind your participation in this study.

Please select "Yes" or "No" in the header of this email and thank you in advance for your participation.

Best Regards

References

- Alabdan, R. (2020). Phishing attack survey: Types, vectors, and technical approaches. *Future Internet*, 12(168). <https://doi.org/10.3390/fi12100168>
- Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26(4), 276-289.
- Ali, A., & Yousef, M. (2020). Novel three-tier intrusion detection and prevention system in software defined network. *IEEE Access*, 8, 109662-109676. <https://doi.org/10.1109/ACCESS.2020.3002333>
- Alnatheer, M. A. (2015). Information security culture critical success factors. In *Proceedings of the 12th International Conference on Information Technology* (pp. 731-735).
- Aviv, S. S. (2019). *An examination of user detection of business email compromise amongst corporate professionals*. (Publication No. 27667282) [Doctoral dissertation, Nova Southeastern University]. ProQuest Dissertations and Theses Global.
- Bada, M., & Nurse, J. (2019). Developing cybersecurity education and awareness programmes for small-and-medium-sized enterprises (SMEs). *Information & Computer Security*, 27(3), 393-410. <https://doi.org/10.1108/ICS-07-2018-0080>
- Brown, S. D., Levy, Y., Ramim, M., & Parrish, J. L. (2015). Pharmaceutical companies documented and online privacy practices: Development of an index measure and initial test. *Online Journal of Applied Knowledge Management*, 3(2), 68-88.
- Bul'ajoul, W., James, A., & Shaikh, S. (2019). A new architecture for network intrusion detection and prevention. *IEEE Access*, 7, 18558-18573. <https://doi.org/10.1109/ACCESS.2019.2895898>
- Bullee, J., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organizations explained. *Information & Computer Security*, 25(5), 593-661.
- Carlton, M., & Levy, Y. (2015). Expert assessment of top platform independent cybersecurity skills for non-IT professionals. *Proceedings of the Institute of Electrical and Electronic Engineers Southeast Conference* (pp. 1-6). <https://doi.org/10.1109/SECON.2015.7132932>
- Chou, F., Chen, A., & Lo, V. (2021). Mindless response or mindful interpretation: Examining the effect of message influence on phishing susceptibility. *Journal of Sustainability*, 13(1651). <https://doi.org/10.3390/su13041651>
- Cialdini, R. B. (2009). *Influence: The psychology of persuasion*. Google Books. <https://books.google.com/books?id=5dfv0HJ1TEoC>
- Cornish, D. B., & Clarke, R. V. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology*, 25(4), 933-948. <https://doi.org/10.1111/j.1745-9125.1987.tb00826.x>

- Costantino, G., La Marra, A., Martinelli, F., & Matteucci, I. (2018). CANDY: A social engineering attack to leak information from infotainment system. *In Proceedings of the IEEE Vehicular Technology Conference, Porto, Portugal* (pp. 1–5).
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications, Inc.
- Cross, C., & Gillett, R. (2020). Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. *Journal of Financial Crime*, 27(3), 871-884. <https://doi.org/10.1108/JFC-02-2020-0026>
- Crowdstrike (2022). *2022 crowdstrike global threat report*.
<https://www.crowdstrike.com/resources/reports/global-threat-report/>
- Cybertalk (2022). *Top 15 phishing attack statistics (and they might scare you)*.
<https://www.cybertalk.org/2022/03/30/top-15-phishing-attack-statistics-and-they-might-scare-you/>
- D’Qrill, N., & Hendricks, V. F. (2018). Phorced to phish: Benefits of a phishing equilibrium. *Review of Behavioral Finance; Leeds*, 10(2), 183- 191.
<https://doi.org/10.1108/RBF-07-2016-0045>
- Earthweb (2022). *How many phishing emails are sent daily in 2022?*
<https://earthweb.com/how-many-phishing-emails-are-sent-daily/>
- Ernst and Young (2015), Creating trust in the digital world: EY’s global information security survey. [http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/\\$FILE/ey-global-information-security-survey-2015.pdf](http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf)
- Federal Bureau of Investigations (2017, February 27). *Business e-mail compromise: Cyber-enabled financial fraud on the rise globally*.
<https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise>
- Federal Bureau of Investigations Internet Crime Complaint Center (2019, September 10). *Business email compromise the \$26 billion scam*.
<https://www.ic3.gov/media/2019/190910.aspx>
- Federal Bureau of Investigations Internet Crime Complaint Center (2020, March 17). *2020 Internet crime report*.
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
- Federal Bureau of Investigations Internet Crime Complaint Center (2021, March 23). *2021 Internet crime report*.
https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

- Federal Bureau of Investigations Internet Crime Complaint Center (2022, May 4). *Business email compromise: the \$43 billion scam*. <https://www.ic3.gov/Media/Y2022/PSA220504>
- Feng, B., Li, Q., Ji, Y., Guo, D., & Meng, X. (2019). Stopping the cyberattack in the early stage: Assessing the security risks of social network users. *Security and Communication Networks*, 2019. <https://doi.org/10.1155/2019/3053418>
- Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture awareness. *Journal of Computers and Security*, 59, 26-44. <https://doi.org/10.1016/j.cose.2016.01.004>
- Fortino, G., Guerrieri, A., Pace, P., Savaglio, C., & Spezzano, G. (2022). IoT platforms and security: An analysis of the leading industrial/commercial solutions. *Sensors*, 22(2196). <https://doi.org/10.3390/s22062196>
- Furnell, S., Millet, K., & Papadaki, M. (2019). Fifteen years of phishing: Can technology save us? *Journal of Computer Fraud and Security*, 7, 11-16. [https://doi.org/10.1016/S1361-3723\(19\)30074-0](https://doi.org/10.1016/S1361-3723(19)30074-0)
- Gandhi, F., Pansaniya, D., & Naik, S. (2022). Ethical hacking: Types of hackers, cyber attacks and security. *International Research Journal of Innovations in Engineering and Technology*, 6(1), 28-32. <https://doi.org/10.47001/IRJIET/2022.601007>
- Ghafir, I., Hammoudeh, M., & Prenosil, V. (2017). Disguised executable files in spear-phishing emails: Detecting the point of entry in advanced persistent threat. *PeerJ Preprints*, 5(e2998v1). <https://doi.org/10.7287/peerj.preprints.2998v1>
- Greitzer, F. L., Strozer, S. C., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of unintentional insider threats deriving from social engineering exploits. *Institute of Electrical and Electronic Engineers Conference on Security and Privacy*. <https://doi.org/10.1109/SPW.2014.39>
- Hamid, H., & Dali, N. (2019). Empirical study on the influence of security control management and social factors in deterring information security misbehavior. *2nd International Conference on Recent Advancements in Science and Technology*.
- Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails. *Online Information Review; Bradford*, 40(2), 265-281. <https://doi.org/10.1108/OIR-04-2015-0106>
- Ho, A. (2018). Rules of three lines of defense for information security and governance. *ISACA Journal*, 18(4), 1-5.
- Humayan, M., Niazi, M., Almufareh, M., Jhanjhi, N., Mahmood, S., & Alshayeb, M. (2021). Software-as-a-service security challenges and best practices: A multivocal literature review. *Journal of Applied Sciences*, 12(3953). <https://doi.org/10.3390/app12083953>

- IBM (2021). *Cost of a data breach report 2021*.
https://www.ibm.com/partnerworld/content/05477C943AB64485?mhsrc=ibmsearch_a&mhq=cost%20of%20data%20breach%202021
- ISACA, RSA (2015). *State of cybersecurity: Implications for 2015*. An ISACA and RSA Conference Survey. https://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdg
- Jain, A. K., & Gupta, B. B. (2017). Towards detection of phishing websites on client-side using machine learning based approach. *Telecommunication Systems; New York*, 68(4), 687-700. <https://doi.org/10.1007/s11235-017-0414-0>
- Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, 2(20), 1-23. <https://doi.org/10.1186/s42400-019-0038-7>
- Kirova, D., & Baumol, U. (2018). Factors that affect the success of security education, training, and awareness programs: A literature review. *Journal of Information Technology Theory and Application*, 19(4), 56-83.
- Kolouch, J. (2018). Evolution of phishing and business email compromise campaigns in the Czech Republic. *Academic and Applied Research in Military and Public Management Services*, 17(3), 83-100.
- Kost, R. G., & da Rosa, J. C. (2018). Impact of survey length and compensation on validity, reliability, and sample characteristics for ultrashort-, short-, and long-research participant perception surveys. *Journal of Clinical and Translational Science*, 2(1), 31-37. <https://doi.org/10.1017/cts.2018.18>
- Kotson, M., & Shultz, A. (2015). Characterizing phishing threats with natural language processing. *Institute of Electrical and Electronic Engineers Conference on Communications and Network Security*, 308-316. <https://doi.org/10.1109/CNS.2015.7346841>
- Krishna, C. V., Swamy, C. N., Mary, A. V., & Selvin, M. P. (2020). Identification of phishing URLs using machine learning. *Journal of Physics: Conference Series, International Conference on Mathematical Sciences*. <https://doi.org/10.1088/1742-6596/1770/012009>
- Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, 3(1), 1-10. <https://doi.org/10.1186/s40163-014-0009-y>
- Laszka, A., Lou, J., & Vorobeychik, Y. (2016). Multi-defender strategy filtering against spear-phishing attacks. *Association for the Advancement of Artificial Intelligence Conference on Artificial Intelligence*, 1-8.
- Levy, Y., & Ellis, T. J. (2011). A guide for novice researchers on experimental and quasi-experimental studies in Information Systems research. *Interdisciplinary Journal of Information, Knowledge and Management*, 6, 1-11.

- Mihaela, C. L. (2020). Current security threats in the national and international context. *Accounting and Management Information Systems*, 19(1), 351-378. <https://doi.org/10.24818/jamis.2020.02007>
- Miranda, M. J. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review*, 14(2), 5-10, 56.
- Mirian, A. (2019). Hack for hire. *Association for Computing Machinery, Communications of the ACM*, 62(12), 32-35.
- Nifakos, S., Chandramouli, K., Nikolaou, C., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cybersecurity within healthcare organizations: A systematic review. *Sensors*, 21(15), 5119. <https://doi.org/10.3390/s21155119>
- Nisha, T. N., Bakari, D., & Shukla, C. (2021). Business email compromise – Techniques and countermeasures. *2021 International Conference on Advanced Computing and Innovative Technologies in Engineering*. <https://doi.org/10.1109/ICACITE51222.2021.9404587>
- Osuagwu, E. U., & Chukwudebe, G. A. (2015). Mitigating social engineering for improved cybersecurity. *Institute of Electrical and Electronic Engineers International Conference on Cyberspace Governance*.
- Pradeep, I., & Sakthivel, G. (2020). Ethical hacking and penetration testing for securing us from hackers. *International Conference on Robotics and Artificial Intelligence*. <https://doi.org/10.1088/1742-6596/1831/1/012004>
- Priestman, W., Anstis, T., Sebire, I., Sridharan, S., & Sebire, N. (2019). Phishing in healthcare organizations: Threats, mitigation, and approaches. *BMJ Healthcare Inform*, 26(e100031). <https://doi.org/10.1136/bmjhci-2019-100031>
- Proofpoint (2021). *Email security & protection*. <https://www.proofpoint.com/us/products/email-security-and-protection>
- Ramim, M. M., & Lichvar, B. T. (2014). Elicit expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management*, 2(1), 122-136.
- Ribero, J., Saghezchi, F., Mantas, G., Rodriguez, J., & Abd-Alhameed, R. (2020). HIDROID: Prototyping a behavioral host-based intrusion detection and prevention system for android. *IEEE Access*, 8, 23154-23168. <https://doi.org/10.1109/ACCESS.2020.2969626>
- Ricci, J., Breitinger, F., & Baggili, I. (2019). Survey results on adults and cybersecurity education. *Journal of Education and Information Technology*, 2019(24), 231-249. <https://doi.org/10.1007/s10639-018-9765-8>
- Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A study. *Future Internet*, 11(89). <https://doi.org/10.3390/fi11040089>

- Samson, R. (2020). *ClearNetwork.com*. The Top 10 Intrusion Detection and Prevention Systems. <https://www.clearnetwork.com/top-intrusion-detection-and-prevention-systems/>
- Schweigert, C. T., & Johnson, R. A. (2021). Testing the susceptibility of employees to phishing emails. *International Journal of Information, Business and Management*, 13(3), 190-203.
- Scott, B.F. (2021). Red teaming financial crime risks in the banking sector. *Journal of Financial Crime*, 28(1), 98-111. <https://doi.org/10.1108/JFC-06-2020-0118>
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th Ed.). John Wiley & Sons Ltd.
- Selvakumari, M., Sowjanya, M., Das, S., & Padmavathi, S. (2021). Phishing website detection using machine learning and deep learning techniques. *2021 International Conference on Computing, Communication, Electrical and Biomedical Systems*.
- Simpson, G., & Moore, T. (2020). Empirical analysis of losses from business email compromise. *2020 APWG Symposium on Electronic Crime Research*.
- Stembert, N., Padmos, A., Bargh, M. S., Choenni, S., & Jansen, F. (2015). A study preventing email (spear) phishing by enabling human intelligence. *Institute of Electrical and Electronic Engineers International Conference on Intelligence and Security Informatics*. <https://doi.org/10.1109/EISIC.2015.38>
- Swiss Cyber Institute (2022). *Cybersecurity facts: Phishing statistics*. <https://swisscyberinstitute.com/blog/cybersecurity-facts-phishing-statistics/>
- Techopedia (2017). *What does commercial-off-the-shelf (COTS) mean?* <https://www.techopedia.com/definition/1444/commercial-off-the-shelf-cots>
- TechTarget Contributor (2021). *What is red-teaming?* TechTarget. <https://whatis.techtarget.com/definitions/red-teaming>
- Thakur, K., Qui, M., Gai, K., & Ali, M. L. (2015). An investigation on cyber security threats and security models. *Institute of Electrical and Electronic Engineers International Conference on Cyber Security and Cloud Computing*.
- Trendmicro (2022). *Definition of spear-phishing*. <https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing>
- Tversky, A., & Kahneman, D. (1972). A subjective probability: A judgement of representativeness. *Cognitive Psychology*, 5(3), 430-454.
- Verizon (2020). *Data breach investigations report*. <https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>

- Volkamer, M., Renaud, K., & Gerber, P. (2016). Spot the phish by checking the pruned URL. *Information and Computer Security; Bingley*, 24(4), 372-385.
<https://doi.org/10.1108/ICS-07-2015-0032>
- Walker, A. M., & Selfe, J. (1996). The Delphi method: A useful tool for the allied health researcher. *British Journal of Therapy and Rehabilitation*, 3(12), 677-681.
<https://doi.org/10.12968/bjtr.1996.3.12.14731>
- Wilkerson, S., Levy, Y., Kiper, J. R., & Snyder, M. (2017). Toward a development of a social engineering exposure index (SEXI) using publicly available personal information. *Kennesaw State University Conference on Cybersecurity Education, Research and Practice*, 1- 9.
- Yoo, J., Park, E., Lee, G., Ahn, M., Kim, D., Seo, S., & Kim, H. (2020). Cyber attack and defense emulation agents. *Journal of Applied Sciences*, 10(2140).
<https://doi.org/10.3390/app10062140>
- Zenko, M. (2015). *Red team: How to succeed by thinking like the enemy*. Basic Books, A Member of the Perseus Book Group.
- Zweighaft, D. (2017). Business email compromise and executive impersonations: Are financial institutions exposed? *Journal of Investment Compliance*, 18(1), 1-7. <https://doi.org/10.1108/JOIC-02-2017-0001>