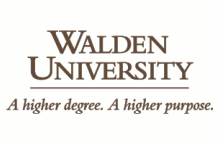





2020

# Information Security Ambassadors' Perceptions of Peer-Led Motivation in Phishing Detection

Kingkane Malmquist
*Walden University*

# Walden University

College of Health Sciences

This is to certify that the doctoral dissertation by

Kingkane Malmquist

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Kourtney Nieves, Committee Chairperson, Health Services Faculty
Dr. Richard Jimenez, Committee Member, Health Services Faculty
Dr. Melissa Green, University Reviewer, Health Services Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2020

Abstract

Information Security Ambassadors' Perceptions of Peer-Led Motivation in Phishing Detection

by

Kingkane Malmquist

MS, Capella University, 2010

BA, Ashford University, 2007

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Healthcare Administration

Walden University

May 2020

## Abstract

Phishing rates are increasing yearly and continue to compromise data integrity. The need to guard business information is vital for organizations to meet their business objectives and legal obligations. The purpose of this phenomenological study was to explore security ambassadors' perceptions of motivating their peers to adopt safe internet behaviors in a large medical campus in Minnesota. Hackman and Oldham's job characteristic motivation theory was used to frame the study. Data were collected from semistructured interviews with 20 security ambassadors. Data coding and analysis yielded 7 themes: rewarding, value, personal interest, limited information security knowledge, increased interest, communication, and topics lacked variety. Participants stated that they perceived the ambassador program to be of value to the organization and employees, to be rewarding to the ambassador, and to generate increased interest in information security topics among their peers. Results may be used to develop intervention techniques and applications to prevent malicious phishing attempts in health care and other industries, resulting in safer patient/client environments.

# Information Security Ambassadors' Perceptions of Peer-Led Motivation in Phishing Detection

by

Kingkane Malmquist

MS, Capella University, 2010

BA, Ashford University, 2007

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Healthcare Administration

Walden University

May 2020

# Dedication

For my three loves.

My children, Olivia and Owen: You have been on this long and arduous journey with me for your entire lives. Your resilience and curiosity of the world will take you far. I hope I have inspired you as much as you have been an inspiration to me to do more, be more, and to give more.

Tim: Your presence, love, and support have changed my life. I could not have asked for a greater man.

# Acknowledgments

Thank you, Dr. Nieves, for your guidance as my chair and your never-ending words of encouragement throughout the exhaustive research writing process. Your feedback has shaped me to be a more polished scholarly writer.

Thank you, Dr. Jimenez, for your guidance as my committee member. Your wisdom and expertise in qualitative research encouraged me to ask more questions and to dig much deeper. Your feedback has been instrumental in my research.

Dr. Nieves and Dr. Jimenez, my sincerest gratitude for helping me meet each milestone along this journey and celebrating with me as I reached them. You both have transformed me into something greater than what I thought was ever possible for myself.

Table of Contents

List of Tables

List of Figures

# Chapter 1: Introduction to the Study

This study addressed security ambassadors' experiences and perceptions related to phishing detection within a 60,000 employee medical organization. Phishing has been a common issue to which many have fallen victim since its first documented presence in 1996 (phishing.org, n.d.). There is continued general belief that the use of technology allows people to feel protected; however, the reality is that it only solves some of the problem (Ashraf, 2005). In the Background section, I summarize research literature related to the scope of the study, the gap in knowledge, and the need for the study. The Problem Statement section provides evidence of consensus, relevance, and significance to the discipline along with findings from research conducted within the last 5 years. This chapter also includes the purpose of the study, the research questions, and the theoretical foundation. Lastly, the nature of the study, definitions, assumptions, scope and delimitations, limitations, and significance are addressed.

The security ambassador program was designed to help users avoid becoming a cyber-attack statistic through motivation by their peers. The social change impact of this study was to understand whether peer-led motivation reduces phishing susceptibility according to Hackman and Oldham's (1976) job characteristic motivation theoretical framework. The focus of this research was to identify the motivational impact of the Security ambassador program through ambassadors' perceptions. In the security ambassador program, the simulation tool is software that allows a spoofed email to be sent to intended targets. The email is an educational tool to aid in identifying characteristics of a potential phish. Once received, the tool tracks the four possible

options a recipient is able to take: record whether the email was opened (neutral), the simulated threat in the email was either clicked or downloaded (failure to detect), the phishing reporter button was activated to report the threat (successful detection), or no action was taken at all (delete email, neutral). Of the four options, the most detrimental action is to click or download on the link or file found within the email. If this happens in the simulation, the email recipient is redirected to an educational page that highlights specific areas to verify before taking action. The intent of the tool is to teach through practice. For those who report the suspicious email by activating the reporter button, a pop-up on the screen reinforces the behavior by congratulating them for being able to recognize traits of a possible phish.

Phishing continues to be on the rise. According to the Anti-Phishing Working Group (2017), an international coalition providing a global response to cybercrime, phishing increased by 10% worldwide from 2015 to 2016. In the current study, I sought to identify whether peer-led motivation was perceived as beneficial when used with a phishing simulator tool. This research addressed ways to promote positive social change in a world where phishing attacks target people and businesses.

## Background

Selected literature reviewed in support of the study indicated two themes: the cyber-security threat landscape and the possible human motivators used to act on them. The themes provided information regarding how intrinsic learning is achieved and how motivation may or may not impact user behaviors when exposed to the electronic environment. Current research has not provided a clear, direct link between accuracy in

phishing detection and peer influence at the organizational level as neither have been used together to promote cyber security awareness. Additionally, findings from security ambassadors may provide first-hand perspectives on what they thought contributed to the success or failure in the motivating process. This research may be used to identify to what degree peer influence promotes learning, resulting in user adaptation to safeguard users from malicious phishing in the business and private environment. Researchers have documented that learning occurs through the support of peers; however, findings were limited to adolescents and did not assess elements of current security threats (Gardner & Steinberg, 2005).

The literature review supported the need for the current study. All studies reviewed had been published within the past 10 years and were found in the Google Scholar database. Search terms used were *social networking*, *peer influence*, *user perception*, *social learning theory*, *behavioral intentions*, *behavior modeling*, *phishing detection*, *learning motivators*, *organizational behavior*, and *cyber security threat landscape*. The study focused on a persistent problem that has been spreading beyond the private domain into the business domain. The threat is no longer limited to email. Phishing has been used in social media where the need to be connected with others has intensified (Anti Phishing Working Group, 2017).

## Problem Statement

Business data are valuable to organizations. The need to guard this data is vital for organizations to be able to meet their business objectives and their legal obligations. As businesses rely on electronic information, data compromise becomes more common (Anti

Phishing Working Group, 2017). Companies depend on technology to protect their most valuable assets yet fail to consider the human contribution and its role in securing organizational assets (Ashraf, 2005). In 2012, the top three vulnerabilities facing organizations included third party access, increased use of mobile devices, and lack of sufficient human awareness, all of which encompassed a human component (Deloitte, 2013).

The purpose of an information security awareness program is to protect business data through user education and awareness to properly handle information security threats and to minimize their impact on the individual and the organization. Researchers have not offered a comprehensive understanding of what is required to develop a security awareness program that includes user training and marketing tools to enhance user awareness (Ashraf, 2005). Varsheny, Misra, and Atrey (2016) reported that although training schemes attempt to educate the end user, the drawback is the dependency on users to understand technical competencies such as Secure Sockets Layer, certificates, and URLs of websites. Varsheny et al. noted that although training is not a definitive solution against phishing, these schemes have been found to be more successful and cost-effective than their counterparts due to hardware and password management requirements.

The focus of phishing prevention has been on the impact of data loss and addressing the importance of establishing user awareness. One option to countermeasure a phishing attack is described as a "multi-layered anti-phishing proposal" (Issac, Chiong, & Jacob, 2014); however, the solution is strictly tool based. In this countermeasure, seven

steps are required: white list and black list email addresses, securing of simple mail transfer protocol servers, implementing grey listing, webpage layout comparison, text extraction from image, matching domain name system names, and implementing filters (Issac et al., 2014). Although these steps may be helpful in detecting potential phishing attacks, the approach is not a failsafe solution because phishing is not limited to email. Phishing occurs in other platforms such as social media. In the current study, I explored whether peer-led motivation promotes behavior adaptation in phishing detection when used in conjunction with a phishing simulation tool. Findings from this study may be used in designing a multifaceted security awareness approach to foster organizational behavioral change.

The use of bring-your-own-device to the workplace is increasing, and the lines between private and public are becoming less clear. Reports showed that there were 164 million smartphone users in the United States in 2014, and over 66 million were iPhone users (Statista, 2016). Software update issues are not uncommon as the threat advances and become more complex. The human element will determine the impact of that threat through actions taken or avoided (Federal Trade Commission, n.d.).

Researchers have not been able to link current cybersecurity threats to the factors that motivate a person to act on a possible attack. Alsharnouby, Alaca, and Chiasson (2015) reported that users view security as a secondary task that is often overlooked due to the user's intended purpose during their online interaction, such as completing a purchase. More compelling is human curiosity as the top driver for phishing susceptibility (Cofense, 2018). One researcher crafted and sent 1,200 email and Facebook

messages to recipients at a college campus with links to a fictitious party along with photos from the party to open and view (Benenson, Gassman, & Landwirth, 2017). The nonexistent sender was able to obtain a high click rate due to a variety of factors. When asked about why the recipient clicked on the link sent to them in the email, curiosity was the highest contributor at 34%. Trailing curiosity was the nature of the email, which appeared to fit the recipient's expectations of being recipients to such emails (Benenson, et al., 2017). The remaining 16% thought they might have known the sender in some way but could not fully confirm the accuracy of their claim (Benenson et al., 2017). The findings suggested that the success of a phishing attack is driven by exploiting these human drivers that tools cannot detect.

The current study was conducted to explore the lived experiences of information security ambassadors regarding motivating their peers to accurately detect phishing. Prior studies provided two areas that promote learning: peer influence and intrinsic drivers (Arachchilage & Love 2014). These studies provided documentation on peer influence and its ability to promote learning, but most of the studies focused on adolescents and not on how peer-influenced learning translates to cybersecurity. The current study provided the foundation for future studies to address learning gaps in conjunction with two identifiable security challenges organizations face: the blending of user education and the use of software to aid in the mitigation of these risks.

## Purpose of the Study

The purpose of this qualitative study was to understand the lived experiences of security ambassadors as they try to motivate their peers to increase phishing detection. I

examined security ambassadors' experiences in their quest to promote safer security practices among their peer groups. The phenomenological approach helped me identify how peer influence was able to increase motivation among work teams to create behavior change. The idea that security ambassadors serve as an important tool in security awareness is based on the influence of peer-motived behaviors, and ambassadors' familiarity with their peers' behaviors in their work environment.

## Research Questions

The primary research question for the study was the following: What are the lived experiences of information security ambassadors on phishing detection among their workgroups when trying to implement behavioral change? Secondary or prompt questions were the following:

RQ1: Do security ambassadors perceive that their department peers have a desire to learn?

RQ2: How many ambassadors choose to share the requested communication to their teams?

RQ3: Why do security ambassadors choose not to communicate certain cybersecurity tips to their peers?

RQ4: What are the different types of communication methods shared by ambassadors to their teams?

RQ5: What do ambassadors perceive as the most successful communication mode?

RQ6: What mode of communication is perceived by ambassadors as the least successful?

RQ7: How much business value is perceived by ambassadors based on the work with which they are tasked?

## Theoretical Framework

The theoretical framework for this study was Hackman and Oldham's (1976) job characteristic motivation (JCM) theory. According to the JCM, people are generally motivated by three specific psychological states when performing a task: meaningfulness of the work they are performing, responsibilities, and the knowledge of outcomes (Hackman & Oldham, 1976). The theory is categorized into five distinct characteristics: skill variety, task identity, task significance, autonomy, and job feedback (Hackman & Oldham, 1976). Skill variety is the degree to which a job requires a variety of different activities in carrying out the work, involving the use of a number of different skills and talents of a person (Faturochman, 1997). Task identity is the degree to which a job requires completion of a whole identifiable piece of work, or doing a job from beginning to end with visible outcome (Faturochman, 1997). Task significance is the degree to which the job has a substantial impact on the lives of other people, whether those people are in the immediate organization or in the world at large (Faturochman, 1997). Autonomy is the degree to which the job provides substantial freedom, thought independence, and discretion to the individual in scheduling the work and in determining the procedure to be used in carrying it out (Faturochman, 1997). Job feedback is the degree to which carrying out the work activities required by the job provides the

individual with direct and clear information about the effectiveness of their performance (Faturochman, 1997).

The JCM theory provided insight into how learning specific skills motivates a person to complete a job accurately and efficiently. The current study addressed whether and how security ambassadors are able to influence their peers through communication in which the user gains increased knowledge that leads to behavior adaptation. Interpretation of behavior adaptation was determined by ambassadors' perception of success. The phishing simulator is software that distributes spoofed emails to the intended target (staff) and records the actions taken or not taken by the recipient. If the email recipient clicks or downloads the attached link or file within the email, they are redirected to an education page because they failed the test. The education page highlights areas from the original message to outline visible giveaways the user should look for the next time they are opening messages from unknown senders. For those who choose to report the suspicious email via the phishing reporter button (an Outlook-supported plugin), a pop-up will appear on the screen to congratulate them on the successful detection (Cofense, 2018). The simulation is run by a group within the organization and is launched at random intervals throughout the year. Ambassadors also participate in simulation exercises and have no information on when they will occur.

I hypothesized that through the influence of department security ambassadors, employees are more likely to become receptive to the desired online user behavior when exposed to the phishing simulation. I further hypothesized that although security ambassadors are tasked to influence their peers, security ambassadors feel an intrinsic

drive to want to promote learning within their respective groups. Because the role of an ambassador is voluntary, financial incentive does not influence performance.

In the current study, the JCM theory was applied to security ambassadors in the following ways: For skill variety, ambassadors were given a variety of communication tools including newsletters, emails, written publications, posters, and webinars. For task identity, ambassadors determined how to best communicate through the tool. For example, if a phishing-related poster was used, ambassadors decided where it should be placed to get the most exposure to the team and for how long. If email was used, ambassadors decided how often one should be sent out. For task significance, ambassadors determined the level of impact of each communication option available to them. For autonomy, ambassadors selected which method of communication they felt would best resonate with their peers based on their conclusions drawn from the previous three actions. For job feedback, ambassadors decided whether feedback should be direct or indirect. Ambassadors were asked whether their contributions as a security advocate were worthwhile and whether they observed any peer and self-growth pertaining to phishing detection.

The JCM theory encompasses key components of social cognitive theory in that self-efficacy drives the behavior whether that motivation is intrinsic, extrinsic, or a combination of both. Other learning theories such as the self-determination theory also support this notion. At the core of human behavior is the intrinsic need to perform successfully (Deci & Ryan, 2012). This phenomenon can be witnessed as early as infancy as the human is predisposed to assimilate, master, and explore for cognitive and social

development (Ryan & Deci, 2000). Cerasoli, Nicklin, and Ford (2014) argued that intrinsically motivated individuals offer a higher degree of intensity or effort behind the tasks they perform. Extrinsic motivation is identified as a passive motivator (Ryan & Deci, 2000), and studies relating to increased job compensation support this claim (Hadi & Adil, 2010).

Researchers have not explored using a phishing simulation tool in conjunction with peer influence. The rationale for the current study was to combine the two to provide insight into a person's intrinsic motivation to adapt to a desired behavioral change. Security ambassadors' views were explored to understand how learning is perceived and motivated by the intended audience. The JCM theory predicts that when job features are presented clearly to the person performing the task, there is greater motivation to produce higher quality work and experience a higher rate of satisfaction (Hadi & Adil, 2010).

Arguments can be made that pay is the greatest motivating factor; however, no direct link has been found between pay and performance. Also, performance appraisals may not always be very well conducted, nor have they been found to be effective. On both accounts, adaptation becomes an issue (Hadi & Adil, 2010). Chamorro-Premuzic (2013) examined 120 years of research and learned that from 92 quantitative studies with a combined data set of over 150,000 people, the correlation between salary and job satisfaction was very low. Chamorro-Premuzic reported that there was less than 2% overlap between a person's pay and their job satisfaction. Results were not limited to one area of the world but included the United States, India, Australia, Britain, and Taiwan (Chamorro-Premuzic, 2013). Chamorro-Premuzic noted that the findings indicated that

for employee engagement, money is not the motivating factor behind performance. According to Chamorro-Premuzic, money was not demotivating, but it deflected from intrinsic goals. In a study with over 200,000 samples from the U.S. public sector employees, Cho and Perry (2012) documented that employee engagement levels were 3 times more likely to favor intrinsic motives than extrinsic.

The JCM is a theory that centers on self-efficacy and acts as the driving force behind human desire and performance. This internal need influences a person's goals that they have chosen for themselves, influences learning and the effort to excel on the job, and dictates persistence (Lunenburg, 2011). I combined two nonoverlapping learning tools (software and peer influence) to investigate the driving force behind why individuals choose to do what they do and what makes them more successful. Security ambassadors' perceptions were evaluated through the lens of the JCM theory. In a study conducted by Hadi and Adil (2010), 150 bank managers were assessed to determine whether there was a correlation between job performance and job satisfaction. An initial questionnaire was used to assess job characteristics, work motivation, and job satisfaction (Hadi & Adil, 2010). A multiple regression analysis indicated that job characteristics predicted both intrinsic and extrinsic motivation and job satisfaction (Hadi & Adil, 2010). The most promising predictor of job satisfaction and intrinsic motivation was task identity, whereas feedback of the task performed provided extrinsic motivation (Hadi & Adil, 2010). This study validated the need to explore the influence of the JCM theory as it relates to phishing detection at an organizational level.

## Nature of the Study

For this phenomenological study, I gathered data from ambassadors through semistructured interviews at an organization that has been using the phishing simulation and ambassadors as complementary tools to generate security awareness since 2015. The phishing simulator tool has been used to conduct over eight million phishing simulations throughout various organizations, and results have indicated that the tool improve employees' ability to detect phishing emails (Korolov, 2016). The idea is that people are the weakest link behind corporate data compromise. The phishing simulator tool has shown that it is possible to change a user's behavior to prevent a future occurrence (Anti Phishing Working Group, 2017). Korolov (2016) noted that when a person has been exposed to a series of simulated phishing exercises, the average failure rate falls from 20% to 13% followed by 4% and then 0.2% after the fifth exposure.

The Security ambassador program is intended to raise awareness through leading by example, delivering timely security-specific information to coworkers and reminding others of their personal contributions to protect the organization. At the study site, the ambassador program has been providing knowledge through educational tools on a monthly basis to assist teams in achieving security objectives. Using a phenomenological approach, I explored whether peer-influenced motivation produced greater likelihood of behavior adaptation though implementation of the program.

## Sources of Data

As part of the program, ambassadors receive periodic communication with information on safe internet behaviors and current phishing threats. After receiving the

messages, the ambassadors determine how they would like to disseminate the information to their peers. Data in the current study were collected from security ambassadors in individual interviews to identify their perception of cybersecurity awareness communicated to their respective departments. Other research questions focused on the mode of communication used to promote learning. Ambassadors were asked whether they felt that their selected mode of communication was effective in achieving their intended goal. The self-discretion of the program allows for the ambassador to use their firsthand knowledge to determine what modes of communication work best for their peer groups.

## Assumptions

I assumed that given the voluntary nature of the security ambassador role, each ambassador has an intrinsic motivation to do what is best for the organization, and wants to promote learning opportunities for their peers. I further assumed that research participants would be candid and answer questions truthfully. I also assumed that ambassadors would analyze the success rate of their selected modes of communication between phishing campaigns to identify which method worked best for their group. At a more basic level, I assumed that ambassadors understood the difference between phishing and spam, and what actions to take when these emails have been received so they can communicate these differences to their teams.

## Scope and Delimitations

The need to protect business data is vital; therefore, the need to provide a comprehensive security program is necessary. Relying on tools to mitigate and prevent

attacks is not possible without the human component. The sole dependency on tools is costly and cannot keep pace with the speed and variations of these attacks; therefore, organizations must also rely on their staff to assist in the matter (Anti Phishing Working Group, 2017). The focus on ambassador perceptions was intended to assess how peer-influenced behaviors promote learning. Findings from this study may contribute to a comprehensive security awareness program among organizations.

The study was delimited to the selected medical organization. All 60,000 employees, including ambassadors, were exposed to random simulated phishing emails throughout the year. Transferability of findings from this study may assist other organizations in both medical and nonmedical settings in the creation of a tailored ambassador program to promote behavioral change. Ambassadors were interviewed to provide clarity regarding how peer-led motivation is necessary to promote behavior adaptation.

## Limitations

Several limitations of this study are evident. First, phenomenology studies have inherent limitations. The Center for Innovation and Research and Teaching (n.d.) noted that phenomenological studies rely on researcher interpretation, assumptions, and preconceived ideas about the experience or phenomenon. Another limitation in phenomenological studies is that because of the small sample size, results are not statistically reliable and not generalizable (Center for Innovation and Research and Teaching, n.d.). Another limitation in the study was the theoretical framework. According to the JCM theory, people are generally motivated to improve their performance when

they can determine the meaningfulness of the work they are performing, the responsibilities expected of them, and the knowledge of outcomes (Hackman & Oldham, 1976). The limitation was the fact that ambassadors already recognize these skills among themselves.

It is possible that certain departments within the organization have more knowledge or exposure to phishing attacks than other departments, which may have influenced study outcomes. Due to the nature of the work performed, I anticipated that two departments might have such an advantage or disadvantage: Information Technology and the Office of Information Security. Although this was a qualitative study with descriptive quantitative elements, one way to mitigate the bias would be to look at the rate of successfully identified phishing attacks across the organization over time to track the growth of learning.

## Significance

This research supported social change by combining two unique areas into one. Firstly, I challenged a tools-only solution to phishing. According to CSO Online (as cited in Korolov, 2016), reported that there are 10 major companies with this aim. With slightly different versions, these companies employ a tools-only phishing solution. Such providers include PhishLabs, IronScales, MediaPro, Wombat, KnowBe4, Inspired eLearning, and Blackfin, all of which provide education and phishing simulation. Other organizations such as the Anti-Phishing Working Group and InfoSec Institute provide training through their programs and educational resources. As more companies join this vendor-driven trend, emphasis on a tools-only solution might not be most effective

solution, as data has shown. The Anti-Phishing Working Group is an international coalition of 1,800 members with a focus to combat security threats. In their 2017 report, phishing attacks increased by 65% from the prior year with 1,220,523 total attacks (Anti-Phishing Working Group, 2017). Additionally, phishing has risen 5,735% in the past 12 years (Anti-Phishing Working Group, 2017). Phishing has increased dramatically over the years, and to date there has not been a tool-only product that can prevent successful phishing attacks.

The value of this study was the combination of a nonsecurity element and a technological tool to produce a holistic approach to fighting phishing. I investigated the human factor to identify the role peer influence plays in learning, thereby leading to behavior adaptation. I also explored the cyber security domain to identify what mode of communication is more effective for some groups than for others. The security ambassadors provided their personal insight to help me answer the research questions. Because each participant had different levels of exposure to phishing, different levels of knowledge of cyber security, and willingness to learn, I hoped to close the research gap by exploring participants' experiences.

Because phishing relies on the human element to fail, phishing exploits will continue to evolve based on the behaviors of the end user, which is why establishing and maintaining end user motivation is critical for success. The security ambassador is an important component of security awareness programs in organizations. The goal of these programs is to promote lasting behavior change among employees. Tope, Chamberlain, Crowley, and Hodson (2005) noted that procedural change is often met with resistance

Because it creates a sense of discomfort among people, which is why procedure sabotage is a common response. The JCM theory is based on motivation and is driven by job satisfaction (Hackman & Oldham, 1976). Applying this theory would create the needed motivation to lessen the resistance to change. Security ambassadors act as the ears and eyes of their group to assist the organization in this transition. Allowing ambassadors this autonomy to produce motivation among their peers may lead to job satisfaction for the ambassadors, which may lead to behavioral conversion for their respective teams and organizations.

## Summary

The prevalence of phishing continues to grow each year. Symantec (2016) reported that in 2015, 1.4 billion smartphones were purchased, an increase of 10% from the previous year, and predicted that by 2020 there would be 6.4 billion smartphones in use. As smartphones become more powerful and have increased bandwidth connectivity, there is a greater chance of data compromise from phishing attacks. These attacks have also become more sophisticated, so there is a greater incentive for organizations and individuals to find ways to prevent these attacks.

This chapter included information to address the phishing epidemic by providing a cause for the study, the gap in the literature, the application of the JCM framework, and the study's limitations and scope. In Chapter 2, I provide further description of the JCM theory and its rationale for the current study. Chapter 2 also contains a detailed review of the literature to support the need for the study, the possible causes for the existing research gap, the research questions, and a summary.

# Chapter 2: Literature Review

The purpose of this section is to review existing literature relating to the problem in the present study. I examine the role of peer influence and how it impacts human behavior, and why people continue to be susceptible to phishing even though numerous technological tools are available to aid its detection. Hackman and Oldham's (1976) JCM theory assisted in the understanding of how motivation is achieved regardless of the task being asked to perform.

The influence of peers in how individuals perceive themselves and operate in their day-to-day lives is unclear. Research has shown human conformity is developed during childhood and serves in the transmission of human culture to create in-group uniformity and stabilization (Boyd & Richerson, 2009; Haun & Tomasello, 2011). Group behavior is acquired through observation and strategically learned even during childhood (Haun & Tomasello, 2011; Gergley, Bekkering, & Kiraly, 2002; Schweizer, van Maanen, Carpenter, & Tomasello, 2006; Tomasello, 1999). In the current study, I explored influence of peers on the accuracy of phishing detection.

Phishing continues to be on the rise and most organization phishing attacks start from a single click in an emailed link (Cofense, 2018). According to Cofense, a phishing detection company that uses simulated phishing attacks through email to educate end users, 91% of attacks start with a phish. In their 18-month study among 1000 users, Cofense found that the top three motivating drivers for a person to click on a link in an email from an unknown sender are evenly split among: curiosity, fear, and urgency. However, it is not clear what happens when an organization attempts to create phishing

awareness by educating users with available technology (phishing simulation) and peer influence. The purpose of this study was to examine how peer-led motivation may contribute to the behavior adoption process.

The selected literature reviews follow two separate themes: the cybersecurity threat landscape and the possible human motivators to act upon them. I emphasize these themes to explain how learning is achieved and how peer influence may or may not impact behaviors when exposed to the electronic environment. Current research has not provided a clear, direct link between accuracy in phishing detection and peer influence at the organizational level. It appears that victim susceptibility for phishing attacks is quite broad, even when the user's level of conceptual and procedural knowledge is evident. Even when the best case scenario was presented and the recipients were computer system knowledgeable (syntax, domain names, etc.), spoofed websites fooled more than 90% of participants (Alsharnouby, Alaca, & Chiasson, 2015; Dahamija, Tyar, & Hearst, 2006). Dahamija et al. (2006) concluded that a different approach outside of the traditional cryptography-based security framework is needed.

Despite new discoveries that the human component is critical in phishing detection, evidence showed that old habits for both the employee and the company die hard. Companies depend on technology to protect their most valuable assets; however, companies fail to weigh the human contribution and its role in securing organizational assets (Ashraf, 2005). In 2012, the three top vulnerabilities facing organizations included third party access, increased use of mobile devices, and lack of sufficient human

awareness, all of which include a human component (Deloitte, 2013). Previous studies addressed user awareness but not the motivation behind users' actions.

## Literature Search Strategy

Google Scholar served as the primary search platform for this study. This resource was used to search for journal articles, conference proceedings, and other publications. Year-of-publication filtering was used to ensure content was current and published within the past 10 years. Keywords used in the search included *phishing*, *security awareness*, *cyber security*, *phishing detection*, *social engineering*, *motivation*, *peer influence*, and *behavior adaptation*. Articles retrieved by keyword search were segmented into two halves: cyber security focused (phishing, security awareness, cyber security, phishing detection, social engineering) and psychology focused (motivation, peer influence, behavior adaptation). In cases where there was limited current research available based on the keywords, synonyms were applied.

## Theoretical Foundation

In the current study, my focus was to look at how peer motivation is perceived by the person delivering the motivation, and how the motivator adjusts their approach based on the perceived level of acceptance from the group. The study was based on the JCM theory as a theoretical basis. Hackman and Oldham (1976) noted that for change to occur, people need to be motivated by each of the three psychological states: meaningfulness of the working being performed, responsibilities, and understanding of the outcomes.

When reviewing the current literature, I identified two challenges when organizations attempt to mitigate phishing attacks: user education and software

enhancements. User education is an attempt to increase a person's ability to accurately detect a potential threat while software is used to assist in detecting the potential threat before it reaches the human (Khonji, Iraqi, & Jones, 2013). Although these two types of mitigation are effective to a certain extent, they present challenges. Khonji et al. (2013) noted that people have a resistance to learning new tasks and/or procedures to some degree, and knowledge retention is not necessarily permanent. Further evidence indicated that work performance and accuracy are not directly associated with motivation and compensation; therefore, the notion that increasing pay will translate to improved performance is not scientifically supported (Chamorro-Premuzic, 2013).

From the software side, technological tools such as authentication and security warnings cannot operate alone and are still heavily dependent on human behaviors. Although these two challenges have been shown to be interrelated when trying to mitigate a potential cyber security threat, the proposed third element has not been previously studied. The idea that peer influence and perception impacts behavior adaptation with respect to cyber security within an organizational setting has yet to be explored. The current study addressed the role of peer groups (identified as security ambassadors) in recognizing, promoting, and retaining desired behaviors among employees.

The literature review supported the need for the current study. All reviewed studies had been conducted within the past 10 years and were found using the Google Scholar database. Search terms used were *social networking*, *peer influence*, *user perception*, *social learning theory*, *behavioral intentions*, *behavior modeling*, *phishing*

*detection*, *learning motivators*, *organizational behavior*, and *cyber security threat landscape*. This research strategy focused on two key areas: the reasons why people fall victim to phishing, and how phishing has evolved over time to trick the end user. I also examined what motivates people to want to change rather than demand for change from another party, such as an employer. I combined two phishing-detection components by looking at studies in which peer influence plays a pivotal role in a person's decision-making and user awareness. By blending these two elements, I hoped to understand how influencing behaviors may aid in phishing detection alongside the use of technological tools. Research on phishing detection has not included a phishing simulation tool in conjunction with peer influence. The rationale to implement the current study was to combine the two learning tools by providing insight into a person's intrinsic motivation to adapt to the desired behavioral change. Security ambassadors' perspectives were explored to understand how learning is perceived and motivated by the intended audience through the eyes of the peer group members.

The JCM theory centers on self-efficacy and acts as the driving force behind human desire and performance. This internal need influences a person's goals that they have chosen for themselves, including the effort they exert to excel and persist on the job (Lunenburg, 2011). I combined the two learning tools (software and peer influence) to investigate why individuals choose to do what they do when an email is received. These perceptions were evaluated through interviews with those responsible for orchestrating the influence: security ambassadors. I used JCM theory to explore phishing detection at an organizational level.

## Literature Review Related to the Key Variables and Concepts

### Electronic Environment

As of June 2018, 55.1% of the world's population of approximately 7.6 billion people used the internet, and of that population of internet users, 95% come from North America (Miniwatts Marketing Group, 2018). Hootsuite (2018), a social media management tool, noted that 3.1 billion users have a social media account, which reflected an increase of 13% from the previous year. Social media has not only infiltrated the young generation but has also influenced the elderly population (Chakraborty, Vishik, & Rao, 2013). The increased use of social media increases the likelihood of oversharing of private information and privacy leaks (Agger, 2012). Chakraborty et al. focused on Facebook because it was the largest social networking platform, and continues to be in the news for privacy leaks due to the oversharing of information by its users.

In one study, the profiles of 134 Facebook users who were at least 55 years of age, and compared their social media behaviors against 61 individuals under the age of 55 who also used Facebook. Chakraborty et al. also collected data from 50 of participants' social media friends, identified as root users. Collecting data from root users was intended to determine whether the participants were influenced by their peers in disclosing information about themselves on Facebook (Chakraborty et al., 2013). In total, there were 5,965 older root users and 3,050 younger root users in the study (Chakraborty et al., 2013). Results indicated that among the older population social media behaviors were significantly different from the younger group (Chakraborty et al., 2013). In the older population, the decision to share information openly on social media relied heavily

on peers' sharing behaviors (Chakraborty et al., 2013). Chakraborty et al. also discovered that the older population was not limited in sharing their background information and pictures, but also shared their location as well.

Social engineering is the obtaining of information through manipulation of the end user. Examples of social engineering include phishing, baiting, quid pro quo, pretexting, and piggybacking. When social engineering was used in conjunction with traditional phishing methods, past research had shown just how successful it became. Shah et al. (2015) examined how phishing attacks have not only become more common but also had become more complex as technology itself had evolved. With newer forms of technology in place, the rise of vishing (voice over IP) and smishing (short message service) had also grown. This particular study looked at how to combat against the different forms of phishing though user identification of a tool called Zero Knowledge Authentication (ZeKo). ZeKo's intent was to assist the user from becoming a victim of a future phishing attack through encryption. While ZeKo provided authentication between client and server namely through a token and password, it did not however eliminate the human element that was required to tackle social engineering. Shah et al. (2015) described social engineering as an art or skill that is used to manipulate people to perform specific actions and is used to extract confidential information from them through the establishment of social relationships.

In the study, the prevalence of phishing stemmed from three key areas: Lack of knowledge which includes lack of computer system knowledge and or lack of security indicators, visual deception, and bounded attention (Shah et al., 2015). Study participants

were individually presented with 20 websites presented in random order. Of these 20 websites, 9 represented phishing websites, 7 represented legitimate websites, 3 were of advanced phishing websites, and one website which required the user to agree to endorse a self-signed secure sockets layer certificate. Twenty emails were sent to each participant and they were instructed to click on the link found in the email, and to interact with the website as they normally would.

Results of the study were then broken down into five categories. Type 1 focused on the security indicators in website content only. Twenty-three percent of the participants used only the contents of the webpage in question to determine its legitimacy. These security indicators included such identifiers as logos, layout, and language. Type 2 looked at website content and domain name. Of the study group, 36% of the participants relied on the website's URL on the address bar to determine the webpage's legitimacy. In type 3 (content and address plus HTTPS) only 9% of the population reviewed the presence of "HTTPS" in the address bar. Piggybacking on types 1-3, type 4 applied all of the about plus the presence of the padlock icon. Results showed that 23% of the participants depended on the four different factors to determine a website's validity. Lastly, type 5 looked at all four types in addition to website certificates. It was found that only 9% of the group verified a website with these requirements.

While this study provided evidence that the general computer user does not always demonstrate safe internet practices, it did not provide enough information on how ZeKo can help the general population other than to provide one layer of protection. This

extra layer of security yet provided a false sense of security as the ultimate line of defense was through user training and awareness however, this was easier said than done. Khonji et al. (2013) argued that the difficulty in detecting phishing was the inability to locate one silver bullet to combat the epidemic and that the limitations were due to the available mitigation techniques which have not have successfully controlled security breaches among organizations. Some of the challenges stemmed from two unique sources that focused to minimize attacks but did not necessarily contain it entirely. These two distinct types of mitigation techniques were user education and software enhancements. The challenge became when both approaches were dependent upon one's motivation to learn, retain, and application. The matter was further complicated by differing viewpoints when focusing on user education. In one aspect, user education was seen as a powerful tool in establishing learning and awareness of the problem while the other saw it as the ability to use the knowledge base to regulate one's behavior, but did not lead beyond it (Khnoji et al., 2013).

From a technological perspective, relying on tool implementation is not a viable solution. Hayes, Shore, and Jakeman (2012) argued that there had been very little progress made when providing perimeter protections even at the government level such protective measures were limited to firewalls and soft internal networks along with limited segregation of applications. Additionally, more advanced security controls such as multifactor authentication and encryption have not fully lived up to the intended capacity. These weak forms of defense created a false sense of security which led to massive security breaches among even the largest of organizations.

The sources of these vulnerabilities are expansive and evolve over time to avoid detection. Hayes et al. (2012) stressed the importance of first understanding the source of the threat when attempting to build a cybersecurity strategy as the threat landscape is vast and constantly changing. Identified as “threat actors” these nine threat sources infiltrate the electronic environment from unique paths (Bucci, 2009). Bot network operators are hackers who coordinate multiple system attacks to distribute phishing, spam, and malware. Criminal groups attack for monetary gain through spam, phishing, spyware and malware with the goal of committing identify theft and online fraud. State-sponsored actors are intelligence collectors who use cyber tools for information gathering and espionage. Another threat source is hackers and typically break into networks to seek the thrill of the challenge and often notably belonging to a hacker community. Insiders are not always the most knowledgeable in terms of computer intrusions; however their deeper knowledge of a targeted system allows them the unique ability to gain unrestricted access to vital information. Phishers may be individuals or a small group of people who execute phishing schemes with the focus of stealing identities to seek monetary gain. Spammers may be organizations or individuals who distribute unsolicited emails which may contain spyware/malware. Along with spammers are the spyware/malware authors who create and sell their product to others. Lastly, are terrorists who look to destroy or threaten critical infrastructure and possibly threaten national security which may lead to mass casualties and weaken the global economy (Bucci, 2009).

**Human Element**

The concept of behavior modeling is not new. The social learning theory encompasses attention, memory, and motivation in that people simply learn from others through observation, imitation, and modeling (Bandura, 1977). According to Bandura (1977) effective modeling must possess four key conditions: attention, retention, reproduction, and motivation.

Behavior modeling continues to be prevalent. With the rise of social media and the speed of information sharing, there has been research to examine just how privacy and disclosure is being perceived and viewed by users. Strater and Richter (2007) conducted a study which qualitatively examined disclosure and privacy behaviors of college students in regard to their attitudes on Facebook. Findings identified that on the very basic level, Facebook users who logged into their account on a daily basis often updated their personal information between one to three times per week. From these updates, 67% of users maintained public profiles which were readily accessible to the general public. The remaining 33% of reported users implemented restricted access to just their Facebook friends and not a single participant used granular privacy controls within their profile (Strater & Richter, 2007). Interestingly noted by one participant, it appeared that privacy settings may have been intentional but incorrectly used as the profile in question was fully accessible to the public when the original intent was set to friends only. While this was only reported by one participant of the study, several participants clearly demonstrated full understanding of how to effectively use the privacy settings on their profile such as untagging themselves from photographs posted by others,

wall posts, and controlling their newsfeed alerts. Important to note was that 42% of users who did not like the newsfeed feature, disclosed that they simply began to accept it rather than learning how to adjust their privacy setting accordingly. In addition to reported privacy awareness, Strater and Richter (2007) reported a high number of participants continued to be at risk simply due to the oversharing of information on their Facebook profile. In summary, this study shed light into just how prevalent users were unaware of privacy threats from online disclosures on social media.

The topic of peer influence has been heavily studied in the past however less commonly studied was the comparison on how impactful it was between the younger versus the older population when making risky decisions. A study conducted by Gardner and Steinberg (2005) investigated 306 subjects who were divided up into three age groups based on their age. The first group was identified as "adolescents" who fell between the ages of 13-16. The second group was the "youth" (18-22), and finally the adult group, containing subjects who were at least 23 years of age. It was hypothesized that risk taking and risky decision making will decrease with age and that on average, those who were more inclined to take more risks were more likely to do so in the company of their peers. Lastly, researchers hypothesized that the adolescent group will show a higher correlation between risk taking and risky decision making based on peer influence compared to the other two study groups.

To measure risk taking, subjects were asked to play a video game called "Chicken" where the focus of the game was to make decisions about whether to stop a moving car on the screen once a traffic light changes from green to yellow. The game

was played in 15 trials and players were informed that at an undetermined point after the traffic light has changed to yellow, a wall would appear in front of the car. The goal of the player was to move the car as far as possible without coming in contact with the wall. While players were able to control the movement of the car, they were not able to control the speed of the movement. Players were awarded points based on how close they were able to get to the wall however would lose points should they crash into it (Gardner et al., 2005).

The second assessment was risky decision making and collected in the form of a questionnaire called Youth Decision-Making, (Ford et al., 1990). Of the five hypothetical dilemmas, each asked the subject to make a risky decision which included allowing friends to bring drugs into one's home, cheating on test, stealing a car, shoplifting, and skipping work. Additionally, each dilemma contained three scenarios. The first asked participants that no matter what their decision was, there were no negative consequences. The second informed participants that negative consequences may occur if a risk was taken and lastly, the final scenario indicated that negative consequences would absolutely occur if the risky decision was made.

Upon completion of the two questionnaires, it was found that risk taking, and risky decision making peaked among adolescents and decreased as one aged. When influenced by peers, risk taking and making risky decisions increased significantly in all three test groups. Findings from this study may help understand how peer influence plays a large role when it comes to both risky and non-risky decision making. Additionally, while certain age groups have been shown to be more predisposed to taking risks more

than others, it may provide an area for researchers to delve into when attempting to modify unwanted behaviors among certain groups.

Risk-taking is one element and user perception is another when trying to understand actions behind online user behaviors. West (2008) argued that user perception is what drives personal motivation to think of risk and that security decision-making is the product of that perception. By understanding key concepts, it is possible to redirect one's risk perception to improve their online security habits. Based on this idea, West (2008) asserted that users quite simply do not think they are at risk even with the facts to back up the claim. Instead, studies have shown that most people believe they are better than their peers when it comes to their decisions and actions such as driving, living beyond the average life expectancy, and less likely to be harmed by consumer products than compared to other individuals. Additionally, the concept of risk homeostasis has been documented in studies where people have a tendency to maintain an acceptable degree of risk that is self-leveling (West, 2008). When applying this concept to the world of online security, the user typically felt a higher level of security when a tool such as a firewall had been installed thus causing the user to be less cautious of their online actions.

Wood (2008) identified safety as an abstract concept therefore is less likely to be persuasive to most than more concrete outcomes as the reward for safety is the lack of a negative occurrence. In terms of security, this concept is difficult to grasp as there is not much to compare in terms of the costs, benefits, and risks in an action taken. The concept of positive and negative reinforcement is another factor to consider. In learning, behaviors are shaped by positive and negative reinforcement. In positive reinforcement,

the desired behavior is rewarded and in negative reinforcement, the non-desired is punished. The difficulty in modifying a user's online behavior is not as simple as in the case of security as the negative reinforcement is typically delayed and in some cases by weeks or months. The failure to identify the cause and effect is not immediate therefore is difficult for the user to pair.

## Conclusion

In conclusion, the online user population is diverse, our electronic environment is growing, and the threat landscape is vast. The above studies help present a better understanding of the importance for organizations to implement a security awareness plan and not just rely on technology or independent decision-making by the end-user to combat technological threats. Past studies have shown the limitations of the effectiveness through use of technology and human motivation in an attempt to change behaviors. The goal of the proposed study is to assist organizations in identifying and combining different types of behavior-modification learning tools to safeguard themselves from a future cyber security attack. Through the use of phishing simulator tool and the security ambassador program, these two elements will be combined to track behavior adaption overtime. When users are thoroughly educated, guided through motivation, and assisted by technology to better detect phishing, the likelihood of a data loss is profound.

The purpose of this study assisted to understand the lived experiences of information security ambassadors as it relates to phishing detection among their peer groups. The role of the ambassador is to be the ears and eyes of their respective areas to

help uncover and close up possible learning gaps to prevent data loss. Understanding the audience is vital in making the proverbial sale.

With the collected literature review, the following major themes were evident. Users appeared to be peer-influenced in the social media setting with respect to their age. Motivations behind actions taken or not taken appear to be linked to the user's lived experiences, knowledge base, perceptions, and immediate rewards and consequences are all tied to their actions. Additionally, the method and frequency of communication will be examined as research has shown learning styles are absorbed differently among individuals.

In Chapter 3, I detailed the selected research design and its rationale by defining the central concepts of the study. Along with the research design and rationale, I will describe the theoretical base chosen for the proposed study and how learning specific skillsets contribute to intrinsic motivation to complete one's job. In this chapter I will identify how and what role, if any, does the researcher play in the collection of the data and of any potential biases and how to mitigate them. Subject collection methodology along with recruitment strategy and justification of the sampling population will be provided in Chapter 3.

# Chapter 3: Research Method

The purpose of this phenomenological study was to explore the lived experiences of security ambassadors as they attempt to motivate their peers with the assistance of an organization-wide phishing simulation tool to foster behavioral change. To identify whether ambassador-perceived influence was effective, I used a qualitative approach to determine the communication methods used by the ambassadors. All participant interviews were conducted by me. As the researcher, I did not have a supervisory role over the participants or any previous contact or communication with the participants prior to the study.

This chapter includes the research design and its rationale. Elements of the research methodology such as population, sampling strategies, the number of participants are discussed. Additionally, research participants and recruitment method are described. Instrumentation and the sources of data are also identified.

## Research Design and Rationale

The aim of this study was to examine the experiences of security ambassadors as they try to advocate safer internet behaviors in their workplace. These experiences are in part driven by their opinion and judgment of their peer group as to which communication method is best for them. The following research questions (RQs) guided this study:

Primary RQ: What are the lived experiences of information security ambassadors when advocating phishing detection in their respective departments?

Secondary or prompt questions:

RQ1: Do security ambassadors perceive that their department peers have a desire to learn?

RQ2: How many ambassadors choose to share the requested communication to their teams?

RQ3: Why do security ambassadors choose not to communicate certain cybersecurity tips to their peers?

RQ4: What are the different types of communication methods shared by ambassadors to their teams?

RQ5: What do ambassadors perceive as the most successful communication mode?

RQ6: What mode of communication is perceived by ambassadors as the least successful?

RQ7: How much business value is perceived by ambassadors based on the work with which they are tasked?

**Research Tradition**

The research tradition for this study was qualitative phenomenology, which was used to explore participants' lived experiences. According to Flick (2014), researchers using qualitative methodology have an interest in analyzing subjective meaning or issues through data that come in the form of text and images rather than numbers. In phenomenological studies, the researcher can explore the phenomenon in-depth.

The theoretical base for this study was Hackman and Oldham's (1976) JCM theory. The core concepts of this theory are the three ideas that motivation occurs when

three psychological states are simultaneously activated as the person is working: meaningfulness of the work they are performing, responsibilities, and the knowledge of outcomes (Hackman & Oldham, 1976). The selected approach provided insight into how learning specific skills influences motivation to complete a job. I explored security ambassadors' experiences regarding how they chose to communicate to their peers, the frequency at which they chose to communicate, and what determines communication success or failure in their eyes.

**Rationale of the Chosen Tradition**

The rationale for the phenomenological approach was the need to collect data from participants based on their subjective experiences and perspectives. Unlike other qualitative designs such as case studies, which focus on a single event or individual, a phenomenological approach focuses on individuals' lived experiences. In this study I examined the overlooked area of security awareness by exploring the influence of peers on phishing detection. The study site has 289 active security ambassadors, and 144 members of this group have served as ambassadors since the beginning of the program in 2015. For this study, 20 security ambassadors were randomly chosen from this pool of 144 to participate in interviews. Selected individuals were sent an email thanking them for their ambassadorship and seeking their participation to conduct an interview of their experiences as an ambassador. This email also indicated that participation in the study was strictly voluntary and they could opt out at any time. Interested individuals signed up to participate by accessing a link found in the email and scheduling a time from the calendar. The interview questions were preselected (see Appendix C), and each

interviewee was asked the questions in the same order. Following the last preselected question, each participant was asked whether they had any comments or feedback about the ambassador program they wanted to share regarding how the program could be improved. Upon completion of the interviews, I transcribed the recordings and transferred the data to NVivo for analysis.

### Role of the Researcher

Given the nature of the study, I allowed participants to dictate their preferred communication methods. Although the research was conducted at the medical campus where I work, I was not in any way involved in the ambassador program. The program is managed by a separate department outside of the Office of Information Security. I did not have any previous exposure to the security ambassadors and had no influence on their participation in the study or their ambassadorship. My role as the researcher was to conduct interviews, record and transcribe participants' responses, and analyze results through NVivo to identify common themes. Researcher bias was avoided as much as possible by asking the same set of open-ended interview questions to each ambassador. Twenty security ambassadors were interviewed for this study. There were no other foreseen ethical issues related to the study.

## Methodology

The study site organization has 289 ambassadors, of which 144 have been in the role since the beginning of the program. Ambassadors were recruited from all departments through a link posted in their intranet site (see Appendix A). In addition to providing their name and contact information, interested individuals were asked to

complete a two-question form addressing how many years they had worked at the organization and whether they had supervisor approval to become an ambassador (see Appendix B).

**Inclusion Criteria**

Ambassadors are employees who protect patients, data, and property and raise awareness by example and by distributing information in a timely manner to their peers. To fulfil this duty, interested individuals are asked to provide a minimum commitment of 1 year and to dedicate 2-3 hours per month. Participation recruitment in the current study was advertised on ambassadors' intranet site, and prospective participants were asked to provide their name and contact information and answer two questions: How many years of service do you have at the organization, and do you have your supervisor's approval to be an InfoSec Ambassador? To participate in the study, participants had to be current ambassadors who had held the role since 2015, had to be willing to have interviews audio recorded, and had to be willing to provide detailed information about their experiences as an ambassador.

**Study Population**

A sample of 20 randomly selected security ambassadors was used for the study. Participants represented various departments within all sites on the medical campus. Due to the type of study being conducted, a large sample size may not have necessary given the possibility of data saturation occurring quickly. According to Mason (2010), the purpose of a qualitative study is to find meaning, not to formulate generalized conclusions; therefore, more data does not always translate to more findings. Although

there is no set sample size in qualitative studies, Creswell (1998) suggested between five and 25 participants for phenomenological studies. Morse (1994) did not suggest a maximum number, and only emphasized that the minimum number be six.

**Instrumentation**

Data were collected from open-ended interview questions. All questions were preselected prior to the interview, and each participant was asked the same questions to ensure consistency and minimize researcher bias during the interview.

**Data Collection Process**

I collected the data from open-ended interview questions (see Appendix C) administered to 20 randomly selected security ambassadors who had held that role since the program's inception in 2015. Each randomly chosen participant was invited through email to participate in the study. Each participant was provided the purpose of the study as well as the time commitment needed to complete the interview. There was no remuneration offered for participating in the study, and follow-up questions were asked only for the purpose of clarity. The interviews were audio recorded and accessible only to me. The purpose of the recording is to ensure response accuracy. Ambassadors were allowed to decline participation at any point of the study.

Participants were given a preinterview briefing 1 week before the start of the interview to help them understand the intent of the study and to answer any questions they may have had regarding their participation. Participants were informed that they had the right to opt out at any time and that the interviews would be recorded and accessible only to me. Ambassadors who had a continued interest were given a link to access within

the email to schedule a time for their interview. If an ambassador declined, a replacement was randomly chosen from the participant pool until a total of 20 participants was reached.

Two days prior to the start of each scheduled interview, I emailed a reminder to each participant of the date and time of their interview. Those who are unable to meet at the scheduled time but would like to participate would be in contact to arrange for a better time. On the day of the interview, I would meet with each ambassador, introduce myself, the purpose of the study, how long the interview will take, the total number of questions, the audio recording of the interview, any questions I can help answer before we start, and ask if they would like to proceed. Each interview followed the same protocol. During the interview, I recorded and wrote down ambassador responses to each question. Should post-interviews need clarity, it would be sought through email. Upon the conclusion of the interview, participants were thanked for their time. There were no remuneration offered for participating in the study and there were no follow-up interviews.

**Pilot Project**

A pilot study consisting of three randomly selected security ambassadors was conducted. Research procedures of the pilot followed in the same protocol as the main research study. I conducted a pilot study with three participants who were similar to, but not included in the main study, in order to practice administering the interviews and to provide an opportunity to revise or refine my approach prior to the main study.

## Data Analysis

The data analysis consisted of four main steps:

1. The information gathered from the interview was transcribed, stored, coded, categorized, and analyzed through the NVivo software by the researcher.
2. A qualified assistant independently coded and categorized the same interview responses.
3. Responses were then loaded into the NVivo software and coded via its automatic coding process.
4. The results generated from NVivo were compared against the two manually coded sets leading to the discovery of emergent themes.

The use of the NVivo aided this study in the brainstorming and mapping of common ideas, patterns, and common themes found. Discrepant data was analyzed for root cause, frequency of occurrence, and assessed to determine inclusion in the final analysis and interpretation.

## Trustworthiness

Internal validity came from: theory, interviews, and quantifiable data. Triangulation was not performed. The focus of this research was to determine the impact of peer-influenced motivation used to achieve desired behavioral change in phishing detection. Data obtained from ambassador interviews was analyzed for common themes. If a theme has been found, the causes will be compared against the Hackman and Oldham's job characteristic model (JCM) to assess why or why not motivation occurred based on the these perceptions. The JCM theorizes that motivation is the product of when

job satisfaction has occurred and to be able to achieve this state, specific criteria must be met.

This research has a high degree of transferability and dependability as the study produced information that can be applied in different application settings. While the focus of this study was to identify critical areas needed to establish a comprehensive security awareness program, the concept of motivating others is applicable in all settings where people interact with one another. The use of influence, in particular those who are viewed as social leaders or popular opinion holders have shown to increase others to shift their own behaviors to conform to the perceived behavioral norms (Valente & Davis, 1999; Carey et al., 2016). Such an example is study that surveyed drinking among college students. The study found that when participants engaged in conversations about either promoting drinking or promoting drinking safety with someone who is viewed as a social leader, the participant is often swayed by the focus of the discussion. Carey et al. (2016) noted that communication variables are highly tied to the social leader's stance when it comes to behavioral influence.

Research confirmability for the study was linked by an audit trail. The audit trail documented the study's data collection process, data analysis, and final interpretation of the data collected. Common themes were found, and a rationale was made to provide insight behind the decision to identify them as such. The purpose of an audit trail is to provide the reader an understanding how the author came to the conclusions they did and to be able to use as a foundation for further research (Carcary, 2009). Research trustworthiness is important in all types of research studies, but even more so for

qualitative studies. Unlike quantitative studies which has a clear-cut approach, qualitative studies rely on interpretation of less tangible information, and possibly whether or not enough evidence was obtained (Marshall & Rossman, 2011), therefore the burden is on the author to provide this level of certainty to the reader.

## Ethical Procedures

Based on the nature of this study and the information obtained, ethical considerations were considered and addressed for both researcher and participant. Study participants participated in a volunteer-only basis, and could opt out at any time, additionally, remuneration was not offered. Twenty participants were randomly selected from a pool of 144 security ambassadors who have held their ambassadorship role since 2015. Participants will be ensured that the information obtained from the study will be kept confidential and participant names will remain unidentified. As a researcher for this study, and also an employee of the organization, I did not have influence nor had previous interaction with security ambassadors as the entirety of the ambassador program is managed by a separate department. Once data was collected, the information was stored on an encrypted thumb drive and no other copies will be made. Participants were informed of the purpose of the study, how data is collected, synthesized, and the study's intent to use collected data to further improve the existing security awareness program at their organization. No further participation or research data was collected until written approval from the Walden IRB was received (IRB #: 07-17-19-0277144).

## Summary

In this chapter I detailed the research design and rationale of the study, along with the role of the researcher. Research methodologies such as participant selection, procedures, instrumentation, and trustworthiness were addressed with the goal of clarifying how data was interpreted, and can serve as a platform for future studies.

# Chapter 4: Results

The focus of this study was to explore the lived experiences of the security ambassadors at a medical organization. In this chapter I detail the results of the phenomenological study addressing the lived experiences of security ambassadors as they motivate their peers through influence to promote phishing detection. The primary research question was the following: What are the lived experiences of information security ambassadors on phishing detection among their workgroups when trying to implement behavioral change? In this chapter, I also describe the pilot study, research setting of the full study, participant demographics, data collection, data analysis, evidence of trustworthiness, and results.

## Pilot Study

I conducted a pilot study with three ambassadors following the procedures for the main study described in Chapter 3. Participants were randomly selected from an ambassador pool of 144 members; participants held the ambassador role since the program's inception in 2015. At the time of the pilot study, there were 289 ambassadors in the organization. There were no unusual circumstances encountered in the data collection process and each respondent completed their interview without issues. Even though the participants agreed to be contacted after the interview for response clarity, none were contacted because it was not needed.

After the completion of the pilot study, a few modifications were made after review of the results with committee members. Modifications from the pilot were implemented in the full study (see Appendix D). With the pilot findings, a revised IRB

approval was requested. Once the revised IRB request was approved, the full study was conducted as outlined in Chapter. The first change made to the main study based on results of the pilot and from consultation with my committee members was the addition of the opening question: Can you describe to me about your experience with the security ambassador program? The decision to add this question was to generate an uninterrupted, unstructured response from the participant. Revisions were also made to the prompt questions to ensure that the areas of focus in the study had been adequately addressed if they were not answered during the opening question. The revised prompt questions were the following:

1. From your perspective, describe your peers' overall level of phishing knowledge prior to the implementation of the InfoSec Ambassador program.
2. Are there any communication methods you found to be less effective within your work area?
3. What motivates you to continue fulfilling the InfoSec Ambassador role beyond the requested one year commitment?
4. Please provide any additional information you would like to share with us to further improve the existing InfoSec Ambassador Program.

Lastly, a decision was made to audio record and transcribe the interviews to ensure completeness of responses and assist data analysis. A request for approval of the revisions was submitted to the IRB. The main study was initiated after written approval from the IRB was received.

## Setting

The research setting was audio recorded telephone interviews. Ambassadors chose to participate based on interest without additional incentive. The research began as outlined in the Chapter 3 after approval from the IRB.

## Demographics

Participants consisted of 14 women and six men in varying career paths across multiple departments throughout the organization. Eight participants provided direct patient care, and 12 provided indirect care (see Table 1). An example of direct patient care is nursing, and indirect patient care includes administrative support roles such as secretarial or administrative leadership positions. Each survey participant was assigned a number based on the order of their interviews ranging from 1 to 20. These numbers were used in lieu of names to protect participants' identity.

Table 1

*Selected Demographic Characteristics of Study Participants*

| Ambassador | Gender | Care type | Work department |
|---|---|---|---|
| 1 | Female | Direct | Nursing |
| 2 | Female | Direct | Sleep medicine |
| 3 | Male | Indirect | Operations support |
| 4 | Female | Direct | Respiratory |
| 5 | Female | Indirect | Clinical nutrition |
| 6 | *Female* | Indirect | Emergency communications |
| 7 | Female | Indirect | Operations support |
| 8 | Male | Indirect | Patient appointment services |
| 9 | Male | Direct | Nursing |
| 10 | Female | Indirect | Medical transcription |
| 11 | Female | Indirect | Program support |
| 12 | Female | Direct | Surgical services |
| 13 | Male | Indirect | Media support services |
| 14 | Female | Direct | Infusion therapy |
| 15 | Female | Direct | Operations support |
| 16 | Female | Indirect | Cancer registry |
| 17 | Male | Indirect | Research |
| 18 | Female | Direct | Surgical services |
| 19 | Male | Indirect | Informatics |
| 20 | Female | Indirect | Finance |

## Data Collection

Interviews were conducted by telephone from October 2019 through January 2020, and each session was allotted 1 hour in length with the average call lasting 34 minutes. Time between interviews was based on scheduling availability of participants and me. One week prior to the scheduled interview, each participant was contacted by email as a reminder of the upcoming interview, the focus of the interview, who would be conducting the interview, and the participant agreement form. Participants were also asked whether they had questions or concerns prior to the interview. This contact was

also to ensure participants were still interested in participating. All 20 randomly selected individuals agreed to continue, and they completed the interviews.

At the beginning of each interview, each respondent was thanked for agreeing to share with me their experiences as a security ambassador. I made it clear that during the interview, I would be audio recording their responses and that the entirety of their responses would be used only for the purpose of transcription accuracy and would not be accessible to anyone but myself. I assured participants that all information would be kept confidential; would not have any impact on their ambassadorship, department, or employer; and would not be linked back to them because all personal identifiers would be encrypted. Lastly, I reminded them that they could end the interview at any time and asked whether they had any questions for me before we began. Each respondent agreed to proceed without concern. At the conclusion of each interview, I thanked participants for their time and asked whether they would be willing to agree for a follow-up email should I have any clarifying questions to ask related to their responses. Each participant agreed.

## Data Analysis

The role of the researcher is to explore the thoughts and feelings of study participants. This interpretive phenomenological study was broken down into several phases. Because qualitative data are dependent on interpretation, results rely on a researcher's analytical and critical thinking skills. In the first step, I conducted manual coding of the 20 interviews. I then proceeded to categorize the collected codes. My assistant independently coded data from the same 20 interviews through the same process by first manually coding the collected data. With the coded data, my assistant then

categorized the coded contents. The research assistant was not affiliated with the ambassador program, had a background in communications and statistics, and had an MBA.

Both coders were responsible for reading and comprehending the interview responses before coding. Next, we individually identified and labeled what we thought were relevant pieces from each interview response. These coded responses were in the form of a single word or short phrases. Once codes were identified, they were then categorized by their respective coder. Categories are groupings assigned to coded segments aggregated to form a common idea (Creswell, 2013).

Next, transcribed data from the interviews were imported into NVivo to assist in the identification of themes. NVivo is software produced by QSR International and is used for qualitative and mixed-methods research for the purpose of analyzing and organizing unstructured text, audio, video, and image data (Kent State, 2020). The generated categories from all three sources (researcher, assistant, and NVivo) were analyzed with the goal of identifying emergent themes. Gibbs (2018) defined *qualitative coding* as the process in which data are indexed or categorized with the goal of establishing a framework of thematic ideas by linking data to the research questions and back to other data.

In the first step of the data dissection, each coder was responsible for the manual inductive coding of the interview responses. From the manual coding, each person conducted a line-by-line analysis and assigned a code for responses to both open and prompt interview questions. For the opening question, notable codes included words or

phrases such as “very excited,” “great experience,” “sharing,” “lead,” “gain,” “positive,” “aware,” “team,” “thankful,” and “educate.”

Regarding their peer’s level of security knowledge prior to the program (RQ1), notable codes were “depends,” “general,” “consensus,” “not really,” “some,” “freighting,” and “significant.” When asked about the least effective method of communication (RQ2), prominent codes included “bulletin board,” “urgent,” “better than nothing,” “read,” hope,” and “unsure.” When asked about the motivation to continue beyond the one year commitment (RQ3), notable codes included “good feeling,” “the news,” “email scams,” “enjoy,” “helping out,” “answer questions,” “connection,” “security threat,” “comfort,” and “learning.” Lastly, the request for feedback on the program (RQ4) produced the following notable codes: “resonates,” “variety,” “subjects,” “liaison,” “required,” “important,” “business,” and “same issues.”

Next, identified codes were sorted into categories for the purpose of theme identification. For the opening question, notable categories included “positive experience,” “gained knowledge in security,” “personal choice to join,” and “great teaching tools offered.” Regarding participants’ peer’s level of security knowledge prior to the program (RQ1), notable categories included “not much knowledge,” “topic not seen as important to work performed,” and “unsure.” When asked about the least effective method of communication (RQ2), prominent categories identified include: “alternate or additional communication,” “not enough time,” “unable to confirm if read,” and “does not encourage communication exchange.”

When asked about the motivation to continue beyond the one year commitment (RQ3), notable categories included: “enjoy helping others,” “sense of duty,” “relatable to real-life experiences,” “sense of personal contribution,” and “enjoy learning new topics.”

Lastly, the request for feedback on the program (RQ4) produced the following categories: “great program,” “same topics/content,” “all departments should participate,” and “important to work and life.”

Yi (2018) noted that themes come in two forms where the larger category provide predominate themes while the smaller categories provide support to the larger theme. The intent to conceptualize the information gathered allows for the storytelling of the data collected. In this phase of analysis, each coder independently determined which codes will be used and which will be omitted based on their relevancy of the study’s focus. Automatic open coding was done through NVivo’s automatic coding process. The purpose of the automatic coding process is to assist in the coding speed of large contextual data. For this study, the assistance from the software was used as an additional layer of filtering and clarity to aid in the identification of themes. In this process, NVivo compared each text passage such as sentence and paragraph to the content already coded in existing nodes (NVivo, n.d.).

Categories are a product of linked codes. Elliott (2018) described qualitative research categories as a collection of similar data codes collected together to form a common idea. NVivo identify categories as “nodes” and from these nodes, themes start to surface.

Qualities of discrepant cases were factored into the analysis. Hackett (2010), LeCompte and Preissle (2008) identified discrepant cases as an attempt to choose cases which aim to modify, elaborate, or enhance an emerging theory after data has been fully collected and analyzed. For this study, all 20 interviews were analyzed and responses that appeared to be substantially dissimilar from other responses, a deeper analysis was done to determine the root cause, then to conclude whether or not that particular data will be factored into theme discovery. Upon analysis of all collected data, all 20 ambassadors described their experience as being a positive one. However, one ambassador's experience was impacted due to the lack of leadership support when they reported to a new manager who limited their ambassadorship capacity. As a result of this being a single case, and due to lack of leadership support, this discrepant case was ultimately acknowledged but eliminated from the final analysis and interpretation.

## Evidence of Trustworthiness

As mentioned in earlier chapters, qualitative studies rely on interpretations of the researcher based on their collected data. In order to be able to produce the most clear data interpretation, the raw data has gone through a well-defined and rigorous process to ensure the reader that all necessary steps have been taken to reach such a conclusion. The researcher bears the burden of ensuring trustworthiness of their findings. Below details the four components of qualitative research trustworthiness that we followed.

### Credibility

Adjustments concerning credibility were made from the findings of the pilot study. Credibility addresses confidence that the researcher has correct understanding of

the context of their data and that the findings presented are true (Watkins, 2012). The entirety of the pilot questions presented to the participants was found to be overly structured. Since this is a phenomenological study, there was a greater interest in allowing participants to freely talk and to overall lead the direction of the discussion. The original questions were replaced with a more open-ended question to allow for this. Without losing focus of the study's purpose, and to ensure key aspects of the study were answered, four leading questions were formed and replaced the remainder of the questions asked in the pilot. Lastly, the addition of the audio recording of the interviews was to ensure accuracy and completeness of the transcribed data.

**Transferability and Dependability**

There were no adjustments made to the transferability or dependability of the study presented in chapter 3. As a researcher, the findings provide rich descriptions to allow other researchers to determine transferability to their own studies (Lincoln, 2007). To confirm transferability and dependability, concepts from the research can be by other researchers to any organizational setting by tailoring to their specific areas of focus. The steps outlined in the study allow for the drawing of further conclusions on studies that are motivation-focused by external drivers. Dependability demonstrates that the researcher is able to trace the steps and taken in a documented, and logical manner (Tobin & Begley, 2004).

**Confirmability**

Confirmability can be validated through the data presented. Defined as the degree to which the data and interpretations claimed can be confirmed by other researchers

(Kortsjens & Moser, 2017). Along with paraphrasing and summarization for clarification during the interview, three layers of assurance were presented in the process of discovering of themes: researcher, assistant, and NVivo.

## Results

With the guidance of the primary research question, categorized codes were analyzed and seven distinct themes emerged (See Table 2). Major themes identified from study results included the following:

1. Ambassadors found the role of ambassadorship to be rewarding.
2. Ambassadors were confident the time invested in the program produced value.
3. The decision to be a security ambassador was driven by a personal interest in information security topics.
4. Ambassadors expressed their peers exhibited limited information security knowledge.
5. Ambassadors observed increase interest among their peers from demonstrated knowledge growth through accurate detection and quick alerting.
6. Ambassadors believed printed communication was the least effective form of communication used to generate awareness among their teams.
7. Ambassadors felt organization-published security newsletter topics lacked variety.

Table 2

*Major Themes*

| Theme number | Identified themes |
|---|---|
| 1 | Rewarding |
| 2 | Value |
| 3 | Personal interest |
| 4 | Limited information security knowledge |
| 5 | Increased interest |
| 6 | Communication methods |
| 7 | Topics lacked variety |

Each theme is presented below in greater detail.

**Theme 1: Rewarding**

Positive feelings have a direct link to helping others. Regardless of the size of the contribution, the sense of purpose, meaning, and happiness can be felt by the contributor (Pogosyan, 2018). While meaning and happiness are achievable, they do not necessarily come from the same source. Baumeister (2013) described meaningfulness as the product of giving to others, while happiness comes from what the receiver gives back in return. In the case of security ambassadors, both meaning and happiness is a form of reward. Participants found their ambassadorship to be rewarding, which in turn encouraged them to continue longer than the requested one year commitment originally asked of them. Ambassador 1 stated, “I think I will be an ambassador for as long as I can because it is rewarding to me, and I learn something new all the time.” The same was said by Ambassador 3, “I like helping people and seeing them get it is a really good feeling.” Ambassador 8’s reward was the witnessing of shared excitement, “I can see how excited

my colleagues are when they hear something about the phishing scams in the news, and when they pass the test". Ambassador 17 also witnessed a similar expression:

> I like it when people ask me questions about email scams because I like seeing the look on their faces when I tell them how easy it is to fall victim and how obvious it was to have spotted it when looking back in hindsight. Many of us clicked without thinking and now it seems we pause before we go ahead and open that email. I am really proud of them.

Reward was also a driver for Ambassador 14:

> Having people tell me they learned something or picked up on something they recently learned is such a great feeling. It is incredibly rewarding. I will continue to do my job even if it means overtime, people don't need my help as much.

The same sentiment was shared by Ambassador 6:

> My previous work colleagues would always tell me proudly when they passed one of the phishing tests you guys send out or they'd ask me a question and I would respond with "what do you think" and they would answer correctly.

From responses, we can see ambassadors do not view their contribution as just an obligation to fulfil a duty; ambassadors feel a sense of accomplishment in the form of reward from their output. When digging deeper into the act of contribution, it is possible that as humans, we seek ways to engage in prosocial behaviors. Researchers Weinstein and Ryan (2010) described that the idea of prosocial actions as an attempt to help meet our basic psychological needs: autonomy, competence, and relatedness. In their study, two groups of participants were given money with one group allowed to freely give any

amount to another study participant, while the other group was instructed to give a specific amount. The group that was allowed to freely give any amount of money reported a greater sense of well-being which contributed to satisfying one of their three basic psychological needs.

**Theme 2: Value**

Of all 20 ambassadors interviewed, all expressed confidence that the efforts they invested into the program and the organization's efforts to implement the program produced value. The primary value was the knowledge gained from the learning materials and conference talks provided to them to share with their peers. Additionally, the program produced an unexpected gain as the knowledge was able to be tied to real life experiences to prevent personal loss. Further broken down, the perceived value of the program came from two areas: professional, and personal. In the former setting, ambassadors were able to directly link the program's focus to their work roles once they better understood the importance of data security. Ambassador 11, who worked in program support said, "It has raised our awareness and adds a layer of value in the work we put out. I can see this each time we have a suspicious email or phone call come in". Ambassador 2 also made the connection after becoming an ambassador:

> Being in direct patient care, we don't think about security like we do with PII (Personally Identifiable Information) or PHI (Protected Health Information) but as I thought about it more, I realized that yes, it is important because security is the element within PHI and PII and we have a duty to protect it.

Ambassador 9 saw the value of the program as a way to deliver a higher quality of care to their patients:

> I think what we are doing is adding more to the care we provide. As a provider for many years, we like to think of the physical aspect of what we do for the patient. Now I see being an ambassador as an extension of that care by further protecting our patient's information.

Similar words were echoed by Ambassador 14:

> I have been making it known to my coworkers that this is a level of patient care we do not take into account, and I think it resonates with my group because a connection was made and examples are shown. This really puts things into perspective.

Ambassador 5 saw the overall value of the program for its ability to produce knowledge, "I think this is an excellent program and really happy to have joined. I have learned so much". The same sentiment was shared by Ambassador 7, "If I can sum up my ambassador experience in one word, I will say priceless because it really has been in so many ways. I talk and think about it so much now."

In addition to the value added to caring for patients at the organization, value was also evident beyond its doors. As clearly stated by Ambassador 9, "The knowledge I gained from the learning tools provided to me are valuable and I have used in my life outside of work." In another statement, Ambassador 17 made a similar remark, "I found the topic on vishing to be really interesting and even more so when I actually got one myself. If I recall, the voicemail said I had a car warranty about to expire, but my car is

too old to still have a warranty. Something didn't sound right." Ambassador 16 spoke about their story of how prevalent security-related scams are becoming:

> Later as I became more familiar with security topics, I started to be more aware of security stuff in the news. One was the Target incident. I shop at Target a lot, and learning how valuable info security is, I got really worried about all the ifs and what would happen if someone were to steal my identity. I was talking to my extended family about it at a reunion and sharing with them what I know from being an ambassador. Many of them were clueless on how damaging this is and many didn't think they could ever be affected by it. It is a very scary thing. What are you without your identity, you know?

Ambassador 11 shared how they were a victim of an identity scam, and why action needs to be taken to prevent it:

> This really hits home because I was a victim of identity theft a few years ago and really don't know how it happened. So when I signed up to be an ambassador, I just had to share with my team why I joined and why it is important for us to be aware of things like this. It is very scary.

One astute ambassador (10) knew how interconnected data security is and recognized that not everyone is technologically savvy, so they took the effort to make the connection for them and explained in simpler terms:

> The biggest thing that I have found is that I try to make the information relevant to people in both their personal and work lives because the risks exist in both

> realms. I try to simplify technological concepts or provide easy to understand educational materials.

Ambassador 15 detailed their preventative measures and their attempt to lead by example:

> My family likes to shop on Amazon so you can't escape paying electronically. Some of the things I do are to make sure I log off each time and not keeping my account signed on. At work, we are required to always lock our workstations before walking away, and that is a really good practice because you never know what will happen if it gets into the wrong hands.

The perceived value of the program was unanimous and ambassadors were able to make the connection from concept to reality. The overall message on theme 2 can be succinctly stated through Ambassador 18's words, "The knowledge I gained from the learning tools are valuable, and I have used them in my life outside of work."

**Theme 3: Personal Interest**

While the details might greatly vary between person-to-person, the main driver to join the ambassador program was one that stemmed from a personal interest of information security topics. Personal interest is compelling as it equates to something we care about, or that it is important to us, in either case, both in turn creates a positive feeling toward it. Ambassador 9 expressed great interest on internet security by saying, "I joined because I am passionate about data security and keeping my fellow colleagues up to date with tips and cautions." Ambassador 6 provided a similar message saying, "I don't remember where I saw the recruiting information, but I know it was from there and

I decided to join because I am interested in the topic." Likewise, Ambassador 4 also had interest in information security, and felt the importance of learning more about the topic was a requirement in our modern environment. She said, "I think it is important and almost required that we do this because technology is not going away." Having interest in something is thought of a process that contributes to greater learning and achievement (Harackiewicz & Hulleman, 2010; Hidi, 1990). Further research has supported this finding by clarifying that interest whether situational or personal, all of which are equal contributors to a person's attention, recall, task persistence, and effort (Ainley et al., 2002; Hidi, 1990; Hidi & Renninger, 2006).

**Theme 4: Limited Information Security Knowledge**

Theme 3 highlighted the appeal to join the ambassador program stemmed from personal interest along with already having some degree of security knowledge. Unlike themselves, ambassadors perceived their peers to have little to no security knowledge. Ambassador 1 stated this perception very confidently by declaring, "slim to none." Other ambassadors (11 and 14) respectively concurred, "I think the general consensus is not much." and "I don't think there was much security awareness at all." Ambassadors 6 and 7 expressed respectively just low little they thought their peers understood security, "I don't think any of my teammates know anything about phishing. I actually had to explain what it was" and, "many of them are not remotely aware of these things happening." Ambassador 3 felt similarly, and provided a clearer indicator of their perception of their peers' security knowledge, "I honestly do not know. I would guess very little knowledge prior. If I were to rate my unit's level of email scam knowledge on a scale of 1-10, I

would probably give it a 4 at best." Similar yet, Ambassador 8 stated, "I am certain my coworkers don't fully grasp how much is going on around us and to know that is honestly very frightening." Ambassador 10 provided a glimpse of the vulnerability of their colleagues likely falling victim to a malicious phishing attack, "We had a handful of people that were wise, but the vast majority of our department were very trusting folks who didn't have a critical eye when looking at emails." Some ambassadors see all of this as an opportunity to take on the task of teaching what they have learned. Ambassador 13 expressed their optimism:

> I don't think most of us in my work area know much about technology and its security, which makes me feel that I have a larger role to fill, which I am absolutely okay with that because it was what I signed up for.

It appears that this learning by teaching style may yield a greater level of memory retention and retrieval than learning alone. In a 2018 study by Koh et al. 124 participants were asked to spend ten minutes studying a text on a topic in which none of them had any previous knowledge on. The participants were then divided into four groups. After studying the content given to them, two of those groups taught their learned knowledge to others. One group taught freely without a script, and the other with a script. With the two remaining groups, one was tasked to solve a math problem without the assistance of notes, and the other attempted to solve the same math problem with notes. One week later, all four groups were tested on their memory retention from the prior week. The researchers reported the two groups which relied on information retrieval (teaching freely, and solving a math problem with notes) outperformed the other two that did not

require information retrieval (solving math problem without notes and the other, teaching from a script). From these findings, researchers concluded that retrieval practice promotes the learning benefits of teaching. Koh et al. (2018) pointed out that the findings is not an attempt to undermine teaching, as it has its own specific benefits, it does however demonstrate its importance when considering memory retention of learned information. In the case of the ambassador program where the ambassador is taught then in turn, freely communicate to their peers might be the critical step in promoting behavioral change as memory is better retained for future retrieval. Ambassador 9 sheds light to this very possibility, "I am unsure of the level of security knowledge my colleagues have, but I would guess that they don't have as much before as they do now."

**Theme 5: Increased Interest**

The influence of others is a powerful one. One such type is group polarization where people gravitate to likeminded people to strengthen their viewpoints; we enjoy being around people who share similar beliefs as us. Influence by others is used as a decision on how we choose to navigate our life and most of us follow the principle of social proof (Henderson, 2017). The principal of social proof is the concept in which we look at the people around us to assess how we should take action. Henderson (2017) described social proof as a shortcut on how we decide to act. Social proof is evident in the ambassador program. As stated by Ambassador 1:

> At work, I do know there have been more interest from my work area and I feel it is a combination of alerts we hear about in the news and them knowing that I am knowledgeable on the topic being that I am an ambassador.

Ambassador 12 also witnessed increased interest:

> Do I think my team demonstrates an interest in learning about security? Absolutely. I know a couple times someone would come up to me to ask about stuff they heard on the news and how much they know about it just from the basic information I have shared with our unit. I can tell the gears are moving and that is what we want.

Another ambassador (5) acknowledged a similar occurrence:

> I can see that many are taking security more seriously and that makes me happy because we look out for each other. I think the phishing tests are good reminders for us because this can happen at any time and when someone passes it, I can hear them talk about it with a smile on their face.

Group polarization was evident in another work unit (Ambassador 20):

> We don't always have time to chat because work needs are unpredictable. When we get those phishing tests, it gives us something to talk about. So when someone passes the test, they announce it, and then others respond affirmatively and then someone else talks about another time when they passed the test. I often hear a part of their chatter.

The idea behind the ambassador program is to promote behavioral change to reduce the risk of data loss aided by peer support and content knowledge. From the theme gathered, it is clear that individual interest to learn more about security increased across multiple departments, and further reinforced by the influence of others beyond their ambassador.

**Theme 6: Communication Methods**

Technology has provided us with expanded opportunities in the way we choose to communicate with others. As part of the ambassador program, ambassadors were asked to fulfil a role that allowed them freedom in how they choose to create awareness within their work units. From the content they received through monthly newsletters, emails, in-person and online presentations, it was up to them on how the messages should be delivered to their audience. The premise of the program believed that ambassadors would be more knowledgeable in the receptiveness of their team's communication style more than the program leaders.

Based on interviews collected, Ambassadors felt published articles (printed announcements, posters, etc.) were seen to be the least effective form of communication in promoting awareness within their teams. Ambassador 13 spoke about their experience of this communication method, and expressed the inability of confirming if the content had been read:

> We have a large communal bulletin board. I have on occasion pinned what I thought were interesting topics on the board, but I don't think many see it or care to read it. They just walk by. Maybe they don't even know it is there? Maybe it gets overlooked or later covered with other signs people put up?

The inability to track or gauge audience interaction was also a concern for others. Ambassador 10 also tried to spread awareness through this method, and indicated that it is questionable if the message gets read, "I've also printed out a copy of the newsletter and put it on our area's bulletin board, and hope people will read it." Of those who did try

to communicate this way, ambassadors agreed that printed communication was the least effective means to create awareness among their teams due to the inability to determine if the message gets read.

When comparing their experience with published articles to email messages, ambassadors agreed email was viewed to be a moderately effective way to communicate their message. Many respondents said they used email to distribute to the masses and in turn, opened the door for greater potential communication from the recipient of those messages. Ambassador 5 said:

> I send out communication I receive through our email distribution list and once in a while someone will email back or ask me in person more about it. I usually just default to email and talking about it and it seems to be effective.

Ambassador 13 shared how they used email to educate and to alert all on time-sensitive matters, “Every month when I get the newsletter or major news events or active reported threats, I send an email out to our distribution list.” Email distribution had been used across multiple departments as a way to communicate and to substitute for the delay of organizing a full discussion. Ambassador 19 said, “When I am unable to be added to the meeting agenda, I default emailing to our group’s distribution list.” Ambassador 10 expressed similarly, “If the newsletter comes out after our department huddles, I will do a separate email to the department where I include the newsletter as an attachment and include a bulleted list of the topics covered.”

Based on given responses, one could argue the use of bulletin boards may be equally effective as email because there is no way to track whether or not recipients read

those messages. Even with read receipts, it acknowledges the opening of the email by the recipient, but cannot discern if it was actually read. Ambassador 2 pointed out a possible and logical explanation that email still does have the advantage, over posters and bulletin board, “They [recipients] know who to ask because the emails have an address they can quickly reply back to for questions.” Responses point favorably to email as a means for ambassadors provide an alternate way to create awareness among their teams.

Verbal communication appeared to be the most favorable means to drum up awareness according to ambassadors. Ambassador 2 asserted, “It might work for other groups, but I know having conversations is more productive in my group. I know this because they start asking questions and some even give advice on what they know.” Another ambassador (8) witnessed the same phenomenon, “It has people talking and that helps to raise the awareness we need.” Ambassador 7 went by personal preference, and the speed of delivering through word of mouth, “I generally like to talk about things that are happening when they happen.”

With the various communication methods available to them, almost all of the interviewed ambassadors chose to verbalize to some degree or another than to put the communication in writing, and if in writing, most preferred to email than to print and post. Many chose to verbalize at their work unit or department meetings with talking points taken from the Security Ambassador published content materials distributed to them. Such is the case for Ambassador 20, “I always try to share new tips I have taken from the program teachings to our monthly team meetings.” Likewise with Ambassador 14:

> I like talking to people so these security tips I get from the [Ambassador Program] emails give me topics and helps to build rapport with others that I might not normally talk to or as often. I make sure to bring these topics up at our staff meetings when I am able and people really have concerns about what is happening and they too want to do something about it. I tell them the best way to defend yourself against the bad guys is to be educated on threats and to spread the word.

Ambassador 3 as well:

> When the timing is right, like when I get a new security bulletin and an upcoming department meeting is approaching, I ask my manager if they have a few minutes for me to be added to the agenda. I think this is the best way to get the message to everyone and you know there will always be someone in the audience asking the one question most of us are too afraid to ask or think people might think it is a dumb question. Asking how to stay safe online these days is a valid question and should be taken seriously.

Ambassador 5 also used this approach on a regular basis:

> The only time I delay items is if they come out right before a team meeting in which I will delay so that we can share them verbally. Doing this way gives me time to better explain to our unit and allow for them to ask me questions, and if I don't have the answer, I know where to go to get it.

Ambassadors favored heavily on creating awareness through verbal communication and it appears that there might be some scientific support behind their

choice. The concept of teaching through dialog is a contrast to traditional teacher-presentation teaching style. Dialogic teaching is an approach between teacher and student(s) with back and forth conversation on a given topic. The University of Cambridge, UK (n.d.) sees this style of teaching as being able to elicit "common sense perspectives" from the learner, aid in the developing of idea to overcome misunderstandings, and allow for exploration of the perceived limits of their ideas. This teaching style engages between student and teacher to explain and clarify ideas, and help grasp new concepts rather than to simply listen to the idea presented to them.

In summary, ambassadors do choose to deliver content they think is important to their mission on a consistent basis however the mode of communication varies. Primarily driven by timing and departmental considerations, the availability to deliver the message in the manner in which they prefer at times may need to be delayed. To avoid not communicating the messages at all, in particular time-sensitive matters, ambassadors resort to a secondary option such as print or email until they are able to deliver verbally and answer questions.

**Theme 7: Topics Lacked Variety**

In this final theme, ambassadors were asked to provide any feedback they may have to better improve the ambassador program. The general consensus gave praise to the program by recommending the continuation of the program and expressed their hope that more ambassadors join in the future. There was one suggestion that seemed to be shared among those who offered room for improvement and that was the lack of topic variety in their teaching content. Ambassador 1 paved the way by saying, "In the early days of

taking on this role, I thought the security tips were interesting; exciting actually."

Ambassador 5 also shared the excitement downward trend:

> When I was new to this, each message I got, I was very excited to read about and would send and discuss with my team. I think I am losing steam for two reasons. One, I have been doing this for several years and it seems that the same topics keep coming back. I wish they would come out with new topics but then again, it must be the same issues keep on resurfacing out there.

Ambassador 13 experienced the same and offers more insight as the likely cause:

> I think there should be more variety in the topics they write about. I get it that phishing is super common but I know there are other equally scammy things going on in the web. I don't know what those specific topics would be but I would encourage the author or authors of the newsletters to widen their research because I would be very interested to hear more about how we can help.

Ambassador 16 would like to see more technical content:

> I would say the materials they share with us should be more complex. Instead of telling us what phishing is or what spam is, I want for them to give more technical background behind some of these articles. I like to think I'm somewhat of techie person, and I think these stories would be way more interesting to hear about. I know not everyone is techie and I think they would add some of it in there for people like me who do like it. But definitely keep the other stuff too.

Ambassador 8 expressed the desire to receive information that is not so localized, "I would like to see topics from all over the world. We can know and then share to show

what is really going on out there." The same ambassador went on to note the possible cause, "One thing I did pick up on is that the writers tend to use the same sources, it wouldn't hurt to capture a wider range." Ambassador 9 felt not enough information is being provided and would welcome a greater volume of content from the program, "It wouldn't hurt to give us more information whether it is in email or whatever way they would like to use because in some way, it is useful to all of us."

Addressing the lack of content variety should be on the forefront of the program leaders to ensure ambassador interest does not wane.

The concept of boredom is an interesting one. Contrary to the notion that boredom is simply the opposite of interest, boredom is the absence of interest along with emotional distress (Daschmann et al., 2014; Pekrun et al., 2010). As expressed by ambassadors, the teaching content provided to them on a regular basis lacked variety which can result in monotony. According to Toohey (2012), monotony plays a large role in boredom as it focuses on repetition and causes mental fatigue. Actions or experiences that are repetitious and predicable become boring.

In regard to discrepant cases from the study, all but one ambassador expressed or implied support of their efforts from their department's leadership through their positive responses outlined in theme 1. Ambassador 6 however expressed otherwise:

> Since I joined, I don't have much support from my manager to be an ambassador and it is very frustrating because I know it is our duty to protect and by not having this support implies that they don't see the value in it.

In addition to the expressed value of the program, Ambassador 6 conveyed enjoyment, reward, and continued desire to fulfil the role in future job opportunities under a new, more supportive manager:

> I really enjoy helping people out and knowing that I've helped spread the word by having people come to me with questions related to info security, even with their home PCs and cell phones. My previous work unit colleagues would always tell me proudly when they passed one of the little phishing tests or they'd ask me a question and I would respond with "what do you think" and they would answer correctly. I am hoping my next work unit will be more open to me filling the role again. For now, I just read the newsletters and bulletins to keep up on things.

When comparing this ambassador's experience to others, it is evident that program success involves support from leadership to promote awareness and the desired change. In contrast, Ambassador 2 stated, "I can see my manager is also interested in this stuff and comes to me with questions, as do others in my workgroup." Ambassador 1 also shared how their department perceives value by actively supporting their efforts, "I send it to the ambulatory managers for inclusion in their newsletters and to my department colleagues who then pass it on to newsletters in other areas." In this research, the single discrepant case out of 20 is not enough to reevaluate the study's conclusion of themes therefore this discrepant case has been disregarded.

## Summary

For this study 20 security ambassadors were interviewed; collected data was coded, categorized, and analyzed which ultimately yielded seven distinct themes. Each of

these themes were outlined and discussed along with a discrepant case analysis. Seven major themes identified through the analysis were: rewarding, value, personal interest, limited information security knowledge, increased interest, communication methods, and topics lacked variety. In chapter 5, I will present an interpretation of findings, limitations and recommendations will also be discussed based on the study's strengths and its confines. Implications of the study will detail how findings may promote social change at the organizational level. Lastly, recommendations will be given for future practice.

# Chapter 5: Discussion, Conclusions, and Recommendations

Phishing continues to increase in health services and other business institutions. The prevalence of phishing is a current issue organizations face (Anti-Phishing Working Group, 2017). As pointed out by Fraley and Cannady (2017), phishing is on the rise and can lead to significant changes to the cybersecurity landscape, and machine learning must be leveraged to combat it. The belief that the solution to the problem can be handled by a technological tool neglects the human awareness component (Cofense, 2018). The purpose of this qualitative study was to understand the lived experiences of security ambassadors as they try to motivate their peers to increase phishing detection at their organization. The aim of this phenomenological research was to gain a clearer perspective on how security ambassadors promote security awareness among their work groups from the information provided to them by the organization's ambassador program. By listening to what these ambassadors had to say, I was able to achieve a richer understanding of their experiences through their own words. Seven major themes were identified through the data analysis:

1. Rewarding: Ambassadors found the role of ambassadorship to be rewarding.
2. Value: Ambassadors were confident the time invested in the program produced value.
3. Personal interest: The decision to be a security ambassador was driven by a personal interest in information security topics.
4. Limited information security knowledge: Ambassadors expressed that their peers exhibited limited information security knowledge.

5. Increased interest: Ambassadors observed increased interest among their peers from demonstrated knowledge growth through accurate detection and quick alerting.
6. Communication methods: Ambassadors believed printed communication was the least effective form of communication used to generate awareness among their teams.
7. Topics lacked variety: Ambassadors felt organization-published security newsletter topics lacked variety.

## Interpretation of the Findings

The themes from the study provided evidence of how people are influenced, and that their motivations are deeply rooted in their lived experiences, knowledge, and perceptions. The following sections provide greater detail regarding the connection between the literature and the themes from the current study.

### Theme 1: Rewarding

Ambassadors felt rewarded by their work, and because of this they chose to contribute longer than the requested 1-year commitment originally asked of them. Because the ambassadorship is a voluntary role without financial or role incentive, drivers to perform and to perform well came from an internal source. In a study by Brown, Meer, and Williams (2018), volunteers placed more significance on the gift of time than on the financial exchange even when it resulted in being more costly to the volunteer to do so. The example used in Brown et al.'s study was a consultant who made $100 an hour who could donate that money, but instead they chose to donate their time in

a soup kitchen. This display of altruism led to a greater sense of contribution and satisfaction than donating money.

**Theme 2: Value**

Value is a perception and is the product of exchange between the benefit of gain and the sacrifice of an offering (Heinonen, 2004). Value can be made through connections between what is being taught and then applied to day-to-day applications (Heinonen, 2004). Ambassadors in the current study linked the program's focus to their work roles once they better understood the importance of data security and their peers were able to use the information provided to them in relatable scenarios. According to Ramsey (2000), nurses were able to learn from others through storytelling as a way to encourage new staff members to reinforce the importance of providing nursing care to the most critically ill patients so that they can achieve expertise.

**Theme 3: Personal Interest**

The decision to participate in the ambassador program was from a personal interest of information security topics and had no direct ties to participants' professional job roles. This interest fueled their motivation to join. The influence of personal interest can have profound effects. According to Harackiewicz, Durik, Barron, Linnenbrink-Garcia, and Tauer, (2008), a person who sees a painting and is captivated by it will pay more attention to its details and will be more likely to reengage over time. When a person participates in an activity based on interest, the interest then becomes a source of self-expression (Amabile, 1993).

**Theme 4: Limited Information Security Knowledge**

Knowledge sharing is seen as an indispensable component in organizations to facilitate creativity and innovation leading to value creation and quality solutions (Wang & Noe, 2010). Ambassadors perceived their peers to have little to no security knowledge, and felt that there were significant benefits to educate them through knowledge sharing. Knowledge sharing occurs when team leaders are actively practicing and promoting knowledge (Srivastava, Bartol, & Locke, 2006). Because knowledge sharing does not occur automatically, ambassadors actively engage often with their teams in various methods and again upon receiving new teaching content or security alerts.

**Theme 5: Increased Interest**

Trust plays an important role when organizations implement knowledge-sharing techniques because vulnerabilities can surface. Through the ambassador program, one person leads by example, and trust forms among teams because knowledge sharing requires interdependence and collaboration (Mayer, Davis, & Schoorman, 1995). Ambassadors in the current study were able to achieve this momentum by creating an inclusive environment within their workgroups, which allowed the support for learning and change to occur.

**Theme 6: Communication Methods**

According to Giri (2006), communication and culture influence one another and offer members an unspoken directive on how to behave and communicate within that culture. Ambassadors in the current study were given the freedom to choose how they would like to educate others. By doing so, they were able to experiment with different

communication methods to determine which was the most effective and which did not support their team's culture. For certain groups, there were multiple communication methods implemented, and each was based on the group's communication culture and on the needs of the message being communicated.

**Theme 7: Topics Lacked Variety**

Many ambassadors reported the educational content delivered to them lacked variety, but expressed understanding that the content was likely driven by current threats. Research indicated that variety-seeking behavior is a common occurrence among people when choices are available. Ratner, Kahn, and Kahneman (1999) reported that when a person is given the opportunity to choose between their favorite item and a less desirable one, there is a preference to alternate between the two options. Further exploring this idea, Ratner and Kahn (2002) found that when decisions were made for others, there was a greater likelihood for variety than when people made decisions for themselves.

In the area of human motivation, the current study findings corroborated those from peer-reviewed literature regarding how observed and strategically learned behaviors may contribute to learning in a group setting. Ambassadors in the current study described how excitement within the team was visible, which reinforced the desired behavior and provided the momentum to keep going. This finding had twofold implications. The displayed excitement reinforced ambassadors to continue teaching and to continue to lead by example. The other implication was the security threat landscape. Previous studies indicated that the lack of knowledge or recognition of security indicators is a significant contributor to security scams (Marforio, Masti, Soriente, Kostiainen, & Capkun, 2015).

Ambassadors in the current study provided knowledge regarding how to stay protected when online, and the phishing simulator sent out at random provided the means to test that knowledge. Through these two learning tools, team members were able to identify a phish, and some were able to take that learning and extend it to real-life situations.

The JCM theory addresses the drivers needed to create motivation within individuals. In this theory, three factors must be present: the meaningfulness of the work being performed, responsibilities expected from the person, and the knowledge of outcomes. Within these three areas, the following five characteristics also have to occur: skill variety, task identity, task significance, autonomy, and job feedback (Hackman & Oldham, 1976). According to findings in the current study, all five areas within the three characteristics were targeted and reached by the ambassadors. Individuals interested in signing up for ambassadorship were given the necessary information to determine whether this was a commitment they were able to make (see Appendix A). According to the JCM theory, the three areas were targeted and met.

**Meaningfulness of the Work Being Performed**

Supporting Themes 1 (rewarding) and 2 (value), the program provided a purpose for ambassadors to show why they are critical to the success of the program. Ambassadors will aid in the protection of patient data and personal and private business information through teaching and practice.

**Expected Responsibilities**

Supporting Theme 3 (personal interest), one of the first qualifiers to consider becoming an ambassador is a person who is passionate about security. To someone

uncertain about whether to take on the role, the word *passionate* should steer them away; however, to those who feel strongly about security and to help the organization protect its data, this term would further capture their interest. The study site program information also outlines what an ideal ambassador can expect to do by helping promote awareness and adherence to the organization's security best practices and the time requirements to do so.

**Knowledge of Outcomes**

Supporting Themes 2 (value) and 5 (increased interest), ambassadors knew the effects of their work. They knew their reach would be far, they would lead by example, and they would gain valuable information regarding the health care industry's greatest security issues. Five task characteristics of the JCM theory within the ambassadorship were identified. Faturochman (1997) defined these task characteristics as follows: skill variety, task identity, task significance, autonomy, and job feedback.

**Skill Variety**

Supporting Theme 6 (communication methods), skill variety is the degree to which a job requires a variety of different activities in carrying out the work, involving the use of a number of different skills and talents. Ambassadors were given security topics that were of importance to the organization, which they were then tasked to either receive or deliver. Such tasks ranged from forwarding critical security alert emails to their coworkers to participating in educational webinars.

**Task Identity**

Supporting Themes 4 (lack of security knowledge) and 6 (communication methods), task identity is the degree to which a job requires completion of a whole, identifiable piece of work; that is, doing a job from beginning to end with visible outcome. Ambassadors are given security-focused content on a regular basis to distribute. In their process of doing so, they must first determine how much of the content their peers already know and how to best convey the message clearly and easily. Ambassadors then followed up with questions asked by their audience.

**Task Significance**

Supporting Theme 2 (value), task significance is the degree to which the job has a substantial impact on the lives of other people. This characteristic was quite possibly the most clearly defined contribution in their ambassadorship. Ambassadors in this study are patient care providers regardless if they interact with patients or not. Their industry made them all patient care providers in varying degrees. Like their peers, they all have a responsibility to protect patient and business information. Ensuring patient information remains in the hands of the organization, they are making a direct contribution to protecting the patient and the organization.

**Autonomy**

Also supporting Theme 6 (communication methods), autonomy is the degree to which the job provides substantial freedom, independent, and discretion to the individual in scheduling the work and in determining the procedure to be used in carrying it out. Ambassadors are credited to be the most knowledgeable in knowing how to best

communicate with their peers. For this reason, they are given full control on how and when they choose to distribute their message.

**Job Feedback**

Supporting Theme 1 (rewarding), job feedback is the degree to which carrying out the work activities required by the job provides the individual with direct and clear information about the effectiveness of his or her performance. One predominate theme documented in Chapter 4, was feedback received in the form of feeling rewarded through their colleagues' smiles and expressed interest.

The JCM theoretical framework is based on the belief that tasks alone are viewed as an obligation and stifles motivation. When a job is enriched by variety, autonomy, and has a degree of decision authority, the motivation increases and yields greater productivity. The single most distinct sign of motivation exhibited by ambassadors was in their choice to contribute longer than their one year program commitment.

When the program was implemented in 2015, phishing detection accuracy has been trending in an upward direction and continues to do so even as the total numbers of simulated emails sent have also increased. In Figure 1, from years 2015 to 2019, the total average simulated phishing emails sent by the organization increased by 8.1%, with a 3.4% and 4.5% growth between each reported year since the program's implementation.

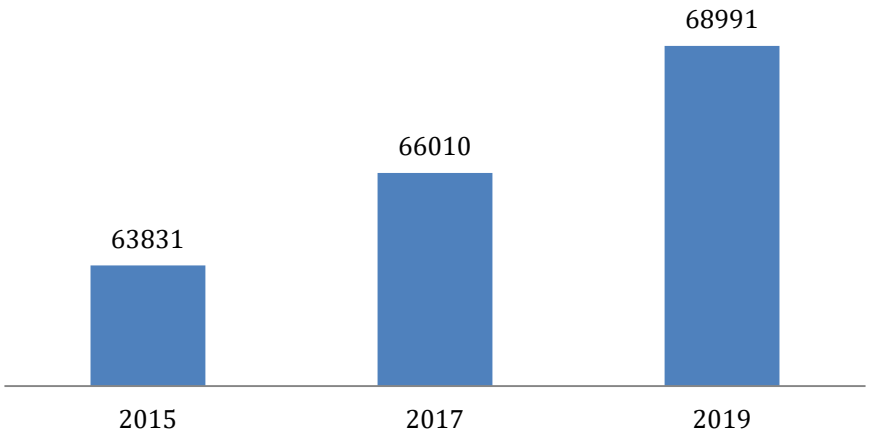



*Figure 1*. Total average simulated phishing emails sent by year.

Phishing detection accuracy through the simulation tool has also seen significant growth. Phishing detection occurs when a simulated phishing email has been received by the recipient who then determines by learned visual cues, and reports it as phishing via the phishing reporter button. Since the program's launch in 2015, the report rate accuracy had increased by 9.7%. Between 2015 and 2017, there was a 3.9% increase and additional increase of 4.1% from 2017 to 2019 (See Figure 2).

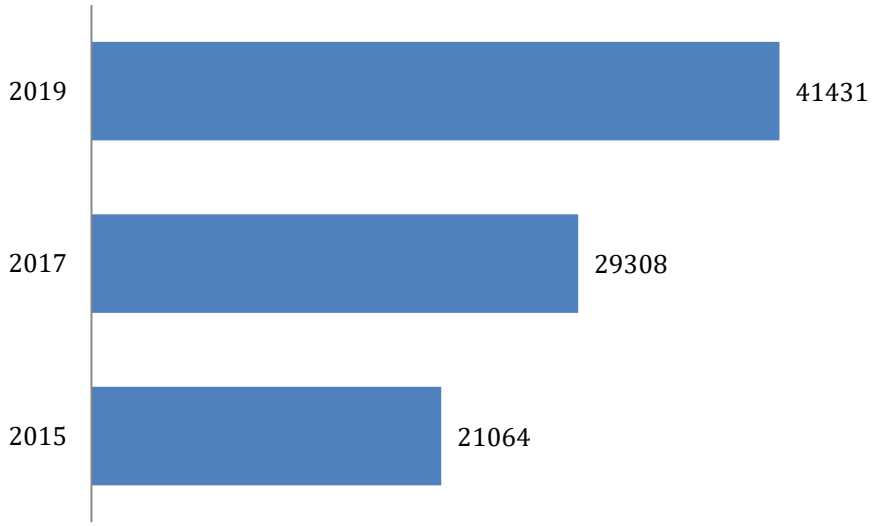



*Figure 2*. Total average simulated phishing detection accuracy by year.

## Limitations of the Study

Limitations exist in this study and should be considered when evaluating and drawing conclusions from its findings as well as generalizing findings. Firstly, phishing is an ever-evolving threat and the findings are based on those current threats. As with all phenomenological research, the current experiences are only for that given time and for that particular. This exact experience is not something that is identically reproducible. Secondly, limitations from this study are the ambassador themselves. Each participant has been an ambassador since the start of the program in 2015, while their responses provided valuable insight, there is no way to assess if motivation continues if the ambassador leaves the program without a replacement.

This study explored a modern issue concerning information security and the valuable data that can be taken from people and businesses. With all the security tools available claiming to prevent data loss, other researchers have shown that no matter how

sophisticated technology becomes, it simply cannot replace the human factor. The focus of this research was to look at how pairing a preventative technological tool with people-led motivation created the precise mix of awareness and behavioral change needed to safeguard electronic data. The study's strength is in its ability to translate established theory into current practice on a modern situation with contemporary tools.

## Recommendations

Based on the research findings, current and future healthcare and business leaders should consider the human contributors when developing a security awareness plan, and to not only rely on technology as a gap exists.

Secondly, leaders should welcome the power of team and self-led motivation. Specific recommendations would include (a) allowing a degree of autonomy by the task performer, (b) provide significance of the task being asked to perform, and (c) to provide job feedback as it acknowledges recognition of their performance.

Lastly, future research should study how behavior deviates from acquired behavior when the presence of the main driving motivator has been removed as the current study only looked at acquiring learned behavior and not its extinction.

## Implications

Potential impact for positive social change from this study would benefit schools, businesses, health administration research and practice that wish to be proactive rather than reactive by applying their most valuable asset- the people. The Ponemon Institute is a research center committed to privacy, data protection and information security policy, and in their report, businesses average 130 security breaches a year and if not addressed

properly, severe threats can lead to an event that is extremely damaging to the business. Examples of areas that can be impacted by a breach include: loss of strategic information, increased cost of capital, damage of reputation, and regulatory penalties. The average cost to mitigate a malware attack cost companies on average of $2.4 million annually and takes an average of 50 days to resolve the attack (Ponemon Institute, 2017). In the same report, security experts highlighted the need for businesses to implement innovative techniques to aid in the control of breaches, and to simply rely on technology to meet compliance is not enough to increase security. Businesses should take the advice of experts from the report and implement a program similar to the ambassador program as a way to apply innovative techniques to solve a complex problem. Following the research study findings, this solution is able to generate the highest return (reduced phishing susceptibility) with the lowest financial investment (2-3 hours per month commitment from ambassadors). Schools have a greater benefit as the core of the ambassador program is to motivate and educate. Schools can implement an ambassador program on data protection for staff and to age-specific students. The same application can be applied for subject-specific learning. Quantitative validation of subject-specific learning through the ambassador program can be in the form of classroom, school, to district-wide test results. The ambassador platform does not need to be a complex program for organizations to implement nor must it evolve around data protection as the idea behind it is steered by environmental drivers.

A theoretical implication of this study is the reduction of data compromise when organizations shift their data protection approach to a more human-based solution. In a

recent RSA conference publication (2019), the dollars spent on security tools was staggering:

> In addition to the 141 percent increase in overall budgeting since 2010, cybersecurity spending has increased around the world and across industries. The top cyber spending area worldwide is on security services, as many companies and consumers are increasingly nervous after the recent data breach scandals. Spending on security services has reached $64.2 million in 2019. Also this year, spending on infrastructure protection is at $15.3 million, and companies have spent $13.2 million on network security equipment.

The research outlined in this study suggests otherwise. Heavier emphasis should be on the people who are in front of the screen than what is inside the device to protect data. Businesses may have difficulty fully adopting this mindset as there is a multitude of software companies claiming to have better detection tools than their competitors to solve data protection needs, yet their marketing still focuses on technology-only solutions. According to one of the nation's top security expert, companies might have good intentions by boosting budgets on security but it is spent in the wrong areas (Morgan, 2019). The recommendation is not to suggest businesses drop all technological efforts to tackle security issues, as these tools do aid in the prevention and detection. Tools however can only do so much. As an alternative, businesses should place more resources in training, and trust in their staff to make more informed decisions.

## Conclusion

In this study, the value of the ambassador program produced high value results with minimal associated costs in helping to keep an organization stay protected against security threats. The perceived value of program was based on intrinsic drivers by both ambassadors and their peers. Ambassadors' desires to motivate were established in their perceived level of contribution to the larger picture of protecting the organization against business data loss, breach of HIPAA, and all other patient/client privacy violations. As a result, their perceived success of their committed efforts was a sense of reward though recognition and observation of their peers. In summary, I have outlined how the application of an ambassador program can produce high value results because those involved become invested in the program instead of perceiving additional responsibilities as an obligatory task asked of them. The results of this study may contribute to positive social change as it empowers those involved to feel a sense of ownership and personal responsibility in their contributions in the protection of client/patient privacy in all health care environments.

# References

Agger, B. (2012). *Oversharing: presentations of self in the internet age*. New York: Routledge.

Ainley, M., Hidi, S., & Berndorff, D. (2002). Interest, learning, and the psychological processes that mediate their relationship. *Journal of Educational Psychology*, *94*(3), 545–561. doi.org/10.1037/0022-0663.94.3.545

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *Int. J. Human-Computer Studies*. doi.org/10.1016/j.ijhcs.2015.05.005

Amabile, T. M. (1993). Motivational synergy: Toward new conceptualizations of intrinsic and extrinsic motivation in the workplace. *Human Resource Management Review, 3,* 185-201. doi.org/10.1016/1053-4822(93)90012-S

Anti-Phishing Working Group. (2017). Phishing activity trends report 4th Quarter 2016. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

Arachchilage, N., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312. doi:10.1016/j.chb.2014.05.046

Ashraf, S. (2005). Organization need and everyone's responsibility: Information security awareness. *SANS Institute*. Retrieved from http://www.giac.org/paper/gsec/4340/organization-everyones-responsibility-information-security-awareness/107113

Bandura, A. (1977). *Social learning theory*. New York, NY: General Learning Press.

Baumeister, R. F., Vohs, K. D., Aaker, J. L., & Garbinsky, E. N. (2013) Some key differences between a happy life and a meaningful life. *Journal of Positive Psychology*, *8*(6), 505-516. doi:10.1080/17439760.2013.830764

Benenson, Z., Gassmann, F., & Landwirth, R. (2017). Unpacking Spear Phishing Susceptibility. Financial Cryptography and Data Security Lecture Notes in Computer Science, 610–627. doi: 10.1007/978-3-319-70278-0_39

Boyd, R., & Richerson, P. J. (2009). Culture and the evolution of human cooperation. Philosophical Transactions of the Royal Society B: *Biological Sciences, 364*(1533), 3281–3288. doi: 10.1098/rstb.2009.0134

Brown, A. L., Meer, J., & Williams, J. F. (2018). Why Do People Volunteer? An Experimental Analysis of Preferences for Time Donations. *Management Science, 65*(4), 1455–1468. doi: 10.1287/mnsc.2017.2951

Bucci, S. (2009). The confluence of cybercrime and terrorism. The Heritage Foundation, Retrieved from https://www.heritage.org/defense/report/the-confluence-cyber-crime-and-terrorism

Carcary, M. (2009). The research audit trial: Enhancing trustworthiness in qualitative inquiry. *Electronic Journal of Business Research Methods, 7*(1), 11-24. Retrieved from https://www.researchgate.net/publication/228667678_The_Research_Audit_Trial-Enhancing_Trustworthiness_in_Qualitative_Inquiry

Carey, K. B., Lust, S. A., Reid, A. E., Kalichman, S. C., & Carey, M. P. (2016). How mandated college students talk about alcohol: Peer communication factors

associated with drinking. *Health Communication*, *31*(9), 1127-1134. doi:10.1080/10410236.2015.1045238

Center for Innovation Research and Teaching. (n.d.). Strengths and limitations of phenomenology. Retrieved from https://cirt.gcu.edu/research/developmentresources/research_ready/phenomenology/strengths_limits

Cerasoli, C. P., Nicklin, J. M., & Ford, M. T. (2014). Intrinsic motivation and extrinsic incentives jointly predict performance: A 40-year meta-analysis. *Psychological Bulletin, 140*(4), 980. doi.org/10.1037/a0035661

Chakraborty, R., Vishik, C., & Rao, H. R. (2013). Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decision Support Systems*, *55*(4), 948-956. doi.org/10.1016/j.dss.2013.01.004

Cho, Y. J., & Perry, J. L. (2012). Intrinsic motivation and employee attitudes: Role of managerial trustworthiness, goal directedness, and extrinsic reward expectancy. *Review of Public Personnel Administration 32*(4), 382-406. doi.org/10.1177/0734371X11421495

Cofense (2018). Phishing Awareness Training: Phishing Email Simulation. Retrieved from https://cofense.com/product-services/phishme/

Creswell, J. (1998). *Qualitative inquiry and research design: Choosing among five traditions*. Thousand Oaks, CA: Sage.

Creswell, J. (2013). *Qualitative inquiry and research design: Choosing among five*

*approaches.* Los Angeles, CA: SAGE.

Daschmann, E. C., Goetz, T., & Stupnisky, R. H. (2014). Exploring the antecedents of boredom: Do teachers know why students are bored? *Teaching and Teacher Education*, *39*, 22-30. doi:10.1016/j.tate.2013.11.009

Deci, E. L., & Ryan, R. M. (2012). Self-Determination Theory. *Handbook of Theories of Social Psychology: Volume 1*, 416–437. doi: 10.4135/9781446249215.n21

Deloitte. (2013). Blurring the lines: 2013 TMT global security study. Retrieved from https://www2.deloitte.com/na/en/pages/technology-media-and-telecommunications/articles/2013-tmt-global-securitystudy.html

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI 06*. doi: 10.1145/1124772.1124861

Elliott, V. (2018). Thinking about the Coding Process in Qualitative Data Analysis. *The Qualitative Report, 23*(11), 2850-2861.Retrieved from https://nsuworks.nova.edu/tqr/vol23/iss11/14

Faturochman (2016). The Job Characteristics Theory: A Review. Retrieved from https://pdfs.semanticscholar.org/3694/829c985349fa423e535681264b2218eef6de.pdf?_ga=2.68655959.735046617.1585167098-1289694345.1581012195

Federal Trade Commission. (n.d.). How to Recognize and Avoid Phishing Scams. Retrieved from https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Flick, U. (2014). *An introduction to qualitative research*. Los Angeles: SAGE.

Ford, M., Wentzel, K., Wood, D., Stevens, E., & Siesfeld, G.A. (1990). Processes associated with integrative social competence: emotional and contextual influences on adolescent social responsibility. *Journal of Adolescent Research, 4*, 405-425. doi.org/10.1177/074355488944002

Fraley, J. B., & Cannady, J. (2017). The promise of machine learning in cybersecurity. *SoutheastCon 2017*. doi:10.1109/secon.2017.7925283

Gardner, M. & Steinberg, L. (2005). Peer influence on risk taking, risk preference, and risky decision making in adolescence and adulthood: an experimental study. *Developmental Psychology, 41*(4), 625-635. doi:10.1037/0012-1649.41.4.625

Gergely, G., Bekkering, H., & Király, I. (2002). Rational imitation in preverbal infants. Nature, 415(6873), 755–755. doi: 10.1038/415755a

Gibbs, G. (2018). *Analyzing qualitative data*. Los Angeles: Sage.

Giri, V.N. (2006) Culture and Communication Style, *Review of Communication, 6*:1-2, 124-130, doi:10.1080/15358590600763391

Hackman, J. R., & Oldham, G. R. (1976). Motivation through the design of work: test of a theory. *Organizational Behavior and Human Performance*, *16*, 250-279. doi.org/10.1016/0030-5073(76)90016-7

Hackett, P. (2015). *Qualitative research methods in consumer psychology: ethnography and culture*. New York: Routledge.

Hadi, R. & Adil, A. (2010). Job characteristics as predictors of work motivation and job satisfaction of bank employees. *Journal of the Indian Academy of Applied*

*Psychology, 36* (2), 294-299. Retrieved from https://psycnet.apa.org/record/2011-19930-015

Harackiewicz, J.M. Durik, A.M., Barron, K.E., Linnenbrink-Garcia, L., Tauer, J.M. (2008). The role of achievement goals in the development of interest: Reciprocal relations between achievement goals, interest, and performance. *Journal of Educational Psychology*. 100:105–122. doi:10.1037/0022-0663.100.1.105

Harackiewicz, J. M., & Hulleman, C. S. (2010). The Importance of Interest: The Role of Achievement Goals and Task Values in Promoting the Development of Interest. *Social and Personality Psychology Compass*, *4*(1), 42–52. doi: 10.1111/j.1751-9004.2009.00207.x

Haun, D. B. M., & Tomasello, M. (2011). Conformity to Peer Pressure in Preschool Children. *Child Development, 82*(6), 1759–1767. doi: 10.1111/j.1467-8624.2011.01666.x

Hayes, S., Shore, M., & Jakeman, M. (2012). The changing face of cybersecurity. ISACA Journal, 6, 1-8. Retrieved from https://gattonweb.uky.edu/Faculty/Payne/ACC624/8-ISACA%20-%20The-Changing-Face%20of%20Cybersecurity.pdf

Heinonen, K. (2004), "Reconceptualizing customer perceived value: the value of time and place", *Managing Service Quality: An International Journal*, *14*(2/3), 205-215. doi.org/10.1108/09604520410528626

Henderson, R. (2017). The science behind why people follow the crowd: Why do people influence us so much? *Psychology Today*. Retrieved from

https://www.psychologytoday.com/us/blog/after-service/201705/the-science-behind-why-people-follow-the-crowd

Hidi, S. (1990). Interest and Its Contribution as a Mental Resource for Learning. *Review of Educational Research*, *60*(4), 549–571. doi: 10.3102/00346543060004549

Hidi, S., & Renninger, K. A. (2006). The Four-Phase Model of Interest Development. *Educational Psychologist*, *41*(2), 111–127. doi: 10.1207/s15326985ep4102_4

Hootsuite. (2018). Social media trends. Retrieved from https://hootsuite.com/research/social-trends

Issac, B., Chiong, R., & Jacob, S. M. (2014). Analysis of phishing attacks and countermeasures. Retrieved from https://arxiv.org/ftp/arxiv/papers/1410/1410.4672.pdf

Kent State University. (2020). Statistical & qualitative data analysis software: About NVivo. Retrieved from https://libguides.library.kent.edu/statconsulting/NVivo

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing Detection: A Literature Survey. *IEEE Communications Surveys & Tutorials*, *15*(4), 2091–2121. doi: 10.1109/surv.2013.032213.00009

Koh, A. W. L., Lee, S. C., & Lim, S. W. H. (2018). The learning benefits of teaching: A retrieval practice hypothesis. *Applied Cognitive Psychology*, *32*(3), 401–410. doi: 10.1002/acp.3410

Korolov, M. (2016). Companies that can help you fight phishing. CSO Online. Retrieved from https://www.csoonline.com/article/3066532/phishing/10-companies-that-

can-help-you-fight-phishing.html

Korstjens, I., & Moser, A. (2017). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120–124. doi: 10.1080/13814788.2017.1375092

LeCompte, M. D., Preissle, J., Tesch, R., & Goetz, J. P. (2008). *Ethnography and qualitative design in educational research*. Bingley, U.K.: Emerald Group Pub.

Lincoln, Y. S. (2007). Naturalistic Inquiry. *The Blackwell Encyclopedia of Sociology*. doi: 10.1002/9781405165518.wbeosn006

Lunenburg, F.C. (2011). Self-efficacy in the workplace: implications for motivation and performance. *International Journal of Management, Business, and Administration, 14*(1). 1-6. Retrieved from http://www.nationalforum.com/Electronic%20Journal%20Volumes/Lunenburg,%20Fred%20C.%20Self-Efficacy%20in%20the%20Workplace%20IJMBA%20V14%20N1%202011.pdf

Marforio, C., Masti, R.J., Soriente, C., Kostiainen, K., Capkun, S. (2015). Personalized security indicators to detect application phishing attacks in mobile platforms. Retrieved from https://arxiv.org/abs/1502.06824

Marshall, C., & Rossman, G. B. (2011). *Designing qualitative research*. Thousand Oaks, CA: SAGE.

Mason, M. (2010). Sample Size and Saturation in PhD Studies Using Qualitative Interviews. Qualitative Forum: *Qualitative Social Research, 11*(3). Retrieved from http://www.qualitative-research.net/index.php/fqs/article/view/1428/3028

Mayer, R. C., Davis, J. H., & Schoorman, F. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), 709-734. doi: 10.2307/258792

Mills, A., Durepos, G., & Wiebe, E. (2010). Encyclopedia of case study research. Retrieved from https://www.jstor.org/stable/258792

Miniwatts Marketing Group. (2018). Internet users in the world by regions. Retrieved from https://www.internetworldstats.com/stats.htm

Morgan, S. (2019). Global security spending predicted to exceed $1 trillion from 2017-2021. Retrieved from https://cybersecurityventures.com/cybersecurity-market-report/

Morse, J. M. (1994). Designing funded qualitative research. Automatic coding in document sources. Retrieved from http://helpnv11.qsrinternational.com/desktop/procedures/automatic_coding_in_document_sources.htm

Patton, M. Q. (2001). Qualitative Evaluation and Research Methods (2nd Edition). Thousand Oaks, CA: Sage Publications.

Pekrun, R., Goetz, T., Daniels, L. M., Stupnisky, R. H., & Perry, R. P. (2010). Boredom in achievement settings: exploring control value antecedents and performance outcomes of a neglected emotion. *Journal of Educational Psychology*, *102*(3), 531-549. doi.org/10.1037/a0019243

Phishing.org. (n.d.). History of phishing. Retrieved from https://www.phishing.org/history-of-phishing

Pogosyan, M. (2018). In helping others, you help yourself: the benefits of social regulation. Psychology Today. Retrieved from https://www.psychologytoday.com/us/blog/between-cultures/201805/in-helping-others-you-help-yourself

Ponemon Institute, (2017). Cost of cybercrime study. Retrieved from https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017

Ramsey, C. A. (2000). Storytelling can be a valuable teaching aid. *AORN Journal*, *72*(3), 497–499. doi: 10.1016/s0001-2092(06)61281-7

Ratner, R. K., & Kahn, B. E. (2002). The Impact of Private versus Public Consumption on Variety-Seeking Behavior. *Journal of Consumer Research*, *29*(2), 246–257. doi: 10.1086/341574

Ratner, R. K., Kahn, B. E., & Kahneman, D. (1999). Choosing Less-Preferred Experiences For the Sake of Variety. *Journal of Consumer Research*, *26*(1), 1–15. doi: 10.1086/209547

RSA. (2019). The future of companies and cybersecurity spending. Retrieved from https://www.rsaconference.com/industry-topics/blog/the-future-of-companies-and-cybersecurity-spending

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist, 55*(1), 68. doi: 10.1037//0003-066x.55.1.68

Schwier, C., Van Maanen, C., Carpenter, M., Tomasello, M. (2006). Rational Imitation in

12-Month-Old Infants. Infancy, 10(3), 303–311. doi: 10.1207/s15327078in1003_6

Shah, K. (2015). Phishing: An Evolving Threat. International Journal of Students' Research in Technology & Management, *3*(1), 216-222. Retrieved from https://giapjournals.com/ijsrtm/article/view/143

Srivastava, A., Bartol, K. M., & Locke, E. A. (2006). Empowering leadership in management teams: Effects on knowledge sharing, efficacy, and performance. *Academy of Management Journal, 49*(6), 1239-1251. doi: 10.2307/20159830

Statista. (2016). iPhone users in the United States from 2012 to 2015. Retrieved from https://www.statista.com/statistics/232790/forecast-of-apple-users-in-the-us/

Strater, K., & Richter, H. (2007). Examining privacy and disclosure in a social networking community. *Proceedings of the 3rd Symposium on Usable Privacy and Security - SOUPS 07*. doi: 10.1145/1280680.1280706

Strauss, A., & Corbin, J. M. (1990). *Basics of qualitative research: Grounded theory procedures and techniques.* Sage Publications, Inc.

Symantec. (2016). Symantec internet security threat report. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Tobin, G. A., & Begley, C. M. (2004). Methodological rigour within a qualitative framework. *Journal of Advanced Nursing*, *48*(4), 388–396. doi: 10.1111/j.1365-2648.2004.03207.x

Tomasello, M. (1999). The cultural origins of human cognition. Harvard University

Press.

Toohey, P. (2102). *Boredom: A lively history*. New Haven, CT: Yale University Press.

Tope, D., Chamberlain, L. J., Crowley, M., & Hodson, R. (2005). The Benefits of Being There. *Journal of Contemporary Ethnography*, *34*(4), 470–493. doi: 10.1177/0891241605276692

University of Cambridge. (n.d.). Dialogic: What is dialogic teaching? Retrieved from https://www.educ.cam.ac.uk/research/projects/dialogic/whatis.html

Valente, T. W., & Davis, R. L. (1999). Accelerating the diffusion of innovations using opinion leaders. *Annals of the American Academy of Political and Social Science*, *566*, 55–67. doi:10.1177/0002716299566001005

Varshney, G., Misra, M., & Atrey, P. K. (2016). A survey and classification of web phishing detection schemes. *Security and Communication Networks*, *9*(18), 6266–6284. doi: 10.1002/sec.1674

Wang, S., & Noe, R. A. (2010). Knowledge sharing: A review and directions for future research. *Human Resource Management Review*, *20*(2), 115–131. doi: 10.1016/j.hrmr.2009.10.001

Watkins, D. C. (2012). Qualitative Research: The Importance of Conducting Research That Doesn't "Count." *Health Promotion Practice*, *13*(2), 153–158. doi.org/10.1177/1524839912437370

Weinstein, N., & Ryan, R. M. (2010). When helping helps: Autonomous motivation for prosocial behavior and its influence on well-being for the helper and recipient. *Journal of Personality and Social Psychology*, *98*(2), 222–244. doi:

10.1037/a0016984

West, R. (2008). The psychology of security. *Communications of the ACM*, *51*(4), 34–40. doi: 10.1145/1330311.1330320

Yi. E. (2018). Themes don't just emerge: Coding the qualitative data. Retrieved from https://medium.com/@projectux/themes-dont-just-emerge-coding-the-qualitative-data-95aff874fdce

# Appendix A: Ambassador Program FAQ

Home

News & Resources
Epic Implementation Training Post Go-Live Electronic Health Record Updates

Ambassador Program

## Frequently Asked Questions

**What is the purpose of the Office of Information Security?**

The Office of Information Security (OIS) is dedicated to securing the organization's data against the threat of cyber attack.

OIS is also committed to educating employees about the importance of protecting patient, personal and private business information. All employees have a role to play in keeping our information safe, and OIS provides the necessary resources and guidance to ensure that the needs of the patient come first – today and in the future.

**What does an InfoSec Ambassador do?**

By raising awareness, leading by example, distributing timely information to co-workers and reminding everyone of their role in keeping the organization safe, InfoSec Ambassadors are champions of safe behaviors.

**Why should I be an InfoSec Ambassador?**

With more than 60,000 employees in multiple regions of the country, it's important to have dedicated colleagues in each of these locations to support k ey information security objectives.

If you are a person who feels passionate about protecting the organization's patients, data and property, gain key insights into one of healthcare's most pressing issues.

**Who can be an InfoSec Ambassador?**

Any employee with the desire to advocate for a safer environment at our organization. OIS asks that you receive your direct supervisor's approval.

**What is the minimum commitment?**

InfoSec Ambassadors are asked to commit to a term of one year, and to dedicate approximately 2-3 hours each month.

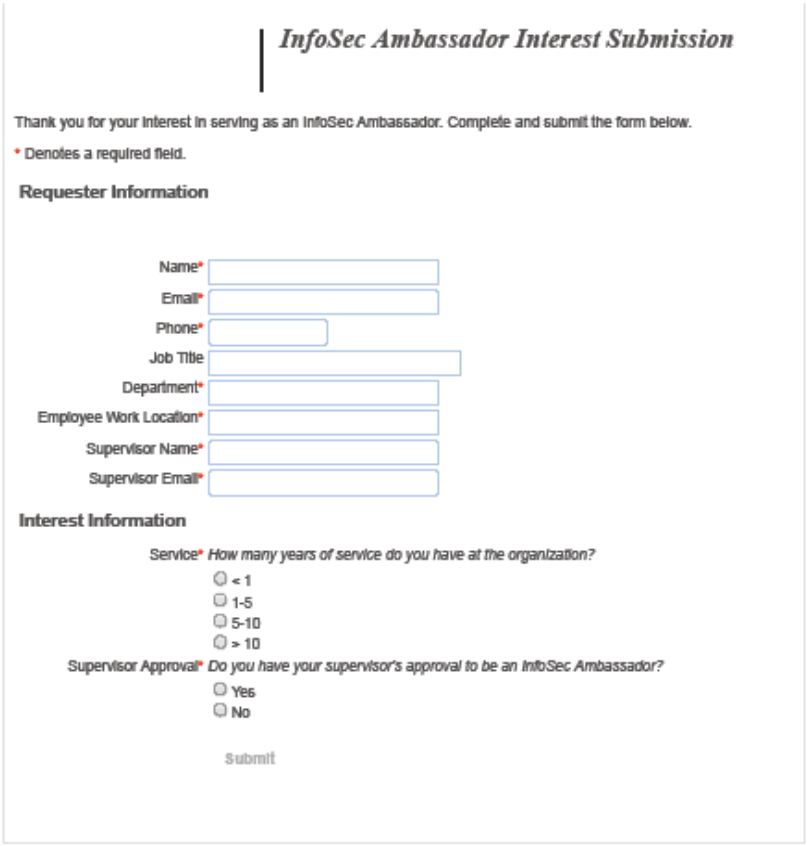
**How do I promote information security?**

Each month, OIS will provide InfoSec Ambassadors with the knowledge and tools to assist with achieving security objectives within a specific topic area.

From identifying potential threats to the encryption of data, several topics will be discussed with employees during the next several months.

**Interested? Click here to fill out the form to become an ambassador.**

Appendix B: InfoSec Ambassador Interest Submission



*InfoSec Ambassador Interest Submission*

Thank you for your interest in serving as an InfoSec Ambassador. Complete and submit the form below.

* Denotes a required field.

**Requester Information**

Name*
Email*
Phone*
Job Title
Department*
Employee Work Location*
Supervisor Name*
Supervisor Email*

**Interest Information**

Service* *How many years of service do you have at the organization?*

- < 1
- 1-5
- 5-10
- > 10

Supervisor Approval* *Do you have your supervisor's approval to be an InfoSec Ambassador?*

- Yes
- No

Submit

# Appendix C: Original Interview Questions

InfoSec Ambassador Information

1. How did you hear about the InfoSec Ambassador program?
2. Why did you choose to become an InfoSec Ambassador?
3. Did you have any hesitations prior to becoming an InfoSec Ambassador? If so, what made you decide to volunteer?

Prior to joining the InfoSec Ambassador program

1.) Prior to becoming an InfoSec Ambassador, what safeguards (if any) did you take when accessing the internet and checking your email?
2.) From your perspective, describe your peers' overall level of phishing knowledge prior to the implementation of the InfoSec Ambassador program.

Communication as an InfoSec Ambassador

1.) Please describe your preferred method of communication when sharing Information Security best practices with your peers.
2.) Are there any communication methods you found to be less effective within your work area?
3.) How often do you communicate information security-related knowledge with your peers?
4.) *Timing of communication:* Please explain how you determine when to best share messages with your peers.

Impact of the InfoSec Ambassador Program

1.) Do you feel your contributions as an InfoSec Ambassador have helped those within your work area to become more aware of information security threats at the organization? If so, describe any changes in your peers' overall level of phishing knowledge and confidence since the implementation of the InfoSec Ambassador program.
2.) Success can be measured in many different ways. How do you measure your team's information security awareness success?
3.) How do you measure your own success as an InfoSec Ambassador?
4.) What motivates you to continue fulfilling the InfoSec Ambassador role?

Additional Experience

1.) Please provide any additional information you would like to share with us to further improve the InfoSec Ambassador Program.

# Appendix D: Revised Interview Questions

**Opening Question:**

**What have been your experiences so far with the security ambassador program?**

Prompt questions:

RQ1: From your perspective, describe your peers' overall level of phishing knowledge prior to the implementation of the InfoSec Ambassador program.

RQ2: Are there any communication methods you found to be less effective within your work area?

RQ3: What motivates you to continue fulfilling the InfoSec Ambassador role beyond the requested one year commitment?

RQ4: Please provide any additional information you would like to share with us to further improve the existing InfoSec Ambassador Program.