

Information Security's Perception of Phishing Tactics

by

Brandon Laur

A Thesis Submitted to the Faculty of Social and Applied Sciences
in Partial Fulfilment of the Requirements for the Degree of

MASTER OF ARTS
In
PROFESSIONAL COMMUNICATION

Royal Roads University
Victoria, British Columbia, Canada

Supervisor: DR. CHASETEN REMILLARD
SEPTEMBER, 2018

COMMITTEE APPROVAL

The members of Brandon Laur's Thesis Committee certify that they have read the thesis titled Information Security's Perception of Phishing Tactics and recommend that it be accepted as fulfilling the thesis requirements for the Degree of Master of Arts in Professional Communication:

DR. CHASETEN REMILLARD [signature on file]
DAVID LEACH [signature on file]

Final approval and acceptance of this thesis is contingent upon submission of the final copy of the thesis to Royal Roads University. The thesis supervisor confirms to have read this thesis and recommends that it be accepted as fulfilling the thesis requirements:

DR. CHASETEN REMILLARD [signature on file]

Creative Commons Statement

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 2.5 Canada License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/2.5/ca/>.

Some material in this work is not being made available under the terms of this licence:

- Third-Party material that is being used under fair dealing or with permission.
- Any photographs where individuals are easily identifiable.

Abstract

This research develops qualitative knowledge from the information security industry about communication tactics as a type of security vulnerability in infosec. These perspectives included security practitioners and popular security news media sources. Both aspects of this research are used to determine the difference between multiple areas of the information security industry. The focus of the research is how phishing is understood as an attack method by information security professionals to test weakness in organizational workforces and average information technology users. The perceptions and understanding of security professionals that use phishing as a method to test information security can provide further knowledge in how to assess and implement anti-phishing procedures and training. The results of this analysis aim to support broader security research by focusing on an area absent in the literature, thereby furthering the holistic approach in the security field and providing greater knowledge of phishing, tactics, understanding, and mitigation of cybersecurity threats.

Table of Contents

Introduction	6
Definition of Phishing	9
Phishing as a Cybersecurity Problem	12
Current Phishing Tactics and History	14
Phishing Literature on Content Prior to Attacks	18
Limitations with Phishing Research	21
Methods	21
Interview Participants and Recruitment	23
Data Collection and Procedure	25
Data Analysis Methods	30
Results	31
Part 1: Interview Descriptive Results	31
Part 1: Interviews Qualitative Results	32
Legitimacy	33
Data Gathering	35
Loss	36
Part 2: News Articles Descriptive	36
Part 2: News Articles Qualitative	38
Legitimacy	38
Loss	39
Benefit	39
Comparison	40
References	50

Introduction

Cybersecurity is not solely a computer science problem as many sociological and communications weaknesses can disrupt computer security just as much as insufficient technological safeguards. Cybersecurity is common public discourse resulting from uncertainty from new technologies, aging infrastructure, and data breaches (Smyth, 2015). Regardless of spending and technological innovation to combat security threats, social and communications concerns continue to be an important area to study and secure against threats. Security experts have commonly outlined the importance of studying sociocultural influences that impact security weaknesses (Dodge, Carver, & Ferguson, 2007). The relevance of the communication used in today's information security practices is just as important as the digital cybersecurity. Security research in the social schools of study can improve the effectiveness of cybersecurity practice (Pfleeger & Caputo, 2012). Despite the growth of social research in security, there remains a lack of communication-based research and focus away from mainly victims.

Past research results and industry experts have stated that focusing on security behaviours will far greater protect end-users than traditional hardware and software protection (Arachchilage & Love, 2014). The training against manipulative technology communication methods is a critical component of security, both for individuals and for organizations. Reviewing communications influences of security is more of a rarity, as most research on cybersecurity is focused around the traditional disciplines of computer sciences and engineering (McGraw, 2004). Given modern technological expansion, information security is a growing field of work and public importance.

Phishing, a form of manipulation to circumvent cybersecurity, is one security concern that has been identified as a significant issue due to the fact that it preys on multiple security

weaknesses. Research is being conducted on the communications tactics used by malicious hackers (Atkins & Huang, 2013). However, communications research on phishing is very limited. Additional research has also examined the efficacy of training programs to educate internet-connected device users on how to mitigate phishing threats (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010). Despite the significant amount of work conducted on this topic, little information at a qualitative perspective on the part of security professionals exists. Literature about behaviours prior to phishing attacks remains scarce. A critical component of organizational technology infrastructure is the testing preparedness and implementation of educational programs. Those security professionals' perceptions, knowledge, and understandings of the subject of phishing can have a significant impact on how they effectively prevent possible threats.

This research attempts to fill the gap between the academic literature on phishing and the understanding of active information security professionals tasked with prohibiting phishing threats. The goal of this study is to expand on current phishing research by narrowing the focus by analyzing the phishing tactics examined in research with what is being experienced by the security industry. Research results were achieved by examining a specific group of individuals within the information security profession with an expert, firsthand knowledge on phishing security and prevention. Looking at phishing from the lens of those tasked with preventing phishing threats instead of researching the victims can uncover new ways to reduce phishing by identifying weaknesses in both academic literature and security professionals' knowledge. This research aims to address this specific question of what exactly are the held beliefs toward phishing of active industry information security professionals. Despite the wide research on the topic of phishing in academic peer-reviewed literature, this research concludes that from the

perspective of information security practitioners there are only a few categories of phishing being used in real-world instances.

Two main aspects are used in this current research to address some of the limitations of past phishing literature. These two aspects were semi-structured interviews with information security practitioners as well as an analysis of information security news sources that was carefully conducted, transcribed, and coded. The data collected here offers a different perspective opposed to the traditional way phishing research is conducted and how conclusions are made.

With this study posing new research questions to assist security professionals seeking answers to phishing encounters, the following study aims to provide a foundation upon which to design methods for improved phishing awareness and alleviation. Combining the relevant academic research with industry-leading experience can offer some of the best solutions to phishing problems. Additionally, this research seeks to understand the modes by which phishing information is disseminated and the ways information is congruent with current research. The findings present in this research support previous literature while also offering a narrower focus to address phishing within the most commonly experienced scenarios. Not only does the present conclusion provide a precise topic for research on the experiences of security practitioners, but it also acts as a call for action to find ways how to better communicate phishing information to all professionals that seek to reduce this problem.

Phishing Literature

Phishing is a cyberattack using manipulation tactics to allow a technology user to willingly circumvent security behaviours. Extensive literature has been published on the tactics used by malicious hackers (Twitchell, 2008). Additional research has also examined

predispositions that potential victims may have to phishing attacks and the perceptions of victims following a successful phishing attack (Vishwanath, Herath, Chen, Wang, & Rao, 2011).

However, despite the extensive research there remains absent areas of study that could provide great insight into how to prevent or lessen phishing dangers.

Both academic researchers and active security professionals have identified phishing as a major concern for organizations and personal cybersecurity (Dodge et al., 2007; James, 2006). The psychological manipulation strategies used by malicious phishers have been studied in regard to their effectiveness (Davinson & Sillence, 2010). Furthermore, the victims of phishing attacks have been studied in relation to phishing and the victims' personality traits (Darwish, El Zarka, & Aloul, 2012). Larger participant studies have examined overall public susceptibility to phishing strategies (Alsharnouby, Alaca, & Chiasson, 2015; Vishwanath et al., 2011). Further research projects have tested methods to educate people with varying results and critiques (Kumaraguru et al., 2010). What is missing in the current literature on phishing is information pertaining to those tasked with training users against phishing, testing phishing preparedness, or preventing these threats. Given all the actors involved in cybersecurity, such as the attackers, defenders, researchers, and victims, each stage of a cyberattack deserves careful and meaningful analysis.

Definition of Phishing

Phishing is a unique cybersecurity threat that encompasses both technological vulnerabilities and mix of psychological, sociological, and communication-related influences. Phishing is a category of social engineering that is a preferred form of manipulation used by malicious hackers. From a cybersecurity perspective, they are those individuals that use computers to gain unauthorized access to data to persuade an intended victim of an attack to

permit the attack to happen (Abraham & Chengalur-Smith, 2010). The general purpose of social engineering is to convince a person of something false or misleading that looks legitimate to bypass any suspicions and unwanted attention. The risk of this threat is that it cannot be completely eradicated by technological solutions (Pfleeger & Caputo, 2012). Despite great advances in security systems, human error exists as a major vulnerability. It is the responsibility of the potential victim to identify any cybersecurity attack and address the event.

Industry and academia categorize phishing as a semantic attack (Heartfield & Loukas, 2015; Schneier, 2000). This type of attack is based on how humans interact with computers or understand communications. Researchers studying security have labelled phishing attacks as a concern, prompting greater research and training, as training has been shown to improve phishing identification, thereby preventing individuals from falling victim (Jansson & Von Solms, 2011; Kumaraguru et al., 2010). These psychological, sociological, and communication-related tactics are advantageous to attackers because they comply with supported social and communications theories on manipulation (Workman, 2008). The strategies used in successful phishing attacks are not different than what is used in professional industries of influence such as marketing.

Given the importance of the social components that facilitate phishing at both the attacker and victim perspective, phishing is considered more of a communication topic than a computer science topic. Reviewing the literature of online phishing manipulation tactics implemented by today's cybercriminals shows similar research in marketing and other social sciences disciplines. Reviewing phishing within the communications discipline addresses the crux of the security concern: manipulation by one social agent against another.

Technology has a large part to play in mediation of this threat and there are various tactics that have been developed by computer scientists to help filter phishing messages before they are even seen by potential victims (Abdelhamid, 2015; G. Gupta & Pieprzyk, 2011; Wenyin, Fang, Quan, Qiu, & Liu, 2010). Phishing can be interpreted as a broad term with many research studies examining different aspects, mediums, and strategies. The most commonly researched types of phishing attackers are by websites and emails (Dodge et al., 2007). However, phishing can occur in the context of many other media forms such as social networking and other messaging services (Aleroud & Zhou, 2017). Often, if there is an affordance for digital communication, there is a potential for phishing. Technical solutions to decrease phishing threats are not always successful as they rely on the end user to decide how to interpret every communication and detect what messages are malicious. Education and training by industry experts is necessary to help achieve awareness and prevention of phishing.

The scope of phishing can range quite dramatically from generic phishing to targeted phishing. Spear phishing is a targeted communications attack where the context of the phishing messages is specific to a particular target and therefore would not make sense to any other target (Benenson, Gassmann, & Landwirth, 2017). Typical generic phishing refers to messages that apply to a much wider audience that are not tailored to each target. Spear phishing attacks can be directed towards a particular person, department, or organization. In essence, these messages are personalized and assumed to have greater believability and effectiveness. Research does support spear phishing as being more effective than generic phishing (Bullee, Montoya, Junger, & Hartel, 2017). A further subcategory of phishing is also called whaling, where the spear phishing attack is focused on high-value business executives (Abraham & Chengalur-Smith, 2010). These

“whale” sized targets when compromised by a hack can win the hacker greater financial benefits or allow further access into an organization.

Phishing as a Cybersecurity Problem

Phishing is a significant cybersecurity issue. According to Symantec, a cybersecurity provider and research company, in Q2 2017 phishing rates had increased across most industries and around 1 in 1,975 emails delivered were phishing (“Latest Intelligence for June 2017,” n.d.). Securelist identified about 9% of unique users encountered phishing (Securelist, 2018). Industry estimates say phishing attempts have grown 65% since 2016 (PishMe, 2017). 30% of phishing messages get opened by targeted users and 12% of those users click on the malicious attachment or links (Verizon, 2018). Phishing observations by those tracking the activities are showing a steady increase year by year.

Cybersecurity is a widespread public concern and phishing is a large component of that. Being less technical and more of a communication concern than traditional malicious software cyberattacks, phishing protection can be practiced by anyone, but only if they know what to look for. Recent research has concluded that only about 50% of people can successfully detect phishing (Alsharnouby et al., 2015; Vishwanath et al., 2011). This practical result does vary across different types of phishing approaches, but in general, it can be hard to detect because most people do not know what to look for. There are many studies examining the types of phishing methods used and the level of reception and responses of average people to these plans (Vishwanath et al., 2011). Most researchers agree that education is the best method to prevent being exploited by phishing (Jansson & Von Solms, 2011). The same research into education regarding phishing has been shown to increase participants’ abilities to detect phishing following training. The current research literature concludes that public training and education on phishing

significantly reduces the likelihood of falling victim to this threat, and that education and training should be actively promoted.

Contradictory research has criticized certain phishing education models for their pedagogical approaches. Critics have considered the time and costs associated with training as not being practical in work environments, as the cost and time required to implement training is not readily seen as a financial benefit (Mohammad, Thabtah, & McCluskey, 2015). Other researchers have studied ways to better implement training in less conventional approaches, such as using comics and embedded training (Jansson & Von Solms, 2011; Kumaraguru et al., 2010). These studies have produced positive results showing an obvious alleviation by participants using alternative training methods. Drawing on research from educational fields is proving to be a useful tool in assessing the best security training procedures.

Despite institutional costs and debate about the most effective pedagogical approach to address phishing, research supports education as an effective defence strategy to thwart phishing (Arachchilage & Love, 2013; Jansson & von Solms, 2013; Kumaraguru et al., 2009; Mohammad et al., 2015; Robila & Ragucci, 2006; Srikwan & Jakobsson, 2008). These studies thus support the claim that phishing is a communications topic based in the educational model used primarily as an effective mode of solving this cybercrime issue.

In further support of the importance of communications in phishing, the language used in these attacks has different impacts based on the population. Cultural differences have been suggested to increase the likelihood of falling for a phishing attack, as users who are not fluent in English are more unlikely to understand security warnings in an unfamiliar language (Alseadoon, Ramadan, & Khedr, 2017). People who are unfamiliar with technology are more likely to rate emails as spam regardless of the message being legitimate, fake, or actually spam, specifically in

regard to emails and electronic documents (Sarno, Lewis, Bohil, Shoss, & Neider, 2017).

Culture, language, and education all contribute to the different categories and efficiency of phishing attacks.

Current Phishing Tactics and History

Phishing tactics have not changed over the last few years, though the technology used has. Academic research is constantly further studying the impact of manipulation tactics. The concept of the tactics used in phishing is nothing new; the history of phishing can be traced back to “phone phreaking” in the late 1950’s (Gold, 2011). The most commonly publicised events of phone phreaking were the events following Kevin Mitnick, who was at one time on the Top 5 of the FBI’s Most Wanted list (Mitnick & Simon, 2012). The goal of this attack is to call into a phone switchboard and convince the operator to grant access to the attacker. Phone phreaking is much less technical than today’s phishing, but it contains some similar communications tactics used in its modern counterpart (Gold, 2011; Hinde, 2004). As technology has become more advanced, so have the media used in socially engineered phishing attacks.

A wide array of manipulation tactics used in phishing has been identified by the academic community. Table 1 outlines various methods used in phishing and social engineering from the academic literature. This table shows results of the tactics used by phishers in an attempt to compromise victims’ security. The list encompasses mostly emotional and psychological tools that can be seen in phishing attacks. Some studies have identified these threats and have emphasized the importance of education in combating falling victim (Jansson & Von Solms, 2011). Other studies test the types of education that are most effective to train organizational staff (Jansson & von Solms, 2013; Kumaraguru et al., 2010). None of these research projects

consider the importance of the security professionals or HR managers tasked with implementing anti-phishing systems.

Table 1 below is a product of this literature review and acts as the baseline for the data analysis process. Throughout the phishing literature, certain projects have categorized different types of phishing communications. These groupings of manipulation methods are present here in table 1. How these categories were developed differs between studies. Atkins & Huang (2013) developed their categories from three other studies. Twitchell (2008) developed their list based on the literature from industry society practitioners both preventing phishing and those who have developed phishing attacks. Workman (2008) used industry focused participants and persuasion research in developing phishing typology. Tetri & Vuorinen (2013) used researched social engineering techniques and then labeled similar methods. Parsons, McCormac, Patterson, Butavicius, & Jerram (2015) collected actual phishing emails and categorized them by similar intention.

Table 1

Types of Phishing and Social Engineering Tactics in Literature

Source	Label	Definition
(Atkins & Huang, 2013)	Authority	Using signs of power to elicit behaviour. Can include legitimacy, trust, and credibility. Also includes signs such as memberships and titles
	Pity	Using sympathy and charity emotions that influence behaviours
	Tradition	Appealing to values such as honour and legacy that lead to behaviours fulfilling those values
	Attraction	Eliciting anticipation, enjoyment, or excitement increasing behaviours to achieve the attraction
	Urgency	Framing responses as imperative and stressful time-sensitive action
	Fear/threat	Using intimidation or distress to cause behaviours to prevent those emotions
	Politeness	Build rapport or convince being a real human and not a robot

	Formality	Convincing of legitimacy and safety to prevent suspicion
(Twitchell, 2008)	Feeling overloaded	Producing overwhelming information, preventing clear thinking
	Urgency	Setting a strict time restraint on behaviour, causing panic and preventing clear thinking
	Fear	Using frightful emotions to overcome any logical and rational thinking
	Scarcity	Using economic influences by convincing of shortage, causing a desire to acquire what is limited
	Other strong emotions	Eliciting various human emotions that influence behaviours
	Reciprocation	Expecting behaviours in return for doing something of benefit
	Trust	Building a trusting relationship to avoid suspicions
	Similarity	Mimicking behaviour or personality, to cause relaxation by preventing unfamiliarity
	Helpfulness	Eliciting helping emotions and behaviours
	Integrity	Using a sense of self-respect to cause behaviours that fulfill that respect
	Legitimacy	Information made to seem to be from a credible, authoritative source
	Authority	Using a name, title, or other symbol that is of influence; typically signifying power over
	Conformity	Using social pressure to cause behaviours to follow social normalities
	Curiosity	Using human interest to lead someone to a desired behaviour
	Diffusion of responsibility	Giving assurance that undesirable behaviours will not be punished
	Cognitive and cultural biases	Using biases that are related to the psychological triggers
	Truth bias	Tendency for people to believe information coming from someone in a trust relationship
	Prospect Theory	Tendency for losses to be considered more in decision-making than gains
	The Representative Heuristic	Tendency for people to believe a situation that has more supporting detail than one with less
Anchoring and Adjustment	Tendency of people to establish a baseline and adjust behaviours from that baseline	

(Workman, 2008)	Elaboration likelihood model	A model of persuasion by outlining ways of processing stimuli using <i>central</i> and <i>peripheral</i> routes of processing
	Protection motivation theory	People may think economically, thereby engage in risky behaviours to gain something they value
	Self-concepts	Tendency for people to uphold their social identity
	Affective commitment	People will behave in ways to satisfy emotional ties
	Reciprocation	Economic or social viewpoint where there is a perceived obligation to make even
	Consistency	People are motivated to maintain consistent and coherent attitudes and behaviours
	Social proof	People will follow and model the behaviours of their peer group or other associated communities
	Likeability	Trust is increased when people are liked and may be seen to be above average
	Authority	Power-based relationship where those of lesser power will obey commands of a superior to avoid a negative consequence
	Scarcity	Rare items are perceived as more valuable
(Tetri & Vuorinen, 2013)	Fabrication	Proving misleading cues such as impersonation, name-dropping, jargon, piggybacking, and using false ID
	Data gathering	Collecting information about a target to then use against them: open source information gathering, dumpster diving, shoulder surfing, stealing, eavesdropping, loggers
	Persuasion	Using psychology and rhetorical tactics to convince a target to comply with an inappropriate request
(Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2015)	Risk or Loss	Rhetorical strategy to convince in preventing a loss
	Benefit or Gain	Rhetorical strategy to convince obtaining a benefit or additional service
	Account Information	Email containing content about an account that includes a phishing link to click on
	Information Only	Email containing nothing in particular except with a phishing link attached, typically contains product advertising

Table 1 gives a good overview of the types of phishing and social engineering tactics experienced in previous literature. It is apparent that many of the identified codes overlap across many different studies. Reviewing each study on their own also reveals that the way these codes were developed have different origins for example some were derived from traditional

manipulative communications research, expert experience, and phishing email textual analysis. As a whole field of study, the range of phishing tools identified by research is broad.

Phishing Literature on Content Prior to Attacks

There is an extensive amount of academic literature on phishing. The majority of this literature focuses on information following phishing attacks using victims as the primary research participants or analyzing manipulation tactics afterwards from an attack. Only a small focus in the literature pertains to content prior to a phishing attack from the perspective of the attacker or professional security penetration tester. While looking at the entire process of phishing and agents involved in the process, the literature selectively focuses on a few parts. Some studies have outlined this process in diagrams, outlining the steps from creation of attacks to successful victimization (Gondim, de Oliveira Albuquerque, Nascimento, Villalba, & Kim, 2016; B. B. Gupta, Arachchilage, & Psannis, 2017).

In all the phishing diagrams there is always an attacking entity initiating a cybercrime attack as the source of the threat. From the source of an attack, depending on the communications strategy used by the source, illustrative diagrams of an attack process can differ. What remains constant in all phishing explanations is the human attacker starting the phish. Yet, research does not address that part. The role of the hacker or security professional in the phishing process is an important part, as it is clearly labelled as a component and should be duly researched.

One perspective missing from research is how professional security penetration testers attempt to simulate real attacks on systems in order to test the security preparedness against potential malicious attacks. Penetration testing or *pentesting* is a commonly used security practice where a security professional simulates being a harmful hacker and attempts to break

into systems in order to find issues to correct (Felderer, Zech, Breu, Büchler, & Pretschner, 2016; Gondim et al., 2016). In the case of phishing, pentesting methods are used in organizational settings to measure a workforce's baseline security efficacy against any potential attack. Cybersecurity research regularly uses pentesting methods against research participants to test their baseline and improved responsiveness to simulated attacks. These research studies use the same social engineering tactics used by malicious attackers to measure behavioural responses from phishing tactics.

Often, security research takes place in laboratory settings where data is collected. However, laboratory settings do not always transfer well in everyday workforce environments or provide information on how to implement the research into security procedures. Further, some action-oriented research studies have taken the initiative to develop studies within everyday organization workforces to best simulate real-world environmental influences (Kumaraguru et al., 2010). These real-world settings provide information on how to implement anti-phishing programs into the workplace. Even those real-world studies pose some practical issues, as academic researchers who are not all career security professionals conduct them. Therein lies potential disconnects between academic research and information security practitioners. Researchers may conduct experiments a certain way and claim results that may contradict what security professionals do or conclude. There is little current credible research on the relationship between research and everyday security testing and training.

To accomplish what is suggested from research in promoting education and training towards manipulative cybersecurity threats, careful attention must be taken into looking at those tasked with organizational anti-phishing procedures that produce education and testing. This is a missing link in the literature. There are still areas for more experiments testing educational

effectiveness on phishing topics, but attention should start to shift away from the actual educational material and victims to, instead, look at those that are tasked with solving the issues outlined in the academic literature. Research describes methods and tools but fails to suggest ways to have those tools used by those that matter. Future research should look at how to best educate the trainers on how to better secure against phishing. Before that, we must first examine the current state of security with what security professionals' perceptions are on the success of phishing communication tactics in information security testing.

There is no doubt that phishing is a significant computer and network security issue ranging from the individual technology user to large organizational workforces. Technological solutions are being utilized to combat this threat. As phishing is a major communication topic, social, cultural, and psychological defences also need to be utilized. Research in this area is clear that there needs to be more widely promoted education on the topic. Various research studies have tested different types of training and education with measurable results on the effectiveness of training. This field of research, however, neglects the importance of the security workers tasked with utilizing training and testing phishing threats. These individuals are worth critical study as they are the professionals tasked with penetration testing, security preparedness, and promoting phishing-mitigating behaviours through education.

There is little research examining if the results of peer-reviewed work in academia on phishing after publication are being accepted and regularly managed by the everyday security professional. Despite great work in the social sciences on the risks, effectiveness, tactics, training, and types of education on phishing mitigation, there is no indication of if these studies are being directly utilized outside of the academic sphere. Questions then arise as to if security professionals have easy access to academic research or if security professionals not affiliated

with research or academic institutions may not have access to the research. For those who do not have access to research, what channels are used to gather new information and is this information derived from personal experiences, external expert experiences, or careful research?

Limitations with Phishing Research

Throughout this research literature review, there arose a clear division between the types of anti-phishing research conducted. This deviation can be placed into two categories: computer sciences and social sciences. However, of the over 150 articles collected relating to phishing tactics and mitigation for the review of this research, only a small percentage of articles were based in social sciences. Of note towards communication researchers, there was a significantly smaller amount of literature from communications scholars on the topic of phishing.

What is also absent from the literature is the first-hand account of phishing from the perspective of the phishers. Outside of the technical papers, when researching social components of phishing, the common methods are divided into three categories: education strategies, victim experience, and message analysis. There are multiple different stages of a phishing attack and each of these categories helps facilitate the understanding of phishing.

Methods

This study is comprised of two parts: semi-structured interviews with information security practitioners, and an analysis of information security news sources. Each part is used as a comparative study of each other and previous research. Using all three sources about phishing offers a more holistic approach in assessing the prevalence of the type of phishing attacks happening. These methods also provide the wider understanding of phishing outside of the academic community.

Introduction and Design

The first component of the research was studying security professionals' perceptions on the efficacy of communication tactics on phishing attempts. Six active security professionals were recruited to participate in a qualitative analysis of their experiences with phishing. The smaller qualitative research design used in this study better describes the circumstances and communicative nature of the social aspects of phishing. This study examines the phishing tactics outlined in academic research with what security professionals experience. Previous phishing academic literature is the basis for the coding frame for the interview data collected. After the interview data was collected, transcription and analysis were conducted by thematic analysis using phishing tactics as the coding frame.

The second component of this research was an examination of the three most popular information security news websites that report and update on current cybersecurity threats. threatpost (threatpost.com) Nakedsecurity (nakedsecurity.sophos.com) infosecurity (infosecurity-magazine.com) were the chosen data sources in this part of the research. Given the publication size, publication rate, popularity, and reputation among the information security industry, these sources were deemed the most valuable for this study. All phishing related articles from these sources in 2017 were selected for coding. A combined total of 217 articles on phishing in the year 2017 were collected and reviewed. For consistency, these articles were coded with the same list of codes as the first part of the research. Uniformity between the coding in both research sections was key to ensuring comparable and measurable results. These data sources were used to compare the relevancy and range of phishing within the security industry.

Descriptive frequencies on the prevalence of phishing tactics were collected between both parts of this research and used to evaluate the predominance of the identified phishing tactics from academic research. The frequencies of the present codes in all parts of the research

aid to identify the relevancy of each phishing tactic found in academia within the context of the security industry. The combination of both what is being publicly reported within the security industry and what is understood by active security professionals offers a significant overview of phishing from an alternative source than what is traditionally used.

At an organizational level, this research provides a brief overview towards the strengths or weakness of the messaging of phishing between stakeholders. More significantly, the strength of this study's design is the ability to understand the connection between different stakeholders of phishing mitigation and further explore a relatively unresearched area of research in regard to what information security practitioners experience.

Interview Participants and Recruitment

The firsthand accounts of security practice and experience with non-simulated phishing offers the richest source of data to begin in understanding phishing from a new perspective. Simulated or mock phishing exercises are limited, as participants in such studies would be primed to expect phishing; whereas, in real world circumstances, phishing attacks can occur if alerted to them or not. Requirements for participation in this research are active security professionals involved in preventing phishing by educating or testing phishing preparedness among workforces and individuals. These persons were identified based on their firsthand experience with phishing mitigation. This target population was selected to directly address the weakness in previous security research focusing on only the victims of phishing and the tactics used. The direct experiences dealing with phishing as part of an occupation will provide further research data on the real-world circumstances of phishing rather than simulated online or laboratory experiments.

The participant recruitment process followed convenience sampling, given the specific participant requirements necessary for the research (Marshall, 1996). This sampling method is designed to purposefully select cases that will produce information-rich data (Coyne, 1997). The participant recruitment method is done by scanning publicly available contact information associated to credible potential interviewees from conference websites, clubs, social media, and corporate webpages. Given the wide array of information technology and the content-rich, qualitative nature of the research, care was given to select those individuals that best fit within the scope of this research. Following initial contact, snowball methods were used in attempt to utilize secondary sources in finding research participants. To avoid geographical restriction toward participant recruitment, the interview recruitment and process encompassed distance interviewing tools. The decision to select participants from across North America was to ensure that any cultural and locational differences were incorporated into the study. North America-wide selection also allowed for a more diverse selection of participants in different jobs and with different roles related to phishing. The choice of what communication medium used was at the discretion of the research participant. Both VoIP and cellular communication were available to participants. These interviews were recorded and transcribed for analysis following the interview.

Once potential qualifying participants were identified, and they accepted to participate, they were presented with a written information sheet of the study and a participant consent waiver. The consent waiver follows all ethical requirements as outlined by the project's supervisory institution, Royal Roads University. Following all introduction and consent processes, the interview was then conducted. Each interview session was audio-recorded and later transcribed for textual analysis. Along with recordings, the interviewer also maintained

notes. These interview notes contain information such as environmental stimuli including office influences, voice levels, and the date and time of the interview.

Based on current qualitative research standards, six in-depth research participants are sufficient as a minimum participant count (Mason, 2010). Participants were selected until repetitive data already collected from previous instances with no sign of new information emerged. Although six is the set minimum, the overall objective from the data collection was to reach the point of saturation, being the optimal participants interview size (Baker & Edwards, 2012). Through the process of the study, it was determined by the sixth participant that saturation was reached, as recurring themes had been established by the fourth interview. As an introductory study, a smaller number of participants is sufficient to determine if more investigation is necessary. The data collected here will be the baseline for any future investigation.

Data Collection and Procedure

Section one of the research data is derived from the semi-structured interviewing with the research participants. Each interview session was audio-recorded and later transcribed for textual analysis. In addition to the active note-taking, the interviewer also maintained a checklist of all topics, predetermined, on topic points that could potentially be brought up by the interview participant. Data from section two derived from security industry leading news sources on phishing were coded similarly under the same parameters as the coding process in section one.

A semi-structured interview schedule was the best selection for this research given its balance between its rigidity and flexibility. The purpose of this study is for participants to elaborate, if applicable, the relevancy of phishing tactics from those identified in previous

research. Given the openness of subjective experiences on predefined topics gave best fit to this type of data collection.

The interview questioning follows the process as outlined in traditional semi-structured format (Rubin & Rubin, 2011). The interview schedule targeted the specific conditions summarized in Table 2. This table is an amalgamation of known phishing tactics present in current phishing research as summarized in Table 1. Given the crossover of phishing strategies researched among different studies, the codes in Table 2 are the best incorporation of all similar topics discussed in the research literature. Collected interview data, once transcribed, is coded from the content in Table 2.

The interview questions are primarily open-ended, each relating to an overarching theme derived from the Table 2 codes. Each question theme was an exhaustive catalogue of Table 2. The beginning portion of the interview was the most open and was directed by the interviewees themselves, having the interviewee explain their experience with phishing and their professional roles with the security aspect of it. As the interviewee is explaining, the researcher is recording what content from Table 2 is being discussed by the interviewee.

Table 2		
<i>Code List</i>		
Code	Label	Definition
1	Authority	Using signs of power to elicit behaviour. Also includes signs such as memberships and titles. Using a name, title, or other symbol that is of influence, typically signifying power over. Power-based relationship are where those of lesser power will obey commands of a superior to avoid a negative consequence

2	Pity	Using sympathy and charity emotions that influence behaviours
3	Tradition	Appealing to values such as honour and legacy that lead to behaviours fulfilling those values
4	Attraction	Eliciting anticipation, enjoyment, or excitement increasing behaviours to achieve the attraction
5	Urgency	Framing responses as imperative and requiring stressful, time-sensitive action, setting a strict time restraint on behaviour, causing panic and preventing clear thinking
6	Fear/Threat	Using intimidation or distress to cause behaviours to prevent those emotions. Using frightful emotions to overcome any logical and rational thinking
7	Politeness	Building rapport or convince being a real human and not a robot
8	Formality	Convincing of realness and safety to prevent suspicion
9	Overload	Producing overwhelming information, preventing clear thinking
10	Scarcity	Using economic influences by convincing of shortage, causing a desire to acquire what is limited; rare items are perceived as more valuable
11	Reciprocation	Expecting behaviours in return for doing something of benefit, economic or social viewpoint where there is a perceived obligation to make even
12	Trust	Building a trusting relationship to avoid suspicions
13	Similarity	Mimicking behaviour or personality, to cause relaxation by preventing unfamiliarity

14	Helpfulness	Eliciting helping emotions and behaviours
15	Integrity	Using a sense of self-respect to cause behaviours that fulfill that respect
16	Legitimacy	Information made to seem to be from a credible source not using authority
17	Curiosity	Using human interest to lead someone to a desired behaviour
18	Diffusion	Diffusion of responsibility, giving assurance that undesirable behaviours will not be punished
19	Cognitive and Cultural Biases	Using biases that are related to the psychological triggers
20	Truth Bias	Tendency for people to believe information coming from someone in a trusting relationship
21	Prospect	Prospect Theory: the tendency for losses to be considered more in decision-making than gains
22	Representative Heuristic	Tendency for people to believe a situation that has more supporting details than one with less
23	Anchoring and Adjustment	Tendency of people to establish a baseline and adjust behaviours from that baseline
24	Elaboration Likelihood Model	A model of persuasion by outlining ways of processing stimuli using <i>central</i> and <i>peripheral</i> routes of processing

25	Protection Motivation Theory	People may think economically, thereby engaging in risky behaviours to gain something they value
26	Self-Concepts	Tendency for people to uphold their social identity
27	Affective Commitment	People will behave in ways to satisfy emotional ties
28	Consistency	People are motivated to maintain consistent and coherent attitudes and behaviours
29	Social Proof	People will follow and model the behaviours of their peer group or other associated communities; using social pressure to cause behaviours to follow social normalities
30	Likeability	Trust is increased when people are liked and may be seen to be above average
31	Fabrication	Providing misleading cues such as impersonation, name-dropping, unfamiliar jargon
32	Data Gathering	Collecting information about a target to then use against them: open source information gathering, dumpster diving, shoulder surfing, stealing, eavesdropping, loggers
33	Loss	Rhetorical strategy to convince in preventing a risk or losing something of value
34	Benefit or Gain	Rhetorical strategy to convince obtaining a benefit or additional service

35	Account Information	Messaging containing content about an account that includes a phishing component
36	Information Only	Email containing nothing in particular, except with a phishing link attached, typically contains product advertising

Data Analysis Methods

The examination of the interview transcripts was done by thematic analysis. Thematic analysis allows for themes to be unpacked from the interviews regarding an experience (Braun & Clarke, 2006). Thematic analysis permits for comparisons of frequent and conflicting commonalities or topics within a single interview and between multiple participants. The thematic approach conducts its analysis by careful reading and re-reading of the data (Saldaña, 2009). Using the identified phishing tactics outlined in the academic literature allows for the analysis of what tactics emerge as the most predominate with the research participants. In addition, comparing interview data with the literature will also identify relationships between what is discussed in academia and what is experienced by security professionals.

The coding process is a mix of inductive and deductive approaches. The primary analysis is deductive, using methods as outlined by Crabtree and Miller (1999), using predetermined coding frames derived from the literature review (Table 2). To allow for new emerging information not in the literature but presented in the transcript, an inductive approach is also used, as outlined by Boyatzis (1998). The inductive approach examines particular parameters for the inductive method being the same as those in the deductive method. Emerging inductive codes are related to only phishing tactics that are not already included in the coding frame and that have occurred from the interview participants' responses. Any new code will then be reassessed

again towards all previous coded transcripts already completed in order to thoroughly assess all relevant codes before and after interviews and transcript analysis. These approaches allow for a comprehensive process in examining the collected interview data and evaluation of the primary research questions.

Results

Part 1: Interview Descriptive Results

Six participants were recruited across North America with differing experiences in the information security industry, all with varying degrees of experiences with phishing. Qualitative interviews were conducted with backend information technology support workers, computer help desk personnel, senior system administrators, crime investigators, and security awareness educators. Each participant was selected based on their professional role of mitigating phishing.

From the six interviewed participants, a clear strength in the usage of legitimacy, data gathering, and loss were the top three most common codes shared about the types of phishing tactics experienced by participants. Legitimacy was the strongest in frequency, equalling roughly the total of the following three most common codes. Table 3 outlines the frequency of codes extrapolated from the research interviews.

Part 1 interviews, aside from legitimacy, showed a significant prevalence of data gathering themes. What was discussed often in the interviews was phishers using data collection methods with collecting information to leverage in phishing attacks. Some information sources mentioned include social media, company websites, and news reports.

Table 3		
<i>Interview Code Frequency</i>		
Code	Frequency	Percentage

Legitimacy	43	35.54%
Data gathering	21	17.36%
Loss	14	11.57%
Authority	10	8.26%
Benefit	9	7.44%
Urgency	7	5.79%
Fear & Threats	5	4.13%
Curiosity	3	2.48%
Helpfulness	3	2.48%
Trust	3	2.48%
Information	1	0.83%
Likeability	1	0.83%
Similarity	1	0.83%

Part 1: Interviews Qualitative Results

Although the descriptive aspects of the interviews reveal a great deal of information regarding the types of phishing and frequency of those messages, the qualitative aspects of how participants describe these phishing attacks offer insight into how phishers are conducting their attacks. In addition, the similarity between participants in some of the phishing tactics shows how these experiences are not isolated instances. From the top three topics, experiences discussed within the interviews are legitimacy, data gathering, and loss. These show how these individuals directly experience these communications in their particular professional circumstances.

Legitimacy

The aspect of legitimacy among interviewees was routinely described as an attacker's ruse in impersonating a seemingly valid source. Two distinct aspects emerged from participants about how a phishing ruse originates: an external source, or internal source. Also, the similarity in the experiences supports how the types of attacks experiences are not in seclusion, despite the research participants having different roles within different organizations.

The external aspects of phishing attacks involve providing information from a legitimate outside source. These sources include clients, suppliers, and manufacturers. Each of these cases provided relate in some way to how a business already conducts its trade. During the interviews, when phishing topics discussed phishing towards personal home users who were not a part of an organization, these topics involved a personal relationship with an organization most people deal with, such as a government tax collection agency. Speaking in regard to external phishing attacks, an investigator and security consultant said:

“I think the method that seems to be the most successful is when they provide some of the personal information to the person about themselves, because it convinces the individuals that are being phished that the entity knows about them like, ‘oh, well, they wouldn't have my phone number it wasn't, legit or my date of birth if it wasn't the bank.’ I think I have seen the successful ones of those are when the entity provides some relevant personal information that a normal member of the public wouldn't have about that person.”

It was also a circumstance that phishing was experienced from sources within an organization. These situations are usually facilitated through a compromised internal account. These accounts are used as a foothold to gain sensitive information such as credentials or financial transactions.

A senior information security manager stated, “I have seen that they will somehow get access to certain employee email addresses and information, so they'll tailor their email sounding like they are someone from within the actual company, and so that can be successful.”

There was consistency of understanding with how phishers manipulate communications and digital tools to achieve their ruse. Participants spoke about the reliance of exploiting human mistakes and this usually leveraged seemingly minute details. Two individuals spoke about this tactic in more detail:

“It's also no more than creating a fake website, a spoof website or even a spoof email address and changing one small letter, or having an email go somewhere else that looks convincing and enable somebody to either to go to a different website and put in information or make a phone call, or it's some kind of very rudimentary enticement”

Another participant said, “Typically, there will be a domain that is not a valid domain, maybe Google with 3 O's, or a misspelled Microsoft or something like that.”

Overall, with legitimacy the most discussed topic from the interview participants, there are many stories shared in which hackers try to phish for information. However, legitimacy was not discussed in isolation. The stories shared were often prefaced with legitimacy ruses, followed by some other tactic. An IT manager shared an example, “I would say the most effective one in Canada is the CRA [Canada Revenue Agency], where people are asking people say that somebody has a tax return. They have to go into a certain place to provide some details in some cases, send a check or send a money order, or wire transfer for the fee.” This is an example of how multiple manipulative communication tools are used. In the above case, the whole ruse is prefaced with being from the CRA and followed by using a benefit claim in receiving a tax

return. Another interviewee talked about similarly using the CRA but followed with a loss claim in the form of a fee needed to be paid to the CRA.

Data Gathering

Data gathering was discussed among almost all interviews. It was also phrased as a critical component of phishing attacks. One individual claimed that the success of a phishing attack was gathered on the data collected and used prior to the manipulative communication:

“It really kind of depends on what information they can gather from your company... Where they've actually spent the quality of time to understand who they're actually hitting. I think that in itself will be most successful why phishing attacks may have a better chance of getting to a larger number of people and getting to them quick, but to actually get these or to click on it, it would require a spear phishing attack.”

Another interviewee describes the value of data gathering in similar manner,

“In terms of successful phishing, it's going to be if attackers are not lazy and they are ones that are the ones that actually do a little bit of reconnaissance and make a little bit of effort and do something where they craft something and make it look pretty realistic.”

This same person also shared their experiences with generic phishing attempts within their organization:

“Sometimes they're using really lame attempts, this is like bad English, it doesn't make any sense. Does not apply to the organization. They're getting people to click on links that are obviously not related to totally bogus the hosted on mass hosting websites or not hosting websites with really lame forums. Like who in their right mind would actually do that? For the most part, nobody here, at least that we're able to detect the success rate for that is quite low. However, I have a suspicion that they're actually doing that on purpose

to actually get the really gullible people who are just gonna do anything. There's that tactic of just making it super lame and obvious, but then there's the other tactic of being very close and doing a lot of reconnaissance on whether research and making it look really, really good, and perhaps targeting certain individuals or groups or high profile or high-risk type individuals”

Loss

Most of the research participants focused on how phishers will use negative circumstances to play on the natural human desire of self-preservation. The experiences discussed all relate to a single aspect of loss. Money and finance were the most talked about objects of loss, as one interviewee summarized the attitudes of all the interviews:

“Money talks. That’s the motivation of the attackers too, and certainly in some of the ones that I’m aware of that hit the news. Hey, there might be something wrong with my account and it’s going to cost me something or I'm going to get something monetary if I do this. And I think that money is a big motivator for attackers and/or their victims.”

This experience and belief of financial loss toward phishing victims and the monetary benefit for the hacker was echoed across all participants.

Part 2: News Articles Descriptive

90 out of the total 217 news articles collected contained content related to discussing phishing tactics, excluding any technical hacking tactics. From the top three security news websites identified, a significant weight towards legitimacy phishing methods is apparent. Just under half of all phishing tactic themes discussed in 2017 security industry news sources accounted for content related toward legitimacy. This accounts for almost half of all themes

discussed for security news articles. Table 4 outlines the frequency of codes extrapolated from news articles in order from most prevalent to least.

Table 4		
<i>News Source Phishing Frequency</i>		
Code	Frequency	Percentage
Legitimacy	115	47.92%
Loss	21	8.75%
Benefit	17	7.08%
Curiosity	16	6.67%
Urgency	13	5.42%
Data gathering	12	5.00%
Authority	11	4.58%
Likeability	8	3.33%
Formality	7	2.92%
Pity	5	2.08%
Fear & Threats	4	1.67%
Helpfulness	4	1.67%
Social proof	2	0.83%
Scarcity	1	0.42%
Reciprocation	1	0.42%
Trust	1	0.42%
Biases	1	0.42%
Affective commitment	1	0.42%

Part 2: News Articles Qualitative

The results gathered from the news sources revealed simplistic descriptions of phishing tactics among the security industry. Although various topics about phishing were mentioned in all categories researched, the way in which phishing was facilitated was limited. Overall, phishing in the security news media focuses content about informing the security community around phishing instances rather than informing on the specific phishing tactics. Out of all the reviewed news articles, three main phishing themes emerged: legitimacy, loss, and benefit.

Legitimacy

Legitimacy is significantly the most discussed topic in the news articles that were collected. The explanation of how legitimacy was used among security news updates is limited. In almost all cases, phishing news stories are described with simply a fake product or service. A common example involves a fake app, website, or false email. These fake items were merely mentioned by name of the products such as Apple, Microsoft, CRA, IRS, etc. The manner in which the falsehood was conveyed is not described within the news articles.

When examining the scope of news material on phishing in 2017, it is apparent that there are almost limitless possibilities in the ways that legitimacy is used in the way of impersonation. Larger, more popular organizations appear to be more prominent in headlines. This shows that the services and products that are more popular are incorporated into phishing attempts more often. The power of symbols in media is obvious. What is also clear is the ubiquitous use of symbols, such as name recognition and logos, and how they can be hijacked for malicious intent. No organization is immune from having their brand appropriated.

Loss

The theme of loss in the collected news articles primarily related to instances of financial loss or account loss. In some cases, reports would announce certain types of phishing attempts being noticed in the public that were related to manipulations around loss. The most prevalent example of these attacks were phishing emails claiming an account would be deleted if certain actions were not completed by the phishing target. In most cases with account loss phishing, the desired goal of the attack is to have a target open a malicious weblink to a fake account login page where the credentials entered by the victim would then be captured by the phisher. Oftentimes, phished accounts were from financial institutions or other accounts with financial activity. However, simple social media phishing account login attempts were also identified, but less often compared to that of financial use.

Another similarity apparent with news sources was the ending of many of the reports providing simple end-user tips in preventing being victim to phishing attempts. These cases usually reduced a phishing instance to its most basic form by describing an alternative example. Commonly, this was seen in phishing stories followed by notes to the reader. In parts, these news sources both reported on current security events and they also intended to provide readers helpful tips. Some common helpful tips include, double-checking senders of emails, not logging into accounts through email links, and checking website URLs are correct.

Benefit

Articles with benefit-themed phishing attempts encompass a wide range of topics. Overall, the main benefit claim was financial, with a few cases of free items. Financially motivated phishing attempts included bank transfers, refunds, and pay raises. These were seen as the primary motivators. This topic was far less a discussion topic but still remained among the

top three themes present in the news sources. A main similarity between the few articles reporting on phishing with benefit-based influencers was a message stating directly or implying it was “too good to be true” in hopes of informing the reader to be on the lookout for these types of scams. Overall, considering this theme was in the top three most common phishing tactics, it displayed little importance in the content discussed within the articles.

Comparison

Reviewing both parts of this study and comparing them to material discussed within previous research projects, some commonalities between particular phishing tactics appear. Across all categories, legitimacy prevailed as the single most common and distinct characteristic when discussing phishing communication tactics with news media and security practitioners. The phishing communication tactics shared between both research parts include legitimacy, loss, and benefits. Across both parts of this research, some codes present in the academic literature had no frequency in the data collected from interview participants. These codes included integrity, diffusion, cognitive and cultural bias, truth bias, prospect, representative heuristic, anchoring and adjustment, Elaboration Likelihood Model, Protection Motivation Theory, self-concepts, affective commitment consistency, social proof, and fabrication.

News articles in the security media compared with the academic literature (Table 2) shows a good comparative look of how security is being publicly discussed in different professions. The quality of data gathered from interviews with security professionals is far greater. The quality increase could contribute to the ability for the qualitative nature of the interview equalling roughly 45-minutes on average, significantly longer than any single news article that can be read in a matter of minutes. Yet, despite the significant time dedicated to IT professionals, the overall frequency of communications topics is minimal.

Between both parts of the study, when legitimacy was discussed in the data, it was prefaced or followed by an additional code. This would imply multistage rhetorical communications tactics targeted to support the legitimacy strategy most commonly employed by phishers. This was mostly supported by the interviews as they elaborated more in-detail about the language used in phishing messages. In addition, in the rare cases from the news sources that were more extensive on phishing, tactics show similar sequences of the legitimacy code preceded or followed by additional topics.

Social and political contexts had similar occurrences between both parts of the study. Some of the interview participants saw an increase of phishing attacks as certain significant political or social events were happening nationally or globally. A good example of this that was mentioned by one person was how they would see phishers use natural disasters where they would impersonate a charity asking for donations to support relief efforts. Another industry expert shared that they see an increase of tax-related phishing scams in and around tax time among any country. Lastly, one IT manager said when their organization had a data breach that they saw hackers using that news as leverage to convince employees to give up banking information. All these experiences with the interviewees are mirrored with the news articles examined. Common examples In 2017, following a company disclosing a data breaches, news reports would later emerge about scams targeting those corporations. During Canadian and American tax deadlines for citizens, a higher number of articles about tax-related phishing were present.

Twelve themes classified in academic literature were absent from both parts of the study: account information, anchoring and adjustment, attraction, consistency, diffusion, integrity,

overload, politeness, representative, self-concepts, tradition, and truth bias. These influencers, although not present in the sources in this study, have been extensively researched.

Many of phishing topics collected by this research involve a variety of communications methods of manipulation and information gathering. The impersonation of a client or internal stakeholder is the most common example in the data collected. Some instances also indicated the use of the collection of information to better convince and build a legitimate looking entity.

Discussion

The analysis and results of the study identify the importance of communications in phishing as an underlying category of this type of cybersecurity threat. Examining phishing from a communications perspective reveals far more complex components of a false message with the intent of installing malicious programs or collecting sensitive information. The biggest challenges identified with mitigating phishing in this study and supported by peer-reviewed literature is that the education of end users is critical to address the social vulnerabilities in information security. From the interview data collected and textual content within security news reporting, the need and push for phishing education is heavily supported by industry stakeholders.

The information collected in this research mirrors most similarly to Atkins & Huang's (2013) analysis of frequencies with persuasion tactics used in phishing emails shows some similar results as shown by both parts of this study. Atkins & Huang's definition of authority best relates to this study's definition of legitimacy; this should not be mistaken for the definition of authority used in this study. Authority in this study makes a strong distinction in power imbalances, as Atkins & Huang's study does not. However, the strength of legitimacy in both this and their research is similar. The overall commonality with legitimacy claims among both

news reports and professionals in regards to experiencing legitimacy phishing attacks supports the importance of this topic.

Considering the overwhelming support for education to identify and deal with phishing within the academic community, the understanding of phishing within the information security industry is lacking. Given the disconnect of information between academia, industry-specific media, and security practitioners, the overall education awareness of phishing is limited. Besides those professionals that have a specific role in educating in regards to phishing, other roles have an incomplete understanding of this cybersecurity threat. What some interview participants had mentioned in part to this lack is the funding and observable direct financial benefit of phishing educations within organizations. Interviewees expressed interest in the multiple aspects of phishing being studied, but they hesitated to provide information to describe circumstances of phishing tactics beyond legitimacy, loss, and benefit.

Based on the data collected in the two research parts of this study, urgency, politeness, and formality are not shared among the common themes of phishing messages experienced by the information security industry. This is not to suggest these tactics are not used, as it has been shown in other research of phishing messages coded in similar ways shows these tactics used by phishers (Atkins & Huang, 2013). Rather, this further supports the claim of disconnect in the security industry with the communication literature with phishing identification and prevention. The strength of Atkins & Huang research is the code analysis of actual phishing messages. Yet from this content messages are not carried over to security news media and security practitioners.

Compared with industry-specific news media, security practitioners were able to elaborate on the topics used, but this was more limited than what was examined in the academic literature when first starting this study. Interview participants remained reluctant to expand on

sequences of phishing communications tactics. Again, at the surface level, it shows that these individuals are not directly familiar or comfortable with the social side of phishing despite support by them to educate end users on the topic. Both security news media and IT security practitioners share a reluctance to dig deeper into the communication tactics surrounding manipulation in phishing. At points within both parts of the study, social communications were mentioned as an important topic, but sources could not elaborate on the subject.

This research fits among the academic security literature by showing how information on phishing tactics is readily accessible, although limited in quantity from a communications perspective. The content contained within the research literature does not contradict the conclusions made in this research. In addition, the conclusions made in the literature were not inaccurate, but too broad in scope to relate to the reality of what is being experienced within the security industry. There were no new phishing tactics that were discovered through the process of this research. Rather, the research offers a more focused approach for researchers which allows the emergence of other areas of phishing incidents in order to address immediate concerns being experienced on a daily basis.

When it comes to information security, the primary discussion regarding solutions to social vulnerability is skewed towards technical solutions. Enhanced training for IT professionals to better understand phishing nuances can assist, inform, and protect end users for whom security practitioners are responsible.

By comparing all three components of this research (literature, interviews, and news articles) a few conclusions become clear. Legitimacy is a common component of phishing cybersecurity attacks. This conclusion is supported by all security stakeholders as shown in the news media, academic literature, and interviews. There are some disconnects in the

understanding of phishing between some information security stakeholders. The works in the academic sphere of phishing are not always relevant to the actual practice in the mitigation of phishing attacks. In addition, the research that is of benefit to the security industry may not always be shared effectively to change practice and increase awareness for both consumers and security practitioners.

There is not any material present from the interviews and news articles that was not present in the academic literature. The scope of information present in each phishing information source differs based on the intended audience. What is common across each source is the shared goal of minimizing or preventing phishing attacks. The crossover between news media, practitioners, and academic literature is absent. When discussing sources of information about phishing, no interview subjects mentioned academic sources and only a few cited security news media. Security news articles focused solely on events and did not mention academic research. The academic literature collected for this research seldom referred to phishing events as the basis for their study and none included the experiences of information security professionals.

Conclusion

Given the evidence collected from active information security professionals tasked with mitigating phishing, legitimacy is the most important manipulative strategy when it comes to phishing and cybersecurity attacks. This strength is only further supported by security news media as legitimacy also ranked as the most discussed topic in published works. For the phishers, communicating with a target of a cyberattack and providing information made to be seen from a credible source are the utmost priorities. The communications from phishers are centered primarily on legitimacy, followed by additional supporting rationale by the attacker. These

additional rationales included one of the many other phishing tactics outlined within the phishing literature.

The information security industry is most familiar with false messaging regarding phishing attempts to circumvent security through appeals of legitimacy. These attacks are where an aggressor will attempt to provide convincing information of a false identity or impersonation. In everyday situations and media discussions, legitimacy ploys are often followed by other manipulative strategies to support their claims. This was clear in the coding process in both the interviews with information security professionals and security news sources describe multistage approaches in successful phishing cyberattacks. Phishing was commonly described as using a legitimacy manipulation scheme conjoined with at least one other of the manipulative communications methods.

The information present in all industries working toward anti-phishing goals is valid information; however, this information is not always shared between these industries and every industry has its weakness. The academic sphere of phishing research focuses more on technical systems-oriented solutions and little research has been done on the communications aspect of phishing. The breadth of current academic literature identifies, examines, and explains phishing tactics in great detail. As concluded in this research, not everything researched is being experienced among current real-world phishing instances, despite current academic study on phishing.

Between interview participants and news media sources, the details of the communication tactics used in phishing in the data collected of this research are limited in the explanation and understanding of how it works. It is common for any data source in this research to have mentioned legitimacy or any other type of manipulation without further explaining the meaning

and rationale for those manipulators. The description of phishing in many of these cases is limited by describing the event only by the definition or giving an instance of it occurring. Case examples were commonly used in both interviews and news media reports as ways to describe the phishing behaviours. The deeper meaning and importance of these various manipulation tactics were lacking, unlike the information present in the current academic literature.

Limitations

There are a few limitations to this research that should be recognized as areas of improvement for future study. First, the nature of qualitative research; with only six participants, this study does not directly measure the viewpoint of information security practitioners as a whole. However, the nature of the data demanded careful and detail-rich instances of phishing experiences by interviewees. Attempts were made to build a diverse and representative group of participants from across North America with relevant experience in security. Given the nature of the study, as a more explorative assessment of an area of security research that is often an oversight, it does provide a foundation from which to branch into other research topics.

Limitations to the second part of the research include the fact that the news articles were only collected from three sources. The quality and quantity of data gathered justifies the rationale for using only three media sources given the extensive information collected reaching a saturated point. Extending the data collection scope to incorporate more types of sources would be a benefit. Choosing from the most popular sources gave the most accurate overall attitudes to phishing at a global perspective. In addition, these are not the only sources of information security literature that is available to professionals. Trade magazine and industry white papers or some other sources of information mentioned among the research participants on how they may gather new knowledge.

The study relies on the recall of participants' ability to assess their experiences. This does not indicate that the information provided by the research participants is inaccurate. Rather, it must be noted that their recollection, viewpoints, and experience may not indicate what they actually experience. Given the relevancy of phishing within the daily basis in security practice among the professionals present in this study has a good reliability towards the data provided.

Future Research

Communications research and practitioners have a lot to offer the information security industry. Within the academic literature, there exists a justification for communication and training to prevent successful phishing attacks. Organizational communications research, theory, and practice can offer aspects to address the disconnects and miscommunication between security stakeholders. This research on phishing tactics has shown that most of the traditional studies on phishing have been examined and may not even contribute any more significant data for the security industry. The greatest benefit to phishing mitigation stakeholders is greater exploration of the social aspect of security, significantly within the communications of security.

Apparent from the literature review and this research, there is a need to explore the communications research with the way phishers organize cybersecurity attacks. The sharing of phishing research with industry stakeholders is crucial to cybersecurity practice and needs further development to build consistency between stakeholders.

Part of what this research provides is grounds to explore future projects for studying information security professionals' knowledge base and directing new perspectives for academic researchers to study phishing. Future research is needed to understand the communications landscape of phishing. Despite this study's attempts to advocate for the importance of

communications research and theory in information security and phishing, more work is needed to understand the complexity of this field.

Based on the conclusions of this research, recommended further projects should investigate the communications perspectives of industry-leading reports on phishing and self-proclaimed black hat, or malicious, hackers. Although this research examined the leading security news reporting sources and professionals, one common theme that emerged from the interviews with industry experts was their gathering of new security information from white papers and company reports on security topics.

Lastly, there is a clear disconnect between some of the understanding, importance, and complexity of phishing between academia, industry reporting, and IT security professionals. Based on the data in this paper and supported by former literature, there exists a need to expand research projects about phishing. Research into the practice of how information security knowledge is shared by academics and industry stakeholders is needed. Further research should focus on assisting security industry leaders with the knowledge and tools to better address phishing and to train others to do so.

References

- Abdelhamid, N. (2015). Multi-label rules for phishing classification. *Applied Computing and Informatics*, 11(1), 29–46. <https://doi.org/10.1016/j.aci.2014.07.002>
- Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, 32(3), 183–196. <https://doi.org/10.1016/j.techsoc.2010.07.001>
- Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, 68, 160–196. <https://doi.org/10.1016/j.cose.2017.04.006>
- Alseadoon, I. M., Ramadan, R. A., & Khedr, A. Y. (2017). Cultural impact on Users' Ability to protect themselves against Phishing websites. *IJCSNS*, 17(11), 1.
- Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, 82, 69–82. <https://doi.org/10.1016/j.ijhcs.2015.05.005>
- Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 29(3), 706–714. <https://doi.org/10.1016/j.chb.2012.12.018>
- Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304–312. <https://doi.org/10.1016/j.chb.2014.05.046>
- Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences*, 1(3), 23–32. <https://doi.org/10.4236/jss.2013.13004>
- Baker, S. E., & Edwards, R. (2012). How many qualitative interviews is enough?: Expert voices and early career reflections on sampling and cases in qualitative research.
- Benenson, Z., Gassmann, F., & Landwirth, R. (2017). Unpacking spear phishing susceptibility. In *International Conference on Financial Cryptography and Data Security* (pp. 610–627). Springer.
- Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*. Thousand Oaks, CA: Sage Publications.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations

- explained. *Information and Computer Security*, 25(5), 593–613.
<https://doi.org/10.1108/ICS-03-2017-0009>
- Coyne, I. T. (1997). Sampling in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries? *Journal of Advanced Nursing*, 26(3), 623–630.
<https://doi.org/10.1046/j.1365-2648.1997.t01-25-00999.x>
- Crabtree, B. F., & Miller, W. L. (1999). *Doing Qualitative Research*. SAGE Publications.
Retrieved from <https://books.google.ca/books?id=MEd2AwAAQBAJ>
- Darwish, A., El Zarka, A., & Aloul, F. (2012). Towards understanding phishing victims' profile. In *Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on* (pp. 1–5). IEEE. Retrieved from
<http://ieeexplore.ieee.org/abstract/document/6454454/>
- Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Online Interactivity: Role of Technology in Behavior Change*, 26(6), 1739–1747. <https://doi.org/10.1016/j.chb.2010.06.023>
- Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security*, 26(1), 73–80. <https://doi.org/10.1016/j.cose.2006.10.009>
- Felderer, M., Zech, P., Breu, R., Büchler, M., & Pretschner, A. (2016). Model-based security testing: A taxonomy and systematic classification. *Software Testing, Verification and Reliability*, 26(2), 119–148. <https://doi.org/10.1002/stvr.1580>
- Gold, S. (2011). The rebirth of phreaking. *Network Security*, 2011(6), 15–17.
[https://doi.org/10.1016/S1353-4858\(11\)70064-2](https://doi.org/10.1016/S1353-4858(11)70064-2)
- Gondim, J. J. C., de Oliveira Albuquerque, R., Nascimento, A. C. A., Villalba, L. J. G., & Kim, T.-H. (2016). A methodological approach for assessing amplified reflection distributed denial of service on the internet of things. *Sensors*, 16(11), 1–31.
<https://doi.org/10.3390/s16111855>
- Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2017). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems*. <https://doi.org/10.1007/s11235-017-0334-z>
- Gupta, G., & Pieprzyk, J. (2011). Socio-technological phishing prevention. *Information Security Technical Report*, 16(2), 67-73. <https://doi.org/10.1016/j.istr.2011.09.003>
- Heartfield, R., & Loukas, G. (2016). A taxonomy of attacks and a survey of defence mechanisms

- for semantic social engineering attacks. *ACM Computing Surveys (CSUR)*, 48(3), 37.
<https://doi.org/10.1145/2835375>
- Hinde, S. (2004). "All you need to be a phisherman is patience and a worm." *Computer Fraud & Security*, 2004(3), 4–6. [https://doi.org/10.1016/S1361-3723\(04\)00038-7](https://doi.org/10.1016/S1361-3723(04)00038-7)
- James, L. (2006). *Phishing Exposed*. Rockland, MA: Syngress.
- Jansson, K., & Von Solms, R. (2011). Social engineering: towards a holistic solution. In *Proceedings of the South African Information Security Multi-Conference: Port Elizabeth, South Africa, 17-18 May 2010* (p. 23). Lulu. com. Retrieved from <http://books.google.com/books?hl=en&lr=&id=RnzIAgAAQBAJ&oi=fnd&pg=PA23&dq=%22organizations+spend+large+amounts+of+money+to+ensure+that+their+information%22+%22is+compromised,+unavailable+or+unprotected,+the+organization+can+in%22+%22can+deceive+an+employee+into+compromising+sensitive%22+&ots=LAfcHDTwSD&sig=I8QaMFbY1gcrCMiF2Hfj1gLcHFU>
- Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, 32(6), 584–593. <https://doi.org/10.1080/0144929X.2011.632650>
- Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: A real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (p. 3). New York, NY, USA: ACM. <https://doi.org/10.1145/1572532.1572536>
- Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2), 7. <https://doi.org/10.1145/1754393.1754396>
- Marshall, M. N. (1996). Sampling for qualitative research. *Family Practice*, 13(6), 522–526. <https://doi.org/10.1093/fampra/13.6.522>
- Mason, M. (2010). Sample Size and Saturation in PhD Studies Using Qualitative Interviews. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 11(3). doi:<http://dx.doi.org/10.17169/fqs-11.3.1428>
- McGraw, G. (2004). Software security. *IEEE Security Privacy*, 2(2), 80–83. <https://doi.org/10.1109/MSECP.2004.1281254>
- Mitnick, K., & Simon, W. L. (2012). *Ghost in the wires: My adventures as the world's most wanted hacker* (1st ed.). New York: Back Bay Books.

- Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review*, *17*, 1–24.
<https://doi.org/10.1016/j.cosrev.2015.04.001>
- Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers & Security*.
<https://doi.org/10.1016/j.cose.2015.02.008>
- Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597–611. <https://doi.org/10.1016/j.cose.2011.12.010>
- PhishMe. (2017). *Enterprise Phishing Resilience and Defense Report*. Retrieved from <http://cofense.com/wp-content/uploads/2017/11/Enterprise-Phishing-Resiliency-and-Defense-Report-2017.pdf>
- Robila, S. A., & Ragucci, J. W. (2006). Don't be a phish: Steps in user education (p. 237). ACM Press. <https://doi.org/10.1145/1140124.1140187>
- Rubin, H. J., & Rubin, I. (2011). *Qualitative interviewing: The art of hearing data*. Thousand Oaks, Calif: Sage Publications.
- Saldaña, J. (2009). *The coding manual for qualitative researchers*. Los Angeles : Sage,.
- Sarno, D. M., Lewis, J. E., Bohil, C. J., Shoss, M. K., & Neider, M. B. (2017). Who are Phishers luring?: A Demographic Analysis of Those Susceptible to Fake Emails. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *61*(1), 1735–1739.
<https://doi.org/10.1177/1541931213601915>
- Schneier, B. (2000). Semantic network attacks. *Communications of the ACM*, *43*(12), 168-168.
<https://doi.org/10.1145/355112.355131>
- Securelist. (2018) *Spam and phishing in 2017*. Retrieved April 11, 2018, from Securelist website: <https://securelist.com/spam-and-phishing-in-2017/83833/>
- Smyth, V. (2015). Cyber-security fortresses built on quicksand. *Network Security*, *2015*(8), 5–8.
[https://doi.org/10.1016/S1353-4858\(15\)30068-4](https://doi.org/10.1016/S1353-4858(15)30068-4)
- Srikwan, S., & Jakobsson, M. (2008). Using cartoons to teach internet security. *Cryptologia*, *32*(2), 137–154. <https://doi.org/10.1080/01611190701743724>
- Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2013). Information security professionals' perceptions about the relationship between the information security and internal audit functions. *Journal of Information Systems*, *27*(2), 65–86.

- <https://doi.org/10.2308/isis-50510>
- Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behaviour & Information Technology*, 32(10), 1014–1023. <https://doi.org/10.1080/0144929X.2013.763860>
- Twitchell, D. P. (2009). Social engineering and its countermeasures. In *Handbook of research on social and organizational liabilities in information security* (pp. 228-242). IGI Global
- Verizon. (2018). *2018 Data Breach Investigations Report*. Retrieved April 11, 2018, from <http://www.verizonenterprise.com/verizon-insights-lab/dbir/>
- Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51(3), 576–586. <https://doi.org/10.1016/j.dss.2011.03.002>
- Wenyin, L., Fang, N., Quan, X., Qiu, B., & Liu, G. (2010). Discovering phishing target based on semantic link network. *Future Generation Computer Systems*, 26(3), 381–388. <https://doi.org/10.1016/j.future.2009.07.012>
- Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 59(4), 662–674. <https://doi.org/10.1002/asi.20779>