



# What Makes People Click? Designing an Effective Phishing Test

Andrew Bates, Thomas Caldera, Carolyn “Kari” Grafton, Shanita Hunt, Pedro Valencia

University of Illinois Springfield  
MIS 584 – Capstone  
Spring 2021  
Dr. Sahar Farshadkhah

Submission Date: 30 April 2021

## Table of Contents

Executive Summary	4
Introduction	6
Problem Statement	9
Purpose and Research Questions	11
Scope, Assumptions, and Limitations	12
Research Methodology	13
Literature Review	15
Preparation	17
Social Engineering	20
<i>Defining Social Engineering</i>	20
<i>Themes of Phishing Emails</i>	21
<i>Susceptibility Characteristics</i>	23
<i>Effects of Social Engineering</i>	24
Training	26
Literature Review Findings	28
Phishing Test Methodology	29
Why a Phishing Test?	29
Test Design	30
Education Page Design	34
Test Setup	40
Data Analysis & Results	44
Results & Metrics	44
CompanyN Phishing Test	50
Conducting the Test	50
Cleaning Server Logs	52
Cleaning other Data	54
Building the Database	55
Test Metrics	57
Recommendations	60
Conclusion and Recommendations	62
References	68

Appendix A: Institutional Review Board Approval Letter	74
Appendix B: Code	77
index.php	77
list_upload.php	83
mailer.php	84
Appendix C: Report Provided to Client	85
Background	87
Test Design	87
Results	89
Recommendations	93

## Executive Summary

This study provides a comprehensive review of the various components of phishing emails and what makes them successful. In this case, the definition of “success” is from the standpoint of a phisher. A successful phishing attempt is one in which the user engaged in clicking on a link or opening an attachment, thus, releasing the threat. The intention of our review is twofold. The first intention is to determine if there are specific templates or features of a phishing email that make them more or less tempting to the targeted user(s). Second, we aim to identify areas of opportunity employers can focus on for employee education and training to limit the number of successful phishing attempts at their organization. This study is based on a review of scholarly literature, case studies of successful phishing attacks, and a phishing email test performed at a local organization, henceforth known as the “client”.

A thorough review of literature found that successful phishing attacks can be created keeping in mind two key points: preparation and social engineering. With regards to preparation, the sender focuses on the audience, be it a company, organization, or individual. Our review of literature found emails that invoked fear, urgency, or greed have the highest likelihood of success. Additionally, using personalization builds a level of trust with the recipient, creating an emotional connection, increasing the probability of success. Some examples our review found to be most successful include bank related spoofs, tax scams, and failed delivery package messages. Over the past year, phishers have used the COVID-19 pandemic as another scare tactic to tap into the fear and emotions of the victim.

In addition to the review of literature on the topic, we also conducted our own phishing email test with an organization of over 500 employees. The client provided a list of 521 company emails, to which we sent a phishing test email. The traits of the email included a nearly

identical company name and email address, and asked users to check their secure message from IT by clicking the link in the email. Further details of the test and methodology can be found in the “Test Design” section of this paper. The implementation of our test email produced the following results:

- Emails sent: 521
- Emails sent successfully (not bounced back): 513
- Emails opened: at least 212
- Unique link clicks: 66
- Reported as suspicious to IT: 95

These results were shared with the client so they can better understand their employees’ current level of ability to identify and report potentially harmful emails. The client intends to use the results to design and provide further education and training to their employees. Based on our test results and literature review findings, we offer the following recommendations to decrease the likelihood of a phishing breach:

- **Emphasize how to identify key factors of a suspicious email.** The main factor in preventing a breach through a suspicious email is to understand the elements that make up a phishing email. These items include the use of emotional triggers such as scare tactics and an appeal to feeling sorry for the sender. Physical traits include the sender masking themselves as a legitimate sender by using a nearly identical email address, oftentimes just a single character different. Other items include attachments or links embedded in the email.

- **Implement a robust inbound email scanning system.** Automatically flag external emails with an indicator to the recipient to serve as an immediate identifier for the recipient to examine the email before opening attachments or clicking links.
- **Test employee knowledge and training using test phishing emails.** Send regular test phishing emails from external sources with various traits so employees are constantly faced with having to thoroughly review emails before acting on them.

## Introduction

Since the advent of computer systems, there have been many methods by which hackers attempt cyber-attacks. While some of these methods have become obsolete, one prevalent and still-effective attack technique is phishing. There are many ways to describe phishing, but for the purposes of this report, we are using the United States Federal Trade Commission definition (United States Federal Trade Commission, 2021):

“A form of fraud in which a scam artist sends an email (or places a phone call) purporting to be from the recipient's bank, internet service provider, or other trusted source and asking for personal information such as credit card or bank account numbers, passwords, or Social Security numbers.”

Phishing has become one of the most commonplace hacking attempts due to its focus on the use of social engineering. Research has revealed almost 90% of all companies in the United States have experienced a phishing attempt (Proofpoint, 2020). Additionally, phishing attacks comprise between 80 and 90 percent of all data breaches, with an average price tag of \$3.8 million. In 2019, phishing scams increased 65% over 2018 (Cost of a data breach report, 2020). With regards to awareness and knowledge of phishing, a recent survey found that only 49% of Americans correctly understood what phishing is (Proofpoint, 2020).

Depending on the type of attack, in addition to financial ramifications, successful phishing breaches can hinder productivity, cause data loss, and result in a damaged company reputation. These facts outline the importance of understanding what phishing is, how to identify an attempted attack, and providing regular training and phishing simulations to employees. Existing literature provides insight into each of the various aspects of phishing, training, education, and impacts, but none combine all of them into a single review. As such, we set forth to provide a comprehensive review of phishing, the use of social engineering, and how to focus training to thwart attacks. This paper combines this qualitative review with a real-life phishing simulation at 500+ employee organization. To better understand the effectiveness of phishing and how we can thwart future attacks, we must first understand the history of phishing and how it works.

As described in *Steal this Computer Book 3: What they won't Tell you About the Internet* by author Wally Wang (2003), the first known case of a widespread phishing attack occurred in 1995 when a hacker created a toolkit, called AOHell, to steal passwords and credit card information from America Online (AOL) users. This program sent mass instant messages to AOL users claiming AOL customer service needed to perform a security check. In order for AOL to perform the security check, the message asked users to enter their username and password to continue. In reality, the program was simply recording the keystrokes of the users, effectively stealing their AOL credentials (Rekouche, 2011).

Electronic phishing is akin to actual sport fishing. In sport fishing, the fisherman baits a hook to entice a fish into biting it, resulting in the hooking of the fish and successful capture. Similarly, with electronic phishing, the hacker baits the victim with false information, leading to the hooking of the victim and successful capture of confidential and sensitive information. The

term fishing was transformed to phishing to relate it to “phreaks” (Merriam-Webster). In the 1990s, a phreak was someone who hacked telecommunications systems to make free phone calls. According to AOHell creator, Koceilah Rekouche (Early phishing, 2011), he is the first to use of the term phishing, when he used it in his AOHell program.

While there are many forms of phishing—SMS, voice, instant messaging—to name a few, this report focuses on email spoofing. Email spoofing is when a hacker sends an email that appears to be from a legitimate sender but is actually littered with harmful links and/or attachments. A variety of attacks can occur through the use of spoofing emails. A masked link, when clicked, take the user to a page that contains a form to fill out personal or confidential information. An infected file attachment, when opened, can unleash malware or ransomware.

As we review education and training methods that could help thwart attacks, we first need to understand why people fall for the tricks. This concept is called Social Engineering. Social engineering has historically applied to governmental or private company efforts to influence or trick citizens into changing behaviors and decisions. This same concept has expanded into the cyber world, where social engineering tactics are used to trick people into providing confidential information, clicking harmful links, or opening infected attachments. The United States Cybersecurity & Infrastructure Security Agency (2020) explains social engineering as the use of

“human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity.”



No matter the attack method, phishing attacks rely heavily on social engineering to trick users into falling for the attack.

This paper will identify effective phishing techniques and how education and training focused on identifying phishing tactics can help reduce breaches. The paper will include the following sections: Problem Statement; Purpose and Research Questions; Scope, Assumptions, and Limitations; Literature Review; Methodology; Results and Discussion; Recommendation and Conclusion; References; Appendices.

## Problem Statement

As previously mentioned, phishing has been a common form of cyber attack since the early 1990s. Through the use of social engineering techniques, hackers are able to take advantage of human misjudgment and penetrate security measures. Many phishing attacks are mass emails sent to many users with hopes that even just a small percentage of recipients fall for the trick. Successful data breaches caused by phishing attacks can have devastating, long-term impacts on companies across all industries.

The FBI stated in their *2019 Internet Crime Report* that business email compromise (BEC) scams accounted for over \$1.77 billion in losses for victims in 2019 (Internet Crime Complaint Center IC3, 2019). According to a report published by IBM (Cost of a data breach report, 2020), the global average cost of a data breach between August 2019 and April 2020 was \$3.86 million. The same IBM report also found that data breaches cost United States companies more than double that of the international average: \$8.64 million (2020). In addition to financial impact, data breaches can cripple companies in other ways. High profile attacks that receive major media coverage can damage the reputation of a firm and lose both employee and consumer

trust. Losing trust of customers and employees can result in indirect financial losses due to decreases in productivity and customer loss.

Another negative impact that can result from a phishing attack is the loss of intellectual property (IP). A 2017 report published by The National Bureau of Asian Research on behalf of The Commission on the Theft of American Intellectual Property (2017) found that annual costs to American companies related to IP theft range between \$225 billion and \$600 billion. Depending on the IP stolen and company size, one single breach can completely render a firm irrelevant. In one case, a systems administrator destroyed his engineering firm's intellectual property (software). Ultimately, the company couldn't rebuild its software which led to the company losing all competitive status in the market (Gaudin, 2002).

Phishing related data breaches can cost companies as a result of legal and regulatory implications. Depending on the industry, a data breach can lead to additional fines and penalties from the government. For example, the healthcare industry is regulated by the Health Insurance Portability and Accountability Act (HIPAA) and companies that accept credit cards must adhere to the Payment Card Industry Data Security Standard (PCI DSS). Fines and penalties levied as a result of these regulatory bodies are in addition to the aforementioned impacts. According to the U.S. Department of Health and Human Services, minimum penalties related to HIPAA data breaches range from \$117 to \$58,490 per incident (Annual Civil Monetary Penalties Inflation Adjustment, 2020). Per healthcare compliance watchdog HIPAA Journal (2021), in 2020 alone, there were 527 healthcare organizations that suffered a data breach, and more than 21 million patients' information was exposed. So far, nineteen of the 527 cases have been settled at a staggering cost of over \$13 million.

Phishing attacks will never be 100% preventable, but appropriate training and education can help thwart attacks. Due to human curiosity, people are intrigued to click links or open attachments that seem interesting. Another problem is that some people simply do not pay attention to what they're doing and click the infected links or open the attachments. These factors are key to building effective training and education, so a thorough review of the email becomes second nature to the employees.

## Purpose and Research Questions

The main purpose driving our research is to dissect the most effective aspects of phishing emails to better understand which training and education methodologies can be implemented to prevent attacks. To accomplish this, we must first understand the structure and components of phishing emails. To better understand phishing emails and components, we've developed the following two research questions:

### **1. What traits do a majority of successful phishing emails contain?**

We examined the various features of successful phishing emails. We also reviewed literature on social engineering and how humans can be manipulated into doing something against security policy.

### **2. What does a successful phishing email template contain?**

The first research question examines specific traits of successful phishing emails.

This research question aims to address how we can combine the key traits that make phishing emails successful into a single, gold standard phishing email template.

The first two research questions focus on the construction of a successful phishing emails. Once we identify the makeup of a successful phishing email, we can focus on creating effective

training and education to prevent attacks. As such, we've asked the following additional research questions:

**3. What areas of training do companies need to focus on to educate their employees better on identifying phishing emails? And what steps are available for an organization to educate their employees better?**

We reviewed training and education techniques available at various organizations.

This allowed us to realize which methods are effective and which methods leave areas of opportunity for improvement. As we learned more about current training and education techniques, we were able to determine which were most effective.

After researching these questions, we will recapitulate our findings to determine the most effective phishing email template and best path forward in phishing attack prevention.

## Scope, Assumptions, and Limitations

The concept of cybersecurity and the various threats we face can expand into endless discussion. Even within the specific topic of phishing, there are many facets and sub-attacks to review. Similarly, there are different methods of prevention training and education depending on the type of cyber-attack tactic. This review focuses on phishing attacks using emails as the delivery mechanism. Regarding attack prevention education and training, we concentrate on what can be done to improve (decrease) the number of times employees fall for a phishing scam distributed through email.

As with any research study, there are limitations. In our case, time and sample size are the biggest limiting factors to produce a more thorough review. The timeline provided allows for about ten weeks to complete a full literature review of the two key topics as well as conduct testing to determine the most effective phishing email template. This is a fairly short turnaround

time to complete this work. We are also limited to a small sample size through a single organization with a finite number of resources to implement our A/B testing. Since we have a small sample size, the results cannot necessarily be extrapolated to other companies and the broader population.

We made three assumptions during this project. First, we assumed all employees at the testing organization have access to email. Second, we assumed that the employees were not told about the testing and are unknowing of our work. Finally, we assumed that with a better understanding of specific traits that make a phishing email successful, employees will be less likely to fall for the attack.

## Research Methodology

We conducted a systematic literature review to identify key aspects that impacted the effectiveness of a phishing email. A systematic literature review involves using a specific method to search and analyze as many studies as possible to learn about your topic, answer your research questions, and identify areas of improvement for future research. The team initiated the literature review by searching for studies in different databases (Business Source Complete, ACM Digital Library, IEEE Digital Library, and Google Scholar) published from 2015 - 2021. However, if a publication were referenced multiple times in peer reviewed studies, it was considered relevant to the research if the keywords matched.

The studies reviewed successful phishing attacks, social engineering that is associated with those attacks, and studies involving training techniques used to prevent phishing success (a failure for the organization). The keyword phrases for the searches were as follows: *Phishing*, *Social Engineering*, *Phishing Security*, *Phishing Training*, *Phishing Email*, *Phishing Crime*,

*Phishing Statistics.* From those six searches, the team was able to reduce the publications based on the parameters above, recency, relevance, and citation accountability. The team also relied on statistical information provided by government organizations as well as professional associations concerned with tracking cyber-attack activities.

We utilized our findings to answer three research questions, design an ‘ideal’ phishing email to test on a company, and to use those results to develop general recommendations for training in phishing prevention. The successful portions of the email were emphasized and explained in detail. Possible variations to those portions of a successful phishing email were also highlighted to bring attention to the ever-expanding universe of phishing emails.

The team separated the publication research into three overarching themes to best support our research questions: Emails and Social Engineering, Training Recommendations, Government/Statistical Publications. Table 1 reveals the number of the references for each theme and the year they were published. We had a total of forty-seven sources. Twenty-three of these sources were experiments related to phishing tests. The other twenty-four studies discussed social engineering, successful email attacks, and statistics. Most publications contained data on phishing attacks, such as the percentage of data breaches that were successful and other pertinent information. Most of the studies were used to identify key aspects of phishing tests.

<b>Year</b>	<b>Themes</b>		
	<i>Emails and Social Engineering</i>	<i>Training Recommendations</i>	<i>Government/Statistical Publications</i>
<b>1997</b>	1		
<b>2002</b>	1		
<b>2003</b>	1		
<b>2005</b>		1	
<b>2007</b>	1	2	
<b>2008</b>		1	
<b>2009</b>	1	1	
<b>2010</b>	3	2	
<b>2011</b>	1		
<b>2013</b>	2		
<b>2015</b>	1	1	1
<b>2016</b>	3		
<b>2017</b>	1	3	1
<b>2018</b>			1
<b>2019</b>		2	1
<b>2020</b>	7	1	5
<b>2021</b>			1
<b>Total Studies</b>	<b>23</b>	<b>14</b>	<b>10</b>

*Table 1 - Analysis of references by theme and year*

## Literature Review

Cyber attackers have always posed a threat to the security of information systems and sensitive data. While companies have become more aware of the threats and began to increase its countermeasures, phishing attackers have become more sophisticated (Jakobsson et al., 2016). The rise of the Internet, the age of digitalization, and the COVID-19 pandemic has increased the prevalence of phishing attacks. Google reported registering 2.02 million new phishing websites in 2020 (Chandler, 2020). Many organizations have employees working from home and students, from kindergarten through college, enrolled in virtual learning. This increases the opportunities for attackers to use cyberattacks, such as phishing, to gain access to people's corporate credentials to steal the organizations' sensitive information. Employees' activities are not being monitored and trained as securely as it can be from on-site. Thus, companies are not being protected as efficiently as they could be from phishing attacks.

Phishing attacks negatively impact companies' finances, reputation, data, security, and employees. We analyzed several experiments, systematic literature reviews, and articles that focused on the design of effective phishing tests. This literature review was conducted to dig deeper into understanding why phishing attacks are so successful in getting people to click illegitimate links and sometimes even give up their sensitive credentials. This study examined the cause of failure to reject attacks from the employee and company side. We identified key aspects needed to design an effective phishing test. These attributes can be categorized into three main issues: preparation, social engineering, and training.

We begin the review by discussing how attackers prepare for phishing attacks such as setting goals, research on targets, choosing the right topic and campaign to trick victims, and what is done after the test is executed. These actions are very similar to the steps that companies take when it designs and utilizes phishing tests to train its employees. From this overview, we provided deeper research into two of the major elements of phishing attacks: social engineering and training. Next, we examined various social engineering techniques that are used in phishing emails. We discussed which psychological manipulation practice has the greatest effect on victims. We concluded the social engineering section with actions that employees and companies should take to reduce the effectiveness of social engineering attacks. Finally, our literature review identified training methods that have been used, the frequency of training, and its impact on preventing phishing attacks.

Our final analysis of the research allowed us to design an effective phishing test to conduct on a company. It also aided in the production of our recommendation to companies on an effective training plan for employees to be successful in identifying and rejecting attempted attacks. We hope that our research can be of use to more than IT professionals. Currently many

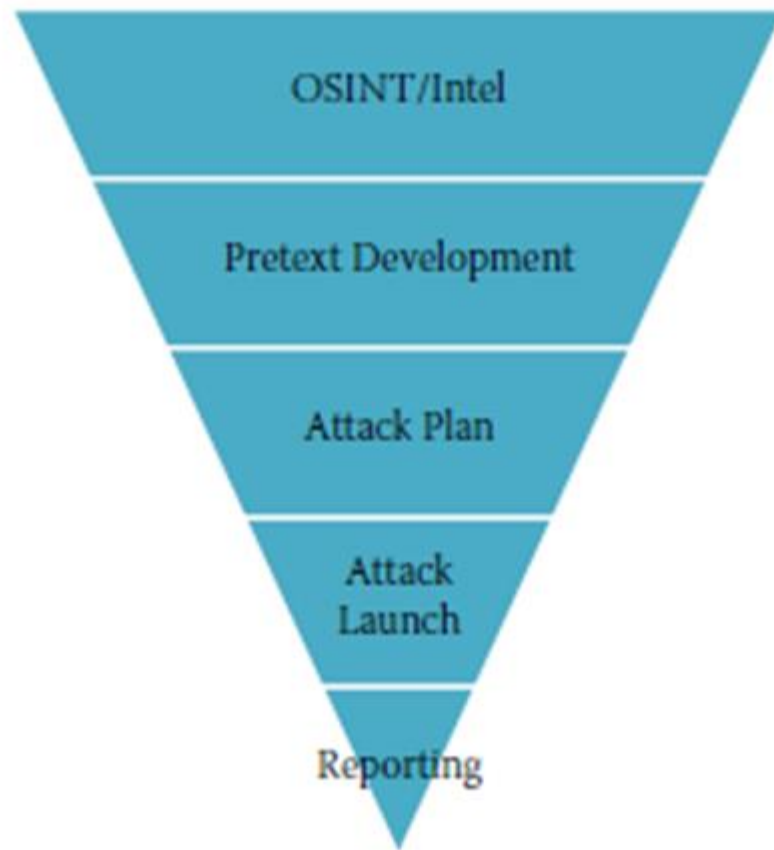


people are facing a major attack on identity and financial theft. Many people get phishing emails that appear authentic and claim to be companies that they frequent but have the sole intention of stealing sensitive information. We want to provide knowledge on ways to identify and avoid these phishing attacks.

We used a systematic literature review approach to synthesize about forty-seven papers from credible sources that examine vital characteristics of effective phishing tests. Our literature review has helped answer our research questions by identifying key attributes of phishing emails and effective training techniques.

## **1. Preparation**

Designing phishing attacks requires planning, research, social engineering, and training. Although we are discussing phishing attacks from the attacker's point of view, it is important to note that companies complete the same steps when it is creating phishing campaigns to train its employees. Christopher Hadnagy created the SE (social engineering) Pyramid, shown in Figure 1, to define how to perform social engineering attacks so that companies can identify security issues and its ability to prevent attacks. Attackers can also apply these steps to launch their own phishing attack. Open-Source Intelligence (OSINT) is at the top of the pyramid because it is important to research your targets and gather enough information to deceive them with your phishing attack (Hadnagy, 2018). The next step is pretext in which you decide on a phishing campaign and theme. During the attack plan stage, you determine your goals, metrics, initial attack date, and the frequency of the next attacks. Then it is time to launch the attack. The final step is reporting, in which you would log any issues that can be improved or detail steps that were effective.



*Figure 1 - The SE Pyramid which is used to conduct social engineering attacks (Hadnagy, 2018)*

Other studies list less formalized steps to conduct phishing attacks. They give a general overview of necessities that can be tailored to any situation. The first step is to determine the goals of the phishing attacks. The attacker must decide if they are creating a link and measuring success by the number of clicks. They may also decide to use HTML attachments in the emails and measure effectiveness of the attack by the number of opened attachments. The HTML attachments would contain malicious code that would give attackers access to personal information on your computer. This phishing technique has a low chance of detection and a high chance of deception because most banks use HTML files (Boyle & Panko, 2015).

Attackers must also decide the frequency of executing phishing attacks. Sending a few emails could imply small benefits because they aren't reaching and tricking enough users. On the other hand, sending too many attacks to the same user could cause them to realize the scam and prevent the attacker from getting any information. Companies that are using phishing emails for training purposes should conduct phishing attacks on a monthly basis. This improves employees' abilities to identify and prevent security attacks (Kumaraguru, 2008).

The next step is to choose the email topic. It should invoke fear, urgency, or greed to get the user to react immediately and without thinking. For example, informing a user that their bank account will be closed if they do not verify their credentials. Another example is telling someone to click a link in an email to learn about the recent pandemic outbreak in their local town. The topic should have an effective theme that focuses on financial institutions, package delivery, natural disasters, common trends, online shopping, etc.

The content and appearance of the email must be convincing. The content should be personalized to include companies that the user frequents. The logo, URL, grammar, links, subject line, name, and security disclosure at the bottom of the email must all appear authentic. These are major aspects that users look for when identifying cyber-attacks. The next step is to execute the attack. The final step is to analyze the success or failure, identify areas of improvement, and apply any necessary changes before the next attack. Despite the importance of the email contents, social engineering is the leading factor in designing effective phishing attacks.

## **2. Social Engineering**

### ***2.1 Defining Social Engineering***

The Cybersecurity and Infrastructure Security Agency (CISA) describe phishing attacks as a type of social engineering attack (2020). It is important to note that there are several types of social engineering attacks, but when discussed throughout this paper we are referring to phishing attacks. The success of phishing attacks is dependent on the susceptibility triggered by social engineering. Social engineering occurs when attackers attempt to trick users into doing something that is against their better judgement and the interests of security (Boyle & Panko, 2015). This technique exploits human vulnerabilities and error to obtain information for attackers. Phishing attacks are more challenging to stop than other attacks because humans are less rational, and it is more difficult to prevent their mistakes when their emotions are triggered.



*Figure 2 - Harvey, a dog with deep burns that was rescued by the Charleston Animal Society (photo by Charleston Animal Society)*

What emotions are you overcome with when you see Figure 2? How does it make you feel to know that someone abused this dog? The Charleston Animal Society rescued Harvey

from an animal cruelty situation that left him with severe burns across his body. Would you donate to an organization like the Charleston Animal Society or feel encouraged to adopt a pet? Most people that receive a phishing email with a picture of this dog would fail by clicking the link to donate, adopt, or sign a petition. Phishing attackers use aspects like Figure 2 to manipulate people into acting off emotions rather than thinking first. The objective of social engineering is to get people to act without thinking (Hadnagy, 2018).

## ***2.2 Themes of Phishing Emails***

All phishing attacks are executed using elements of social engineering. The theme of each phishing email must be convincing and appeal to human emotions. Typically, attackers use key words that evoke a sense of urgency, importance, greed, or fear to react immediately. There are various themes that are frequently used in phishing emails. Our research show that the most frequently used topics in phishing attacks are:

1. **Bank Scam:** Attackers design phishing emails that appear to be from the victim's bank or other financial institution. The email context usually states that your account has been compromised, change your password, check your account immediately, or confirm your login information. When you click the link in the email it takes you to a fake website that appears to be your financial institution. The goal is to use fear and urgency to trick you into giving up your sensitive information. Although this scam has been around for years, some people still fall victim due to the authentic appearance of the email and website. In 2019, banking phishing scams accounted for 37% of all phishing attacks (Gendre, 2020).

2. **Tax Scam:** In these phishing emails, scammers pretend to be the Internal Revenue Service (IRS). They claim that you owe taxes, have a tax lien, and threaten to garnish your wages if you do not take immediate action. Victims suffer identity and financial theft. This scam is effective because most people are familiar with the IRS and have communicated with them in the past (IRS, 2018).

3. **Failed Attempt to Deliver Package:** Attackers design phishing emails that appear to come from a delivery courier such as FedEx or UPS. The message states that they were unsuccessful in an attempt to deliver a package. The email may request personal and/or credit card information to reschedule the delivery. It could also have a link that downloads malware to gain access to confidential information stored on your computer (Better Business Bureau, 2020).

Some other notable themes are emails that appear to come from someone you know, threaten legal action, or request donations for holiday charities. Social media has become a major tool in phishing attacks due to the high volume of users and the awareness that people use it to connect with other people across the world. Scammers send friend requests with fake names of people you may know, then they send messages or emails with links that will capture your credentials. The top two social media platforms that have been affected by phishing emails are Facebook and LinkedIn. PayPal is another company whose name is frequently used in phishing emails to trick users into giving up their financial credentials.

The most current phishing scam uses COVID-19 as the subject to manipulate users. The subject of some of the emails are: COVID-19 vaccinations, local COVID outbreaks, COVID-19 Relief checks, and messages from the Centers for Disease Control and Prevention (Warburton,

2020). This scam has been highly effective since the pandemic is ongoing and there is still some fear associated with the topic.

### ***2.3 Susceptibility Characteristics***

There are several factors that increase users' susceptibility to phishing attacks. These elements include demographics, psychological indicators, personality traits, behavioral traits, persuasion principles, and security and cyber threats training. Demographic attributes include age and sex. Studies find that females are more likely to fall victim to phishing attacks than men are (Heartfield et al., 2016). Another study found that 77% of females not only click the links in phishing emails but provide personal information as well (Sumner & Yuan, 2019). People between the ages 18-25 are more susceptible.

Psychological indicators reveal information on cognitive, emotional, social, and other abilities. These indicators drive personality and behavioral traits. A 2013 study conducted by Halevi et al., reported that women that behave neurotically are more vulnerable to phishing attacks than men and women that do not have these traits. Openness, extroversion, and conscientiousness are characteristics that reduce the likelihood of risk due to phishing. People that have personality traits such as agreeableness, neuroticism, trust, guilt, and curiousness are more susceptible to phishing (Sumner & Yuan, 2019).

Compliance principles are reasons why people give up their sensitive information during attacks. The principles include friendship, commitment, scarcity, reciprocity, social validation, and authority. People are more likely to provide information to their friends or people they like. The commitment principle refers to people committing to requests that are consistent with their positions (Mouton et al., 2016). People comply with requests that are scarce in availability. An

example of this may be an email telling you to change your password in the next 24 hours or you will lose access to all of your data. With the reciprocity principle, people are prone to make decisions if they were treated well in the past. Social validation means that people will do what is socially acceptable. With the authority principle, people submit to requests from people that have more authority than they do. A study found that 50% of successful phishing emails were associated with the authority principle indicating that using authoritative figures to persuade users increases phishing susceptibility (Sumner & Yuan, 2019).

Our research indicated a few more characteristics that impact susceptibility to phishing. A study conducted by Jakobsson et al., reported that people judge relevance before authority (2007). The participants considered emails safe if they appeared to provide information only without asking for credentials or mentioning money. Another conclusion of the study states that participants would trust emails that are personalized and have some personal information such as zip code or mother's maiden name. The subjects also suggested that they would trust emails if they could call to verify the authenticity. While these vulnerabilities may seem minor, the consequences of this behavior and rationale can be detrimental.

## ***2.4 Effects of Social Engineering***

In 2017, social engineering techniques were used in eighty percent of all data breaches (Hadnagy, 2018). These breaches usually result in lawsuits, other financial consequences, stricter IT regulations, and a diminished reputation for the company. Figure 3 depicts a pie chart of various industry sectors that are targeted by phishing attacks. Software-as-a-Service/Webmail and financial institutions lead the sectors with 31.4% and 19.2% of phishing attacks respectively.



All industries should be aware of the rise in cyber-attacks and be prepared with countermeasures to stop the theft of confidential information.

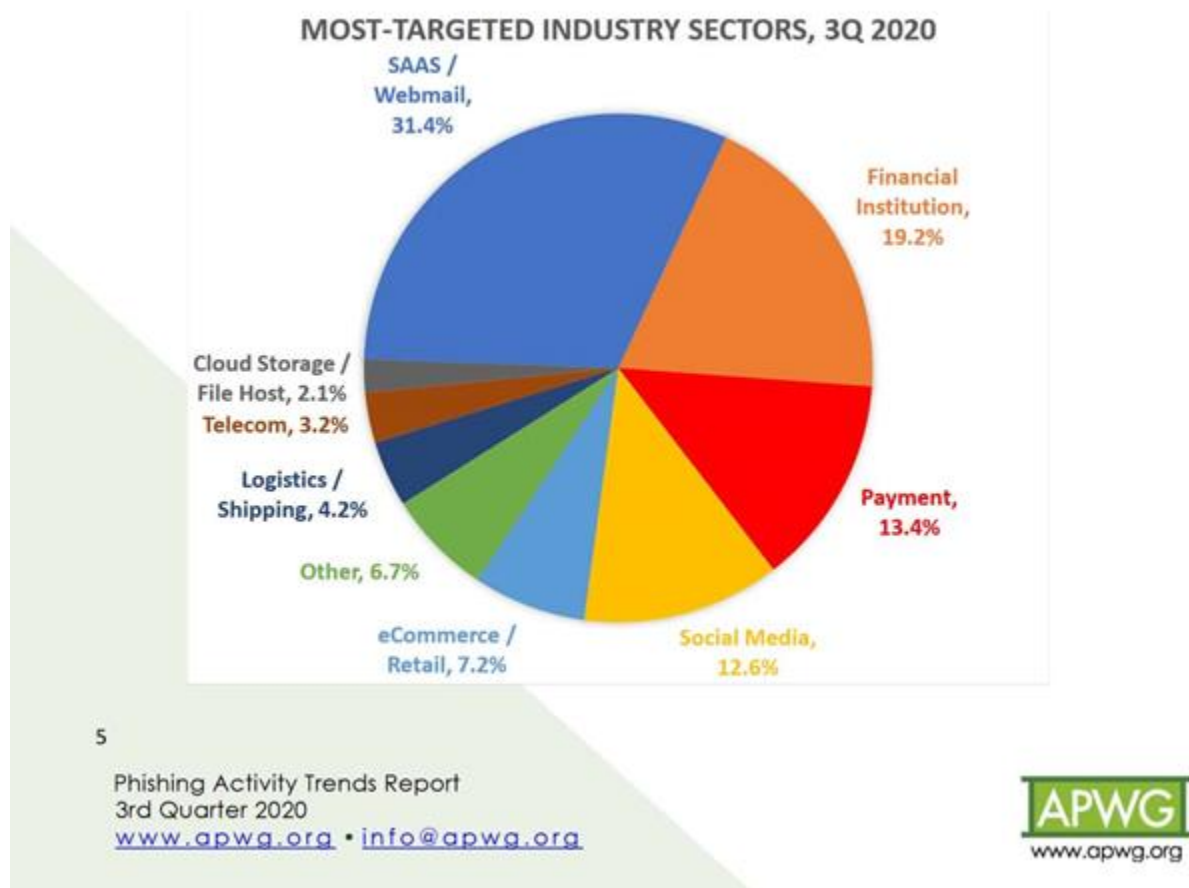


Figure 3 - Industries targeted by phishing attacks (from APWG Phishing Activity Trends Report, 2020)

If employees fall victim to phishing attacks, their employer may assign training or give a verbal warning. If the security violations increase in frequency, this could lead to investigations to determine if the employee is intentionally leaking confidential information and to decide if firing is the appropriate consequence.

Attackers have low setup costs for social engineering attacks, but reap immense benefits when they are effective (Hadnagy, 2018). Attackers design phishing emails on their computers

and have low software costs. But if an employee falls for one of their phishing attacks they can gain access to the company's information as well as their employees and customers. The impact to companies, their employees, and the potential loss to attackers are all key reasons that warrant the need for effective security training to protect companies.

### **3. Training**

The next issue that we will discuss is training. Most of us have had some form of training, either under the yearly mandatory IT Security Training program our employers provide or phishing-specific training. These training programs are designed to help users learn how to identify phishing and spam emails so that they do not click on a bad link and compromise themselves, their computers, and their organization. What are the best methods of training? Do any methods offer better results when compared against other training methods? How often should training be done? When is the best time for training? What can the IT/Security department do to help align with their organization's needs?

When it comes to training, there are a variety of methods used to teach users how to spot phishing and not get scammed. Tschakert and Ngamsuriyaroj describe four methods in their article "Effectiveness of and user preferences for security awareness training methodologies". These four methods include video-based training, game-based training, text-based training, and instructor-led classrooms (Tschakert & Ngamsuriyaroj, 2019). Video-based training involves showing the user pre-recorded videos with information about phishing and gives recommendations on how to not get tricked by bad emails. Game-based training uses interactive mini-games and quizzes to help educate users in a "fun" way. Text-based training involves educational text designed to explain phishing and best practices on how to deal with it. One

advantage that should be mentioned is that these three methods are all used in self-paced training programs, i.e., they can be completed at the user's convenience. Instructor-led classrooms incorporate trained experts and IT professionals that incorporate a variety of tools to help the user learn about phishing emails.

Research was not decisive when testing the methods of training against each other to see which method was most effective. Tschakert and Ngamsuriyaroj found classroom-based training achieved the best results for reducing phishing susceptibility, but the statistical percentage was insignificant from text-based training (Tschakert & Ngamsuriyaroj, 2019). Kumaraguru et al. compared embedded training (using PhishGuru) and web game-based training (using Anti-Phishing Phil) and found participants that received PhishGuru training were less likely to click on a bad link when encountering phishing emails after receiving the training (Kumaraguru et al., 2008). Davinson and Sillence also used "Anti-Phishing Phil" to train the users after sending them phishing emails but their study found no significant change in the secure behavior of their users (Davinson & Sillence, 2010). Another interesting study proposed using mindfulness training that taught users how to dynamically allocate their attention to better evaluate emails, but the benefits of the training were also limited (Jensen et al., 2017).

IT Security Training is usually only done once a year, many organizations align their training schedules with the Cybersecurity & Infrastructure Security Agency's National Cybersecurity Awareness Month in October. Is training once a year enough for the users to learn and retain knowledge on how to spot phishing? Siadati et al., argue that in addition to annual training, organizations should focus on creating "teachable moments" by conducting phishing campaigns on their users (Siadati et al., 2017). When a user falls for one of the phishing emails, they are taken to a training page where they are presented with phishing information. One of the

recommendations made by Dahbur et al. is for a continuous training regimen for all employment positions by incorporating security workshops throughout the year on new security threats on how to identify them (Dahbur et al., 2017). At the end of the day, training can only go so far. Sometimes the best approach organizations can take is to invest in tools that can filter out phishing attempts. Shahbaznezhad et al. suggest preventive countermeasures will continue to play a pivotal role in detecting phishing emails (Shahbaznezhad et al., 2020).

#### **4. Literature Review Findings**

The goal of this literature review was to identify key attributes of effective phishing tests and to make recommendations for a template and training plan to mitigate phishing attacks. We synthesized data from several studies to discover how these aspects complement one another and are used to benefit attackers. We found that phishers depend on preparation, social engineering, and security training to design effective phishing attacks. The preparation stage involves setting goals and deciding on a plan of attack, picking targets that are vulnerable, and ensuring that the email content appears as authentic as possible as well as appeals to emotions and psychological traits that increase the susceptibility of phishing. The final step of the preparation stage is to document, review, and learn from mistakes to improve the next attack.

Social engineering involves manipulating people into giving up sensitive information. There are many common attacks that rely on deceptive techniques to scam people. The biggest takeaway is that phishing emails use different themes to create fear, trust, guilt, greed, and a sense of urgency to get users to furnish credentials without thinking. Different personality traits and demographics also play a part in the effectiveness of social engineering in phishing attacks. Studies showed that women are more likely to fall for phishing emails than men (Heartfield et

al., 2016). Younger people between the age of 18-25 are more vulnerable to attacks (Sumner & Yuan, 2019). People that have personality traits such as openness, conscientiousness, and extroversion are less likely to fall for scams (Sumner & Yuan, 2019). People that are easily persuaded by authority figures or have traits such as agreeableness, neuroticism, trust, curiousness are more predisposed to phishing attacks.

Our findings allowed us to easily create a template for effective phishing tests. We were able to choose a theme that would resonate with users and increase their susceptibility. We knew to pay attention to common spelling and grammar mistakes that users tend to catch. Our research taught us that the logo, email address, and content needed to look as real as possible. Most importantly our research helped us create security training plans that are effective. We can identify methods, policies, and frequency of implementation that increase employees' retention of ways to identify and combat cybersecurity attacks.

## Phishing Test Methodology

### Why a Phishing Test?

IBM looked at 524 companies who experienced a data breach between August 2019 and April 2020, and found that 19% of the breaches were a result of compromised credentials. The average cost of the studied data breaches was \$3.86 million and took an average of 280 days to contain the breach (2020). For some companies, data breaches are catastrophic, while others can recover. But the monetary cost is not the only consequence. The time it takes to contain the breach can result in a significant disruption to business. Companies facing a data breach also suffer a loss of reputation and trust, not only with customers, but also with potential partners and investors. These losses are harder to quantify, but a survey of adults in Great Britain in 2015 found that 73% would consider no longer doing business with a company who lost or failed to

keep their personal data safe (Deloitte, 2015). Intellectual property loss is another potential consequence whose costs are difficult to quantify. Once intellectual property has been leaked, there's no practical way to remove it from general circulation on the internet. In an extreme case resulting from a phishing attack, a hospital in Germany had a patient die because malware had disabled their equipment (Goodin, 2020). Public services have been a target of attack, as well. There have been at least two instances of a hacker taking over Ukraine's power grid (Greenberg, 2017) and in 2016, hackers took over a US water treatment plant and changed the levels of chemicals being used to treat the water (Leyden, 2016).

The popularity and success of phishing attacks can be attributed to the human element, social engineering. We do not yet have technology that thinks like a human, and that can identify all phishing attacks without misidentifying a significant number of legitimate emails as malicious. Anyone can be the target of a phishing attack, and anyone can fall for it, no matter how experienced or knowledgeable they are. We should remember that the attackers are often several steps ahead of the technologies and personnel intended to defend against them. Since we cannot rely on technology or IT professionals to identify all attacks, we must also train users on how to identify a phish, and what to do if they have been targeted. But the trickiest part of this type of training is getting users to care. We have all sat through training presentations that take way too long, and we're not paying attention, and by the time we've left the room we've nearly forgotten it all. So how do we convince users to care so they retain the training and make use of it?

## **Test Design**

The majority of users are unlikely to seek out training to help stop themselves from falling for phishing attacks, but several studies (Hadagny & Fincher, 2015; Jansson & von

Solms, 2013; Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010) have shown that embedded training, a simulated phishing attack inserted into a person's regular daily activities, is a highly effective training tool. The simulated attack gives the user a bit of a shock, showing the user that they can both receive a phishing email and fall for an attack. The phishing test outlined here consists of a simulated phishing email where the link the user may follow in the email leads to a site with a brief (less than ten minute), concise training on phishing. The shock provided by falling for the phishing email introduces a "teachable moment" that makes the user more receptive to training (Siadati, Palka, Siegel, McCoy, & Hamilton, 2017). A study by Kumaraguru et al. supports this; they found that users who received training following a phishing test spent over twice the amount of time, on average, reading the training material than users who received the training material in a direct email. The phished users also seemed to retain the information longer and be able to transfer the knowledge to new phishing emails more reliably (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, Teaching Johnny Not to Fall for Phish, 2010). There is also data to suggest that a second round of training increases the effectiveness (Kumaraguru et al., 2009), so a follow-up email containing the same information will also be sent so that A) users who fell for the phish get the information a second time and B) users who did not fall for the phish still get the information. It is also preferable to keep the training brief so that it does not intrude significantly upon the user's day and keeps the user's attention (Hadnagy & Fincher, 2015).

While there are two potential intervention points for teaching users to protect themselves against phishing, the email, and the web site, Kumaraguru et al. recommend focusing on the email portion, because if users can learn to identify phishing emails and not click the link, they're prevented from being exposed to the web site portion (Kumaraguru, Sheng, Acquisti,

Cranor, & Hong, Teaching Johnny Not to Fall for Phish, 2010). Wright et al. also suggest that by the time a user has followed the link to the phishing website, there is less chance of detecting that it is not legitimate (Wright, Chakraborty, Basoglu, & Marett, 2010).

We chose to use just an email link and no login page, and decided on this method for three reasons. First, while the previous phishing test done for CompanyN attempted to collect credentials, we did not think this was necessary as the research suggests that the majority of users who will click on a phishing site will also provide their credentials (Kumaraguru et al., 2007). Second, collecting credentials also introduces extra security complications that we would prefer to avoid. And finally, research has shown that users who log in before seeing the education page are confused as to why they are seeing information about not clicking on links, likely because the login created a gap between clicking the link and seeing the education (Kumaraguru et al., 2007).

We took care in designing the email with the appropriate level of persuasiveness. Research by Siadati et al. found that the more persuasive the phishing email was, the more effective the training was. Their theory is that only highly susceptible users are likely to fall for the least persuasive phishing emails, and that these users are also the most difficult to educate on the subject (Siadati, Palka, Siegel, McCoy, & Hamilton, 2017). So we wanted something that wasn't so easy as to be obvious (like a 419 scam), but also wasn't so difficult that a user would almost need to be a security professional to recognize it as a phish, as this could be discouraging to the company.

Rather than try to attack the computer system directly, phishing uses social engineering to attempt to take advantage of the human element in the system, which is the part of the system most prone to errors. The email for our test is shown in figure 4 below. This message uses the



social engineering element of importance. It looks like it could legitimately be secure messages that the user needs to retrieve, which implies importance because it is unlikely that extra security precautions would need to be taken for an unimportant message. The importance and the fact that the email address appears to come from within the business's domain give it an air of authority, in a sense implying the user is expected to open the secure messages as part of their job. The large box this client's email client provides indicating that the message is from an external sender should cause users to stop and take a second look, but in practical experience, this is all too often ignored by the users. In this case, a user may also think that the external sender warning refers to the messages that will be retrieved by following the link.

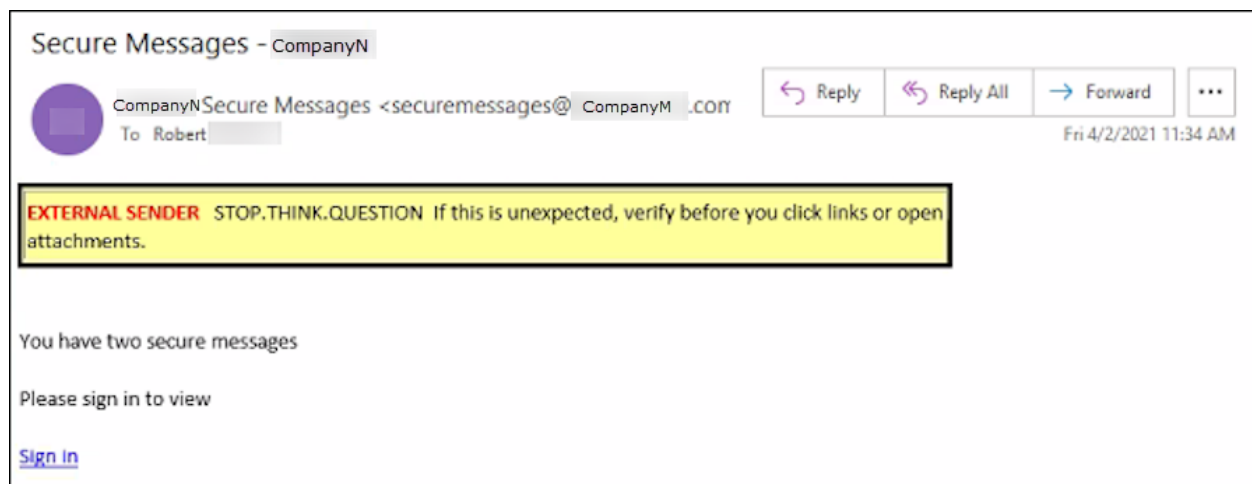


Figure 4 - Phishing email for this test

The time we are sending the email is also strategic, as part of the goal of social engineering is to get people act without thinking, (Hadagny, 2018) so we want to send at a time when the user is likely to be busy and preoccupied. We could not find research that specifically suggested a time of day or week that results in more clicks. We checked suggestions for marketing emails since they also have the goal of generating clicks, but the advice was, at best, inconsistent. An anonymous former hacker and current security professional who was interviewed for the project suggested that the best time is when users are in a hurry for one

reason or another. Mondays are a good time, because people are trying to get caught up from the weekend and may not be giving things the attention they should be. The former hacker also suggested sending either shortly before lunch or shortly before the end of the day, with a preference for shortly before lunch. For this reason, we believe that sending the email around 11-11:30 a.m. on a Monday is the best choice for this test.

## **Education Page Design**

This type of test should be paired with immediate education on phishing. This style of training uses what, in reinforcement theory, is called positive punishment. Positive meaning that a stimulus is applied (the training about phishing) and punishment meaning its goal is to decrease the behavior that triggered the positive punishment (in this case, clicking on a phishing link) (Pierce & Cheney, 2013). Research has shown that the closer the correction is to an undesirable behavior, the more effective it is, so the immediacy of this training is important. It is also important that while telling the user that they did something they should not have done, you tell them what you would like them to do if the situation comes up again in the future (Robbins, Judge, Odendaal, & Roodt, 2009). The phishing test and following education page is also done privately, which has shown to be the most effective when correcting undesirable behavior (Redmond, 2010).

Part of the challenge of training users against phishing attacks is that there are so many different types of attacks and hackers are coming up with new ones all the time. Even if we could train users on everything we know exists, this is reactive, and it can only prevent against attacks we have already seen. To help guard against new attacks we need to be proactive; users need to be taught to think critically before they click a link or give away sensitive information. For this purpose we will use a combination of rule-based training and mindfulness training, as suggested

by Jensen et al (2017). This research also suggested that mindfulness training can reduce the susceptibility of users who may think they can identify phishing emails, but in reality may not be doing so accurately. People have a tendency to judge the relevance of the email before its authenticity (Jakobsson, Tsow, Shah, Blevis, & Lim, 2007) and teaching mindfulness techniques can help to overcome this. This is not to say that rule-based training is not effective, rather that the two types of training in tandem have been shown to be more effective than either one on its own (Jensen et al., 2017).

The article “Teaching Johnny Not to Fall for Phish” recommends a set of seven instructional design principles that should be applied when designing phishing education, six of which we use in this test.

- *Learning by doing principle* gets the user involved which helps hold their attention and increase retention of the information. We do this by having an image of the email and asking the users to see if they can identify indicators of phishing, before clicking the image to reveal the indicators.
- *Immediate feedback principle* has been shown to be more effective than delayed feedback. We do this by forgoing a login page and having the link in the email take the users directly to the education page.
- *Conceptual-procedural principle* suggests that alternating between concepts (the education portion) and procedures (the test portion) strengthened the learners’ understanding and retention. This is one of the reasons we recommend periodically repeating the test. (Discussed more later in the “Recommendations” section.)

- *Contiguity principle* says that computer-aided instruction is more effective if text and images are interspersed with one another rather than separate. Our education site places the images we use right with the text.
- *Personalization principle* says that using conversational instead of formal language enhances learning. We do this by speaking directly to the reader as “you” in the education page, rather than talking about some theoretical user.
- *Reflection principle* says that learning increases if users are encouraged to reflect back on what they have learned. We do this by giving the readers several ways to think critically about an email to decide whether they think it may be a phish (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010).

The education page starts with a brief attention-getter as shown in figure 5, an image that shows phishing in a slightly amusing way, and large text telling the user they have clicked on a simulated phishing test. We wanted to incorporate more than just the images of the email itself, as the research suggests that interspersing text and graphics together increases information acquisition and knowledge retention (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010). It is important that the page is completely explicit to the user why they are there, so they are not confused as to the purpose (Kumaraguru et al., 2007). This part of the page also reassures the user that the simulation was authorized by the client as an educational tool.

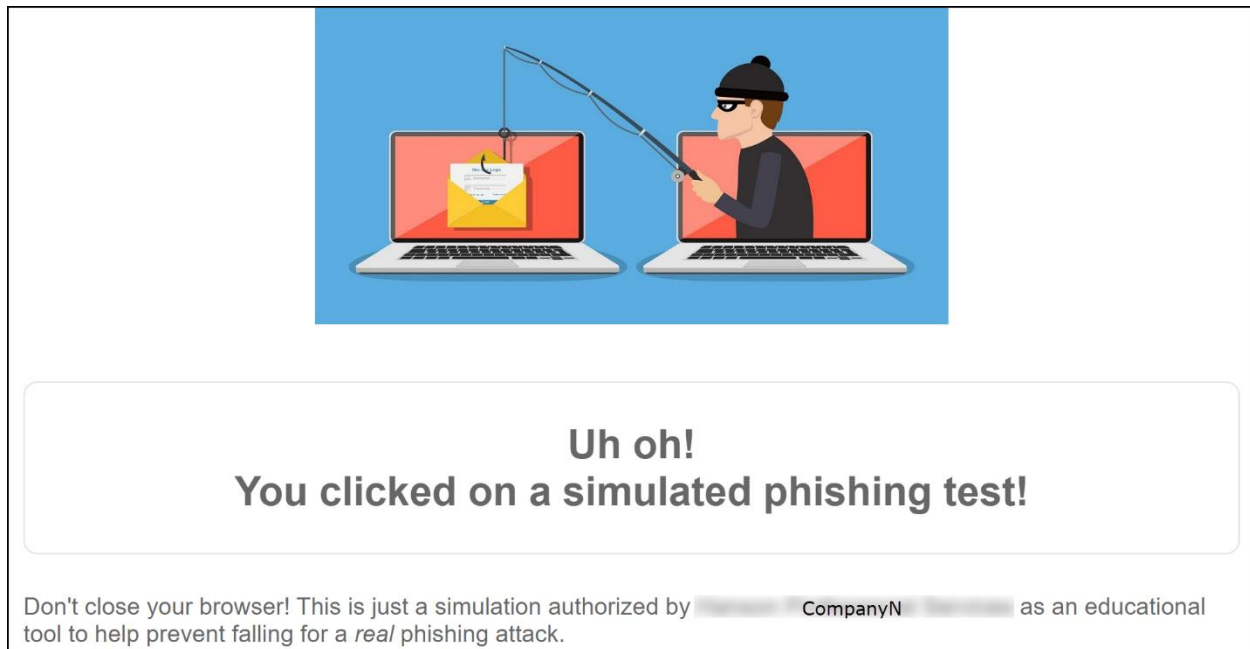


Figure 5 - First part of the education page

Then the page goes on to give the user a very brief overview of what phishing is. (see figure 6) If periodic tests are being done or other computer security education is being provided, the users should know what phishing is, but we do not want to make the assumption that they will, because how well they understand the rest of the page depends on knowing what phishing is. Research on how users understand security suggests that many users have misconceptions about computer security, and that advice, no matter how good, is likely to be ignored if it is not understood, so we need to include this explanation (Wash, 2010). It would not be practical to include a comprehensive definition of phishing – that could fill an entire class – but we believe the brief description we have provided here is enough to emphasize to the user what it is and why it is important to be wary of phishing emails.

## What is phishing?

Phishing is often an attempt to trick you into giving out sensitive information you wouldn't normally provide. It may be done through e-mail or websites. A common method is to e-mail a large group of people a link to a page that appears legitimate in an attempt to collect login credentials, credit card information, etc. Another common type of phishing consists of attempting to get you to click a link or open a file that actually downloads malware onto your system. Don't worry, this simulation neither collects your information nor gives you malware.

Figure 6 - Second part of the education page

The next section of the page is an interactive piece telling the user that two things in this particular email could have indicated to them that it was a potential phishing email, and asking the user to see if they could identify them (figure 7). Clicking on the image reveals these indicators to the users with callouts that give more information (figure 8). This section, especially with repeated testing, uses rule-based training to teach users specific things to watch out for.

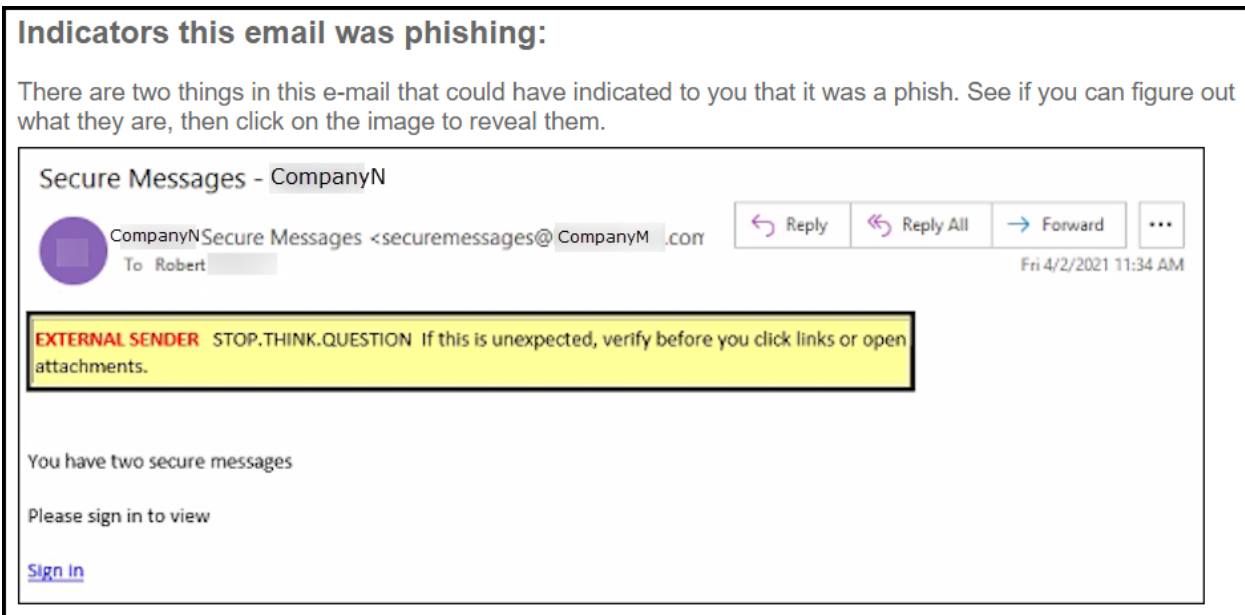


Figure 7 - Third part of the education page without phishing indicators

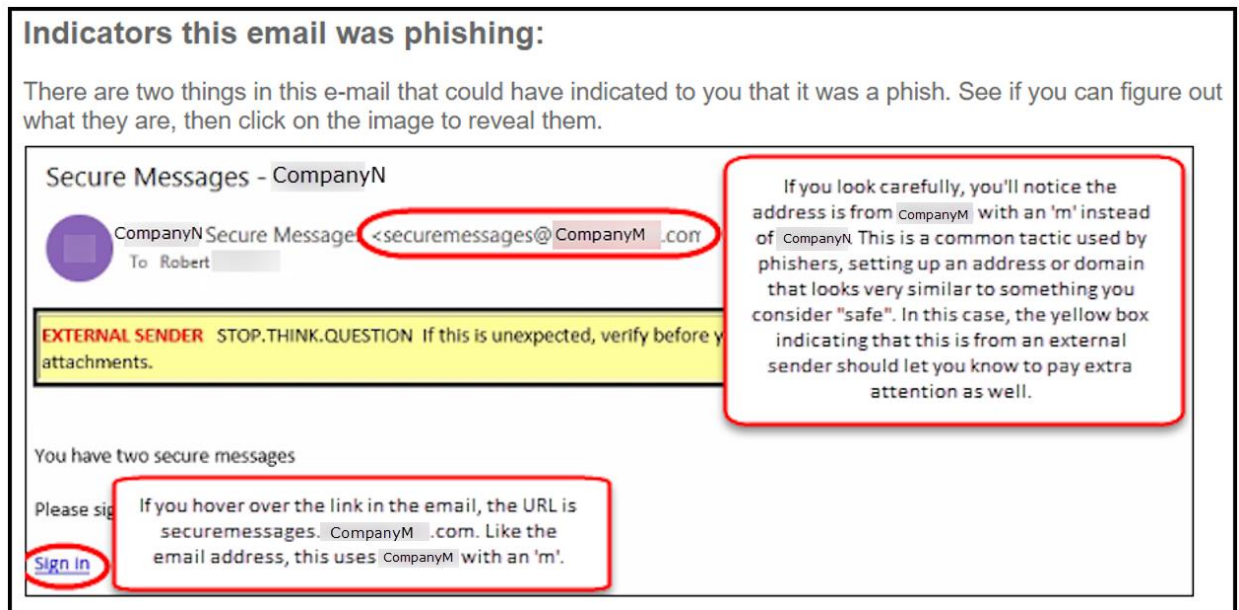


Figure 8 - Third part of education page with phishing indicators

The following section, shown in figure 9, uses the mindfulness training discussed above, and gives the users several things to think consciously about when evaluating whether any particular email may be a phishing email. This section tells the user to think critically about each email before acting and gives the user three things in particular to ask themselves. First, does the email make a request for action? If not, there is less need to worry (Jensen et al., 2017). Second, is the sender external? Some email clients are configured to specifically call out when a sender is external, but others (especially personal email) are not. A common phishing tactic for businesses is like the one we use in this test, to obtain a domain or email address that appears very similar to the business's name in the hopes that the user will overlook minor differences, like the change from 'n' to 'm' in our test. Research suggests that most users are not adept at catching this kind of change in an email address or URL (Jakobsson, Tsow, Shah, Blevis, & Lim, 2007). This is not a sure thing however, as once a hacker has obtained credentials, they can access a user's email to send phishing emails, malware, etc. so it is prudent to always use the other critical thinking steps even if the sender is internal. Third, is the email using tactics such as fear, curiosity, or greed?

These emotions are commonly used by hackers because when evoked, they can cause attempt to “short-circuit” a user’s rational decision-making using strong emotion (Hadnagy & Fincher, 2015).

**Think critically about the email before acting:**

- What are the calls to action? For example, does the email ask you to click a link, open an attachment, or reply with information?
- Is the sender external? If so, use extra caution when acting on the email. Make sure to review the actual sender address, not just the name.
- Does the email use fear tactics such as fear, curiosity, or greed? If so, this is reason to be suspicious.

*Figure 9 - Fourth part of the education page*

The final part of the education page caps off all the information we’ve given the user with the most important part of all: what to do if you suspect an email may be a phish. (figure 10, below) Given the environment we are conducting the test in, these directions apply specifically to a business environment (a home user would have different steps to take, but that is outside the scope of this project). Step 1 is to not click a link, open an attachment, or reply to the email. Any one of these actions could be what the hacker is looking for. Step 2 is to report the email to the help desk. This should not be done by forwarding the email to the help desk (or anyone else) because spreading the email gives more opportunities for the attack to succeed. Step 3 is to wait to hear from IT before doing anything else with the email, including deleting it. Most of the time, IT will have the user delete the email, but if they do not yet have a copy of it, they may want a copy before the user deletes it. This can be particularly beneficial if someone else has clicked the link in the phishing email and not reported it, so the IT team can investigate how the attack is supposed to work. The research is indecisive as to whether phishing training makes users less likely to click on legitimate links, and it likely varies from user to user, so we end the page by



clarifying to the user that it is better to ask about an email and find out it's not phishing, than vice versa.

**Steps to take if you suspect phishing:**

- 1 Do not click a link, open an attachment, or reply to the email!
- 2 Report the email to the help desk. DO NOT FORWARD the email to the help desk or to anyone else.
- 3 Wait to hear from IT before you do anything else with the email. DO NOT delete it yet.

Even if you incorrectly identified the email as phishing, it's better to be safe than sorry! Remember: Stay alert! You are what keeps us safe.

Figure 10 - Fifth (final) part of the education page

## Test Setup

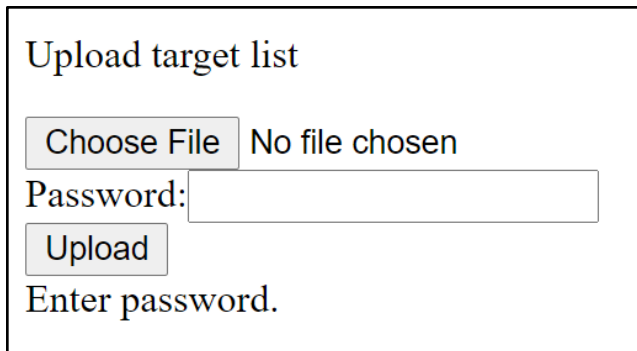
The first step of setting up the test was to purchase a domain name and email through hosting provider Network Solutions, including private registration so the WhoIs information did not point back to us. For privacy purposes, we will refer to the client we did this test for as “CompanyN”, and since the URL we used for the test was just one letter off from the actual company’s URL, we will use “CompanyM” in its place to emphasize the similarity between the two. We purchased the domain name `companym.com` and the email address `securemessages@companym.com`.

Next, we set up the server. For this we used virtual private server provider `prgmr.com` and deployed their smallest server, with 1.25 GiB RAM and a 15 GiB SSD. On this server we installed Debian Linux 10 (Buster), Apache, and PHP. We pointed the domain name at the server we created, and created the page `securemessages.companym.com` to hold the education page (`companym.com` also resolves to this same page).

There are three pieces of code to the test. (see Appendix B) The first is `index.php`, which holds the main page of the website; it has the HTML, CSS, and JavaScript of the site, as well as

a small PHP script that records the time the page was accessed (in UNIX time) and the ID, if one is present in the URL, to a log file. This gives us our list of page visits without having to go through the server logs.

Then there are two PHP scripts that run the test. The list\_upload.php script presents the simple upload interface shown in figure 11 below. This script takes in a list of email addresses in a text file, each on its own line. A password is required so only authorized users are able to send the phishing test. After uploading the file, it shows the list of addresses for you to verify (see figure 12 below) then clicking the “Execute” link tells it to hand the list off to the next script, mailer.php



Upload target list

No file chosen

Password:

Enter password.

*Figure 11 - List upload interface*

Upload target list

Choose File

No file chosen

Password:

Upload

The file targets.txt has been uploaded. If the list looks ok, click the link at the bottom to start sending.

Uploaded list:

abate5@uis.edu  
clast2@uis.edu  
pvalen4@uis.edu  
shunt26@uis.edu  
tcald3@uis.edu

[Execute](#)

Figure 12 - List upload interface with email addresses

Mailer.php does the bulk of the work here. For each email address, it assigns a 16-digit random number as the ID and records the email and ID pair to a file so everything can be combined later for the metrics. While the script does not specifically check that each ID is unique, the chances of two IDs being the same is 1 in  $1 \times 10^{16}$ , or 1 in 1 quadrillion. We can also check the list of assigned IDs to be sure that no users were assigned the same ID.

Next the script adds a 1-pixel white image to the body of the email, assigning the ID as the name of that image. If the user's email client is configured to display remote images, this should let us know which users opened the email and which did not, by checking the server logs to see which images were accessed.

Finally, the mailer script appends the ID to the end of the URL in the body of the email and sends each one out. As it sends, sever log information is displayed for each email that is sent, followed by a custom message that says either "Message has been sent" if sending was successful, or "Message could not be sent" and the error information from the server logs if the

message did not send successfully. This will allow us to search through these logs for any messages that were not sent successfully to attempt to figure out what went wrong and see if it is worth making a second attempt to send the email. The resulting email on the client side looks like what you see in figure 13 below, with the URL of the “Sign in” link being [securemessages.companym.com](https://securemessages.companym.com).

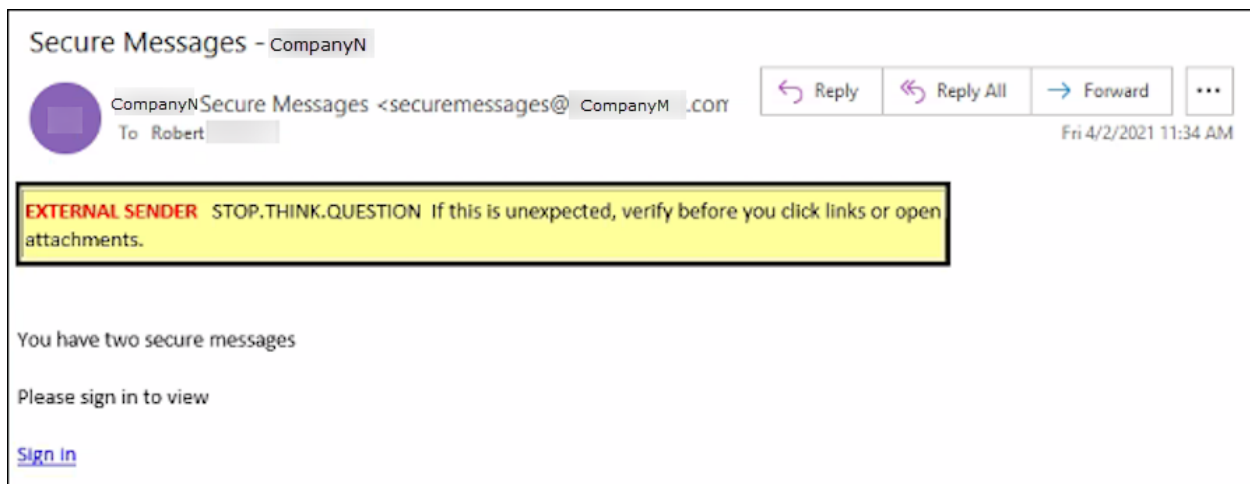


Figure 13 - Phishing email for this test

As the literature review mentioned, one of the reasons phishing attacks are so prevalent is they are very cheap to carry out. The information on how to execute a phishing attack is readily available on the internet, as is the open-source software available to do so. Table 2 shows our monetary cost of running this test, which totaled at \$22.34. For this same cost, we could have sent anywhere from one phishing email to millions. In a real phishing attack however, it may cost the attacker no money, as they are likely using previously compromised resources (networks, servers, etc.). This has the added benefit of the attack leading back to the compromised resources, instead of anything linked directly to the attacker’s identity.

Service	Cost
prgmr.com server for 1 month	\$ 5.00
domain name from network solutions	\$ 4.95
private registration for domain name	\$ 9.99
e-mail through network solutions for 1 month	\$ 2.40
<b>Total</b>	<b>\$ 22.34</b>

*Table 2 - Costs of running this phishing test*

## Data Analysis & Results

### Results & Metrics

In the literature review portion, we mentioned that if an employee falls for an actual phishing attack, they may be reprimanded or assigned training. And if employees repeatedly fall for phishing attacks, further action may be taken against the employee, up to and including termination. However, these repercussions should not happen if an employee falls for the phishing test, as it is designed to educate users. It is not necessary to notify managers of employees who fall for the phish and need to be trained, because the training is built into the simulation. So to keep the exercise low risk for the individual employees, only aggregate, statistical data will be reported.

The literature gives mixed opinions on whether demographic attributes contribute to the likelihood of someone falling for a phishing attack (Heartfield, Loukas, & Gan, 2016; Wright, Chakraborty, Basoglu, & Marett, 2010). While it would be possible to gather this information and report metrics on it, it is only useful if it can be used to tailor the training in some way. Given the literature's disagreement on this matter and the extra amount of work that would go into trying to tailor the training to different groups of demographics, we do not believe this is useful information to report on. Psychological factors could also come into play. Research suggests that certain personality traits and psychological factors could make a person more susceptible to phishing (Sumner & Yuan, 2019). But equally influential can be environmental

factors that affect a user's mood, such as lighting, temperature, and the people nearby (Hadnagy & Fincher, 2015). These would be incredibly challenging to measure accurately, and the environmental factors could change from one test to the next, so we do not believe it would produce any actionable information worth creating metrics for.

When calculating metrics, we are making the assumption that only the person the email was directed to will click the link in their email. While this may not be true 100% of the time, the likelihood of a user clicking someone else's link is low, so the benefit of doing so is small and the difficulty of trying to account of it is high, and therefore not worth trying to account for in the metrics.

The majority of the data needed for the metrics can be gathered from the server logs, with the remaining data received from the client. Table 3 below lists each metric and how it is obtained. All values and metrics exclude the people at the company who knew the test was taking place.

Abbr	Name	Metric	How Gathered
P	population	users the email was successfully sent to	received list from the client
C	clicked	users who clicked the link in the email	count of IDs in the server logs who have a GET request for index.php
T	trained	users who clicked the image to see the indicators of potential phishing	count of IDs in the server logs who have a GET request for img2.png
R	reported	users who reported the email as suspicious	received list from the client
A	active participants	users who opened the email	count of IDs in the server log who have a GET request for the hidden image in the email
N	non-active participants	users who did not open the email	population minus active participants (P-A)
LI	location: in office	users who clicked the link from one of the client's office locations	count of IDs whose GET request for index.php shows as from an IP in the list of IPs the client provides as their NAT addresses
LR	location: remote	users who clicked the link from a remote location	count of IDs whose GET request for index.php shows as from an IP not in the list of IPs the client provides as their NAT addresses

Table 3 - How the numbers for each metric are obtained

The most obvious metric to report is click rate, which is the number of users who clicked the link (C) divided by the number of people in the test population (P). Multiplying this by 100 gives us a percentage:

$$\text{click rate} = C/P * 100$$

We can also show is how many of the people who went to the phishing page clicked on the image to reveal what the phishing indicators in this email were. We will use the same C value from click rate, and T (trained) for the number of users who clicked to the second image. This gives us the rate of phished users who were also trained by reading at least some of the page.

$$\text{trained rate} = T/C * 100$$

But just looking at the click rate and trained rate fails to show us the whole picture. We would also like to know how many people reported the email as suspicious through the proper channels. By matching up whether each person clicked the link or not and whether each person reported the email as suspicious or not, we get the following matrix:

	<i>Reported</i>	<i>Did not report</i>
<i>Clicked link</i>	1	2
<i>Did not click link</i>	3	4

By dividing each quadrant by P and multiplying by 100, we again get a percentage for each value. This gives us a better breakdown by quadrants, as follows:

Quadrant 1 – These users are halfway there. Despite clicking on the phishing link, they then followed up by reporting it through the proper channels.

Quadrant 2 – These users are the most dangerous. Not only did they click the link, they did not report it through the proper channels so mitigating action could be taken as soon as possible.

Quadrant 3 – This is ideally where you want your users, not clicking the link, but reporting the email as suspicious.

Quadrant 4 – This is a mixed bag. It contains some people who are halfway there, in that they did not click the link, but they also did not report the email as suspicious (a second best to being in quadrant 3). But it also contains the people who never even opened the email and so never would have had the chance to click the link.

If the email client is configured to display remote images, we can calculate one more set of metrics that gives a good overall picture. To account for the people who never opened the email in our metrics, we turn to “Measuring Resistance to Social Engineering” for the social engineering resistance (SER) set of metrics. SER corresponds to the probability that an adversary selecting one user at random, will obtain secret information (Hasle, Kristiansen, Kintel, & Snekkenes, 2005). We have slightly modified the metric as it is used in the article because we are adding the average assumption. It is important to note that since the metrics measure how likely the hackers are to succeed, lower numbers are better. (The original article inverted these numbers to show a preference for higher values so the numbers look better, but skipping this step makes it slightly easier to understand.) This set of metrics uses the same P and C values used in the previous metrics, but also takes into account the number of people who did and didn’t open the email. Three metrics are computed here, each based on a different assumption of how the people who did not open the email would have acted if they had opened the email. We will let A stand for active participants, the people who did open the email, and N stand for non-active



participants, the people who did not open the email. Note that these two values together should equal the population value. The three parts of the social engineering resistance metrics are:

Optimistic assumption – This value assumes that none of the non-active participants would have clicked the link, so we need divide the population by the number of clicks. (Note that this calculation is the same as the click rate above.) This gives us the low bound for the range.

$$SER_{LOW} = (C/P) * 100$$

Average assumption – This value assumes that the non-active participants would have clicked the link at the same rate as the active participants, so we need to find what percentage of the active participants clicked the link.

$$SER_{AVG} = (C/A) * 100$$

Pessimistic assumption – This value assumes that all of the non-active participants would have clicked on the link, so we add together the number of clicks and the number of non-active participants, then divide by the population. This gives us the high bound.

$$SER_{HIGH} = (C+N)/P * 100$$

Together these three numbers give us a social engineering resistance of:

$$SER = \langle SER_{LOW}, SER_{AVG}, SER_{HIGH} \rangle$$

which gives a fuller picture of the state of things. The actual value had everyone opened the email likely lies somewhere within this range.

Because of the current pandemic, we can do one more thing with each of the above metrics: we can look at if there is a difference in any of the metrics between people who are working from home and people who are working in the office. If we know the list of IP addresses that would show from people accessing the page at the office, we can split the users into these two groups and examine each of the above metrics for any differences between the two groups. The groups will be LI for workers who are in the office and LR for workers who are working remotely.

$$\text{Ratio of in-office : remote clicks} = LI:LR$$

## **CompanyN Phishing Test**

### **Conducting the Test**

For this test, the client wanted to test the entire company, so they provided us with a list of 521 email addresses, and we broke the list up into groups so the client's email server did not see over 500 identical emails coming in at the same time and stop them. We divided the list up by time zones, assigned a random number to each email address, and used those random numbers to parse the list into groups of 25-26 addresses, with one group of 6 addresses for the small group of users in the Pacific time zone. This gave us 21 lists of email addresses.

Based on our testing of our system, it takes around 35 seconds to send a group of 25 email addresses, and we wanted to space the groups out with several minutes in between for the sake of the email server, so within each time zone set, a group of emails was scheduled to be sent out every four minutes. Table 4 shows the planned schedule. The Eastern time zone groups were scheduled to start at 10:30 CST, the Central time zone groups to run from 11 a.m. – 12 p.m. CST, and the Pacific time zone group to be sent at 1:30 p.m. CST, so all the groups would be around the recommended time frame for their time zone.

Group	Time Zone	Send Time (CST)	Count
A01	Eastern	10:30 AM	25
A02	Eastern	10:34 AM	25
A03	Eastern	10:38 AM	25
A04	Eastern	10:42 AM	26
A05	Eastern	10:46 AM	26
B01	Central	11:00 AM	26
B02	Central	11:04 AM	26
B03	Central	11:08 AM	26
B04	Central	11:12 AM	26
B05	Central	11:16 AM	26
B06	Central	11:20 AM	26
B07	Central	11:24 AM	26
B08	Central	11:28 AM	26
B09	Central	11:32 AM	26
B10	Central	11:36 AM	26
B11	Central	11:40 AM	26
B12	Central	11:44 AM	26
B13	Central	11:48 AM	26
B14	Central	11:52 AM	25
B15	Central	11:56 AM	25
C01	Pacific	1:30 PM	6
<b>Total</b>			<b>521</b>

Table 4 - Schedule of email groups and send times

The majority of the emails were sent while one group member was on a video call with the client's IT Manager and Information Security Analyst, to help make sure everything ran smoothly. Server logs were monitored from our side and email logs were monitored from the client's side during the test. The group member marked the beginning of the test by attempting to visit [company.com/start-test](http://company.com/start-test), which was not a valid page, but this made an entry in the server logs. Sending of emails ran smoothly throughout the test, each group was sent within 2 minutes of the scheduled time. We caught a few email addresses during the that quickly came back as undeliverable, we corrected the email addresses and added them back to a later list. The call concluded several minutes after the last group of emails for the Central time zone was sent. At the correct time to send the last group of emails (for the Pacific time zone), the group member

sent the last group, then made an entry in the server logs by attempting to visit [company.com/done-sending](http://company.com/done-sending). The group member then informed the client and the rest of the group that the emails had all been sent.

We had decided to leave the test running through Friday of the same week, ending it at 5 p.m. at the local time of the office in the latest time zone, which was 7 p.m. CST. At this time, the group member attempted to visit [company.com/end-test](http://company.com/end-test) to clearly mark the end of the test in the server logs. The group member informed the client and the rest of the group. For reporting purposes, the client provided a list of all the users who reported the email as suspicious through the proper channels.

## **Cleaning Server Logs**

We looked through the server logs for the “GET /start-test” and “GET /end-test” log entries, collected all the logs in between, and combined them into one file. Any log entries before the start of the test and after the end of the test were trimmed off. The log files were imported into Excel which delineated the different parts of the log entries into separate columns, allowing for easier cleaning and gathering of metrics.

The login and authuser columns were removed from the logs completely, because every entry had a value of “-“ for both. The remaining columns were kept: IP address, datetime, request, HTTP status code, bytes returned, referrer, and user agent. We made additional columns from the request to make things easier to work with: request method and path, request method, request path, and protocol version.

Next, we sifted through the log entries themselves to remove any that would not be useful to gathering our metrics. If there was even a chance the entry might be useful, it was left in the

file. We defined the groups for removal by first looking for things we knew to look for (e.g., GET /robots.txt, empty requests) and groups of similarities we noticed (e.g., requests looking for WordPress vulnerabilities). When we got to the point that no more useful groups of more than a few entries could be defined, we filtered out what we knew could be useful information (e.g., requests containing a user ID, requests for one of the images on the page) and checked the remaining list to make sure we hadn't missed anything we might need. The remaining seemed to both provide no useful information that could be correlated back to a user ID and seemed to most likely be bot activity looking for vulnerabilities, so it was discarded. Table 5 shows what was removed from the server logs, along with the justification for removal, and the number of entries that were removed in that group. They are listed in the order they were removed, but the order is mostly unimportant, as all groups except for the last are mutually exclusive. There were 3043 log entries before cleaning, and 902 log entries remaining afterwards. These remaining log entries were put into a CSV file to be used for metrics.

Following this, the protocol version column was removed as every remaining value was "HTTP/1.1". Finally, anywhere the referrer was listed as "-" was changed to an empty cell.

removal group	removal reason	entries removed	remaining
(starting rows)	-	-	3043
request is empty or just "/"	provide no useful information & cannot be correlated back to a user ID	297	2746
request path is /list_upload.php or /mailer.php	scripts to send e-mails being called and run - we already have this information and do not need to know from the logs that the scripts were called	65	2681
OPTIONS * with an IP of ::1	apache logging quirk	11	2670
GET /robots.txt	related to managing webcrawler traffic	24	2646
request contains "wp" or "wordpress"	seem to be related to looking for wordpress vulnerabilities to exploit	478	2168
entries with requests like "\x16\x03\x01"	appear to be bots looking for vulnerabilities to exploit to add the server to an existing botnet	21	2147
request method of CONNECT	appear to be bots looking for vulnerabilities to exploit to add the server to an existing botnet	7	2140
not containing known useful terms *	provide no useful information & cannot be correlated back to a user ID AND appear to be bots looking for vulnerabilities to exploit to add the server to an existing botnet	1238	902

\* The following are considered to be containing known useful terms: request path is /index.php (the home page), request path or referrer contains /index.php?id (the home page with our added user identifier), request path contains unique\_pnxs (indicates the image within the body of the e-mail was accessed), request path contains /favicon.ico, /phishing.jpg, /img1.png, or /img2.png (the images related to loading the page), request path is not /start-test, /done-sending, or /end-test (markers we placed in the logs to indicate significant time points during the test).

Table 5 - Removal of server log rows not relevant to metrics

## Cleaning other Data

Minimal cleaning was needed in the other datasets.

The email and id dataset had all rows before the phishing test trimmed, as they were from testing the code and not related to the phishing test itself. There were no rows after the relevant rows.

The NAT addresses file required one row to be moved to be in line with the others.

From the help desk tickets file we removed header information from the spreadsheet being formatted as a report, and removed the “related to”, “priority”, and “days open” columns because each row had the same value for each of the three columns, and removed the “assigned to” column both because we do not need that data and to anonymize the dataset.

The undeliverable and auto reply datasets were manually created from what was in the securemessages@company.com email inbox.

## Building the Database

The next step was to put all the relevant information into a database so the metrics we need could be more easily extracted. The following datasets were gathered, cleaned, and saved as .csv files to be imported into the database:

- cleaned\_server\_logs.csv – the cleaned server logs
- email\_and\_id.csv – the list of datetime, email address, and user ID created by the mailer.php script
- client\_NAT\_addresses.csv – the list of NAT addresses from the client for determining who is accessing the email and site from the office vs. off-site
- help\_desk\_tickets.csv – the list of tickets sent to the help desk through the appropriate channel, informing the help desk of a potential phishing email
- undeliverable.csv – the list of email addresses that came back as undeliverable
- auto\_reply.csv – the list of email addresses that sent an autoreply to the phishing test email, along with the reason for the autoreply
- whois\_final.csv – information gathered from WhoIs lookups of users' IP addresses

MySQL was used due to accessibility of and familiarity with the software. MySQL Workbench was used as the interface. The tables were created, and the data was imported into each using the Table Data Import Wizard, and at this point we were able to start writing the queries to get the data needed for the metrics. Several views were created to organize the information, and the final query resulted in the data columns as shown in table 6 exported to a csv file to work with.

column name	data type	definition
user_ID	text	unique identifier for each user
time_phish_sent	datetime	server log datetime stamp from when the e-mail was sent
active_participant	datetime	represents the user opening the e-mail; server log datetime stamp from the GET request for the png with the name matching the user's ID
active_internal	integer	1 for yes, 0 for no
clicked	datetime	represents the user clicking the link and loading the page; server log datetime stamp from the GET request for the first image on the page
clicked_internal	integer	1 for yes, 0 for no
trained	datetime	represents the user reading at least some of the training on the page; server log datetime stamp from when the user clicked over to img2.png
trained_internal	integer	1 for yes, 0 for no
reported	datetime	represents the time the user e-mailed the help desk to report the e-mail as suspicious; datetime stamp the ticket was created
reported_no_forward	datetime	same as above column, but only if the user did not forward the phishing test e-mail to the help desk to report it
internal	integer	1 if any of the 3 internal values equals 1
sent_to_clicked	text	time elapsed between when the e-mail was sent and when the link was clicked
sent_to_reported	text	time elapsed between when the e-mail was sent and e-mailing the help desk to report the e-mail as suspicious
clicked_to_reported	text	time elapsed between the user clicking the link in the e-mail and e-mailing the help desk to report the e-mail as suspicious
clicked_to_trained	text	time elapsed between the user clicking the link in the e-mail and clicking over to img2.png

Table 6 - Final output from database, to be used for analysis



## Test Metrics

The metrics for the test we conducted are as follows. An anonymized copy of the full report provided to the client can be found in Appendix C.

The population started from a list of 521 email addresses, and an extra 5 were sent because the initial email address was incorrect and bounced. 10 of these were removed for being undeliverable, and 3 were removed for knowing about the test ahead of time. This gives a population of

$$P = 521 + 5 - 10 - 3 = 513$$

The number of users who clicked on the phishing link, the number of users we considered to be trained, and the numbers of users in in-office and remote locations were straightforward counts from the exported data. (See table 7 below) These numbers give a click rate of

$$\text{click rate} = C/P * 100 = 66/513 * 100 = 12.87\%$$

and a trained rate of

$$\text{trained rate} = T/C * 100 = 4/66 * 100 = 6.06\%$$

The active versus non-active participants is where things became tricky. While our trial run showed the 1-pixel white image planted in the body of the email accessed by the user's email client, the output at the end of the test showed some users we had flagged as non-active but who had clicked the link, so this suggests that only some users' email clients are loading the images without first asking for an ok from the user. For this reason, we worked out a way to estimate the number of active and non-active users.

Abbr	Name	value
P	population	513
C	clicked	66
T	trained	4
R	reported	95
A	active participants	counted: 212 estimated: 288
N	non-active participants	counted:301 estimated: 225
LI	location: in office	22
LR	location: remote	44

Table 7 - Values to calculate the metrics for this test

While the number of active and non-active users who did not click the link are unknowns, the number of users who showed as active and not active within the group of users who clicked the link is known. If we assume that the percentage of users who clicked the link but did not show as active holds the same for the overall population, this gives us the following estimated numbers:

	$C = 66$	$notC = 447$
$A$	37	251
$notA$	29	196

Two abbreviations have been added here:  $notC = P - C$ , and  $notA = P - A$ . The values in the C column are known, and the values in the notC column are the estimates. The percentage of users who clicked who do not show as active is 43.94%, so to find the estimate users who did not click and were not active, the number of users who did not click the link (notC) was multiplied

by the percentage, for a value of 196.41, which rounds down to 196, and simple subtraction gives us the estimated number of active users who did not click as 251. Error checking was done at this point to verify that the numbers in this matrix added up to the population value.

The metrics values for this test came out to a click rate of 12.87% and a trained rate of 6.06%. The matrix of clicked \* reported was calculated as:

	<i>Reported</i>	<i>Did not report</i>
<i>Clicked link</i>	0.39%	12.48%
<i>Did not click link</i>	18.13%	69.01%

Since the users have been specifically told not to forward a phishing email to the help desk to report it, we also calculated the clicked \* reported properly matrix, where reported properly is the list of users who reported, excluding the users who reported the email by forwarding it to the help desk:

	<i>Reported properly</i>	<i>Did not report properly</i>
<i>Clicked link</i>	0.19%	12.67%
<i>Did not click link</i>	7.60%	79.53%

34 users also directly contacted one of our two IT employee contacts at the client, either by phone or through Microsoft Teams, but we did not count these reports in the metrics at all as they did not report to the proper people or through the proper channels.

The social engineering resistance (SER) values for the test calculated as:

$$SER = \langle SER_{LOW}, SER_{AVG}, SER_{HIGH} \rangle = \langle 12.87\%, 22.92\%, 56.73\% \rangle$$

And the ratio of in-office to remote clicks was:

$$\text{Ratio of in-office : remote clicks} = 1:2$$

Based on this information, we wrote our follow-up report and recommendations.

## Recommendations

This test only includes one phishing email, but periodic repetition of a phishing test combined with the regular training will keep the information fresh in the minds of long-time users and help train up new users. Each iteration of the test serves both as an opportunity to teach and an opportunity to test the education that has been given in the past (Kumaraguru et al., 2009). Literature review recommends phishing emails for training purposes should be done on a monthly basis (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2008). Returning to reinforcement theory, with positive punishment, if you take away the training completely, the behavior is likely to return (Pierce & Cheney, 2013) and research by Jansson and Solms reinforces this in their research that suggests that users retain the information from this type of training even after 28 days (2013). In this type of situation, when you will not know when real phishing attacks happen, it will not be possible to give the training every time an employee clicks on a phishing email, but an intermittent training schedule has been shown to have more lasting effects than other types of training schedules (Huitt & Hummel, 1997).

The major weakness of this test is the same issue that plagues so much of computer security: how do you get the users to care about the education and putting it to use? While this is essential to examine and would be expected of a professional company contracted to do regular

testing, that is outside the scope of this particular project, especially as it could be a whole project of its own.

If monthly testing is found to be too much work and the company is seeing consistently positive results, an alternate suggestion is to pick an acceptable threshold for the metrics (e.g., the SER is below a certain percentage and at least a certain percentage of users are reporting the phish), and once the numbers have met this threshold for several tests in a row, decrease to quarterly testing as long as the metrics stay within the threshold. But the rate of employee turnover should also be taken into account – remember that you are not just retraining existing users, you are training your new users as well.

It is a good idea to vary the content of the phishing emails and the tactics pointed out to the users to help them learn as much as possible. That being said, Jansson and Solms found that users are able to learn to behave securely even when exposed to types of phishing attacks they have not previously seen (2013). Data should be kept about the different tests in relation to how the test was performed, what the test attempted to get the user to do (e.g., click a link, enter credentials, open an attachment), and difficulty of the phishing test to the user. Chapter 5 of the book “Phishing Dark Waters” outlines how the authors see three different levels of phishing tests (Hadnagy & Fincher, 2015), which we believe is a bit simplistic, but the qualities they use to determine the difficulty level of the test could be used to help determine the difficulty level of tests that are more similar. This metadata about the tests should be taken into account when comparing the metrics from different tests.

Technological security methods against phishing should continue to be used and strengthened wherever possible. Human training and technological prevention are

complementary to each other. Hackers will always be looking for new types of attacks and utilizing them, so it is essential to keep up your security measures as well.

## Conclusion and Recommendations

In conclusion, we have analyzed the information we obtained from conducting a literature review on phishing and have answered why people fall for phishing attempts. We have highlighted the traits of successful phishing emails so that others can learn what types of phishing attempts trick users the most. Using those traits of successful phishing emails, we have created a sample phishing campaign of our own. See Appendix A. From our literature review, we have also examined the different types of training available and examined which type of training is more effective.

Designing a phishing campaign can be broken down into three components: preparation, social engineering, and security training. During the preparation phase, we determine the goals of the phishing campaign. Here you will determine your target, initial attack date, attack frequency, and how you will record your metrics. This information needs to be decided early because without metrics you will not be able to compare your organization's progress. Once this information is decided the next step is to choose the theme for the phishing email. Our research showed emails that invoked fear, urgency, or greed seemed to obtain the biggest response out of users. The context should be varied so that the users do not detect a pattern. It is also important to make sure the phishing email looks convincing. Use personalization to make the targets feel an emotional connection and more likely to trust the sender.

As mentioned earlier, social engineering occurs when attackers attempt to trick users into doing something that is against their better judgement and the interests of security (Boyle &

Panko, 2015). Phishers feed off the fact that users may make bad judgements when their emotions are triggered. A few themes of phishing emails that our research showed caused emotions to stir in the targets were bank scams, tax scams, and failed delivery package scams. More recently, the phishers have used the COVID-19 pandemic as a theme to manipulate the targets. There were several factors that increased a users' susceptibility to phishing attacks including demographics, psychological indicators, personality traits, persuasion principles, and security and cyber threats training. All industries should be alert to the rise in cyber-attacks and be prepared with countermeasures to protect their organizations.

Organizations use regular IT security training to help protect their users and in turn, protect the organization from cyber threats. Training programs have used video-based training, game-based training, text-based training, and instructor-led training to inform the users of the threats and damages that come with phishing and other cyber-attacks (Tschakert & Ngamsuriyaroj, 2019). When looking at the frequency of the training programs, our research showed in addition to mandatory once-a-year training, organizations that provided training more frequently to their users saw better results when compared to organizations that did less. We saw that self-phishing campaigns were a good way to create teachable moments for the users. If the user was duped by the phishing email, they'd be taken to a website with additional training materials on ways to better identify phishing emails.

From our research done for our literature review we can make the following recommendations:

- Organizations should provide regular training for their users. This helps educate the users on the dangers of phishing and helps them learn how to identify phishing emails better.

- The training should be frequent enough so that the knowledge does not get lost on the users. Periodic reminders and warnings on new phishing tactics should be sent to the users to be up to date on the latest trends in phishing.
- If possible, organizations should periodically phish their employees in order to keep the knowledge from the training fresh in the employee's minds. Phishing tests help create teachable moments for the users that will lead to better awareness of the dangers of phishing.

Our phishing test was designed to be used as a training tool. We wanted to create a teaching opportunity for the company. We designed the phishing email to be persuasive enough so that the users would be tricked into clicking the link in the email. The goal was to give the user a shock and prove that they are vulnerable to phishing attacks, without the consequences of an actual phishing attack. After clicking the link, the user would then be taken to a webpage that notified them they had been phished. The phished user was then presented with a short amount of text-based training materials on how they could have detected that this phishing email was not sent from their company.

The data for our metrics were collected mostly from server logs and information that the company also agreed to at the end of our testing period. We sent 513 emails that successfully made it to the users. There were 66 users who clicked on our phishing link after opening the email. A total of 95 users reported the phishing email to the IT department as suspicious. We were unable to get the exact numbers of active and non-active participants, but we estimated 288 active and 225 non-active) From this data, we were able to calculate the following metrics:



- Click rate – The number of users who clicked the link divided by the number of people who were sent the phishing test (excluding any bounced back addresses) multiplied by 100 to give us the percentage. Click rate =  $(C/P) * 100 = (66/513) * 100 = 12.87\%$
- Trained rate – The number of users who went to the phishing page and clicked on the images to reveal the training materials. This value is the number of trained users divided by the number of people who clicked the link multiplied by 100 to give us the percentage. Trained rate =  $T/C * 100 = (4/66) * 100 = 6.06\%$
- Click matrix – The percentage of users that clicked or did not click on the link versus the number that did or did not report the phishing email correctly.

	<i>Reported</i>	<i>Did not report</i>
<i>Clicked link</i>	0.39%	12.48%
<i>Did not click link</i>	18.13%	69.01%

- Reported rate – The number of users that reported the email as suspicious through the proper channels. Users had been previously advised not to forward the email to the IT help desk.

	<i>Reported properly</i>	<i>Did not report properly</i>
<i>Clicked link</i>	0.19%	12.67%
<i>Did not click link</i>	7.60%	79.53%

- Social engineering resistance – The probability that a phisher can randomly select a target and obtain information.
  - Optimistic assumption =  $(C/P) * 100 = (66/513) * 100 = 12.87\%$
  - Average assumption =  $(C/A) * 100 = (66/288) * 100 = 22.92\%$

- Pessimistic assumption =  $(C+N)/P * 100 = (66+225)/513 * 100 = 56.73\%$
- $SER = \langle SER_{LOW}, SER_{AVG}, SER_{HIGH} \rangle = \langle 12.87\%, 22.92\%, 56.73\% \rangle$
- Ratio of in-office to remote clicks – The ratio of users that clicked on the link that were working in-office to working remote = 22:44 = 1:2

From the phishing experiment we created, we can make these additional recommendations:

- Regular phishing training should be conducted to help keep security information fresh in the users' minds.
- Training should be conducted monthly if needed. Otherwise, a slightly less frequent time (quarterly) can be used if monthly training is too stressful for the company.
- The company should phish their users (after securing approval from executives) to keep their users' knowledge current
- The content of the emails in the phishing campaign should vary from previous campaigns
- Incorporate a way to ensure users are completing the training if they do get phished. This was outside of the scope of our project, but perhaps adding a keyword that needs to be sent to the IT helpdesk that is revealed at the end of the training materials would help get the users to reach the end of the training materials.
- Incoming emails from outside the company should be flagged as “EXTERNAL” to indicate they are being sent from outside the company

This study has provided a summary of the various components of phishing emails and what makes them successful. It also provided details on a variety of other phishing studies. We were able to examine what traits most successful phishing emails contain so that others can learn and not get phished. We created our own phishing email campaign and discussed the results. We

have also provided recommendations that our volunteer company and others can learn from and implement to protect their users. While there is no single reason for what makes people click on phishing emails, our hope is that after reading this paper you will be better prepared to identify phishing emails and swim in safer waters on the Internet.

## References

- Anandpara V., Dingman A., Jakobsson M., Liu D., & Roinestad H. (2007, February). *Phishing IQ Tests Measure Fear, Not Ability*. In: Dietrich S., Dhamija R. (eds) Financial Cryptography and Data Security. FC 2007. Lecture Notes in Computer Science, vol 4886. Springer, Berlin, Heidelberg. [https://doi.org/10.1007/978-3-540-77366-5\\_33](https://doi.org/10.1007/978-3-540-77366-5_33)
- Annual Civil Monetary Penalties Inflation Adjustment, 45 C.F.R §102 (2020).  
<https://www.govinfo.gov/content/pkg/FR-2020-01-17/pdf/2020-00738.pdf>
- Better Business Bureau. (2020, September 4). *Scam Alert: Don't Be Fooled by a Fake Package Delivery Scam*. Better Business Bureau. <https://www.bbb.org/article/news-releases/20283-scam-alert-dont-be-fooled-by-a-fake-package-delivery-scam>
- Boyle, R. J., & Panko, R. R. (2015). *Corporate Computer Security* (4<sup>th</sup> edition). Pearson.
- Burda, P., Chotza, T., Allodi, L., & Zannone, N. (2020, August). *Testing the effectiveness of tailored phishing techniques in industry and academia: a field experiment*. [Paper presentation]. ARES 2020: The 15th International Conference on Availability, Reliability and Security, Virtual Event, Ireland. 1-10. 10.1145/3407023.3409178
- Chandler, S. (2020). *Google Registers Record Two Million Phishing Websites In 2020*. Forbes. <https://www.forbes.com/sites/simonchandler/2020/11/25/google-registers-record-two-million-phishing-websites-in-2020/?sh=29a9abc81662>
- Cybersecurity and Infrastructure Security Agency (CISA). (2020, August 25). *Avoiding social engineering and phishing attacks*. <https://us-cert.cisa.gov/ncas/tips/ST04-014>
- Dahbur, K., Bashabsheh, Z., & Bashabsheh, D. (2017). Assessment of Security Awareness: A Qualitative and Quantitative Study. *International Management Review*, 37-58.

- Davinson, N., & Sillence, E. (2010). It Won't Happen To Me: Promoting Secure Behaviour Among Internet Users. *Computers in Human Behavior*, 1939-1747.
- Deloitte. (2015). *Consumer Data Under Attack: The Growing Threat of Cyber Crime*. London: The Creative Studio at Deloitte.
- Gaudin, S. (2002). *Computer saboteur sentenced to federal prison*. Computerworld.  
<https://www.computerworld.com/article/2587925/computer-saboteur-sentenced-to-federal-prison.html>
- Gendre, A. (2020). *Bank of America Leads List of Most Spoofed Banks in Phishing Attacks*. VadeSecure. <https://www.vadesecure.com/en/blog/bank-of-america-leads-list-of-most-spoofed-banks-in-phishing-attacks>
- Goodin, D. (2020, 9 19). A Patient Dies After a Ransomware Attack Hits a Hospital. Retrieved from Wired: <https://www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital/>
- Greenberg, A. (2017, 6 12). 'Crash Override': The Malware That Took Down a Power Grid. Retrieved from Wired: <https://www.wired.com/story/crash-override-malware/>
- Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. John Wiley & Sons, Inc.
- Hadnagy, C., & Fincher, M. (2015). *Phishing dark waters: The offensive and defensive sides of malicious emails*. Indianapolis, IN: Wiley.

- Hasle, H., Kristiansen, Y., Kintel, K., & Snekkenes, E. (2005). Measuring Resistance to Social Engineering. *International Conference on Information Security Practice and Experience* (pp. 132-143). Springer-Verlag Berlin Heidelberg.
- Heartfield, R., Loukas, G., & Gan, D. (2016, October). *You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks*. [Paper presentation]. In *IEEE Access*, vol. 4, (pp. 6910-6928). doi: 10.1109/ACCESS.2016.2616285
- HIPAA Journal. (2021, January 13). *2020 HIPAA violation cases and penalties*. <https://www.hipaajournal.com/2020-hipaa-violation-cases-and-penalties>
- Huitt, W., & Hummel, J. (1997). An Introduction to Operant (Instrumental) Conditioning. Retrieved from Educational Psychology Interactive: <http://www.edpsycinteractive.org/topics/behavior/operant.html>
- IBM Security. (2020). *Cost of a data breach report 2020*. Armonk: IBM Corporation. <https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf>
- Internet Crime Complaint Center IC3. (2019). *2019 Internet crime report*. Washington, DC: Internet Crime Complaint Center IC3. [https://ic3pdfs.blob.core.usgovcloudapi.net/docs/2019\\_IC3Report.pdf](https://ic3pdfs.blob.core.usgovcloudapi.net/docs/2019_IC3Report.pdf)
- IP Commission. (2017). "The Report of the Commission on the Theft of American Intellectual Property." National Bureau of Asian Research. [https://www.nbr.org/wp-content/uploads/pdfs/publications/IP\\_Commission\\_Report\\_Update.pdf.4](https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf.4)

IRS. (2018, May 7). *Phishing, Identity Theft and Scams*. IRS.

<https://www.irs.gov/newsroom/phishing-identity-theft-and-scams>

Jakobsson, M., & Ratkiewicz, J. (2006, May). Designing ethical phishing experiments.

*Proceedings of the 15th International Conference on World Wide Web - WWW '06*, 513-522. doi:10.1145/1135777.1135853

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., & Lim, Y. (2007, February). *What Instills Trust?*

*A Qualitative Study of Phishing*. [Paper presentation]. Financial Cryptography and Data Security, 11th International Conference, FC 2007, and 1st International Workshop on Usable Security, USEC 2007, Scarborough, Trinidad and Tobago. 4886. 356-361. 10.1007/978-3-540-77366-5\_32.

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems*, 597-626.

Jansson, K., & von Solms, R. (2013). Phishing for Phishing Awareness. *Behaviour & Information Technology*, 584-593.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M., & Pham, T. (2009, July). School of Phish: A Real-World Evaluation of Anti-Phishing Training. Symposium on Usable Privacy and Security (SOUPS). Mountain View, CA.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. CHI 2007, (pp. 905-914). San Jose, CA.

- Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010, May). Teaching Johnny Not to Fall for Phish. *ACM Transactions on Internet Technology*, pp. 7:1-7:31.
- Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L., & Hong, J. (2008). Lessons from a Real World Evaluation of Anti-Phishing Training. *eCrime Researchers Summit*, eCrime 2008. 1 - 12. 10.1109/ECRIME.2008.4696970.
- Leyden, J. (2016, 3 24). Water treatment plant hacked, chemical mix changed for tap supplies. Retrieved from The Register:  
[https://www.theregister.com/2016/03/24/water\\_utility\\_hacked/](https://www.theregister.com/2016/03/24/water_utility_hacked/)
- Merriam-Webster. (n.d.). Phishing. In Merriam-Webster.com dictionary. Retrieved February 21, 2021, from <https://www.merriam-webster.com/dictionary/phishing>
- Mouton, F., Leenen, L., & Venter, H.S. (2016). Social engineering attack examples, templates and scenarios. *ScienceDirect Computers & Security*, 59 (1), 186-209.  
<https://doi.org/10.1016/j.cose.2016.03.004>
- Pierce, W. D., & Cheney, C. D. (2013). *Behavior Analysis and Learning*. New York: Psychology Press.
- Proofpoint, Inc. (2020). 2020 State of the phish: An in-depth look at user awareness, vulnerability and resilience.
- Redmond, B. (2010). Reinforcement Theory: What are the Rewards for my Work? Work Attitudes and Motivation. The Pennsylvania State University; World Campus.
- Rekouche, K. (2011, June 23). *Early phishing*. <https://arxiv.org/abs/1106.4692>



- Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2020). Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter? *Journal of Computer Information Systems*.
- Siadati, H., Palka, S., Siegel, A., & McCoy, D. (2017). Measuring the Effectiveness of Embedded Phishing Exercises. *CSET @ USENIX Security Symposium*.
- Summer, A. & Yuan, X. (2019). *Mitigating Phishing Attacks: An Overview*. ACM SE '19: Proceedings of the 2019 ACM Southeast Conference. ACM Digital Library.  
<https://dl.acm.org/doi/10.1145/3299815.3314437>
- Tschakert, K. F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, 5(6), e02010.  
<https://doi.org/10.1016/j.heliyon.2019.e02010>
- United States Federal Trade Commission. (n.d.). *Glossary of Scams and Legal Terms*. Retrieved February 21, 2021, from <https://www.ftc.gov/news-events/media-resources/glossary-scams-legal-terms>
- Wang, W. (2003). *Steal this computer book 3: What they won't tell you about the internet*. No Starch Press.
- Warburton, D. (2020). *2020 Phishing and Fraud Report*. F5.  
<https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report>
- Williams, E. J., & Joinson, A. N. (2020). Developing a measure of information seeking about phishing. *Journal of Cybersecurity*, 6(1), 1-16. <https://doi.org/10.1093/cybsec/tyaa001>

## Appendix A: Institutional Review Board Approval Letter

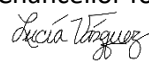
The following pages are the letter from the Institutional Review Board approving this research project. It is presented (as much as possible) with all formatting the same as we received it.

# UNIVERSITY OF ILLINOIS SPRINGFIELD

Office of Research and Sponsored Programs  
Public Affairs Center 515  
One University Plaza, MS PAC 525  
Springfield, Illinois 62703-5407

## MEMORANDUM

To: Carolyn Grafton  
Andrew Bates, Thomas Caldera, Shanita Hunt, and Pedro Valencia  
Sahar Farshadkhah, Assistant Professor, Management Information Systems

From: Lucía Vázquez, PhD, Interim Associate Vice Chancellor for Research & Innovation  
Human Subjects Review Officer & IRB Chair 

Date: March 17, 2021

Re: What Makes People Click? Designing an Effective Phishing Test;  
IRB Protocol #21-024

---

Thank you for submitting the proposed protocol for review. The protocol qualifies for review under the University of Illinois at Springfield Institutional Review Board (IRB) policies and procedures. However, given that this is unfunded research, federal wide assurance requirements do not apply. The project has been assigned Protocol Number 21-024, and I have carefully reviewed the protocol information to determine the applicable level of human subjects review.

The research methods outlined in this protocol qualify for expedited review as stipulated in the Code of Federal Regulations policy regarding human participants in research (Title 45 Public Welfare CFR Part 46 Protection of Human Subjects Subpart A, Federal Policy for the Protection of Human Subjects, Section 46.110), because the proposed research:

1. presents no more than minimal risk,
2. involves deception, and
3. will record data in such a manner that the identity of the human subjects cannot readily be ascertained, directly or through identifiers linked to the subjects.

Therefore, this project qualifies for review by the Human Subjects Review Officer, and a meeting of the UIS Institutional Review Board will not be necessary. Protocol 21-024 is approved. This determination of expedited review and approval applies solely to the research as described in Protocol 21-024 and constitutes approval for one year.

Any subsequent modifications to the Protocol 21-024 must be submitted to the UIS Human Subjects Review Officer so that review requirements can be reassessed. Approval must be formally granted

before any modifications can be implemented. Waiver of Informed Consent is included as detailed in the approved Protocol 21-024.

The expiration date for the research activities specified in Protocol 21-024 is March 17, 2022. **Annual reporting is required** (UIS IRB Policy Section 7.5.2). If research under this protocol will continue beyond March 17, 2022, you must submit a Continuation Review Form (available on the IRB website) to my office at least 45 days before the expiration date.

In accordance with University of Illinois policy, all human subjects-related records from this research should be retained in a secure location for three years beyond its completion, and be accessible for inspection should the need arise.

The Responsible Principal Investigator must report any adverse events or unanticipated problems to the IRB as soon as possible, but in all cases within 5 working days, as outlined on page 16 of the UIS IRB Policy

(<https://www.uis.edu/academicstaffhandbook/wpcontent/uploads/sites/84/2019/02/Institutional-Review-Board-Policies-2019-2-19.pdf>).

I appreciate the attention you have given to the issue of the protection of human subjects, and I wish you success with this endeavor. Please feel free to contact me if you have any questions about this review or the UIS IRB process.



Phone (217) 206-7409

Fax (217) 206-7623

## Appendix B: Code

### index.php

```
<?php
    $phished=fopen("phished.txt","a");
    fwrite($phished,time().'.'.$_GET['id']."\n");
    //echo("Hello unique ID # ".$_GET['id']);
?>
<!DOCTYPE html>
<html>
    <head>
        <title>Phishing Test</title>
        <meta name="description" content="">
        <meta name="viewport" content="width=device-width, initial-scale=1">
    </head>
    <body>
        <div class="img_area">
            
        </div>
        <div>
            <h1>Uh oh! <br>You clicked on a simulated phishing test!</h1> <br>
            <h3>Don't close your browser! This is just a simulation authorized by CompanyN as an
educational tool to help prevent falling for a <em>real</em> phishing attack.</h3>
        </div>
        <div id="steps0">
            <h2><strong>What is phishing?</strong></h2>
            <h3>Phishing is often an attempt to trick you into giving out sensitive
information you wouldn't normally provide. It may be done through email or websites. A common
method is to email a large group of people a link to a page that appears legitimate in an attempt to
collect login credentials, credit card information, etc. Another common type of phishing consists of
attempting to get you to click a link or open a file that actually downloads malware onto your system.
Don't worry, this simulation neither collects your information nor gives you malware.</h3>
        </div>
        <div id="steps1">
            <h2><strong>Indicators this email was phishing:</strong></h2>
            <!--<h3>**Enter marked up image here**</h3>-->
            <h3>There are two things in this email that could have indicated to you that it was a
phish. See if you can figure out what they are, then click on the image to reveal them.</h3>

<script type="text/javascript">

var tracker = 'img1';

function change(){
var image = document.getElementById('imageX');
if(tracker=='img1'){
```

```

image.src='img2.png';
tracker='img2';
}
else{
image.src='img1.png';
tracker='img1';
}
}

</script>


  <div id="steps2">
    <h2><strong>Think critically about the email before acting:</strong></h2>
    <table id="subway">
      <tbody>
        <tr>
          <td>
            <ul>
              <li class="sidebarSubwayStepTitle">
                <h3>What are the calls to action? For example, does the email ask you to click a
link, open an attachment, or reply with information?
                </h3>
              </li>
              <li class="sidebarSubwayStepTitle">
                <h3>Is the sender external? If so, use extra caution when acting on the email.
Make sure to review the actual sender address, not just the name.</h3>
              </li>
              <li class="sidebarSubwayStepTitle">
                <h3>Does the email use fear tactics such as fear, curiosity, or greed? If so, this is
reason to be suspicious.
                </h3>
              </li>
            </ul>
          </td>
        </tr>
      </tbody>
    </table>
  </div>
  <div id="steps3">
    <h2><strong>Steps to take if you suspect phishing:</strong></h2>
    <table id="subway">
      <tbody>
        <tr>
          <td>
            <div class="sidebarSubwayStepWrapper">
              <div class="sidebarSubwayStep">1</div>
              <div class="sidebarSubwayConnector"></div>

```

```

        </div>
      </td>
      <td>
        <div class="sidebarSubwayStepDetailsWrapper">
          <h3 class="sidebarSubwayStepTitle">Do not click a link, open an attachment, or reply
to the email!</h3>
        </div>
      </td>
    </tr>
    <tr>
      <td>
        <div class="sidebarSubwayStepWrapper">
          <div class="sidebarSubwayStep">2</div>
          <div class="sidebarSubwayConnector"></div>
        </div>
      </td>
      <td>
        <div class="sidebarSubwayStepDetailsWrapper">
          <h3 class="sidebarSubwayStepTitle">Report the email to the help desk. DO NOT
FORWARD the email to the help desk or to anyone else.</h3>
        </div>
      </td>
    </tr>
    <tr>
      <td>
        <div class="sidebarSubwayStepWrapper">
          <div class="sidebarSubwayStep">3</div>
        </div>
      </td>
      <td>
        <div class="sidebarSubwayStepDetailsWrapper">
          <h3 class="sidebarSubwayStepTitle">Wait to hear from IT before you do anything else
with the email. DO NOT delete it yet.</h3>
        </div>
      </td>
    </tr>
  </tbody>
</table>
<div>
  <h3>Even if you incorrectly identified the email as phishing, it's better to be safe than sorry!
Remember: Stay alert! You are what keeps us safe.
</h3>
</div>
</body>
</html>

<style>
.img_area {

```

```

    text-align: center;
}

html, body {
    max-width: 960px;
    font-family: 'Open Sans', sans-serif;
    font-weight: normal;
    color: #676767;
    text-align: left;
    /*margin: 1vw 10px 1vw 10px;*/
    margin: auto;
    padding-bottom: 3em;
    font-size: 1em;
}

h1{
    margin: auto;
    text-align: center;
    border: 1px solid #e2e2e2;
    border-radius: 11px;
    width: 100%;
    padding: 30px 10px;
    margin-top: 3vw;
}

h2{
    padding: 0.75rem 0 0.5rem;
}

.sidebarSubwayStep {
    width: 30px;
    height: 30px;
    border-radius: 50%;
    font-size: 22px;
    color: white;
    line-height: 30px;
    text-align: center;
    background: #054f7d;
}

#subway {
    height: fit-content;
    -webkit-border-vertical-spacing: 0;
}

.sidebarSubwayStepWrapper {
    height: 1px;
}

```



```

.sidebarSubwayConnector {
  border-left: 4px solid #054f7d;
  min-height: 40px;
  width: 4px;
  margin-left: 13px;
  height: 100%;
}

.sidebarSubwayStepDetailsWrapper {
  padding-bottom: 1rem;
  max-width: 100%;
}

#subway > tbody > tr > td {
  height: 100%;
  vertical-align: top;
  padding-left: 10px;
}

.sidebarSubwayStepTitle {
  padding-top: 5px;
  padding-bottom: 0px;
}

.subway {
  margin: 0;
  overflow-x: auto;
  min-height: 7em;
  max-width: none;
  width: calc(100% + 2rem);
  margin-left: -1rem;
  white-space: nowrap;
  -webkit-overflow-scrolling: touch;
}

.subway.noScrolling {
  overflow-x: hidden;
}

.subway .line {
  margin-bottom: -0.333em;
  top: calc(2.25rem + 0.325em);
}

.subway .line:after, .subway .line:before {
  content: "";
  display: inline-block;
}

```

```

    height: 0.333em;
    width: 4.25em;
}

.subway .line .trainrail {
    margin-bottom: 0.667em;
}

.subway .showMobile {
    display: inline-block !important;
}

.subway .line .trainrail, .subway .stops .trainstop {
    padding: 0 0.3em;
    white-space: normal;
    width: 8.5em;
}

.subway .trainstop {
    -webkit-hyphens: none;
    -ms-hyphens: none;
    hyphens: none;
}

.stops .trainstop span.trainstation {
    border-radius: 0.5em;
    height: 1em;
    width: 1em;
}

.stops .trainstop span.description {
    vertical-align: top;
}

.trainstop a {
    -webkit-tap-highlight-color: transparent;
}

.subway .line, .subway .line .trainrail {
    height: 0.333em;
}

h3 {
    display: block;
    font-weight: normal;
    padding: 0.75rem 0 0.5rem;
    width: 100%;
}

```

```

* {
    box-sizing: border-box;
    margin: 0;
    max-width: 100%;
    padding: 0;
}

ul{
    list-style: disc;
    list-style-position: outside;
    padding-left: 20px;
}

</style>

list_upload.php

<!DOCTYPE html>
<html>
    <head>
        <title>Upload</title>
    </head>
    <body>
        <form enctype="multipart/form-data" action="list_upload.php" method="POST">
            <p>Upload target list</p>
            <input type="file" name="uploaded_file"></input><br>
            Password:<input type="password" name="pass"><br>
            <input type="submit" value="Upload"></input>
        </form>
    </body>
</html>
<?PHP
    if(!isset($_POST['pass'])){
        echo "Enter password.";
        exit();
    }
    if(hash(ripemd160,$_POST['pass'])!=PASSWORD_HASH_REMOVED){
        echo "Incorrect password.";
        exit();
    }
    if(!empty($_FILES['uploaded_file'])){
        $path="./targets/targets.txt";
        if(move_uploaded_file($_FILES['uploaded_file']['tmp_name'], $path)) {
            echo "<br>The file ". basename( $_FILES['uploaded_file']['name'])." has been
uploaded. If the list looks ok, click the link at the bottom to start sending.";
            echo "<br><br>Uploaded list:<br><br>";
            $targets=file("../targets/targets.txt");

```

```

        for($i=0;$i<count($targets);$i++){
            echo $targets[$i];
            echo "<br>";
        }
        echo "<br><a href=\"mailer.php\">Execute</a>";
    }else{
        echo "There was an error uploading the file.";
    }
}

?>

```

## mailer.php

```

<?php
use PHPMailer\PHPMailer\PHPMailer;
use PHPMailer\PHPMailer\Exception;
require 'PHPMailer/src/Exception.php';
require 'PHPMailer/src/PHPMailer.php';
require 'PHPMailer/src/SMTP.php';
$targets=file("../targets/targets.txt");
for($i=0;$i<count($targets);$i++){
    $unique_id=random_int(1111111111111111,9999999999999999);
    if(!copy("unique_pngs/0.png","unique_pngs/".$unique_id.".png")){
        echo "PNG write failed. Terminating.";
        exit();
    }
    if(!$f=fopen("../email_and_id/email_and_id.txt","a")){
        echo "Email to ID map file failure. Terminating.";
        exit();
    }
    fwrite($f,time().":".rtrim($targets[$i]).":".$unique_id."\n");
    $mail = new PHPMailer();
    $mail->SMTPSecure = false;
    $mail->SMTPAutoTLS = false;
    $mail->SMTPDebug = 2;
    $mail->isSMTP();
    $mail->Host = 'smtp.companym.com';
    $mail->SMTPAuth = true;
    $mail->Username = 'securemessages@companym.com';
    $mail->Password = PASSWORD REMOVED;
    //$mail->SMTPSecure = 'tls';
    $mail->Port = 25;
    $mail->setFrom('securemessages@companym.com', $name = 'CompanyN Secure Messages');
    $mail->addReplyTo('securemessages@companym.com', 'CompanyN Secure Messages');
    $mail->Subject = 'Secure Messages – CompanyN';
    $mail->isHTML(true);
}

```

```

        $mailContent = "You have two secure messages<br><br>Please sign in to view<br><br><a
href=\"http://securemessages.companym.com/index.php?id=\".$unique_id.\">Sign in</a><img
src=\"http://www.companym.com/unique_pngs/\".$unique_id.\".png\"</img>";
        $mail->Body = $mailContent;
        $mail->addAddress($targets[$i], 'test');
        if($mail->send()){
            echo 'Message has been sent<br><br>';
        }else{
            echo 'Message could not be sent.';
            echo 'Mailer Error: ' . $mail->ErrorInfo;
        }
    }
}

```

## Appendix C: Report Provided to Client

The following pages are the end deliverable of the phishing test – a follow-up report provided to the client. The report has been anonymized to protect the privacy of the client. It is presented (as much as possible) with all formatting the same as when it was presented to the client.

**<<LOGO>>**

**CompanyN**

**Prepared for:**

**President**

**IT Manager**

**Information Security Analyst**

**Prepared by:**

**Andrew Bates, UIS graduate student**

**Thomas Caldera, UIS graduate student**

**Kari Grafton, UIS graduate student**

**Shanita Hunt, UIS graduate student**

**Pedro Valencia, UIS graduate student**

**Sahar Farshadkhah, faculty research supervisor**

**Management Information Systems**

**Capstone course project, Spring 2021**

**<<This is an anonymized copy of the follow-up report provided to the client  
after the completion of the phishing test.>>**



## Background

Phishing attacks are on the rise, and we should remember that the attackers are often several steps ahead of the technologies and personnel intended to defend against them. Even the best anti-phishing tools are merely reactive, and can only prevent against known attacks. To help guard against new attacks we need to be proactive; users need to be trained to be the front line against these attackers. A survey of 524 companies who experienced a data breach between August 2019 and April 2020 found that 19% of the breaches were a result of compromised credentials. The average cost of the studied data breaches was \$3.86 million, and it took an average of 280 days to contain the breach.<sup>1</sup>

CompanyN has had multiple phishing tests done in the recent past and been less than happy with the results of the tests. Each test has resulted in credentials being obtained that have allowed the tester to gain access into one or more of CompanyN's information systems. Education has been provided to the employees, and the goal of this test was to gauge the training's effectiveness and provide ongoing phishing training for the employees.

## Test Design

While previous phishing tests have attempted to acquire user credentials, this test uses just an email link in this test for three reasons. First, research has shown that users who log in before seeing the education page are confused as to why they are seeing information about not clicking on links, likely because the login created a gap between clicking the link and seeing the education.<sup>2</sup> Second, the same research also suggests that the majority of users who will click on a phishing site will also provide their credentials, so it seemed unnecessary. And finally, because collecting credentials also introduces extra security complications that would be preferable to avoid in this particular case.

Care was taken in designing an email with the appropriate level of persuasiveness. Phishing scams as common and obvious as "Nigerian prince" scams should be well-known enough at this point that it would limit the usefulness of any training provided. The most complex phishing emails tend to include elements that are beyond the average computer user's understanding, and this level of attention to detail is less commonly seen in real-world phishing attacks. While these are important to train, without enough details of previous tests to create a baseline to compare against, the decision was made to design a more average-difficulty test to both give the most accurate overall predictive metrics and to create a baseline that a training program of repeated phishing tests can be built off of.

Figure 1 shows a screenshot of the email for this phishing test from within CompanyN's environment. The primary strategy chosen for this phish was to acquire a domain one letter off

---

<sup>1</sup> IBM. (2020). *Cost of a Data Breach Report 2020*. Armonk, NY: IBM Corporation.

<sup>2</sup> Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. *CHI 2007*, (pp. 905-914). San Jose, CA.



from the company's real domain in the hopes that the users would miss the subtle difference. The domain companym.com was available and was acquired for the test. There are two places that the user could have noticed this discrepancy: in the from address or by hovering over the sign in link to view the actual URL. The email system is set up to flag external senders as shown in the screenshot of the email, but experience says that many users ignore this warning. The secondary strategy chosen for this phish was to make the email look like something that could legitimately come up in the course of the user's work. It is not unreasonable to think a user would receive a message from a coworker or client that required extra security, and this email was designed based on some simple examples of legitimate emails of this sort.

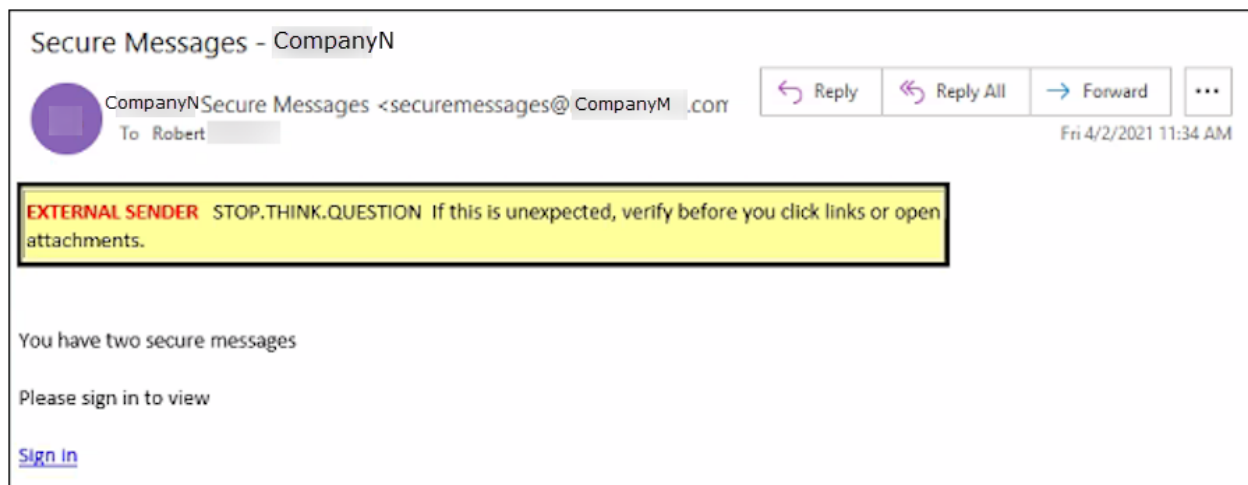


Figure 1 - Phishing email for this test, shown inside the client's environment

The day of the week and time of day selected to send the email was strategic as well. One of the strategies of social engineering is to get users to act without thinking, so a time was selected when users were likely to be busy and/or preoccupied. Mondays are a good day, because people are trying to get caught up from the weekend and may not be giving things the attention they should be. The two times of day considered were shortly before lunchtime and shortly before the end of the day. Shortly before lunchtime was chosen because sending at the end of the day leaves it more likely that the user will ignore it until the next day, whereas if the user leaves the email until after lunch, a much smaller time gap is created.

The client provided a list of 521 email addresses for the test, which were broken up into smaller groups so the email server did not see such a large number of identical emails coming in at the same time, and block it as suspicious. The list was divided up by time zones so all emails would be sent around the recommended time frame for the time zone, a random number was assigned to each email address, and these random numbers were used to parse the list into groups of 25-26 addresses, with one group of 6 addresses for the Pacific time zone. Groups were scheduled to be sent with gaps of 4 minutes in between.

Before the actual phishing test, a trial run of the test was done to make sure the email would successfully make it to a user's inbox. At this point, the server logs were also checked to see if

the 1-pixel white image planted in the body of the email would show as accessed, which would indicate that the user opened the email. This trial run did show the image accessed, but the final test results show some users who clicked the link without showing as having accessed the email, so this suggests that only some users' email clients are loading the images without first asking for an ok from the user. For this reason, estimated active users will be calculated and used in the metrics.

Sending of the emails ran smoothly and the schedule was adhered to  $\pm 2$  minutes. A few emails quickly bounced back as undeliverable, and an attempt was made to correct the email address and add them back into a later list. The test was considered "open" until Friday of the same week, at 5 p.m. at the office in the latest time zone. At this time, the server logs for the duration of the test were pulled to be used to calculate the metrics.

Clicking the link took the user to an education page designed specifically for this test, and structured into 5 parts:

1. A brief, light-hearted attention-getter including an image that represents phishing in a slightly amusing way, and large text telling the user they have clicked on a simulated phishing test authorized by CompanyN.
2. A very brief description of what phishing is.
3. An interactive piece telling the user that two things in this particular email could have indicated to them that it was a potential phishing email and asking the user to see if they could identify them. Clicking the image revealed the indicators to the user with callouts giving more information. This section uses rule-based training to teach users specific things to watch out for.
4. Three ways to think critically about an email before acting. This encourages the user to be mindful in what they are doing, to counteract the attempt of social engineering methods to get the user to act without thinking.
5. The steps the user should take if they suspect an email may be a phish. These are kept as succinct as possible, so the user does not have too much to remember.

## Results

The majority of the data needed for the metrics were gathered from the server logs, with the remaining data received from the client. Table 1 lists each value used in the metrics, how the value was obtained, and the value resulting from this test. All values and metrics exclude the people at the company who knew the test was taking place.

It would have been possible to include demographic attributes of the users in the metrics to see if and how this affected things, but the literature has very mixed opinions on whether demographic attributes actually contribute. Even if there was any significant contribution found, this information only becomes actionable if it can be used to tailor the training in some way. Given the literature's disagreement on this matter and the extra amount of work that would go into trying to tailor the training to different groups of demographics with potentially very little benefit, demographic attributes have not been included in these metrics.

Abbr	Name	Metric	How Gathered	value
P	population	users the email was successfully sent to	received list from the client	513
C	clicked	users who clicked the link in the email	count of IDs in the server logs who have a GET request for index.php	66
T	trained	users who clicked the image to see the indicators of potential phishing	count of IDs in the server logs who have a GET request for img2.png	4
R	reported	users who reported the email as suspicious	received list from the client	95
A	active participants	users who opened the email	count of IDs in the server log who have a GET request for the hidden image in the email	counted: 212 estimated: 288
N	non-active participants	users who did not open the email	population minus active participants (P-A)	counted:301 estimated: 225
LI	location: in office	users who clicked the link from one of the client's office locations	count of IDs whose GET request for index.php shows as from an IP in the list of IPs the client provides as their NAT addresses	22
LR	location: remote	users who clicked the link from a remote location	count of IDs whose GET request for index.php shows as from an IP not in the list of IPs the client provides as their NAT addresses	44

Table 1 – Values for the phishing test metrics

The most obvious metric to report is click rate, the number of users who clicked the link (C) divided by the number of people in the test population (P). Multiplying this by 100 gives us a percentage:

$$\text{click rate} = C/P * 100 = 66/513 * 100 = 12.87\%$$

One interesting extra piece of information is that the first user to click the phishing link did so 4 seconds after the email was sent. This expresses just how important it is for the help desk team to be made aware of any real phishing attacks as quickly as possible.

Also relevant is how many of the people who went to the phishing page clicked on the image to reveal what the phishing indicators were. This divides the number of people who clicked over to the second image (T) by the same C used above to give a rate of phished users who were also trained by reading at least a portion of the education page:

$$\text{trained rate} = T/C * 100 = 4/66 * 100 = 6.06\%$$

But just looking at the click rate and trained rate fails to show the whole picture. An essential piece is to know how many people reported the email as suspicious. Matching up whether each person clicked the link or not and whether each person reported the email as suspicious or not gives the following matrix:

	<i>Reported</i>	<i>Did not report</i>
<i>Clicked link</i>	1	2
<i>Did not click link</i>	3	4

Dividing each quadrant by P and multiplying by 100 gives a percentage for each value. This gives a better breakdown by quadrants, as follows:

Quadrant 1 – These users are halfway there. Despite clicking on the phishing link, they then followed up by reporting it to the help desk.

Quadrant 2 – These users are the most dangerous. Not only did they click the link, they did not report it to the help desk so mitigating action could be taken as soon as possible.

Quadrant 3 – This is ideally where you want your users, not clicking the link, but still reporting the email as suspicious.

Quadrant 4 – This is a mixed bag. It contains some people who are halfway there, in that they did not click the link, but they also did not report the email to the help desk as suspicious (a second best to being in quadrant 3). But it also contains the people who never even opened the email and so never would have had the chance to click the link.

This test grouped users in the following way:

	<i>Reported</i>	<i>Did not report</i>
<i>Clicked link</i>	0.39%	12.48%
<i>Did not click link</i>	18.13%	69.01%

Users have been specifically told not to forward a phishing email to the help desk to report it, so if only the users who reported it to the help desk properly are counted, the numbers are more concerning:

	<i>Reported properly</i>	<i>Did not report properly</i>
<i>Clicked link</i>	0.19%	12.67%
<i>Did not click link</i>	7.60%	79.53%

34 users also directly contacted one of the two IT employees involved in running the test either by phone or through Microsoft Teams, but these reports are not counted in the metrics as they did not go through the proper channels.

The test run with the phishing test email showed that the email client is configured to display remote images for at least some users, so a social engineering resistance (SER) metric can be calculated. SER corresponds to the probability that an adversary, selecting one user at random, will obtain secret information.<sup>3</sup> It is important to note that since the metrics measure how likely the hackers are to *succeed*, lower numbers are better.<sup>4</sup> This set of metrics uses the same P and C values from previous metrics, but also takes into account the users who did and did not open the email.

This is where the estimated numbers of active users come into play. It is unknown how many of the users who did not click the link opened the email, but the number of users who showed as active and non-active within the set of users who clicked the link is known. Using the assumption that users who did not click the link accessed the email in the same ratio as users who did click the link, estimated numbers of active and non-active users for the entire population can be calculated. Those estimated numbers will be used for the social engineering resistance metric as they are likely closer to the actual value.

Three metrics are computed here, each based on a different assumption of how non-active participants would have acted if they had opened the email. The three parts of the social engineering resistance metric are:

Optimistic assumption – This value assumes that none of the non-active participants would have clicked the link, so divides P by C. (Note that this calculation is the same as the click rate above.) This gives the low bound for the range.

$$SER_{LOW} = (C/P) * 100 = (66/513) * 100 = 12.87\%$$

Average assumption<sup>5</sup> – This value assumes that the non-active participants would have clicked the link at the same rate as the active participants, so C is divided by A to find what percentage of the active participants clicked the link.

$$SER_{AVG} = (C/A) * 100 = (66/288) * 100 = 22.92\%$$

---

<sup>3</sup> Hasle, H., Kristiansen, Y., Kintel, K., & Snekenes, E. (2005). Measuring Resistance to Social Engineering. *International Conference on Information Security Practice and Experience* (pp. 132-143). Springer-Verlag Berlin Heidelberg.

<sup>4</sup> Note that the original article inverted these numbers to show a preference for higher values so the numbers look better, but skipping the step makes it slightly easier to understand.

<sup>5</sup> The average assumption was not included in the original paper that designed the SER, but it is a natural extension of the method.

Pessimistic assumption – This value assumes that all of the non-active participants would have clicked on the link, so adds together the number of clicks and the number of non-active participants, then divides by P. This gives the high bound.

$$SER_{HIGH} = (C+N)/P * 100 = (66 + 225)/513 * 100 = 56.73\%$$

Together these three numbers give a social engineering resistance of:

$$SER = \langle SER_{LOW}, SER_{AVG}, SER_{HIGH} \rangle = \langle 12.87\%, 22.92\%, 56.73\% \rangle$$

which gives a fuller picture of the state of things. The actual value had everyone opened the email likely lies somewhere within this range.

Because of the current pandemic and drastic increase in the number of employees working from home, it is worth looking into if there are behavioral differences between users working in-office (LI) and remote (LR). Each user's location was determined by comparing the IP address in the server logs with the list of internal NAT addresses provided by the client. Each set of metrics could be split by in-office and remote, but the most useful information comes from a straight comparison of the ratio of clicks from in-office users to remote users:

$$\text{Ratio of in-office : remote clicks} = LI:LR = 22:44 = 1:2$$

This does not necessarily mean that a user working remotely is twice as likely to click the phishing link as a user who is working in the office. Since this is only one data point, it is not enough to make that much of a prediction. What it does mean is that *for this particular test*, remote users clicked the phishing link at twice the rate of in-office users, so it is a metric worth keeping an eye on and possibly digging further into.

Performing whois lookups of the users' IP addresses could also provide a potential hacker a plethora of information, including approximate user locations, information about the network, and so on. Most of the internal NAT addresses on the list provided by the client were also identified as belonging to the company this way. A determined hacker could also go after very specific information found this way. The whois information on one user's IP address placed them at a specialized medical facility. If the assumption is made that the user is there as a patient (as opposed to doing work for the medical facility), this could give a hacker a very sensitive approach to spear-phish the specific employee.

## Recommendations

This test only included one phishing email, but periodic repetition of a phishing test combined with the embedded training will keep the information fresh in the minds of long-time users and help train up new users. A review of the literature recommends phishing emails for training purposes should be done on a monthly basis.<sup>6</sup> Each iteration of the test serves both as an

---

<sup>6</sup> Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2008). Lessons from a Real World Evaluation of Anti-Phishing Training. *2008 eCrime Researchers Summit* (pp. 1-12). IEEE.

opportunity to teach and an opportunity to test the education that has been given in the past. These future tests are the place to introduce the more complex elements that show up in the more carefully-designed phishing attacks, to further the users' knowledge. This test can also serve as both a design model and a baseline for future testing.

The major weakness of this test is the same issue that plagues so much of computer security: how do you get the users to care about the education? While this is essential to examine and would be expected of a company contracted to do regular testing, that is outside the scope of this particular project for this particular group of graduate students.

We recommend selecting one provider to do the testing, whether it is done in-house or by a penetration testing company, and gathering the same metrics from each test so they can be compared across time. Using the same provider across tests would also let the provider track individuals across tests, at a level of granularity which would not generally be provided to the client, to identify users who are a particular danger to the company and should be provided additional training. A dashboard giving a visual representation of the aggregate metrics from the series of tests would also be beneficial.

If monthly testing is found to be too much and the company is seeing consistently positive results, an alternate suggestion is to pick an acceptable threshold for the metrics (e.g., the SER is below a certain percentage and at least a certain percentage of users are reporting the phish), and once the numbers have met this threshold for several tests in a row, decrease to quarterly testing so long as the metrics stay within the threshold. But the rate of employee turnover should also be taken into account – remember that you are not just continuing training for existing users, you are training your new users as well.

Phishing attacks are unlikely to ever go away, given how successful they can be and often are, and from very little work on the hacker's end. But that does not mean that defending against them is a fruitless task. Users should be seen not so much as the "weakest link"; a shift needs to be made towards seeing them as an integral brick in the defense structure against phishing attacks. Periodic, concise training that is tailored to your company's and users' needs is how you will reinforce this brick and strengthen the mortar between it and the other bricks in your defense structure.