Understanding Phishing as a Social Engineering Problem: Why Societal Educational Efforts Falls Short

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Justin Gou

Spring, 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Bryn E. Seabrook, Department of Engineering and Society

STS Research Paper

Why Phishing is a Problem

"Congratulations! You are the winner of a brand new iPad! Click here to claim your prize." Emails like this are incredibly common with the intent to trick users into clicking malicious links. In the field of cybersecurity and social engineering, this tactic is called phishing and is becoming increasingly popular among attackers. In the year 2020 alone, 75% of organizations reported experiencing some kind of phishing attack (Rosenthal, 2021). Efforts have been made to properly educate employees to avoid falling victim to these phishing attacks. Unfortunately, with phishing being so popular among attackers, phishing technology is rapidly developing, making emails seem more and more realistic (Chabrow, 2014). With ideas such as spear phishing, which is when the email is targeted towards one specific individual after gathering personal information, people continue to fall victim to these attacks. A deeper analysis of this problem would help understand why current efforts remain ineffective and why people still willingly fall for these attacks, despite understanding the risks through training. Wicked problem framing is being applied in order to approach the problem through a different perspective, since address phishing as a whole proves to be ineffective, as it remains a wicked problem. In order to evaluate the problems of general understanding of phishing attacks, the following question must be addressed: how does the average American understand phishing as a social engineering problem?

Methods

The proposed research question is explored through wicked problem framing in hopes to gain a better understanding of why the problem continues to be an unaddressable issue. Phishing certainly falls into the category of a wicked problem, as developing technologies continue to

improve phishing techniques, efforts to counter the attack prove ineffective and the attack continues to be successful. The primary source of information for this paper comes from previous publications studying phishing techniques and efforts to prevent phishing. Keywords to guide this research include “phishing,” “anti-phishing techniques,” “social engineering,” and “cybersecurity.” Past studies help understand which anti-phishing techniques have worked, which techniques have not, and why certain techniques work or do not. Through further analysis of these techniques, the goal of this paper is to understand the most effective way or combination of ways to address phishing based on how society is currently responding to modern anti-phishing techniques.

Background Information

Social engineering is one specific field of cybersecurity that has been increasingly popular for attackers. Phishing is one specific type of social engineering, which is defined as a “cyber attack that uses disguised email as a weapon” with the goal to “trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment.” (Fruhlinger, 2020). This attack has been around for decades, dating back to the 1990s, and continues to be relevant today simply due to the fact that it relies on the inherent psychological weaknesses of humans, which is oftentimes much easier to exploit than modern day security systems (Fruhlinger, 2020).

To better explain why attackers target human weaknesses, consider the common idiom, “a chain is no stronger than its weakest link”; this idiom says that with any given system, if the weakest part falls, the entire system falls. Drawing this back to cybersecurity, engineers are constantly working to improve the physical and digital security of their systems to resist

attackers as much as possible. The continued efforts of these engineers makes it incredibly difficult for attackers to brute force their way into the system, thus, the attackers seek alternative methods. Since employees are already given access to their computer systems, if an attacker is able to convince or trick an employee to let them in, they could easily bypass any security implementations. In this situation, the employees are the weakest link of the system, as they are much easier to trick than computers are to hack. Ultimately, this weakness is what makes phishing such a powerful attack (Bhardwaj, 2020). If employees are not properly trained against these traps, they could easily walk straight into a trap set by an attacker and compromise significant monetary assets.

Efforts to counteract this attack have also been becoming increasingly popular. One common idea is to simply educate corporate employees not to fall for these traps. This effort has been seen in the form of proper, mandatory training, false phishing emails, spam filters, etc. (Witts, 2022). Despite these efforts, phishing attacks continue to be successful, as attackers continue to improve phishing technology, making emails more realistic and more appealing to users (Bhardwaj, 2020). One way attacks have become more sophisticated over time is the rise of spear phishing or whaling. Spear phishing is the idea of a targeted phishing attack. Most standard phishing attacks are a mass email sent to a large list of recipients in hopes that one of the recipients falls for the scam. However, with spear phishing, attackers will gather information on the victim prior to sending an email (Bhardwaj, 2020). The attacker would gather personal information, such as their daily schedule, their bosses name, family names, etc., and construct a personalized email to target the victim and appeal to the victim's psychological weaknesses. For example, an attacker may pretend to be the victim's psychiatrist asking for them to pay their bills. In doing so, the victim would have given the attacker their credit card information or worse,

granted the attacker full access to the victim's computer. Spear phishing is just one example of how phishing is evolving to become more convincing. Unfortunately, as phishing evolves, efforts to counteract it have not improved enough to effectively counter the attacks.

Firstly, one can consider looking at technological ways to reduce phishing attacks, often implemented in the form of spam filters. Spam filters are built into email systems with the hopes to automatically filter out any email that seems suspicious, which may include phishing attacks. Unfortunately, as phishing technology improves, attackers find ways to bypass these filters. The spam filters often work by searching for specific patterns. The most common type of spam filter is known as a content filter, which analyzes the text inside and email and searches for suspicious words or inappropriate, malicious links ("Fortinet", 2022). Other types of filters may include filtering by sender IP address, email language mismatch, or various custom settings ("Fortinet", 2022). In any case, these filters miss a lot of emails, which is why this solution has not been incredibly successful.

With these inherent weaknesses in technological solutions, researchers are left with one main option: properly educating employees to avoid phishing scams through mandatory training, simulations, or other techniques. However, one problem with this method is simply the fact that many Americans do not understand the risk of phishing attacks. Even with training, many do not take the situation seriously, thus making training less effective. This lack of understanding then allows phishing to be successful, causing huge monetary losses. The FBI estimates that in 2018 alone, $1.2 billion was lost due to phishing attacks (Daly, 2021). This fact simply highlights the importance of the problem, yet there has been so little progress in preventing it. The motivation for this research is to attempt to search for a solution that minimizes the effect of phishing in America.

STS Framework

To address this research question, the problem is framed as a wicked problem. The idea of the wicked problem was first introduced by Horst Rittel and Melvin Webber in 1973 (Rittel, 1973). The idea behind wicked problem framing is to draw attention to the complexities and challenges of sociotechnical problems (SBU, 2022). One key characteristic of a wicked problem is the idea that the problem is extremely difficult or impossible to solve completely due to constantly changing requirements that may be difficult to recognize and address properly ("Wikipedia Contributors", 2022). In the case of phishing, efforts are being made to better educate Americans about the phishing problem, however, attackers also construct smarter attacks, rendering the education process useless. The problem simply gets more complex over time, as more forms of phishing and more sophisticated fake emails.

One way to show how phishing is getting more complex is through the concept of whaling, as previously mentioned. Whaling is the idea of specifically targeting phishing attacks towards high-value, high-status individuals, such as corporate titles, presidents, etc. (Pienta et al., 2020). In another paper, researchers framed whaling as a wicked problem with hopes to draw more attention towards the problem and to provide a call for action (Pienta et al., 2020). This study found that most anti-phishing software and training techniques focused on "high-frequency, broadly targeted cyberattacks, like phishing and spear phishing" (Pienta et al., 2020). To do so, this study compared the different types of phishing and tried to comprehend why whaling needed to be addressed. For example, Pienta mentions that attackers do a lot more open-source intelligence (OSINT) gathering to carefully construct an incredibly realistic email. Due to the fact that these attacks are targeted against high-value individuals, one successful attack has a much larger payout than typical phishing, making it more popular for attackers (Pienta et al.,

2020). One interesting point that Pienta makes is that the problem is a “complex interaction of many subcomponents to exploit human cognition” (2020). Further wicked problem framing analysis could involve investigating each of these subcomponents to understand why humans are so easily exploited and could be used to reveal where society and cybersecurity experts diverge on the subject.

Another researcher framed a different cybersecurity attack as a wicked problem, although it draws from similar ideas. In a study by John Coffey from the University of West Florida, the idea of a wicked problem is used to frame data breaches (2019). A data breach is simply when private or proprietary information is mistakenly leaked to the public. Coffey lists phishing as one example of a data breach, as oftentimes a phishing attack will lead to a data breach (2019). While this research focused on data breaches, it simply highlights how wicked problems are incredibly common in cybersecurity, as attackers and engineers constantly battle to improve attacks and defenses, making the problems multi-faceted and constantly changing. Through wicked problem framing, Coffey was able to assess a variety of factors related to data breaches, including post-breach analysis, data breach reporting, etc. Based on these studies, it seems that phishing could be viewed as a wicked problem to attempt to understand why society fails to properly address the pressing issue. The analysis in this research paper will further explore this idea in gaining understanding into specifically why certain techniques in phishing are effective and attempt to address each of those techniques with a proper anti-phishing technique.

Results and Discussion

Modern efforts to prevent phishing attacks within corporations have failed to emphasize the importance and impact of phishing as a social engineering problem. The most common reason for the failure to recognize a phishing attack simply comes from lack of knowledge and

lack of attention. To address these issues, a proposed solution is to use a gamified version of embedded phishing training specifically constructed to help employees retain information and undergo regular training. This proposal combines the ideas from numerous anti-phishing technique studies and attempts to combat the psychological reasons for the success of phishing attacks.

Why Phishing Works

In trying to understand how society views phishing, it is important to first understand why phishing works. In a study from 2006, Rachna Dhamija et al. surveyed 22 participants with 20 different websites to determine which ones were fraudulent (Dhamija, 2006). It was found that participants did not look at many of the security indicators that they should have looked at. In particular, participants lacked knowledge of these cues. The researchers found no significant correlation between sex, age, educational level, or computer experience and their phishing knowledge. This finding simply demonstrates that anyone is susceptible to a convincing phishing attack.

Through this study, Dhamija found three overlying causes to people falling victim to these simulated phishing attacks: lack of knowledge, visual deception, and bounded attention (Dhamija, 2006). In this particular study, lack of knowledge specifically referred to lack of knowledge of computer systems, as well as web security. This is the most common reason why people tend to misidentified phishing websites. Lack of computer system knowledge meant that some people did not understand how email addresses or other website links functioned. For example, thinking “ebay-support.com” and “ebay.com” are both trustworthy domains. Lack of web security meant when presented with a website, participants were unable to identify the key security features, built-in to most web browsers to help users identify secure versus insecure

websites. Such security features include using HTTPS instead of HTTP, checking for a valid SSL certificate, etc. Most Americans are unaware of these security features, nor do they understand what they mean. Many phishing websites will depend on this lack of knowledge in order to trick individuals.

The second cause of the continued success of phishing attacks described by Dhamija is visual deception. This concept refers to attackers sneakily hiding malicious information in plain sight. For example, in some fonts, capital I and lowercase l (el) look very similar, so a website like “paypal.com” may be forged as “paypaI.com” and some unsuspecting victims would not notice the difference. This technique also applies to graphical deception, such as some images linking to websites different than the one listed. While visual and graphical deception are certainly present, it may be difficult to educate people against it, as it simply requires users to constantly be paying attention to every website/email they are presented with. These difficulties further emphasize the idea of the wicked problem. As past research shows, some aspects of the problem cannot be addressed with any viable solution, thus leaving the goal to simply find a solution that reduces the problem as much as possible.

This ties into the third point Dhamija found: bounded attention. Bounded attention simply refers to the inability for users to constantly be attentive about these cues, since they typically would not spend the time looking for these cues. Again, this problem is not one that can be simply addressed with one solution, as humans subconsciously ignore many details throughout everyday life to simplify the difficulty of everyday tasks.

Another study by Arthur Bellore, from Auth0, a growing cybersecurity company, mentions that phishing emails are intentionally crafted to tap into the victim’s subconscious biases, despite their level of tech literacy (2021). One way phishing emails tap into a victim’s

subconscious biases is by taking advantage of truth bias, a phenomenon that all people will assume something is true unless they have reason to believe otherwise. Truth bias in this case means that if victims are to receive an email, most people will believe that this information is true, thus clicking on the links. A recent study by Professor Oliveira from the University of Florida found five psychological targets for phishing attacks: commitment, liking, scarcity, authority, and reciprocity (Bellore, 2021).

The idea of commitment is when attackers make the victim feel as though they need to complete an action they already started. For example, an attacker may ask users to complete an Amazon order that they did not place. This tricks users into believing they need to complete a task they did not begin. Liking is an extension of truth bias, which simply says that people are more likely to fall for a scam if they are familiar with the companies or parties involved. Scarcity is the idea of tricking users into thinking there is a limited number of resources. For example, a phishing email may say “first 1000 people to fill out this survey get a free xbox,” tricking victims into thinking there are a limited number of free things for them to grab, thus pushing them to click it. Authority is rather straightforward, simply the idea that more people are likely to conform to something if it seems like the request is coming from someone with authority. One example of this is an attacker pretending to be the DMV, stating that the victim's license has expired and needs to be renewed. Finally, reciprocation refers to the idea that if the attacker does something helpful for the victim, the victim is more likely to return the favor. This is less common, though one example is if PayPal said they suspended an account due to suspicious activity and asked the victim to update their password (Bellore, 2021).

Through the ideas of weak computer understanding, visual deception, bounded attention, and the five psychological targets, the wicked problem of phishing is clearly brought to light as

an unsolvable problem but with certain potentially targetable aspects to drastically reduce its effects.

How Phishing Has Changed

Over the years, as computer security continues to improve, phishing attacks have become more popular, as humans continue to be the weak link in security. According to Bellore, Google filters out 100 million spam emails a day, leaving only 0.1% of phishing emails to pass their filters (2021). However, despite this small percentage of emails that make it to a victim's mailbox, phishing continues to be successful and incredibly popular, making up 32.35% of all cyber-attacks. The question is then raised, how come phishing continues to be successful even with so many countermeasures? Just like computer system security technology, phishing technology/ideas evolve as well. There has been a rise in various types of phishing, all of which have some special features to be more convincing than the standard phishing email.

Firstly, as mentioned before, the idea of spear phishing has been more popular than ever. To reiterate, spear phishing is the idea of using open-source intelligence (OSINT) gathering to obtain personal information and constructing a personal phishing email. Spear phishing typically involves using a recognizable name to appeal to the victim. OSINT refers to gathering information off the public internet; information that anyone has access to, including but not limited to social media, company websites, and government databases. This technique draws on the idea of the liking psychological technique, as previously described. People tend to believe the attacker when the email contains some information recognizable or trusted by the individual.

Another idea that has recently become popular is called whaling. There are two forms of whaling, however, both methods target higher-valued individuals, such as CEOs, presidents, etc. The first form is essentially an extension of spear phishing, specifically targeting these

individuals. The other form, which differs from previous methods, is more like spoofing than it is phishing. Spoofing is the idea of pretending to be someone else, so in the context of whaling, attackers may pretend to be someone with higher power to request certain information. This idea draws from the psychological reason of authority, as previously described, as victims are more likely to fall for attacks from people with authority, such as these high-value individuals.

There are countless forms of phishing that have been attempted, such as vishing (voice phishing) or smishing (SMS phishing). Attackers have also begun using more sophisticated forms of regular phishing, such as polymorphic phishing, which is the idea of randomly changing parts of emails to attempt to bypass spam filters (Paganini, 2021). In addition, attackers have also begun to implement security features into their phishing websites in order to counteract any educational efforts to prevent phishing. This includes many attackers adding officiated SSL certificates to their websites, using HTTPS instead of HTTP, etc. (Paganini, 2021). With these developments, phishing continues advancing in technology, making it even more difficult to address the problem. These findings further support the use of a wicked problem, as this understanding of the problem helps direct the research towards addressing these advancements.

State-of-the-art Anti-Phishing Efforts

A study by Jampen et al. performed a literature review of multiple studies regarding anti-phishing training to determine the success and failure of each. These training courses included video training, web-based courses, informational material, or simulated phishing attacks (2020). The methodology of this study was simply to compare and contrast different institution's anti-phishing strategies. The first interesting find was that there was a lack of consensus in the literature; there was very little overlap in anti-phishing techniques. This find further enforces the idea of a wicked problem, showing that no one solution has been universally agreed upon to

solve the problem. In addition, many of the studies analyzed by Jampen et al. mentioned that the "need for increased security awareness is evident but designing a generalized approach to achieving such awareness could be a complicated process due to the technical unfamiliarity of users or behavioral differences among them" (2020).

Across many studies, Jampen et al. found that there were two main categories of anti-phishing training: embedded training and general anti-phishing education (2020). Embedded training typically refers to phishing simulations, where employees who clicked on the fake phishing emails were forced to go through a certain training. On the other hand, the general anti-phishing education was typically some form of video or information course provided when employees are first hired. A study was conducted on 300 participants, split into three groups: one exposed to embedded training, one group was given a warning for each failure, and the third group had no training at all. Over a 10-day period, researchers found that there was no significant difference between the groups. However, over an extended period of 63 days, it was found that those who received training scored 10% better than those who received no feedback. This finding suggests that a simple one-time training program is insufficient in properly educating Americans of the phishing problem. Many other papers included in the study found that embedded training tended to have a positive effect on the issue (Jampen, 2020). This conclusion is consistent with a study by Kumaraguru et al., who focused on a specific phishing training system, but concluded that the embedded training system was effective and enjoyable as a part of their everyday email checking (2009).

As expected, training is one of the most important anti-phishing techniques and must be mandated by all companies in order to fully reduce the risk of phishing attacks. However, many researchers have also investigated developing spam filters, which will automatically filter out

emails that seem like phishing attacks based on a variety of key features. While these spam filters are becoming increasingly complex, such as using machine learning to avoid overfitting to a certain set of data, attackers have easily found ways around filters.

A study by Lowd and Meek from the University of Washington found that attackers can easily bypass a spam filter by simply adding words that were deemed "good" by the filter, in that any emails containing these specific words were able to pass the filter, regardless of the other content of the email (2005). Another study found that when the employees were told or knew that there was a spam filter, employees tended to trust the spam filter and assume no spam/phishing attacks would be able to bypass the filter, which is simply not true (Cramer et al., 2009). This finding is particularly interesting because it demonstrates how the typical American understands these types of technology. Anyone in the field of technology understands that it is impossible to guarantee filters up to 100% accuracy. These examples demonstrate how insecure spam filters are, thus these filters could never be the only solution to the phishing problem.

Another type of filter tool that has been explored is essentially like an extension to web browsers that will analyze every website visited and provide a safety rating. Through a deep analysis of 11 different types of web browser extensions, Zhang et al. found that some of these tools reported that many safe websites were unsafe while other tools failed to report dangerous phishing websites (2007). This finding continues to show how technological tools are not very viable on a large scale. In order for these tools to be viable on a large scale, it would require near 100% accuracy to fully avoid all phishing attacks, as every successful phishing attack leads to huge losses within corporations.

Experimental Anti-Phishing Efforts

Aside from the commonly known anti-phishing techniques, including different types of training, spam filters, web browser extensions, etc., researchers have looked into experimental ways to further prevent phishing. Most of these techniques tend to focus on training and educational efforts, as proper security education has proved to be the most effective way to minimize phishing attacks.

One study by Lastdrager et al. studied the effectiveness of training to recognize phishing attacks to children between the ages of 9-12 (2017). The researchers looked at three different results of the phishing training: the ability for children to detect phishing, the effectiveness of the training, and the retention of knowledge over time. Through this study, researchers found that the older children in the experiment performed better than younger children in recognizing phishing attacks and that training was rather effective in younger children, but children had trouble retaining the knowledge over periods of time. The proposed conclusion by these researchers is to provide basic cybersecurity education in schools, as children are constantly being exposed to learn new information anyway. In comparison, many adults are not in the mindset to want to learn new information when they are employed, which is one listed reason why educating children in cybersecurity is being explored (Lastdrager, 2017). As society becomes more dependent on the internet, it is important to properly educate everyone starting at a young age as to avoid developing bad habits.

In an effort to keep adults interested in learning the new material, research has also been done in the gamification of cybersecurity and phishing training. Gamification in this case means to provide the information in a game-like way; almost everyone prefers playing a game over reading an article if given the choice. A study by Tchakounte et al. looked at eight phishing education gamification proposals between 2007 and 2019. The main goal of gamifying phishing

education is that games tend to retain the user's attention and keep the user engaged despite learning seemingly "boring" material (Tchakounte, 2020).

Of these gamification proposals, there were two main categories of gamification: structural gamification and content gamification. Structural gamification tends to focus more on applying game elements to encourage the user to continue learning the content, though the content would be presented in the same way as before. For example, earning points for watching a certain video would fall under this category. The second type is content gamification, where the actual content of the training is gamified. For example, turning the information into a quest-like or a role-playing game (RPG). Researchers also looked at other dimensions of the games, such as objectives (increasing awareness vs. increasing knowledge), target audience, types of phishing covered, designs (user-centered vs. game-centered), etc. One common trend researchers found was that most of these games focused on URL-based phishing, rather than malicious emails, which are more common vectors of attack. However, in all proposals studied, the games seemed to yield a positive outcome for phishing education, making gamification potentially a viable solution.

Searching for a Solution

With this information, it seems as though people have explored many different potential ways to address phishing. However, some have certainly proven to be more effective than others. From the perspective of viewing phishing as a wicked problem, researchers should not expect to find one clear solution. Instead, the most effective way to address the problem of phishing seems to be combining the objectively most effective ideas from various techniques to minimize the problem as much as possible.

As previously discussed, the constant “cat and mouse” game between improved phishing technology and improved anti-phishing technology makes a technological approach near impossible to guarantee results. This relationship naturally suggests the best solution is likely properly educating all Americans of phishing and ensuring that they are constantly aware of the cues. The phishing education curriculum should be standardized across the field and all corporations and should consist of some way to keep the audience engaged with the material. Along with that, the training must be followed up with regular embedded phishing training (i.e. simulated phishing attacks) to further reinforce an employees understanding and awareness of the problem. Again, while this may not be one guaranteed solution to reducing phishing attacks, it will certainly work to reduce attacks drastically and will continue to do so no matter the technological advancement of phishing.

Limitations and Further Work

The research presented in this discussion covers most of the primary anti-phishing solutions at the time this paper was written. Phishing is framed as a wicked problem, implying that it will continue to develop over time and the technology is going to change. The current proposed reasoning and solution may change as people find better solutions; that follows the nature of a wicked problem. Another limitation of this research is the lack of scientific evidence, as no scientific experiment was performed.

However, if research is continued in this area, focus would be placed on carrying out an experiment to verify the validity of the proposed method. This research could be done via survey or scientific research. There are also other ideas that could be worth exploring that are not mentioned in this research. One example is the idea of incentivized phishing training, e.g. if a

company offers free company merchandise or something small in return for passing the embedded phishing training.

Conclusion

Ultimately, it seems as though the biggest issue that allows phishing attacks to continue to be successful is the lack of knowledge from most Americans with weak efforts from corporations to properly educate them. Much of the problem spawns from the way information is presented to users. Various researchers have explored different ways to present information which all had a significant impact on the user's ability to recognize a phishing attack, including embedded phishing training, general anti-phishing training in various forms of media, gamification of information, or even presenting information to children. The best way to address the phishing problem is to standardize a training program which retains the user's attention over a period of time. Regardless of the method of education, cybersecurity attackers will continue to use phishing as a way into systems, and will always be a problem that corporate America will need to deal with in one way or another.

References

Bellore, A. (2021, September 14). *Why Phishing Attacks Work*. Auth0. Retrieved February 28, 2022, from https://auth0.com/blog/why-phishing-attacks-work/

Bhardwaj A, Sapra V, Kumar A, Kumar N, Arthi S. Why is phishing still successful?. *Computer Fraud & Security*. 2020;2020(9):15-19. doi:10.1016/S1361-3723(20)30098-1

Bisson, D. (2021, October 13). *6 Common Phishing Attacks and How to Protect Against Them*. The State of Security. Retrieved February 28, 2022, from https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attac

ks-and-how-to-protect-against-them/

Chabrow, E. (2014, January 7). *Why Training Doesn't Mitigate Phishing*. BankInfoSecurity. Retrieved December 8, 2021, from https://www.bankinfosecurity.com/interviews/spear-phishing-training-weaknesses-idd-i-2148

Coffey, J. W. (2019). Difficulties in Determining Data Breach Impacts. *Systemics, Cybernetics, and Informatics*, 17(5).

Cramer, H. S., Evers, V., Van Someren, M. W., & Wielinga, B. J. (2009, April). Awareness, training and trust in interaction with adaptive spam filters. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 909-912).

Daly, A. (2021). *Phishing Scams Cost U.S. Companies Billions*. Inky. Retrieved February 4, 2022, from https://www.inky.com/blog/phishing-scams-cost-companies-billions

Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April). Why phishing works. *In Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590).

Fortinet. (2022). *Email Spam Filtering: Different Methods & How They Work*. Retrieved February 3, 2022, from https://www.fortinet.com/resources/cyberglossary/spam-filters

Fruhlinger, J. (2020, September 4). *What is phishing? How this cyber attack works and how to prevent it*. CSO Online. Retrieved February 4, 2022, from https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-work

s-and-how-to-prevent-it.html

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences,* 10(1), 1-41.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009,

July). School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (pp. 1-12).

Lastdrager, E., Gallardo, I. C., Hartel, P., & Junger, M. (2017). How Effective is {Anti-Phishing}

Training for Children?. In *Thirteenth symposium on usable privacy and security (soups 2017)* (pp. 229-239).

Lowd, D., & Meek, C. (2005, July). Good Word Attacks on Statistical Spam Filters. In *CEAS* (Vol. 2005).

Paganini, P. (2021, January 14). *How phishing attacks are evolving and why you should care.* CyberNews. Retrieved February 28, 2022, from https://cybernews.com/security/how-phishing-attacks-are-evolving-and-why-you-should-care/

Pienta, D., Thatcher, J. B., & Johnston, A. (2020). Protecting a whale in a sea of phish. *Journal of information technology, 35*(3), 214-231.

Rittel, H. W., & Webber, M. M. (1973). "Dilemmas in a General Theory of Planning." Policy sciences, 4(2), 155-169. https://www.cc.gatech.edu/fac/ellendo/rittel/rittel-dilemma.pdf.

Rosenthal, M. (2021, October 5). *Must-Know Phishing Statistics*. Tessian. Retrieved December 8, 2021, from https://www.tessian.com/blog/phishing-statistics-2020/

SBU. (2022). *What's a Wicked Problem?* Stony Brook University. Retrieved February 3, 2022, From https://www.stonybrook.edu/commcms/wicked-problem/about/

what-is-a-wicked-problem.

Tchakounté, F., Wabo, L. K., & Atemkeng, M. (2020). A review of gamification applied to phishing.

Wikipedia contributors. (2022, February 2). Wicked problem. In *Wikipedia, The Free Encyclopedia*. Retrieved 04:57, February 4, 2022, from https://en.wikipedia.org/w/index.php?title=Wicked_problem&oldid=1069426587

Witts, J. (2022, January 27). *How To Stop Phishing Attacks*. Expert Insights. Retrieved February 4, 2022, from https://expertinsights.com/insights/how-to-stop-phishing-attacks/

Zhang, Y., Egelman, S., Cranor, L., & Hong, J. (2007). Phinding phish: Evaluating anti-phishing tools.