CSE 569S - Final Project Paper
Exploration and Exploitation of Defense Strategies Against Social Engineering

Funda Atik, Erin Miller, Samatha Kodali, Yara Alsiyat
Department of Computer Science and Engineering
Washington University, St. Louis, MO

***Abstract*—With the sharply increasing penetration rate of internet-connected devices across the world, there has been an increased attack surface for social engineering attacks. We conducted a literature review, a survey, and an experiment involving a targeted phishing attack. Ultimately, we found that defenses against social engineering attacks have value in that they can slow down or prevent simpler attacks. However, dedicated attackers with a specific target would be able to circumvent virtually all of the defenses presented in this paper.**

I. Introduction

A. The Project's Motivation

This work explores how social engineering has become a significant security threat as the internet has become more deeply integrated into our daily lives. Our paper will provide a thorough analysis of the current landscape of social engineering attacks and the defenses against them carried out through different mediums. In this project, our primary motivation is to increase our knowledge base about social engineering defenses and apply that knowledge to practice among both private individuals or institutions.

B. The Project's Novelty and Contributions

We conducted a literature review to find the current state-of-the-art in social engineering defenses and mitigations and determine the relative effectiveness of those techniques. Additionally, we designed, collected, and analyzed data from a comprehensive survey on cybersecurity training and awareness. Finally, we tested our social engineering skills in the real world by creating our phishing email, with the plan to covertly log our target's IP and determine if their behavior validates our survey observations.

II. Threat Model

A. Threat Model for Social Engineering

Social engineering cyber attacks rely heavily on human interaction and often involve manipulating individuals into breaking standard security procedures and best practices to gain unauthorized access to systems, networks, or physical locations. Malicious actors are most often motivated by a desire for financial gain, access to proprietary information, or a competitive advantage, with secondary motivations including revenge and just entertainment [7] They use social engineering techniques to conceal their true identities and motives, presenting themselves as trusted individuals or information sources to influence, manipulate or trick users into revealing sensitive information or access within an organization. Many social engineering exploits rely on people's willingness to be helpful or fear of punishment. For example, the attacker might pretend to be a co-worker with an urgent problem requiring access to additional network resources [1].

TABLE I
A synthesis of attack topologies in literature [1], [8], [9].

Strategies	Attacks
Channel	IM, Email, Phone/VoIP, Social Network, Cloud, Website, Physical
Operator	Human-based, computer-based
Vector	Phishing [12], Baiting [13], Pretexting [14], Tailgating [16], Ransomware [15], Fake Software/Tabnabbing [17], Pop-Up Windows [18], Phone/Email Scams [18], Robocalls [19], Other (dumpster, water-holing, impersonation, shoulder surfing, etc.)[1]

Social engineering is a popular tactic among attackers because it is often easier to exploit individual humans than to find a network or software vulnerability. As a result, hackers will often use social engineering tactics as a first step in a more extensive campaign to infiltrate a system or network, steal sensitive data, or disperse malware. Since the most impactful aspect of social engineering is the human factor, it has become one of the most dangerous lines of attack in cybersecurity. Therefore, increasing awareness and education about the issue will become a worldwide issue.

As shown in Table I, we have synthesized the attack topologies offered by the literature into a three-pronged attack classification strategy. First, we can define attacks by their operator — either human-based or computer-based, depending on the originator attack. Next, we can differentiate SE attacks by the channel they take advantage of — for example, phone or email. Finally, we can classify attacks according to the specific attack vector leveraged to carry out the attack, i.e., ransomware or phishing.

B. Case Study: Threat Model for Phishing

Phishing is a cyberattack performed against careless individuals and institutions, where an attacker intends to steal confidential data and identity and cause reputation and monetary damages via phone calls or emails. There are many types of phishing attacks, such as spear phishing, whaling phishing, interactive voice phishing, business email compromise phishing, and vishing phishing [1]. Spear phishing makes false claims using specific individuals by using victims' available data online. Whaling phishing is a type of spear phishing that targets high profiles in companies. Like whaling phishing, business email compromise phishing aims to deceive high-profile big corporations into accessing their confidential information. Vishing phishing is phone phishing where an attacker tries to manipulate specific individuals to share their sensitive data for verification via phone calls from a bank. Finally, interactive voice phishing mimics a fake interactive voice response system of a legitimate business such as a bank to collect victims' private information.

Our case study involved creating our own phishing email targeted at close friends. The steps for our attempt to create phishing email are as follows:

1) Create grabify link to log IPs
2) Masking the grabify URL via TinyURL
3) Craft PayPal phishing email
4) Create an email account to conduct an attack
5) Send phishing emails to friends

We provide more details in section 4.3.

III. Literature Review

A. Methodology

We identify existing state-of-the-art defenses against social engineering cyber attacks into two groups: detection techniques and mitigation techniques. We further divide mitigation techniques into three sub-categories: (i) education, training, and awareness, (ii) technical security policies, and (iii) human-based security policies.

B. Detection Techniques

Intrusion detection and prevention systems collect information from various systems, monitor that information, and analyze the data for potential security threats [2]. As social engineering attacks and cybercrime increase rapidly, detection techniques play a vital role in catching malicious activity early to have more time to prevent further damage.

From our literature review, we have found three broad categories of detection techniques. These three detection systems are intrusion detection systems (IDS), intrusion prevention systems (IPS), and intrusion detection prevention systems (IDPS). Intrusion detection systems, intrusion prevention systems, and intrusion detection prevention systems all collect information from various systems and then monitor those systems to analyze for possible security problems. An intrusion detection system will raise the alarm after a violation is detected. An intrusion prevention system will extend this behavior and attempt to prevent the intrusion with its response. Combining these two systems will attempt to both warn and stop the attack [2].

There are two different detection systems for determining what makes an event flagged as a security issue. These two systems are anomaly-based detection systems and signature-based detection systems. Anomaly-based detection systems work to recognize a malicious event that it should flag by determining if the event's behavior is a statistically significant departure from the normal. Signature-based detection systems recognize that they should flag a particular event by looking at the patterns of events that are occurring and recognizing which patterns commonly go along with attacks [2].

The two domains where detection systems are typically used to monitor events are host-based and network-based systems. Host-based intrusion detection systems are usually implemented in software on top of the operating system to collect events from the host, such as system calls made and accessed files. Network-based intrusion detection systems monitor the events that occur from network traffic. It means they use data such as network packets as input events.

Sender Policy Framework (SPF): The Sender Policy Framework (SPF) identifies the origins of emails. This technique is crucial for preventing social engineering attacks in larger organizations [4].

DomainKeys Identified Mail Policy (DIMP): The DomainKeys Identified Mail Policy (DIMP) has a cryptographic signature that ensures the validity of the email signature. It is valuable for protecting against social engineering. For example, even if employees of an organization receive training where they learn to be cautious about receiving emails from unknown senders, the malicious actor can still try and deceive the victim by making their email address look trustworthy. This social engineering will bypass the human victim, but the computer will check the cryptographic signature, thus taking some security responsibility off the human [4].

Domain-based Message Authentication Reporting and Conformance (DMARC): The Domain-based Message Authentication Reporting and Conformance (DMARC) uses Sender Policy Framework and DomainKeys Identified Mail Policy to restrict unidentified emails. It helps protect against social engineering attacks because it automatically works to remove emails that could be malicious, taking the burden of judging what qualifies an email as dangerous off of the user [4].

Real-time blocking based on hostname and server IP: It allows large organizations to prevent social engineering attacks because they can create a black list of hostnames and IPs that they want to be blocked and then have a system set in place that will automatically block messages from those hostnames and IPs. It means that the employees not only don't need to worry about manually filtering their emails to figure out which ones could be malicious and not open them, but they also won't need to know which organizations are on the black list. As a result, the employees will have less insider information about which addresses the organization wants to block. They

will have less valuable information that could be exploited, thereby improving security against future social engineering attacks [4].

Machine learning algorithm-based techniques: They can be used to do detection with unsupervised learning. Unsupervised learning models try to detect attacks without any prior knowledge of observed attacks. The following five machine-learning algorithms are compared according to their speed, reliability, and accuracy in detecting phishing attacks: (1) support vector machine, (2) biased support vector machine, (3) artificial neural networks, (4) scaled conjugate gradient, (5) self-organizing map.

The support vector machine algorithm achieves the best results among these five algorithms. Machine learning-based detection could help avoid social engineering attacks because they take the responsibility of detecting malicious attacks off users, some of the responsibility of building the detection systems off the organization's security team [1].

Anomaly Detection (DAS): This detection system targets credential spear phishing attacks. Credential spear-phishing attacks are when attackers target a phishing attack at specific individuals or organizations to get their credential/password information. DAS works by looking at the characteristics of spear phishing attacks and noting which attackers use them. Then, attackers use this list of attributes to rank different levels of alerts. It helps prevent social engineering attacks because individuals will only receive the most critical alerts, thereby allowing them to avoid alert fatigue. When individuals avoid alert fatigue, they are more likely to pay attention and recognize dangerous phishing attacks [1].

Flow Whitelisting: It attempts to distinguish between legitimate traffic and malicious traffic based on the following four properties: (i) address of the client, (ii) address of the server, (iii) port number of the server, (iv) protocol used for the traffic transport. These four criteria are captured from network packets during specific times and then used as the base model for what is considered legitimate traffic. It works as a detection system for social engineering attacks because users will not always know what typical network behavior is supposed to look. Furthermore, setting up a system that determines the user strengthens the weak human link that is the basis of social engineering attacks [1].

TabShots: It alerts the user to any observed changes on a web page before continuing to the web page. Therefore, the user can notice any differences in the site. As a result, they can distinguish between a legitimate web page and a malicious page. It helps prevent social engineering attacks because it becomes more likely that the user will notice that they are going to a malicious site and, therefore, more likely that they can avoid it [1].

C. Mitigation Techniques

We divide mitigation techniques into three sub-categories: (i) education, training, and awareness, (ii) technical security policies, and (iii) human-based security policies.

1) Education, Training, and Awareness: According to our literature review, we investigate the implementation of Security, Education, Training, and Awareness (SETA) under six different perspectives: (1) business environmental, (2) social, (3) constitutional, (4) organizational, (5) economical, (6) personal. In addition, we mention common vulnerabilities, attacks, and the current status of each perspective under analysis [1], [4], [5], [7].

Business Environmental Perspective:

- *Common vulnerabilities:* Interactive work locations, technological equipment, organizational culture, employee education, policy, physical control amendment, use of social media, the integration of multiple information systems such as finance and supply chain
- *Common attacks:* Remote network access due to the integration of the internet in business activities
- *Current status:* Numerous studies suggest that increasing employees' knowledge about common SE attacks is the most effective protection.

Social Perspective:

- *Common vulnerabilities:* Informal communication and maintaining social bonds with customers, the influence of cultures such as community interactions, demographic influenc
- *Common attacks:* Phishing emails
- *Current status:* There is no comparative study investigating the impact of cultural or social factors on the effectiveness of SETA.

Constitutional Perspective:

- *Common vulnerabilities:* The medium of choice for political debates, spreading misinformation based on governmental agendas, the confirmation of prejudice, intellectual dissonance, lack of security laws, law enforcement, compliance with legal policies
- *Common attacks:* Phishing, baiting, quid pro quo, pretexting, piggybacking, online guessing to leak passwords due to poor password practice
- *Current status:* Nation-wide PII-based breaches occurred recently. However, there is limited literature on the impact of governments on the effectiveness of SETA.

Organizational Perspective:

- *Common vulnerabilities:* Lack of different levels of awareness programs targeting the needs of specific groups in the same firm
- *Common attacks:* Psychological manipulation to steal information from financial institutions
- *Current status:* Staffs cannot keep up with the continuous evolution of novel cybercriminal attacks, but the user-reflective model is effective.

Economic Perspective:

- *Common vulnerabilities:* The ability to follow security contingency plans to test the readiness and resilience of employees, lack of periodic allocation of economic resources for training personnel

- *Common attacks:* The lack of periodic allocation of economic resources increases the risk
- *Current status:* Providing interactive content for training and awareness programs can significantly impact the effectiveness of SETA.

Personal Perspective:

- *Common vulnerabilities:* Specific personality traits such as neuroticism, various mental states such as anxiety, anger, depression, being extrovert, excitement seekers, openness, obligatory moral guilt, the trusting nature of humans, limited training resources to cover the trust gap, the lack of interest and motivation for regular training due to avoiding responsibility, the different levels of lack of understanding of the nature of attacks, the lack of self-importance due to holding a low-profile in the firm, facing high work pressure due to having a limited work-life balance, the lack of attention, the lack of regular testing the effectiveness of training sessions
- *Common attacks:* The use of different psychological methods to specifically target specific behavioral vulnerabilities of victims. E.g., the bait and phishing emails. The attackers often target low-profile employees to collect data to develop manipulation techniques.
- *Current status:* Awareness campaigns are practical to cover the trust gap. However, individuals often show a lack of interest in regular SETA, which minimizes and limits its effectiveness of SETA. Also, the increased sophistication and complexity of SE attacks make them difficult to recognize.

2) Security Policies: Human-Based: In real-world scenarios, the most crucial factor for social engineering attacks is humans, and their ability to control people's reactions to specific problems is impossible. It leads us to one of the most significant security gaps in society: human awareness. Furthermore, to develop complete strategies that help raise human awareness, we need specific policies that they can follow to establish a security awareness maturity. It starts with policy statements used by businesses to strengthen their information security defenses against social engineering attacks. The policy statement outlines the desired personnel behaviors [4]. The policy statements also spell out the immediate repercussions of not adhering to organizational policies in the face of a social engineering attack. On the premise of building a safe atmosphere, businesses adopt measures to fight socially engineered assaults. Additionally, a policy is developed based on expected employee conduct that the organization's management strives to sustain inside the company.

Human judgments are relative and inefficient since human assessment is subjective, even when there is a high knowledge of social engineering attacks. Therefore, human-based mitigation measures are essential for both enterprises to combat social engineering attacks targeting their employees and individuals. Human-based security policies can be split into two main groups: (i) organizational policies and (ii) individual policies. They are primarily concerned with increasing decision-making skills and providing the skills necessary to recognize malevolent behavior and act accordingly [1] accurately. In addition, each factor should contain a list of policies that we can follow to obtain a secure environment [10].

The policy approach refers to a set of security policies and processes developed in enterprises to assist individuals in detecting social engineering attempts. Policies define these security principles to aid individuals in determining the status of suspicious action. The policy method is a defensive tactic for controlling the individual's reaction to a social engineering attack. The education, training, and awareness approaches pertain to the effective use of the policy approach. They intend to ensure that the organizations follow the stated security policies. Policies, procedures, and standards are crucial for an overall anti-social engineering campaign [10].

Policies should follow some standards to be effective:

- They should not include criteria or directions that are unattainable. When developing standards, collaborate with the user community to determine what can be performed quickly.
- Once these activities have been done, the process should be evaluated every six months and acted upon.
- They should emphasize what can be done and avoid what isn't authorized as often as necessary. Make a list of what the workers can and should do.
- They should always be succinct and to the point and inform them of the requirements and the need for a security awareness program.
- Their requirements must be evaluated regularly and maintained up to date.
- The information and standards should be easily accessible through the corporate intranet. They should be up to date and use an internal website to provide answers and advice.

3) Security Policies: Technical: There is some level of overlap between technical mitigation policies and detection policies that are based on technical methods, but, by-and-large, technical security policies for social engineering mitigation can be divided into several categories: information & communication management, technical operations, physical environmental security, incident management, business continuity, and change management [10].

Information & communication management includes important access control policies like multi-factor authentication and communication policies that take power away from social engineers, such as accurate caller-ID for customer-facing roles [9]. Technical operations policies are arguably the most important of the categories listed above, including fundamental strategies like strong network configuration, anti-virus/anti-spyware software, firewalls, cryptography, logging, auditing, requiring VPNs, biometric security, and multi-factor authentication [4], [10], [11].

The remaining four categories are more specific and thinly defined. Physical environmental security chiefly involves physical asset protection (using tools like security guards, mantraps, or security cameras) and following proper device

disposal procedures [10], [11]. Incident management concerns structure policies and procedures for handling and reporting incidents [10]. Business continuity refers to data backup, retention, and recovery to maintain organization operation after an attack or other data loss. Finally, change management is about a secure change control procedure [10]. Even with perfect technical security, social engineering attacks cannot be *100%* eliminated, as the true weak point of an organization's security will ultimately be the humans that make up that organization. However, deploying serious technical policies can neutralize, or at least slow down, the majority of social engineering attacks, with technical operations policies like firewalls, VPNs, and MFA significantly decreasing the risk of such attacks.

IV. Experiments

We conducted two experiments to understand how social engineering attacks work and how susceptible the average person is to such attacks. First, we conducted a survey *(n=203)* to glean insights into respondents' awareness and attitude toward social engineering attacks and cyber security in general. We then used data analysis to draw conclusions and evaluate our hypotheses about how people behave when faced with the threats posed by social engineering attacks. Next, we created our benign phishing email and attempted to deploy it. This case study allowed us to understand better how SE works from the attacker's perspective.

A. Survey Methodology

Survey Design: We ask participants a diverse set of questions. Our survey is divided into five parts, and it consists of four demographics, four awareness of security concepts, two security awareness training, and five behavioral questions. All questions are designed as close-ended. For instance, a responder can choose from a fixed set of options. In addition, some response choices can be *yes/no* options and rating scales. We also ensure our survey questions are neutral to minimize bias. Moreover, we attempt to keep a balanced set of answer choices so that participants can give honest feedback. We aim to collect insights into participants' awareness and confidence level of standard security practices and topics. For this purpose, we design the last set of questions to understand how participants act in specific scenarios. This way, we can acknowledge how participants apply their security knowledge to practice.

Survey Deployment: We used *Google Forms* as the medium with which to create and distribute our survey. We ensured privacy for the survey participants by not collecting their names and notifying them that they would remain anonymous. We spread the study by sending the survey link and a message requesting them to fill it out to friends, families, and our classmates. Using this method, we gathered *203* responses.

Respondent's Demographics: We asked participants to rate their awareness of security practices to understand their confidence level in security practices, as shown in Figure 1. *73%* of responders feel highly confident about their understanding of security practices. It was good news that our participants were knowledgeable enough in security practices because later, we would ask them more specific questions about cybersecurity. The demographics of respondents are given in Table II .

TABLE II
Demographics of Respondents

Demographics	Category 1	Category 2	Category 3
Age range	30-39 (%49)	21-29 (39%)	Other (12%)
Gender	Woman (71%)	Man (28%)	Other (1%)
Education	Bachelor (52%)	Graduate (38%)	Other (10%)
Employment	Employed (69%)	Looking for Work (18%)	Other (13%)

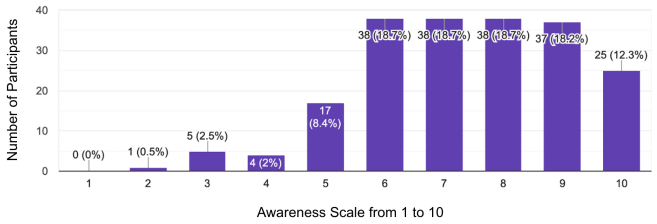

Fig. 1. Rating of awareness of security practices

B. Survey Results and Analysis

You can access the repository with our survey analysis results from this link: *https://github.com/fundatik/se-survey-analysis.git*.

Importance of Security for Web Usage Activities: We started our survey with a simple question that participants will find interesting and engaging such as rating the importance of security for various web usage activities. We provided eight different web usage activities such as entertainment (Fun), social $(Social)$, gaming $(Game)$, banking $(Bank)$, shopping $(Shop)$, education (Edu), information $(Info)$, and email $(Email)$. Most participants believed that security is essential for all web usage activities, as shown in Fig 2.

	Fun	Social	Game	Bank	Shop	Edu	Info	Email
Very	31	58	21	85	61	44	64	76
Fairly	34	29	28	13	23	29	14	19
Important	78	87	64	86	91	99	97	86
Slightly	45	25	52	13	24	21	19	16
Not at all	11	4	32	3	4	7	6	4

Fig. 2. Importance of Security for Web Usage Activities

Awareness of Security Practices: Moreover, we asked them to rate their awareness of basic security practices such as choosing a strong password $(StrongPwd)$, logging off

public PC ($LogOffPublicPC$), taking backup of their data ($BackupData$), protecting personal data ($PersonalData$), avoiding pop-ups and unknown email links ($AvoidPopup$), use of secure Wi-fi ($SecureWifi$), as shown in Fig 3. Most participants were aware of all these security practices. However, they were less aware of security practices for backup and protecting personal data.

	StrongPwd	LogOffPublicPC	BackupData	PersonalData	AvoidPopup	SecureWifi
Completely	105	141	75	95	121	93
Mostly	66	28	76	75	49	58
Somewhat	27	25	45	29	24	37
A Little Bit	5	9	7	4	9	15

Fig. 3. Awareness of Security Practices

Awareness of Security Topics: As shown in Fig 4, we found that respondents generally had the most familiarity with phishing attacks, with *81* responses of *"completely"*, *54 "mostly"*, *29 "somewhat"*, and *39 "a little bit"*. The next most well-known attacks were social engineering *(67, 49, 35, 52)* and man-in-the-middle attacks *(58, 48, 36, 61)*. Ransomware attacks were considerably less known *(51, 47, 37, 68)*, and credential stuffing was the least understood of the attacks considered *(40, 47, 45, 71)*. We were surprised at how relatively unknown ransomware attacks are, considering their prevalence in news coverage of cyber-attacks. Another valuable observation to be gleaned is that the most well-known category, phishing, still had nearly *39%* of participants select the lowest confidence option.

	Ransomware	CredentialSurf	SocialEng	Phishing	MainInTheMiddle
Completely	51	40	67	81	58
Mostly	47	47	49	54	48
Somewhat	37	45	35	29	36
A Little Bit	68	71	52	39	61

Fig. 4. Awareness of Security Topics

Willingness to Engage with Security Awareness Training: We presented survey respondents with two questions on this topic. First, we asked whether participants would be interested in joining a free cyber security course. Conditional on them answering yes to this question, we then asked how much time of the day they would be willing to allocate to such a course. As shown in Fig 5, many responders are willing to take a security course; however, most want to allocate 10-30 minutes daily for security education training. The older generation is more inclined to spend more time on training.

Behavioral Characteristics: Our results revealed a few foundational security flaws common in the general population. Figure 6 shows that despite most respondents rated themselves

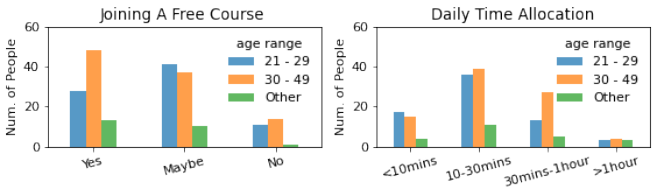

Fig. 5. Willingness to Engage with Security Awareness Training

as at least *"Mostly"* aware of personal data protection security practices, more than half of people are using the same password and around *30%* are willing to share their password. As it appears on the chart the number of candidates who were willing to give their private information to the bank through a phone call is really low. As it appears on the chart the number of candidates who were willing to open a link is really low and that is a good sign that the human security awareness is rising.

C. Case Study: Phishing Attack

In addition to the survey, we also crafted our phishing email, modeled after an actual phishing email one of our group members received. We made our malicious email look like it came from PayPal, warning the recipient that their account has been limited and offering a link for them to log in to their account. We set up a TinyURL that redirects to grabify, then to the PayPal login page, to discreetly log the victim's IP address. It is also important to note that we weren't intercepting information other than their IP. We, at no point, would have been able to take control of anyone's PayPal. We attempted to set up an Outlook email to conduct the attack and planned to target a few close friends to see if we could get any of them to click the link. However, a spam detection system, which was more advanced than we expected, foils our plans. We tried to get around it a few different ways but were unfortunately unable to without completely compromising the viability of the phishing attack.

V. Discussion

From our survey results, we were able to determine that most respondents place a mid-to-high level of importance on security. The majority of participants feel confident about their security awareness. However, when looking at how respondents rated their understanding of security topics, many were only a little aware of security attacks such as ransomware attacks, credential surfing attacks, and man-in-the-middle attacks. It demonstrates that individuals may be overly-confident in their security knowledge, which puts them in danger of unknowingly falling victim to social engineering attacks.

We also drew valuable insights from our other experiments. By going through the process of creating and attempting to distribute a phishing email, we saw that anti-spam detection tools make creating spear-phishing attacks a non-trivial activity. An attacker would have to create an email username that effectively deceives users and bypasses automatic security

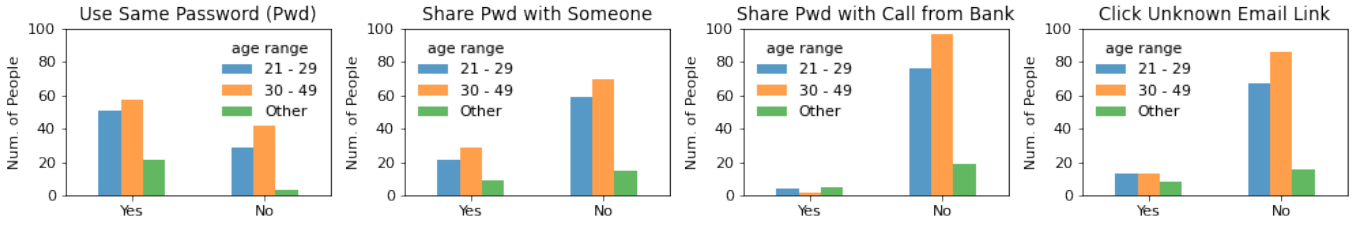

Fig. 6. Behavioral Characteristics under different scenarios

filters to carry out an attack successfully. It demonstrates that the weak link that makes vulnerabilities for social engineering attacks is humans. We came to this finding because while we could create an email domain that was particularly close to PayPal's customer service and could feasibly deceive humans, the bottleneck with the attack was creating an email domain that could successfully bypass email detection systems.

VI. Challenges and Future Work

The most pressing item of future work for our project would be a continuation of our survey to compare the effectiveness of different educational strategies categorically. We would determine this by implementing other cyber security education techniques with varying portions of the survey population, then re-conduct the survey to see which methods were most effective. Additionally, we would like to spend more time attempting to conduct phishing attacks under various conditions (i. e. different email accounts, targets, attack links) to determine what exactly prevented us from beating spam filters.

Beyond our project, we can confidently say that there is a deep need for more interdisciplinary research. Specifically, there is a need to conduct qualitative research with collaboration efforts in computer security, psychology, neuroscience, psychophysiology, and information sciences to answer various fundamental questions. These questions are: (i) under what conditions people trust each other, (ii) what factors that people use to determine whether or not to trust someone, (iii) what factors cause susceptibility to social engineering attacks.

Moreover, there are trust's neural, hormonal, or physiological underpinnings. For instance, the oxytocin hormone regulates social bonding and affiliation behaviors. Therefore, administering oxytocin to people increases people's desire to trust people, which attackers can leverage in certain situations to change people's willingness to trust someone and tend to be deceived. Although the conceptualization of the trust is incredibly multifaceted, collaborative research efforts help understand, mitigate and eliminate the uncertainty and severity of social engineering attacks.

VII. Conclusion

After performing a study on social engineering, we can conclude that an organization, an enterprise, or an individual is fully susceptible even when deploying the most important and most costly security technology. Furthermore, it indicates that a skilled attacker may quickly obtain knowledge by acquiring the victim's trust and being closely associated with them.

The social engineering approach to obtaining private information has become prevalent due to the adoption of social media and the digitization of services. Previously, individuals and corporations were unaware of these attacks' methods and tactics for safeguarding information. As a result, information security is the primary issue of today's world.

In terms of enhancing their understanding of the methodologies and how to recognize them, the security training, awareness, and education of potential victims must be a crucial mechanism for combating social engineering attacks. In addition, policies, processes, and standards are critical components of leading individuals and enterprises.

VIII. References

References

[1] Salahdine, Fatima, and Naima Kaabouch. 2019. "Social Engineering Attacks: A Survey" Future Internet 11, no. 4: 89.

[2] A. Sharifi, A. B. Noorollahi, and F. Farokhmanesh, "Intrusion detection and prevention systems (IDPS) and security issues," International Journal of Computer Science and Network Security (IJCSNS), vol. 14, no. 11, p. 80, 2014.

[3] P. A. Barraclough, M. A. Hossain, M. Tahir, G. Sexton, and N. Aslam, "Intelligent phishing detection and protection scheme for online transactions," Expert Systems with Applications, vol. 40, no.11, pp. 4697-4706, 2013.

[4] H. A. Aldawood and G. Skinner, "A Critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications," 2018 26th International Conference on Systems Engineering (ICSEng), 2018, pp. 1-6, doi: 10.1109/ICSENG.2018.8638166.

[5] I. Ghafir, V. Prenosil, A. Alhejailan and M. Hammoudeh, "Social Engineering Attack Strategies and Defence Approaches," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), 2016, pp. 145-149, doi: 10.1109/FiCloud.2016.28.

[6] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," Computers and Security, Article vol. 59, pp. 186-209, 2016.

[7] Aldawood, Hussain, and Geoffrey Skinner. 2019. "Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues" Future Internet 11, no. 3: 73. https://doi.org/10.3390/fi11030073

[8] K. Krombholz, H. Hobel, M. Huber, and E. Weippl. "Advanced social engineering attacks," Journal of Information Security and Applications, Article vol. 22, pp. 113-122, 2015.

[9] A. Kumar, M. Chaudhary, and N. Kumar. "Social engineering threats and awareness: a survey," European Journal of Advances in Engineering and Technology, vol. 2, no. 11, pp. 15-19, 2015.

[10] H. Wilcox and M. Bhattacharya. "A framework to mitigate social engineering through social media within the enterprise," 2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA), 2016, pp. 1039-1044, doi: 10.1109/ICIEA.2016.7603735.

[11] Conteh, Nabie Y., and Paul J. Schmick. "Cybersecurity:Risks, Vulnerabilities and Countermeasures to Prevent Social Engineering Attacks." International Journal of Advanced Computer Research, vol. 6, no. 23, 2016, pp. 31-38. ProQuest.

[12] S. Gupta, A. Singhal, and A. Kapoor. "A literature survey on social engineering attacks: Phishing attack." Proceedings of the International Conference on Computing, Communication, and Automation, Noida, India, 29–30 April 2016; pp. 537–540.

[13] G. Costantino, A. La Marra, F. Martinelli, and I. Matteucci. "CANDY: A social engineering attack to leak information from infotainment system." Proceedings of the IEEE Vehicular Technology Conference, Porto, Portugal, 3–6 June 2018; pp. 1–5.

[14] I. Ghafir. "Social engineering attack strategies and defence approaches." Proceedings of the IEEE International Conference on Future Internet of Things and Cloud, Vienna, Austria, 22–24 August 2016; pp. 1–5.

[15] L. Segovia, F. Torres, M. Rosillo, E. Tapia, F. Albarado, and D. Saltos. "Social engineering as an attack vector for ransomware." Proceedings of the Conference on Electrical Engineering and Information Communication Technology, Pucon, Chile, 18–20 October 2017; pp. 1–6.

[16] L. Xiangyu, L. Qiuyang, and S. Chandel. "Social engineering and Insider threats." Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Nanjing, China, 12–14 October 2017; pp. 25–34.

[17] P. De Ryck, N. Nikiforakis, L. Desmet, and W. Joosen. "Tabshots: Client-side detection of tabnabbing attacks." Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, Hangzhou, China, 8–10 May 2013.

[18] K. Ivaturi and L. Janczewski. "A taxonomy for social engineering attacks." Proceedings of the International Conference on Information Resources Management, Centre for Information Technology, Organizations, and People, Ontario, Canada, 18–20 June 2011; pp. 1–12.

[19] H. Tu, A. Doupé, Z. Zhao, and G.J. Ahn. "Sok: Everyone hates robocalls: A survey of techniques against telephone spam. " Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 320–338.