International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

The Evolution and Defense Against Social Engineering and Phishing Attacks

Sibaram Prasad Panda

Email: *spsiba07[at]gmail.com*

Abstract: ***A successful security system relies on both technology and operation, however, means and methods cannot substitute for motivation and awareness. Weaknesses in security management and human factors are inevitable and bound to exist. Social engineering malware can be categorized into two types, including online and offline malware. It is believed that building the technical defenses of systems would not be sufficient to defend phishing since phishing attacks inherently booked with the strong reliance on human factors in dealing with security. Social engineering and phishing attacks continue to represent significant threats to organizations and individuals, evolving alongside advancing technology and changing social dynamics. This paper examines the historical progression of these attack vectors, analyzes current trends, and evaluates emerging defensive measures. We present a comprehensive taxonomy of modern social engineering techniques, evaluate the effectiveness of technical and human - centered defenses, and propose a multi - layered defense framework that integrates artificial intelligence, behavioral analytics, and continuous awareness training. Our findings suggest that while technical solutions provide essential protection, the most effective defense strategies combine technological measures with human - centered approaches that enhance users' ability to recognize and respond to social engineering attempts. Any attack, regardless of ideas, motifs and means, shares its dependence on manipulation of human weakness or general vulnerabilities. Malware of online phishing is based on a model of fundamental human weaknesses which can be utilized for attackers' advantage and defenders' design of countermeasures. An analysis of defense based on human weakness is proposed. Constructing social engineering attack model according to the need for Understanding Engineer Behavior in Order to Improve Defense Effectiveness.***

Keywords: social engineering, phishing, cybersecurity, human factors, security awareness, cyber defense

1. Historical Overview of Social Engineering

In 1867, the first usage of the term social engineering was attributed to the British philosopher and jurist Sir Edward Burne - Jones [1]. In his book, he postulated a mechanism or organization to create a frontier between the established and the insecure social order. He believed that a newer social order could be introduced by changing social dispositions for group entities through proper arrangements of institutions or organizations. However, in the same year, V. B. Semenov [2] in Russia used the term to suggest the possibility to apply constraints of engineering to control social processes. Social structural adjustment in view of engineering was perceived as weaving social orders/fabrics of an entity that invigorated outcomes in designed ways. He also perceived that even by proper social engineering, social entities functioned differently from those intended or desired: accumulated and/or uncontrolled side effects would turn embellishment into something horrid. Inspired by an opinion that it was easier to shake a throne than to destroy a beard, he further put forth a cunning idea/question that it was out of the reach of the social engineer to achieve or produce whole social orders or fabrics. Reaction of society and history were beyond reach. Initially, the term social engineering concerned knowledge of and/or implications to innovate social order and institutions. However, for the first time, human weakness was considered. Despite reference to the ablest man - made machinery at the military art of war, financial and legal operations was better left to an automatic machine, one at which no human judgment should intervene. Obedience to constraint of machinery resulted in systematic execution of orders, producing bank notes, lotteries, and insurance, thus obviating human inappropriate affection, or observance at a prescribed distance.

a) Early Techniques (1980s - 1990s)

The concept of social engineering predates modern computing, with early hackers like Kevin Mitnick demonstrating that human manipulation could bypass technical security measures. During this period, attacks primarily relied on telephone - based deception (vishing) and in - person impersonation to gain access to systems or information.

b) Email - Based Attacks (Late 1990s - 2000s)

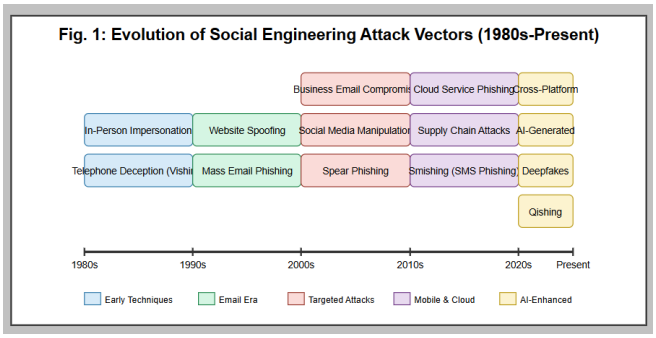
The widespread adoption of email created new attack vectors. Early phishing campaigns typically involved mass - distributed emails with grammatical errors and obvious red flags. However, these attacks succeeded due to users' limited awareness of digital threats and the novelty of the approach.

c) Targeted Attacks (2010s)

The rise of spear phishing marked a significant evolution, with attackers conducting reconnaissance to craft highly personalized messages targeting specific individuals. During this period, business email compromise (BEC) emerged as a sophisticated variation, focusing on high - value targets within organizations.

d) Current Landscape (2020s - Present)

Today's social engineering attacks incorporate advanced technologies, including artificial intelligence for generating convincing content, deepfakes for audio and video manipulation, and automated tools that enable large - scale customized campaigns. The COVID - 19 pandemic accelerated the evolution of these threats, as attackers exploited fear, uncertainty, and the rapid transition to remote work



2. Types of Social Engineering Attacks

The two most widely used attacking methods are phishing and social engineering, which are online methods of deception intended to cause harm to computers and networks [3]. Social Engineering attacks play a vital role in computer security failures. Attackers usually do not rely only on technical resources but tend to utilize social engineers who manipulate people to disclose valuable information. However, there is limited knowledge about the reasons behind susceptibility to social engineering attacks, particularly in relation to employees in organizations. The prevention of a social engineering attack relies mainly on users' attitudes. Education of the users is regarded as being the best defense against social engineering attacks.

Phishing can be defined as a method of attempting to solicit information such as usernames, passwords, or credit card details from internet users by posing as a trustworthy entity in an electronic communication system. This can be done by sending an email or instant messaging to hundreds of people in hopes that someone would give out their information [4]. Phishing schemes come in waves. Occasionally many people get an email message from what appears to be a bank, saying that they need to verify their account information for security reasons. The email provides a link to a page that looks almost identical to the legitimate website of the bank. Users are then instructed to provide their banking information in order to gain access to their accounts. If they choose not to "verify" their information, they are threatened with account suspension on the same email. This technique is called "pretexting".

Pretexting attacks are when an attacker pretends to be someone of authority or someone a user trusts in order to gain sensitive information. For example, an attacker can call an employee in an organization and pretend to be from the IT department. If the employees do not receive enough training about such kinds of attacks and their signs, they will likely fall victim to them. Pretexting attacks often occur over the telephone. Somewhat analogous to pretexting are "prank calls". The difference is that prank calls generally do not aim at obtaining sensitive information.

2.1 Phishing

Phishing is a process to collect sensitive information such as username, password, credit card number, and bank account information, for malicious reasons, and on the victim, usually conducted without the victim's consent. Phishing is typically carried out by email spoofing or instant messaging or directing users to enter personal information at a fake website, the so - called phish website [5]. Phishing is a kind of social engineering attack that can lead to identity theft and fraud that obtaining. Phishing may involve the action of swindlers posing as banks or payment platforms to deflect people to a website and make them enter sensitive information such as usernames, passwords, and account codes [6]. People's identity may be threatened by this kind of attack; furthermore, phishing may leak internal commercial secrets or induce a large sum of economic loss as threats to enterprises. Phishing attacks can mainly be categorized as e - mail phishing, SMS phishing, and social network phishing. It is reported that there were 290 million phishing attacks attempted between mid - 2022 and early 2023, and social media phishing attacks, which grew rapidly that comprise 90 percent of all phishing attempts in 2023, apace threaten the users on the ground.

Mass email phishing usually involves hundreds of thousands of recipients. It focuses on people who are unsuspicious (successful in examining the target) and know little knowledge of IT or internet behavior. E - mail phishing has been very common, and it reflects the most phoney message in cyberspace. In the e - mail phishing process, phishers typically encode a collection of filter - free mass e - mail whose addresses are 90% counterfeit, while the other is from the very famous enterprises and automatically send them to wholes of e - mail users with a goal to harvest unwelcome visitors.

2.2 Spear Phishing

An emerging commercial trend is the business niche, spear phishing, that consists of social engineering failed attacks. Spear phishing targets only one person or organization, hence the name. Its goal is to extract sensitive information. Different techniques are hereby employed. From the attackers' perspective, the victim's field remark abstains the commercial segment, underlining that phishing attacks target everyday users. The methods employed to commit spear phishing have evolved dramatically over the years. Spear phishing's process starts with the 'information gathering step' where relevant data such as identifying personal data is extracted from the social media of the intended victim. The next step is the 'imitation step' where the attacker creates a phony account that imitates a real user to enhance credibility. Founding a link to an online service accounts for the 'bait step. ' The final step of a spear - phishing attack is executing a coveted result to extract sensitive information, known as contagion. On some occasions, the attacker would send malicious hash links known as malware to steal sensitive data and gain audacity on the victim [5]. Spear phishing targets an organization instead of one person. The overall work to be conducted is akin to a spear - phishing attack. Spear phishing would contend of an exploitable IMAP or OpenID user account and a social engineering email connotation containing a malicious link. The developed phishing page is designed to skim the victim's credentials in compliance with business definitions. The exploited payment form page skims the victim's credit card credentials in compliance with a crafted database.

2.3 Vishing

Following the invention of the telephone and with it the advent of technological advances in telecommunications, such as the use of answering machines and the transition to direct calling with numbers, there was a notable increase in criminal activity as well. Even though these innovations created many possibilities, criminals exploited them to implement scams, particularly by making telephone calls, gaining access to private information, and stealing money. These attacks are now known as vishing, or voice phishing, which is defined as "a scam that uses the telephone—both traditional phones and Voice over the Internet (VoIP) —to trick people into giving up personal information so they can be easily robbed or further scammed". Voice phishing attacks can be divided into two categories: novice - issued scams, which can easily be created by inexperienced money thieves and afterwards executed with little knowledge or skills necessary, and advanced attacks, which use different technologies, such as Voice over IP (VoIP) telephony, in order to reach a certain target and safety sneak past conventional tracking methods used by governments and telecom companies. For the latter kind of scam, the advanced scamming service often uses a business - like telemarketing approach, as the amount of research and administrative tasks involved in conducting them ranges at a higher level than "cut - and - run" type scams. Voice phishing attacks can vary from simple "get - rich - quick" schemes aiming at a broad audience to very advanced tele phishing services, such as spoofed calls, which selectively target individuals of interest. Usually, these telephones scams' tactics often utilize automated voice messages claiming that the victim needs to press certain keys to address some undesired consequences (e. g. "To prevent your computer from being blocked, please press 1" etc.), which together with misaddressed returned calls can result in harassed answering machine inboxes. Through social engineering attacks posing as angrily demanding telemarketers or legal opposition, criminals can steal time and chase away uncooperative leads.

2.4 Pretexting

Pretexting is another form of social engineering where attackers fabricate a story or a pretext to gain access to someone's personal information. It is widely accepted that attackers cannot persuade someone to give up a large amount of information at once. Instead, pretexting tries to obtain information over the course of several interactions. Pretexting persuades the victim to give up some pieces of personal information and opens the door to allow the victim to gain trust in the attacker. This form of social engineering relies heavily on the ability of the attacker to gain the victims' trust. By gaining the victims' trust, the attacker is able to get the information they are after much easier. A key to gaining the victims' trust in these types of attacks is to have a solid pretext. Pretexting social engineers are skilled storytellers who develop a story about the victim and their affiliations. The most common type of pretexting social engineer is the impersonator. Impersonation requires the attacker to gain information about the victim before contacting them. This is a standard social engineering tactic across all social engineering attacks. However, for pretexting attacks, the attacker must further develop the character whose affiliation will be used while impersonating the victim. This requires a larger time commitment but amplifies the social engineer's chances of success. When an attacker impersonates someone, they build a fictitious persona that they use to gain access to the cyber resources they are trying to steal. To build this fictitious persona, the attacker performs online reconnaissance on the victim. The attacker discovers a slew of information, including the victim's job title and who they report to. With this information, the attacker drafts a fictitious persona in accordance with the victim's attributes. However, for companies like social media firms that are equipped with diligent engineers, as well as tight verification protocols for outsourced contractors, obtaining access from distant locations would be extremely difficult.

2.5 Baiting

Baiting, using a false piece of media, such as an iPod or a flash drive, is distributed to victims and, when used, exposes them to malware. Some common places are: airports, school grounds, coffee shops. It has the disadvantage of requiring more interaction from the victim but can be carried out in a much more targeted and speculative way than in general spam. This technique requires the presence of physical media; hence, it is more reliable than other remote contact methods such as email [5].

The bait is left in a public location, such as a conference room, a public table, or dropped into a location where people could find it. To work, bait must generally come with some accompanying lure: social engineering would be useful for this, such as a tag attached to bait with details of the last user or some private, intimate communication request. The bait must be placed in a location where it can be legitimately left for someone to find. The tag should appear authentic; it may be more advantageous to invent a false person rather than use a known one or an unacquainted person. The bait would need to be made compatible and easy to access on the target victim's computer, the bait could either infect the system with a regular, widely available worm or install a user - controlled backdoor.

3. Psychological Principles Behind Social Engineering

The definition of "social engineering attacks" is widely accepted. Some hackers mainly use social engineering (SE) attacks to deceive the people of the location to acquire valuable information like account names and numbers, identity numbers, passwords. Generally, there are two main types of SE attacks, targeted and target of opportunity. A targeted attack is very specific in terms of the victim, while a target of opportunity attack is distributed to a plurality with the hope of a response. One way of classifying SE is as follows: locating and using SE. The first phrase is the location of the targets. Some social engineers gather target information, such as gender, age, location, and working units from social networks, online game identities, etc. The second phrase is the psychological method of using SE. SE design is based upon the exploitation of one or more psychological methods. Once an individual targets attacks, social engineers usually determine the false goal in advance and then find a method to manipulate the victim gradually either by

exploitation of asserted authority or manipulation of targets' commitments and relationships. The main goal of being a social engineer is to gain access to the desired information (e. g., passwords, online - banking information, camera access, etc.) by manipulating the victim without their awareness about the information criticality or false goals.

A large number of companies would like to validate the background of the interviewed before they are hired. However, a large amount of financial loss made by the social engineering attack still happened [4].

4. Evolution of Phishing Techniques

Phishing and Spear Phishing (SP) attacks' evolution have undergone various changes and attempts at refinement, and there are still new approaches that ease their dissemination. The tweet of Kultur Schock demonstrates how social media can be exploited for phishing techniques by creating fake accounts of popular cultures and contacting the target. It can be considered a 'classic' example of cyber espionage by a SP attack and removal of the content can be considered the first step of mitigation as the attack does not follow the classical methodology. On the other hand, education regarding phishing can only be partially taken as MCQ, as the attack vector may differ from the questions asked, since question making is not an automated process. New tactics such as using political topics as a hook or claim for plagiarism notice can be expected to grow and may need a new approach altogether [5].

While phishing scams are unfortunately lucrative, cybersecurity attacks using phishing techniques have morphed considerably, possible due to the success of some of them. One tactic is to allow the phishing sites to mimic real ones authentically. The most prevalent targeted organizations are financial institutions so that direct database attacks are circumvented with phishing layout designs, which are mostly disposable. Banking institutions now tend to contact customers through automated phone messages and to contact phishing domain hosting sites through law enforcement agencies, making it a serious deterrent and this may eventually move phishing to the black net. Phishing URL is very often based on patterns like containing the targeted institution's name, length and hopping count but newer versions of URL encoders tend to make the detection process a bit tougher, as well as phishing domain names.

4.1 Early Phishing Methods

A phishing attack traditionally consists of a mass - mailed email to several addresses believed to belong to a certain organization, usually a well - known bank or other business that most of the time is trusted by the public. The email contains a short text designed to make the user suspect a problem with their account, appealing to the user's sense of urgency to motivate them to perform actions involving sensitive and valuable data, including their names and passwords. However, the institution is not involved at all, and the email, which carries a link to a fake website, is instead sent by and created by a phisher, a person engaged in this practice. If the user enters their login information and forwards it, the data is immediately handed to the attacker. At a later stage, the obtained data could be used to permanently compromise the compromised accounts. [5]

For instance, email phishing by straight URL redirection. In this technique, the phisher would directly redirect a URL which at first is considered trustworthy to a page which looks identical but instead directs their login credentials to the attacker. Although the technique is relatively robust, there still exists a possibility for the phisher to get detected. Phishing sites rely on a unique internet address. However, such addresses are limited and there could exist a system such as DNS spoofing that instead directs the user to the real URL after being interrogated to avoid detection [6]. Specially crafted JavaScript would run an automatic log - in to the page, making it look like users navigate to the main page. The main window, however, would disappear and log - in information could be extracted from an invisible frame. This would allow the phishing page to compete with the reputation and reliability of the original page. Consequently, phishing remained and still remains, today, predominantly focused on email.

4.2. Modern Phishing Tactics

A few old tricks, such as getting somebody to visit a spoofed website, still are in play, but the excitement comes from the ever more inventive methods being experimented with. The relevance of phishing is so high that "phishing" operations regularly are more extensive than simple e - mails looking for bank accounts. Examples exist where scam artists get many different companies to send out welcome letters to the public on radio and TV. This is one stage on a big operation aimed at another company. Some fraudulent pages were hijacking real pages or spoofing them to look like real ones until subscriber info was gathered. Phishing isn't a problem to the victim organizations, and removing the pages does little good because the problem just moves elsewhere. The attraction of these kinds of scam is that they are faster, easier, and cheaper than other kinds of attacks [5].

Phishing is generally defined as a method of using spoofed e - mails and "phony" websites to glean personal information from unsuspecting users. Phishers nowadays execute elaborate, clever, and painfully well - crafted scams that have been shown to "catch" even the most astute of Internet professionals. People who seem to be on top of things get caught up in schemes that seem absurd and improbable. Phishers realize that their job is to communicate with the victim and some attempt to hatch real or simply absurd schemes. To see how this is done is a fascinating area of inquiry that brings together many disciplines. What motivates people to be swept into these ridiculous efforts? What do phishers do besides create the initial e - mail? What do they do once contact is made? What sorts of operational tricks are involved? What insights can be gathered from the operations of phishers and leaders of pyramid organizations into the actions of conspirators? What barriers exist to engaging in these behaviors [3]?

Phishing is a way of tricking someone again. To Phish is to fish for personal information. Most used method is e - mail. The name for it comes from the methods often used today; guess authority e - mails and ask for information while posing

as an information or contest person. Phishing scams have been reported for merchant accounts. It was soon learnt that resourcefully inaccurate people would send in proof of authenticity. The actions of criminal phishing by a person taking a big risk has to be a lot of money and seize control of the organization is a sensible way to do it.

4.3. Emerging Trends in Phishing

The phishing scene saw a flood of new ideas in 2018, including new business models, and advanced techniques for social engineering. During 2018, a pattern with the name one - click attack emerged. The objective behind this technique was to install malware as quietly as possible without user interaction. Significantly, any installation request on the target operating systems was denied by the up - to - date browsers like Chrome or Firefox [5]. However, some signalling attacks were still working on operating systems like Android, initiating the installation of fake applications that flooded the target device with adware. In this case, a custom application uploaded to the Google Play Store was also seen to maximise the effectiveness of the installation requests within the target environment.

Another innovation that touched the life of many was WhatsApp's paid business account. Although users had access to both, there were significant differences between them. The aim here was for businesses to communicate quickly with customers in a monitored way without being charged for text messages. However, cold email marketing has now transferred to WhatsApp, with identifiable patterns like the one seen in the past on other platforms. Attackers were impersonating businesses to extort data or showcase malware in both cases. The WhatsApp Web desktop extension didn't guarantee safety, and many more features were abused, including fake accounts impersonating customers, governments, etc. On the other hand, popular applications like Instagram presented opportunities for attackers who were trying to grab profits in the form of impersonation and subscription offers [3]. In both cases, artificially generated numerical handles evaded detection mechanisms.

In terms of textual campaigns, there were not many innovations. The “browser encryption” campaigns were some of the few. An issue with many ongoing campaigns that affected the current pace of threats was the loss of hardware numbers on command and control channels. A carefully crafted email that used the victim’s operating system, email client, and kernel architecture was supposed to grab credentials via advanced configurable data exfiltration channels. A self - executing code or auto - arranging text document for the attack plan was invisible to the text app’s “spyglass” alpha channels.

5. Case Studies of Successful Attacks

The attack that occurred on the bank involved a customer that had accounts at a different bank. The attacker had a copy of the ID showing it belongs to that customer. The attacker had a badge that showed that he was an investigator that worked for the bank. The bank employee was convinced by the attacker that the customer had committed fraud against the bank and after continuous pressure, social engineering and phishing attacks, the bank employee, convinced of the legitimacy of the attacker, gave up an amount greater than US$ 50, 000 in about 30 minutes. The attacker had indicated that he would take care of the rest and there would be no legal repercussions to the bank.

The bank in question had security protocols recommended by the Central Bank that were all bypassed. It was also investigated how such a severe breach of security could have occurred and what remedial actions the bank would take. The objective was to case - study one of the recent incidents. The method employed was by collecting evidence and interviewing employees in the departments concerned.

Prior to 2009, the bank’s security status was described and indicated that they had protocols consistent with recommendation that governed their operations and the recommendations stated 10 recommendations on diligence and control they should adhere to. There were third - party contractors used to establish the security of the bank systems most were checked only upon implementation and not on a regular basis. Each year, the policies in effect were examined, repoliticized, and redrafted the new policies were lacking in terms of their effect as a deterrent as were they updated to keep pace with new technology [3].

The solution was indicated, and it was explained on controlling the adopted security measures, a protocol by which each transaction was examined was amended, and measures taken against decided to compromise employees were also recounted. Most of the plans to justify security measures were stated. Consideration was also given to how the jumps in status and technology of the bank would necessitate a review of security systems and it was ensured that all recommendations were relevant and feasible. The security status after 2009 was reported and there was a description of the new procedures and protocols in effect [5].

5.1 Corporate Breaches

In September 2019, Capital One Financial Corp accidentally exposed the personal data of more than 100 million individuals, making it one of the largest data breaches in history and resulting in the theft of bank accounts, mortgages, and social security numbers. In August 2012, an attack on the network of a US supplier of credit ratings and financial services compromised the financial firm’s accounts of clients such as JPMorgan Chase and Citigroup. In January 2013, hackers stole 20 million credit card numbers from the bulk of Italy’s largest online retailer. These security issues have prompted many organisations to spend billions improving their IT security infrastructure. Commercial - off - the - Shelf (Cots) applications often come with unproven, but functional, security features that may leave their users vulnerable. An unfortunate few find out the hard way. One of these cases includes a capital market company (referred to hereafter as “company X”) and the loss of $5 million. A major client was tricked into sending this money to an accounts department manager impersonated by an external user with an email address created a few minutes before sending the alert to the client. Although the magnitude of this fraud is larger than a

company may have anticipated, the scenario is not new and is often being executed [3].

In recent years, an increasing number of companies have taken less responsibility for any malfeasance regarding web - banking transactions. Emails claiming to be sent from banks requesting sensitive client information or a change in banking behaviour, such as a password or a phone code, are often reported. However frightening, these scripts may seem, surprisingly many people fall for them. One could easily accuse the user of being foolish or misguided. Those who do so, however, fail to look at the other side of the coin: a very valid and worthy question to ask is why the system is not able to defend against such clearly fraudulent attacks? In some extreme cases, clients may transfer their stocks or futures to completely different accounts in other financial companies due to a phishing scam. A case involving investment banking is presented first, outlining measures that could prevent such a so - called "social engineering" attack. Afterwards, other examples of potential deficiency in web - security systems will be discussed, including stock trading, banking, and online password management systems.

5.2 High - Profile Incidents

Phishing attacks have become the most used technique in online scams. Even an inexperienced attacker is able to send tons of emails, courting victims unknowingly and stealing sensitive data. Just by registering on an email - providing platform, choosing a long list of possible domains to pick from, a free hosting of a website to handle victims, and sending a mass email with spam filters bypassed, this type of agent can initiate more than 91% of cyberattacks.

As most users nowadays use email and the number of users is constantly growing, this type of attack also increases. There is no doubt about keeping an eye on the email inbox. Phishing attacks are not only threats to personal affairs but are also dangerous to corporate secrets of great importance. Indeed, once email addresses of executives or well - known companies are leaked, criminal organizations can impersonate them to steal billion - dollar projects, contracts, and plans. In order to understand how to defend and prevent the effects of a Phishing or Spear Phishing attack, it is essential, if not paramount, to investigate how this type of attack is performed. Classic spear - phishing attack will be considered first. This kind of attack is necessary to create a deep understanding of how this task should be better performed and why new attack vectors have become a powerful weapon in the hand of a Phisher [5].

The election of the 45th President of the United States of America can be considered a 'classic' example of cyber espionage by a Spear Phishing attack. However, because of the extremely high - profile of this event and its participants, it is possible to describe the attack and its steps without compromising any user's point. Even in this case, Social Media platforms made this task easier. The so - called 'Russian bots' that impersonated essential positions in companies of the aforementioned election observers were observing the victims in order to draw up an elaborate and customized attack. To better explain this theory, 5 steps through which the Phisher leads the spear - phishing attack should be considered: 1. Collect. Gathering information on a specific target by exploiting all the available information shared throughout social media; 2. Construct. Creating fake social media accounts in order to engage with targets; 3. Contact. Contacting the victims; 4. Compromise. Installing malware on the victim's device in order to compromise it and steal information; 5. Contagion. The last step of this model considers how the Phisher can misuse the information collected during the Compromise stage to further compromise new victims. This step will not be examined since, at this point, the potential targets are already compromised.

5.3 Lessons Learned

This work discussed the evolution of social engineering and phishing attacks over the last two decades and explains the various ways to recede these malicious attacks. Based on the findings of this work, several lessons learned have been identified for enhancing the security against social engineering and phishing attacks. These lessons learned include factors affecting susceptibility to social engineering attacks, password strength, email phishing, anti phishing toolbars, browser plug - ins and web browser filters. Email filters include filter creation, filter evaluation, and filter integration. Awareness of email phishing is still low among email users. Factors affecting the user's awareness include perception of phishing e - mail seriousness, personal contact with phishing e - mails, perception of internal management's competence regarding phishing, and general knowledge about phishing. Detection rates of anti phishing toolbars and browser page reputation services are still low compared to the high detection rates of OS level security techniques. Truly phishing e - mails can evade toolbars, and intelligent attacks can bypass browser plug - ins. Feedback is important for the credibility of the browser plug - ins. A monitored test was conducted on three popular anti phishing toolbars and browser plug - ins to investigate their detection capabilities against various new phishing attacks [3]. A security awareness and training needs assessment was necessary to uncover problems, and a security training program plan was essential to address these problems. The program was partially implemented, and qualitative measures were determined to evaluate how effective the training was against the impersonation social engineering attacks. A case study of a severe security breach and compromise of a major bank in Jordan was discussed as an example to show the importance of recognizing the needs assessment problems and implementing the training program plan. The security status before 2009 and after 2009 illustrates how significant the effect is of improved policies and what still needs to be improved in post attack efforts. Weaknesses in the current password policy in an educational organization were analyzed. The effectiveness and potential of conducting an internal phishing attack and how it could strengthen security awareness were evaluated. Conducting an internal phishing attack could reveal the level of awareness and susceptibility to phishing attacks within an institutional organization. This balanced the fear of conducting this attack with the benefits that could be gleaned from the results.

6. Recognizing Phishing Attempts

Although being constantly bombarded with unsolicited e - mails, many people still don't realize the potential danger associated with clicking e - mail links. Today, Phishing represents the greatest risk in Cyber Espionage. Phishing is a term used to describe the act of searching for victim's intimate information via e - mail or instant messaging [5]. The phisher impersonates a reputable source or tries to convince the victim of a reality that doesn't exist in order to extract sensitive information such as passwords, IBAN numbers or personal credentials. Phishing attacks give attackers the means to access private property, exploit contacts, blackmail, and identity theft.

Having decided on a medium to attack, the phisher has to look for a target. At least five steps can be outlined to describe how a specific e - mail phisher will carry out an attack. Phishing is a layered attack composed of five different but necessary steps. The complexity of the set of information to be harvested and the prestige that the attack wishes to demonstrate will greatly influence how it will be classified. The wonderful world of social networks was a major breakthrough in this field. In fact, after e - mail, they became and continue to be favourite attack sites for phishers. In order to compromise the victim, a fake profile on one of these social networks is usually created. This profile is populated by grabs observed on the victim's one. For months, this backdoor account observes the victim's activity to draw up an elaborate and customized attack. The final scenario consists of the goal of ph … to hack the victim's e - mail account, social network, or online banking. Even though e - mail and social networks are used in several ways, ranging from obtaining intimacy to getting financial advantages, the philosophy behind them all is fundamentally the same: banditry by cyber means. Fortification against phishing is possible and necessary. Whatever the form, phishing represents the highest risk in cyber security.

6.1. Common Indicators

While those details can trigger significant red flags upon analysis of links sent in text messages or emails, these signs are not always as visible on websites. Domain names of phishing websites can sometimes be misleading. For instance, in a phishing attack masked as a bank, a link may direct users to a website whose URL contains "yourbank. xyz" while the real destination in the browser may be "realbank. yourbank. xyz". Domain names of phishing websites with ". com" or ". net" endings are often considered more trustworthy than with ". xyz" or ". exp" or such endings by users. In other attacks, the spoofing of partners' URLs may be common—such as a ticket seller impersonating another selling partner, a tourist agency impersonating an airline's ticket - selling service, and an airline impersonating a partner hotel. In these cases, possible risk signs include the indication of re - routing and a too - sudden appearance or disappearance of such messages.

To protect systems from being exploited, vigilance must be upheld. Identifying signs of social engineering "social" attacks (including clicking harmful links) on devices is a significant threat. Spam emails are common tools for social attacks to lure users into links with malicious codes, or to fill out forms sending away user information or assets. Apparent spam signs include misspellings and grammatical mistakes in texts, unprofessional typesetting of emails, discrepancies in the URLs of links and the services they point to, unusual wording, unexpected receipts, and generic greetings without using the recipient's name. While those details can trigger significant red flags upon analysis of links sent in text messages or emails, these signs are not always as visible on websites. Domain names of phishing websites can sometimes be misleading. For instance, in a phishing attack masked as a bank, a link may direct users to a website whose URL contains "yourbank. xyz" while the real destination in the browser may be "realbank. yourbank. xyz". Domain names of phishing websites with ". com" or ". net" endings are often considered more trustworthy than with ". xyz" or ". exp" or such endings by users. In other attacks, the spoofing of partners' URLs may be common—such as a ticket seller impersonating another selling partner, a tourist agency impersonating an airline's ticket - selling service, and an airline impersonating a partner hotel.

6.2 Analyzing Email Headers

After receiving an email, open it in your email client or website, locate the "view source, " view header, or similar option. The technical details of an email will open in a new window. Every email you've ever received comes with a header that hides the details of the email's interactions. It can reveal the journey the registration message took from its origin to your inbox, and it can also help you discover if an email is coming from a real address or if the sender is trying to impersonate someone.

The first item of information is a field called "X - Originating - IP." If valid, this is the actual person or organization who sent you the email. You can do a quick IP lookup search on it, but if it has been spoofed, it won't help you to confirm the sender's true address.

The sender of the email is sometimes identified just as the email address, but most email providers display the sender differently to obscure the technical details about the address. In these cases, you will need to read through various header fields to hunt down the For example, in Gmail, the sender's details are often placed inside "From" fields. The first one shown in this header is the real name of the sender, which conceals the email address it represents. The actual sending account address can be found in the second instance of the "From" field or the last instance of the "Forwarded" field. The email address itself can be recognized by its "[at]" sign, which separates the two parts of an email account—the latter part being the domain.

7. Defensive Strategies Against Social Engineering

A strategically defined and well - documented security policy is essential in the protection of an organization's information infrastructure. As a minimum and to comply with legislation, this policy should document acceptance criteria for all aspects of IT security and should be reviewed on a regular basis. The policy should also include outlines of the responsibilities of

owners, custodians, users, security personnel, and methods of compliance. Specific details regarding such items as robust user authentication should also be included. As a policy item, user authentication is likely to be one of the first methods addressed. For a long time, security systems relied on passwords. It believed that arbitrary passwords would be impervious to attack, but this has proved to be incorrect. Phishing attacks targeting user credential sets are widespread and have shown various efficiencies in operation. These operations typically exploit poor security awareness amongst users rather than implementing sophisticated technical workarounds. More recent approaches to user authentication have included biometric and token devices. Token devices such as smart cards and mobile - to - 2FA are believed to be a good advance on the previous situation: they provide an additional method of authentication and are, it is believed, more impervious to attack than simple passwords. However, token devices too have been shown to be vulnerable to social engineering attacks. Phishing techniques have made their appearance in attempts to subvert this technology, and with increasing sophistication it was recently found that the operators of malware - as - a - service agencies are broadening their service offering to include the posting of tick mercenaries trained to exploit 2 - FA installations. It is critical to implement an integrated approach to security. Unlike firewalls, which serve as an isolation mechanism to isolate a portion of a network from exposure, security awareness is the means used to enforce compliance with security policy. It is counterintuitive and non - computationally designated and relies on a continuous jump sensitization - feedback loop to achieve some semblance of the safety level required to deploy trusted systems. Humans are the component of computer systems with the greatest vulnerabilities. These vulnerabilities are exploited by attackers primarily through social engineering. Humans are the weakest link in any security system. Information security awareness training is the crucial tool in the fight against social engineering attacks.

7.1. Employee Training and Awareness

Without educating all employees on the possible threats of social engineering, social engineering assessment will most likely fail. Many organizations are starting to enhance training in response to many major incidents. Here are some suggestions for effective training.

Training programs should include an overview ("what is social engineering?") as well as a summary of the relevant risks to the organization. Programs should explain how an attacker might use those risks to compromise someone's credentials and the organization itself. Employees should be taught what types of things might signify a possible threat and how to best cope with those situations. Employees should also be encouraged to report threats as soon as possible while emphasizing the APT nature of such attacks. Employees reporting threats should be seen as an asset to the security team rather than a liability.

The technology division should strive to be transparent in how they work, especially with the helpdesk. Users should understand how to contact the helpdesk, how the helpdesk will contact them, and when and how to report things, they find suspicious. Without that communication, an attacker can simply contact employees and request their password because the individual thinks the email or phone call is legitimate.

Different types of training should be available to users in order to reach as many individuals as possible. Sending the same message in several ways will help reach more of the organization. Emails were created to give tips on a weekly basis. The emails should be short and cover topics that would affect normal users. Hands - on labs were created, demonstrating a phishing email and explaining to users' different items to look for in suspicious emails.

7.2 Implementing Security Protocols

In formative years, typically in early schooling, students are inspired to appreciate math through competitions such as spelling bees. Until now, awards have primarily been given to the winner or first place only. The understanding is that broader recognition of oft - forgotten facts such as math would inspire appreciation of them. A more sober approach to math is suggested, examples of which in the youth sphere are given. Such an approach would eschew the trappings of frivolity that disallow art, poetry, music, or spoken verse on the subject and would instead produce a closer ideal to the greater mathematical awe and artistry of celebrated figures. Moreover, the now - ubiquitous Pythagorean theorem does not permit an appreciation of 3000+ years of geometric proofing and definition.

Other than soft drinks and breakfast cereals, product mascots have now evaporated. The idea of a math mascot might focus youth attention squarely on its entertainment properties. The once - outstanding optical illusion known as Wells' chain of circles could, given today's computer animation technology, become character - driven. Geometric input over which every child could croon songs encompassing numerous perspectives and imploring them to sing along in a similar spirit to a sizable portion of 20th century cartoons. Such digitization would weight learning and appreciation of math with ever greater novelty and amusing sounds, gyrations, and apparitions, fashioning products a trivial force against loss of interest and higher learning.

As surveys of the past decades have shown, math and science are fading in esteem, practice, and in this respect, understanding, at nearly all educational levels. The humanity of math over its outcome cannot be dismissed in fostering along with visual reasoning an appreciation of higher facets and artistry. This comprehension would apply to mathematics as a description, regardless of arbitrary outcomes, and failure to sufficiently complete a proof or homomorphism would abruptly invite criticism of them as a description. What math should be torn from its trappings of utility and elementary cool and returning as a subject of enduring complexity welcome to greater number or use attempt bestowed ennobling recognition achievement and inclusion as an art form.

8. Technical Solutions to Combat Phishing

The main intent of phishing is obtaining private information for corporate accounts and unauthorized access to computers [5]. The idea behind these attacks is social engineering—

manipulation of human behavior rather than the exploitation of vulnerabilities in software or hardware. Phishing generally accounts for over 91% of successful enterprise cyberattacks. Since the online world cannot change how people feel, but only how they think, the idea is to focus on four different layers of defense against phishing. Solutions that warn the victim, but let the last answer be up to the user, are considered a type of Decision - aid Tool. Since phishing depends on deception, it can be expected that whatever the current situation is, some individuals should be working on deceiving targets. Phishing can be much more complicated than just sending a few e - mails with seeded hyperlinks. Nevertheless, the "big picture" of a phishing attempt can be coded simply and effectively. Bots can thus be used to investigate tender information presence on the web proactively, removing most human involvement. It can be considered a semi - automated form of social engineering or even espionage. This type of phishing, automated and relying on data extraction processes, is likely to take precedence over those that exploit human fallacies.

Social media among agency's workers can be checked, and fake profiles used to contact workers who give away relevant information can be created. Furthermore, through fake accounts, the fake identity through which a malicious service is offered can be used. Finally, the victim can be convinced to click on a hyperlink. Understanding how to draw malware, and when necessary, stealing passwords, user files, and other important information enables much more than just destroying a final state. It is essential to persist in the attack, reduce the infected station, score entrepreneur even if on 1–5 devices, and "instantaneously" change phishing profile. A user responsibility, given the modern complexity of systems and behaviors, should gently be requested. Understanding the value of a precise inter - user balance decomposition of responsibility is also indicated to administrators. In turn, it is perceived professionally that insecure user systems are a high - risk level for the agency.

8.1 Email Filtering Technologies

This chapter covers how spam/phishing emails are generated, modelled, filtered, and reported, along with the challenge of email handling. Most of the flood of emails received by users contain unwanted information, such as spam/phishing emails, and are generally dealt with based solely on the detection of subject/headers. To narrow it down, this chapter focuses on classification/label - based filtering where email extraction is performed based solely on the message body. Moreover, as an additional layer of security and user to user collaboration, users need to be able to report spam/phishing emails further filtering them from the system.

Phishing attacks are very common social engineering attacks which target end - users' emails/inboxes to steal their confidential information. Most phishing attacks are email based. These emails, which can be fraudulent and fake, are sent with the underlying intention of stealing the victim's information or infecting their system. These phishing emails can be detected and filtered based on several features. Over the past decade, platforms and tools to combat phishing email attacks have been proposed. In this chapter, PhisTorAlg, an algorithm which exposes a hybrid rule - based approach to email - based web - application phishing and spam attacks is presented. This algorithm generates phishing/spam email templates after extracting attack properties and classifying those properties as features or measures. Anti - phishing approaches may be classified based on where the detection takes place. If detection happens before an HTML page gets downloaded by the browser, it is a pre - fetch approach. If detection happens after an HTML page gets downloaded, it is a post - fetch approach. The resulting URLs from such attacks may be either legitimate or illegitimate. Detection methods may also be classified based on the architecture or the technique they employ.

8.2 Multi - Factor Authentication

Although password - based authentication is strongly recommended for ensuring correct authentication, owing to human factors, attacks on passwords represent most successful attacks against an organization. To alleviate this risk, multi - factor authentication has been introduced as a method for making impersonation attacks more difficult and time - consuming. Multi - factor authentication takes different forms depending on the different factors that it utilizes. Some common methods include hardware tokens, SMS or email codes, and biometric input devices. Multi - factor authentication can be made more difficult to defeat by employing complexity in the factors, for instance using multiple types of factors, like hardware - profiles and telemetry.

However, cyber criminals are continuously discovering new ways to subvert even the most sophisticated multi - factor authentication systems. The problem stems from the fact that, unlike passwords, multiple factors, on their own, still remain valid for the lifetime of the partnership between a user, their devices, and services. So long as this partnership remains intact, the factor continues to be useful, even if it has been successfully extracted. On the other hand, multi - factor authentication performs poorly when faced with the documented, long - term vulnerabilities to replay, impersonation, and reuse attacks. It is essential therefore that hackers be proactively resourced and sophisticated to gain anything through these means.

Over the past year, several alternate solutions to the use of passwords and multi - factor authentication have been proposed. These solutions perform either specification or characterization on the premise that deviation from the expected input constitutes a suspicious circumstance. However, this specification can be defeated by mimicking the target, and characterization will fail to be able to draw a meaningful conclusion when faced with an adversary who has everything expected. Moreover, these solutions cannot be classified as general. In particular, one solution successfully detects replay, impersonation, and reuse attacks, but it is highly invasive and only enables protection of a specific multi - factor authentication transaction at the time.

9. Legal and Ethical Considerations

Social engineering and phishing attacks are often legally ambiguous, as they may not involve traditional malicious conduct. Communication and computer laws may apply, but

in many cases, internet service providers or a small number of corporations are the only parties with enough stake to be able to pursue legal action. Efforts have been made to improve international cooperation in prosecuting cybercrime, but the laws regarding social engineering attacks are generally vague and inconsistent from one jurisdiction to another [3]. On an ethical level, questions arise about whether excess or unsolicited information, such as emails or political opinions, should be considered damaging, and what degree of damage or injury would warrant taking related action. A related avenue of defense against social engineering attacks is a public inquiry into the parameters of private information and a public airing of both sides of the issue to affect public opinion.

The education of an informed populace as a defense remains a major area of focus among researchers and organizations trying to combat social engineering attacks, but many questions remain as to its effectiveness. The vague targeting ethic of these attacks means that developing an entirely aware populace could take far longer than the development of defenses to filter related activities. Lacking the ability to find the perpetrators of specific attacks and nearly universal ethical ambiguity for states, corporations and individuals makes social engineering truly unique in cyberspace. Nonetheless, many hope to be able to stamp out some of its more pernicious varieties through similarly imperfect procedures that have been tried for traditional crime.

10. The Role of Social Media in Phishing

Online scams have evolved significantly, and phishing attacks have taken on a leading role. Research has shown that since 2012 fraud attacks are initiated by Phishing messages more than 91% of the time. Phishing is a fraudulent attempt to obtain sensitive information from an individual by deceit using an e - mail looking legitimate [5]. Phishing can lead to devastating effects: exposure of intimate information, loss of money, and distrust. The goal of this paper is to investigate how a Phishing/Spear Phishing attack is performed. To this end different steps, a Phisher carries out to hack the victim are analyzed.

Phishing/Spear Phishing attacks are performed via the following stages. First, a Phisher needs to gather information available on the victim. Once the target is chosen, the Phisher gathers information about the target such as full name, friends, interests, job title, relevant places, an official e - mail address, and phone number. The information can be gathered through the internet looking for clues or checking social media. In 2017, Facebook detected and blocked about 470 profiles collecting information about Macron's campaign before the French election. Those profiles were created with the intent of observing the other victims in order to customize the attack. Furthermore, social media gives Phishers the opportunity to create fake accounts to start engaging the target. Once there is a connection, contact can be done via direct messages that can be a simple one - liner asking to discuss something "important" containing a link to an infected hyperlink.

Social media also gives attackers a chance to create and introduce ads to obtain information and target users. For example, during the American presidential election, a Russian group used an advertising campaign strategically timed for maximum engagement with posts linking back to a fake group. These ads deceived the Secretary of State and led to credential theft. If the Phisher still has information on the victim, he will proceed to the last part where the malware is installed on the victims' device. The malware steals information on the victim's device and sends it back to the Phisher. Many different malware types are available for keylogging, trojan horses, image or video capturing, etc.

11. Future of Social Engineering Attacks

In cyberspace, many security experts believe this situation will worsen. According to them, game theory can be used to mathematically model the results of an attack and help develop strategies and behavior mitigations against these attacks in cyberspace environments. Cybercrime and social engineering have grown in the past few years, with cybercriminals switching from smart techniques when launching sophisticated attacks targeting high - profile victims to the crude and mainstream techniques against low - profile victims, often involving anomalous techniques, or against targets without previous intelligence gathering. As a result, low - profile users are exposed to current broad - spectrum attacks. Users' thoughtless trust in new technologies is among the factors driving the vectors of future attacks and abuse scenarios for the ongoing threats. Security experts are often in the spotlight to predict what the future may hold when it comes to attacks, feasible technologies, and countermeasures. Many even launch such predictions via predictions lists or timelines published on web pages intending to share insights with the public. Yet, trends and probable future attacks on social engineering, identity theft, fraud, and other opportunistic scams remain unexplored. Social engineers and scammers constantly turn to new technologies and trends, changing the attack landscape. Emerging technologies such as virtual reality and the metaverse expose new obscured personal information, present new interactions of bridging physical and digital platforms, and reformulate security and privacy by design issues, incentivizing social engineering exploitation. The onboarding processes of these new services expose them to identical or similar threats already present. Video conferencing, a valuable tool that became vital with the pandemic, lacks essential security within many digital applications which have experienced success after a long period of anonymity. However, deep fake technologies can easily spoof conference applications and software where users originally cross - validate identities by profile photos. Most of this abuse can happen outside the scope of this topic, and safety measures have recently emerged. Yet, this topic can cause further information leakage or privacy issues even if it became partially silenced thanks to some technical controls.

12. Best Practices for Individuals

The best way to avoid becoming a victim of social engineering is to stay aware of changes in procedures regarding information gathering. Because of the numerous and ongoing changes in social engineering techniques, it is essential to stay informed of recent attacks. This can be

achieved through newsletters, seminars, and other awareness - building programs. When in doubt, be skeptical and double - check the information or claim with a trusted colleague or supervisor before disclosing sensitive information. Calling back the number of the organization being impersonated is good practice, as most organizations will publish their number in another readily available form.

Security awareness training is critical within the organization. Organizations must assume that one or more staff members will fall victim to social engineering attacks. Thus, appropriate countermeasures must be planned, tested, and written into policy. The governing body of the organization must agree to these countermeasures, as these decisions cannot be left to lower levels of an organization. Organizations should ask the following questions: Is lockable paper recycling provided? Are sensitive conversations held private? Is paper shredding enforced? What as - yet - unrevealed sensitive information could someone deduce from the website? Is CCTV used, and are the images monitored? Is there a policy regarding personal e - mail accounts, and is this enforced? Is security awareness and training provided? Are staff encouraged to be wary of surprise suppliers or vendors?

13. Best Practices for Organizations

Once security processes are in place to detect a social engineering attack, processes for investigation, reporting, and remediation must be enacted. Monitoring these threats should be a part of a general approach to monitoring security incidents and events. As such, logs for systems housing user and sensitive data and email servers should be reviewed regularly to watch for signs of these types of attacks. In addition, a feedback loop should be in place to change detection techniques as new attacks are identified. A process for reporting suspicious behavior is also essential. Employees should be educated on just how to spot such activity and who to report it to. Reports should be examined to determine if they are situated in general background noise, a “false positive, ” or a genuine attempt by an attacker to access sensitive information. This determination should feed back into improving detection procedures. Finally, if an attack is identified, a remediation process should be carried out. Often these activities will involve legal authorities to investigate more traditional aspects of the attack.

After appropriate detection processes are in place, a security awareness program should be implemented that focuses on educating employees about this threat. An awareness program will not eliminate all attacks and their fallout, but it will raise the personal costs of falling victim to such behavior. There is little empirical evidence suggesting that security awareness training leads to specific changes in information security behavior, or a decrease in the success of attacks. Firms should nevertheless implement awareness programs, as their absence is often cited as “impressive negligence” in the event of a breach. When developing an awareness program for these types of attacks, organizations should note some characteristics of powerful training programs. Training methods should challenge learners, offer opportunities for multiple approaches, allow for incidental learning, and provide opportunities for task practice. While these items are not strictly necessary, they do contribute to the quality and memorability of a training event. In addition, the nature of the threat should also outline the awareness program.

14. Incident Response Planning

The potential for risk management plans to enhance institutional resilience has emerged as a major area of research and development during the COVID - 19 pandemic. Resilience is defined as the ability of a system to withstand shocks and disruptions while still functioning effectively, and planning and managing risks plays a key role in achieving resilience. However, there is a scarcity of research on resilience concerning communication disruptions, particularly in the context of social media. Planning has gained momentum as it is often seen as the most effective way to cope with the vulnerabilities faced by systems and organization difficulties, which have been exacerbated by the pandemic. So, it is necessary to emphasize the importance of planning against social media - based outreach information manipulation, based on the findings of an analysis that evaluated a resilience plan for the Swedish public health agency.

Human error continues to be the leading cause of cybersecurity incidents affecting organizations. The average human error incident downtime is 45 minutes. Incident response plans must be reviewed, updated, and tested regularly (at least once a year). An increasing focus on preparing organizations to respond to testing, etc., cybersecurity incidents is evident. Although not all organizations are legally or regulatory required to have plans, preparations could be beneficial from a risk and credential perspective.

15. Conclusion

Phishing attacks have increased in sophistication because of their cheaper costs of deployment and use. Sophisticated phishing kits are available for rent to help people launch these attacks, as well as larger attack infrastructures. Sites that serve as phishing hotspots are now generating substantial revenue from advertising and site traffic hijacking. An overview of phishing and anti - phishing research is presented, with emphasis on available detection techniques, followed by other issues in the field of phishing research that remain open and require rigorous investigation through fundamental research and experimentation. Social engineering attacks continue to evolve in sophistication, leveraging new technologies and exploiting human psychological vulnerabilities. Our research demonstrates that effective defense requires a multi - layered approach that integrates technical controls, human - centered interventions, and organizational policies. The proposed framework addresses current limitations in defensive measures by creating systems that work with human psychology rather than against it, providing contextual security guidance, and continuously adapting to emerging threats.
As social engineering techniques continue to evolve, defensive approaches must similarly advance, moving beyond traditional paradigms to create security ecosystems that enhance human capabilities while providing robust technical protections. Only through this integrated approach

can organizations effectively mitigate the persistent threat of social engineering attacks.

References

[1] W. Fan, L. Kevin, and R. Rong, "Social Engineering: I - E based Model of Human Weakness for Attack and Defense Investigations, " 2017.
[2] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, "Social engineering attack strategies and defence approaches, " 2016.
[3] O. S. A. Salem, "An Integrated Intelligent Approach to Enhance the Security Control of IT Systems. A Proactive Approach to Security Control Using Artificial Fuzzy Logic to Strengthen the Authentication Process and Reduce the Risk of Phishing, " 2012.
[4] B. Cusack and K. Adedokun, "The impact of personality traits on user's susceptibility to social engineering attacks, " 2018.
[5] A. Ecclesie Agazzi, "Phishing and Spear Phishing: examples in Cyber Espionage and techniques to protect against them, " 2020.
[6] B. Issac, R. Chiong, and S. M. Jacob, "Analysis of Phishing Attacks and Countermeasures, " 2014.