JOIV : Int. J. Inform. Visualization, 7(3) - September 2023 808-814

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

Security Awareness Strategy for Phishing Email Scams: A Case Study One of a Company in Singapore

Widia Febriyani [a,*], Dhiya Fathia [a], Adityas Widjajarto [a], Muharman Lubis [a]

[a] *Department of Industrial Engineering, Telkom University, Jl. Telekomunikasi No. 1, Terusan Buahbatu, Bandung, Indonesia*

Corresponding author: [*]widiafey@student.telkomuniversity.ac.id

***Abstract*— Social Engineering Procedures and phishing are some of the standard procedures and problems today, mainly through sophisticated media such as email, the official means of communication companies use. Phishing emails are usually associated with Social Designing. They can be sent via joins and connections in this email, but they are not secure. Proliferation can be hacked into private/confidential data or total control over the computer/Email without the client's knowledge. The method used in this research is a cycle that will run continuously in a life cycle, starting from problem identification, then generating ideas and evaluating the Implementation of solutions. At each stage, a thorough checking process is needed to obtain results. Follow what you want. Achieved. The results of this study provide recommendations and some suggestions that companies can make; this aims to be one of the doors that provides restrictions for access from parties who are not entitled to access the application. Some thought has shown that this attack is growing and affecting the population. The evaluation stages in this study consist of 5 phases. Each phase is a step used to prevent both the system and the behavior in the company. Awareness is critical at the start considering this is the basis for the organization to determine who will take care of the personnel's knowledge related to information security. It thinks about using survey writing strategies and recommendations that can be made in anticipation of an attack, such as setting up representation or attention as early and often as possible.**

***Keywords*— Social engineering; awareness; problems; control; email phishing; prevention.**

Manuscript received 10 Apr. 2022; revised 26 Sep. 2022; accepted 24 Dec. 2022. Date of publication 10 Sep. 2023.

I. INTRODUCTION

In advanced data innovation, data security has advanced as an imperative subject. Human components make up the lion's share of security breaches. Concurring to inquire about cyber security by hacking workers, data security depends on three basic establishments: individuals, firms, and innovation. Analysts and specialists. Different organizations refine their strategy and Advanced innovation. The weakest joins are still the human workforce within the prepare [1]–[4]. This puts you in setting the degree to which this survey applies. Cyber security is far-reaching due to social design issues. It impacts since the human individual is negligible. Not as it were for small and medium-sized undertakings but gigantic organizations [5].

Social manipulation tactics are rapidly growing and causing significant harm within the current framework of cybersecurity measures. It's important to engage with employees and provide education to safeguard sensitive information from cybercriminals [6]. Social power is close to this person's security Firewall encryption, encrypted system, and download antivirus system. Households may think humans compared to other humans malicious Activities that interact with humans make psychological people alive and dead Confidential information is secured and broken [7]. Because of this organizational aspect from the social aspect, engineering attacks are issued by their attacks. Programs or programs that train people to prevent these attacks. There are so many approaches to hacking the system without technical weaknesses [8].

For case, Equifax was hacked for a few months, and touchy client information was Compromised in 2018. This corporation operates as a service for handling customer credit reports and monitoring activities. It gathers data on individuals and businesses to oversee their credit records and predict instances of fraud. Due to the data breach, the attackers managed to gain access to the personal information of 145.5 million American consumers. This stolen data encompassed complete names, birthdates, Social Security

numbers (SSN), driver's license details, addresses, contact numbers, credit card particulars, and credit ratings. The breach originated from phishing attacks, where thousands of emails were sent, posing as financial institutions or major banks such as Bank of America [9].

An increasingly prevalent international cybercrime, which doesn't necessitate advanced technical skills but results in substantial financial losses, is Business Email Compromise (BEC). In the United States alone, approximately half of the reported losses to the FBI's Internet Crime Complaint Center (IC3) in 2019 – totaling an estimated USD 1.77 billion – were attributed to BEC activities. The COVID-19 pandemic in 2020 further accelerated the digital transformation of nations and led to a surge in malicious cybercrime. Exploiting the pandemic's circumstances to acquire personal information and credentials, cybercriminals gained access to systems which they subsequently leveraged for financial gain [10], [11]. The effect of cyberattacks on the basic framework isn't constrained to the fetched of the country's economy. It undermines open certainty in fundamental administrations and governments. Cyberattacks too disturb the solidness and solidness of nearby or worldwide financial frameworks and present One of the most critical concerns for national security, these incidents encompass some of the most severe instances of data breaches within the ASEAN region in the year 2020 are shown in figure 1 [10].

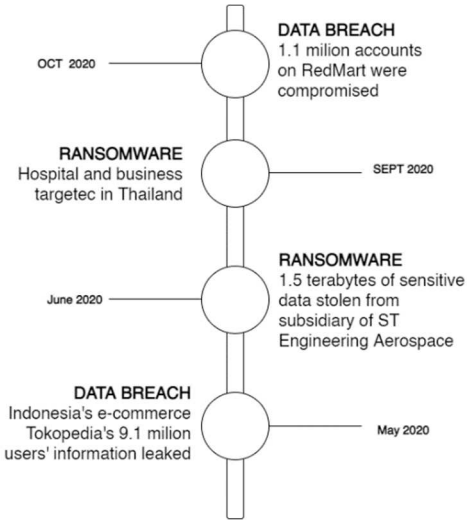

Fig. 1 Major incidents in ASEAN 2020 [10]

Also, the FBI has detailed an increment in CEO extortion. Mail trick in which an aggressor mimics his boss and emails a few workers inquiring questions Those that exchange cash. These companies misplaced more than $2.3 billion. Too, later inquire about ponders appear that 84% of cyberattacks are carried out by exceedingly effective social engineers [12], [13].

Email is one of the foremost common strategies of media transmission. Over 3.9 billion individuals have mail accounts, and collectively they send and get over 290 billion emails per day, counting trade emails and buyer emails. Tragically, a few emails are phishing tricks. A phishing mail is a mail that imagines being something it isn't to induce its beneficiary to require any activity that they something else wouldn't do. Phishing emails are as of now, causing impressive scale harm in society. Numerous current cybersecurity assaults have been followed back to phishing emails [14]–[19].

This paper provides in-depth research and findings on social engineering attacks. This paper provides an overview of the menu of prevention and mitigation techniques. Next, we will go and compare these techniques, create challenges and future directions, and increase employee awareness. Finally, we define the conclusion at the end.

II. Materials and Method

A. Information Security

Information Security is one area that is currently being intensively implemented in companies, so many are taking advantage of information security to maintain data or information in the company, making them look for easy and effective actions or solutions to ensure that all actions taken can improve the company value and optimize all existing processes. In its Implementation, every information security must be part of every process or procedure in every employee's job [20]–[24]. Information security could be a basic angle and plays a noteworthy part in ensuring an organization's trade. Organizations ought to secure their data and resources to maintain their esteem and notoriety. Besides, compelling data security administration requires best administration bolster and commitment in actualizing approaches and strategies[25], [26].

Data Security is "the assurance of data and its basic components, counting the frameworks and equipment that utilize, store, and transmit this data." This concept portrays a few methods to consider: privacy, astuteness, accessibility, known as "CIA TRIANGLE," and after that include precision, genuineness, utilize, and possession [27], [28].

B. Social Engineering

In the effort to combat cybercrime, we possess the CNCS (National Cyber Security Center) at the national level. Its purpose is to implement necessary measures and protocols to prevent, detect, respond to, and recover from situations that pose a threat to the functioning of government entities, critical infrastructure, and the national network. This organization is involved in addressing incidents and cyberattacks, as well as promoting a proactive approach by increasing awareness within cybersecurity organizations [29]. Social Engineering is a data or information theft technique essential and valuable for someone using focus social interactions. In other words, social engineering is a technique that exploits human attack weakness. Social engineering is divided into two: based on social and interaction-based interaction computer. In socially interaction-based type, attackers use excellent communication techniques to deceive the victim. Then on the computer-based interaction, attackers often use various methods such as phishing, Malicious advertising, and phone scams [30], [31]. The actions that often occur with social engineering are phishing, spear phishing, baiting, malware, pretexting, and phishing. Social engineering attacks are different, but they share a familiar pattern. Similar phase. The general pattern has four phases: (1) The collection of information about the target. (2) Build a relationship with the target. (3) Use the available information to carry out an attack. (4) Exit without tracing [32], [33].

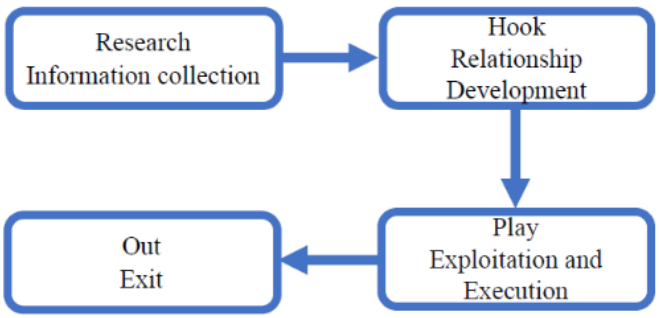

Fig. 2 Social engineering attack stage [34]

Experts have published several reviews in recent years, of course. Each of these thoughts provides a new perspective for understanding phishing and what can be used to anticipate it. The first point of view in carrying out the half breed phishing location approach was conducted by Zuhair et al. [35]. In addition, Varshney et al. [36], [37] conduct research, conduct reviews, classify the most important and new methods proposed on phishing websites detection, and monitor its advantages and disadvantages. In addition, Gupta et al. [36] give a phishing attack review to look at phishing assaults in profundity, past phishing assaults, and assault thought processes culprit.

Phishing emails are focused on emails where social engineers draw the beneficiary into performing particular activities such as clicking on a noxious interface, opening a malevolent connection, or going to a web page and entering their data [38], [39].

Individuals using the internet, financial institutions, governmental bodies, and businesses frequently encounter phishing attacks from various angles. These attacks involve exposing victims' private data, leading to significant financial harm. Phishing attacks have the potential to tarnish one's perception of online interactions and erode trust in the internet. As trust is compromised, users might shy away from online banking, digital shopping, and e-commerce activities. Moreover, a business impacted by a phishing attack could suffer from diminished customer trust, reputational damage, a decline in brand worth, and decreased stock value [40], [41].

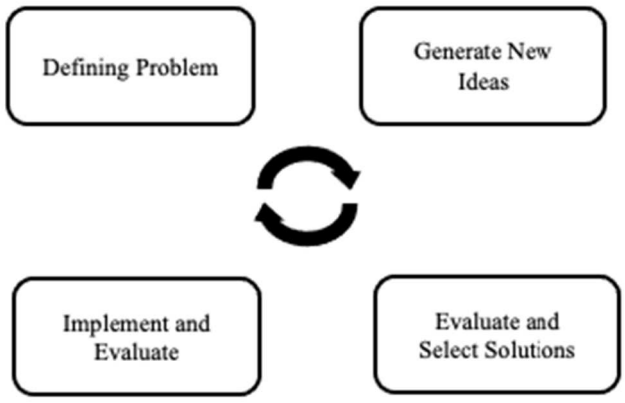

Fig. 3 Research framework (authors)

This section will explain the methodology that we use to support the research. The methodology that we are using is the problem and solving approach. Problem and solving is action and characterizing an issue; deciding the cause of the issue; recognizing, prioritizing, and selecting options for an arrangement; and executing an arrangement. But the scope of this research only discusses defining a problem, generating new ideas, evaluate and selecting solutions. Below is the explanation of each stage in the problem-solving methodology.

C. Defining a Problem

Stage 1, we define the problem by identifying an example of a case in one of the multinational companies in Singapore. Of course, we need to know the cause at the initial stage. Then, we will categorize how many attacks and the effects of this phishing email. So that at the initial stage, we can find out in detail the cases that occurred along with possible incidents.

After identifying the case, we need to identify the factor that might cause this email phishing in the company. We specify the factors into 2: internal factors and external factors. Internal sources come from employee negligence, misuse of data, etc.

Last, we identified the risk that the company will experience or already experience after this email phishing attack. Risk identification is to understand what is at risk within the context. Risk identification involves the identifying and classifying sources of a risk to determine what must be managed in a construction project. Risk identification is the initial step of the risk management process, as the potential problems must be identified before assessing, responding, and controlling the risk.

D. Generating New Idea

Exploring various possibilities can greatly enhance the value of your ideal strategy. Once you've opted for the vision of "what should be," this desired benchmark becomes the foundation for crafting a roadmap to explore alternatives. Methods such as brainstorming and collaborative problem-solving are valuable tools within this problem-solving framework.

Before reaching a final conclusion, several alternative solutions to the issue should be generated. A pitfall in problem-solving lies in evaluating options as they are proposed, often settling for the first acceptable solution even if it's not the most optimal. By fixating solely on achieving desired outcomes, we overlook the potential to acquire novel insights that could lead to meaningful changes in the problem-solving process.

E. Evaluate and Selecting Solutions

We evaluate and select solutions based on identifying cases that are appropriate for the company at this stage. Of course, finding a problem solver requires consideration and alternative selection options that can be said to match the existing problem. We consider to what extent it can be used and solve problems without creating new problems. Of course, in its Implementation, it is necessary to consider the policies and standards that apply in the company.

F. Implemet and Evaluate

This stage will describe the implementation and evaluation steps that need to be carried out. In this case, the company, especially the leadership, will provide clear and precise directions to provide the best solution for the company. In this

case, all parties must actively contribute to supporting changes for the better and minimize the risks that may occur when Implementation occurs. This stage is in the form of integration with each other which are interconnected and need to be monitored regularly and tested for validity and effectiveness and ensure that the chosen technique is by existing conditions. The stage will have a positive impact on future changes.

III. Results and Discussion

A. Defining a Problem

Phishing is global, and tracking down and prosecuting the criminals who testify behind it is difficult. On the other hand, the methods I used work like this: the attacker also started forming a network in which someone else would make the attack [42]. Phishing is not a new cyber threat and will not diminish. Instead, the most common cyber threats of credential theft are focused on other forms of cybercrime, such as data breaches. The reported count of identified phishing incidents during the second quarter of 2020 stands at 14,694.8. The most fraudulent target is a SaaS, accounting for over 35%, and the social media segment increased by 20%. The main factor is attacks such as Facebook and WhatsApp [10].

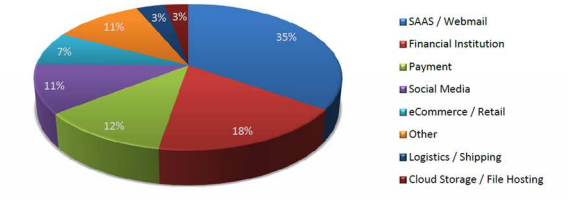

Fig. 4 Targeted industries, the second quarter of 2020 (APWG Phishing Activity Trends Report) [10]

We take an example from a multinational company in Singapore that has experienced this email phishing. The attacker pretends to be the company's CEO and emails the employees, especially the ERP sales department.

Fig. 5 Example email phishing

The above figure 5 is an example of the email that the attacker is pretending to be the CEO. In this case, Hayden Knights are the CEO, but when we see the attacker is using is sondraharris@optonline.net. At the same time, the correct email for the CEO is hayden@poins-technology.com. The email for the employee on the company uses the company's domain, which is employeename@poins-technology.com.

Hayden Knights <sondraharris@optonline.com> Hi Karthikeyan, Good Morning to you, Let me know if you are available for an errand right now. I am available via email. Thanks.
Karthikeyan <karthik@poins-technology.com> Good morning, Hayden. Sure. Let me know what I should do.
Hayden Knights <sondraharris@optonline.com> OK Good, I need you to get me some gift cards from the store either (7eleven, ZOOM, K Circle, Apple Store or any other closer stores), can you arrange that now? So that I can tell you product and denomination required. Thanks

Fig. 6 Email phishing conversation

Based on the email conversation above, the attacker plays a role as the company's CEO. The attacker is asking about the availability of the employee for an errand. Because the employee saw the CEO's email, he replied that he could do it. Then the attacker asks the employee to get some gift cards from the store. The request that the attacker sends to the employee is extraordinary because it is not a daily activity that he is doing in the office. By right, the employee should sell the system.

B. Generating New Idea

All new complex phishing attacks are being developed time attacks, and phishing increases every year. Organizations need to educate themselves and learn computer security strategies and skills to reduce phishing threats with the individual. Most people these days depend on mobile devices like smartphones and tablets in their daily lives and have become scammers. Opportunity to profit from technical systems. So, people need to Find out more about phishing. They take safety measures to avoid phishing threats. Advanced computer users' knowledge increases user confidence in implementing relevant actions to prevent phishing threats. No education.

Increase security awareness. We will avoid user security threats. He looks people need to improve their knowledge of phishing. Young people between 18 and 44 are more likely to be trolled than the elderly. Few Phishing attempts are suspicious because they tend to trust IT security. Take self-defense measures. Unlike 50 years, Seniors and seniors have initial phishing knowledge and personal experience. Being a victim of phishing scams makes you more careful [43].

C. Evaluate and Selecting Solutions

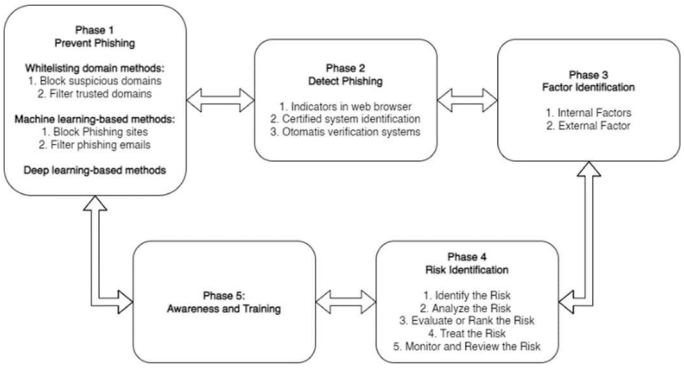

Fig. 7 Proposed solution (authors)

It takes some action to prevent it. In this case, the author defines it into 4 phases: prevent phishing, detect phishing, factor identification, and risk identification. Which is described in detail as follows.

- Phase 1: Prevent Phishing

You can stop phishing before it reaches your email or website by blocking or deleting suspicious emails. In this stage, we define three main methods, namely whitelist domains by blocking suspicious domains and filtering trusted domains. In addition, whitelist takes advantage of perimeter email security connected to billions of databases of malicious domains that are untrusted or commonly used by attackers so that every time an email comes in. It will be checked first by the email domain it is malicious or trusted. Still, the weakness of this method is if the attacker uses a new prayer. Then the perimeter email security doesn't recognize it because it's not in the database yet, so it's vulnerable to attacks. Machine learning-based and deep learning-based methods allow companies to access multiple emails to make the patterns learned even more accurate. Companies may use it to anticipate phishing attacks. The first step by looking at URLs websites for claim, this step can be manually or automatically by machine learning.It can capture some sites, but phishers are unlikely to capture all of them, as scammers can easily create new ones by simply removing a site. If it works, the method can be considered more effective as it prevents users from being exposed to links from phishing sites. Email servers use many effective spam filters, but phishing filters are rarely used due to their more complex nature. Search filters are also designed using machine learning techniques. Classifying Phishing Emails Using Randomly Set Machine Learning Techniques describes the functions used to classify phishing emails. Examples include URLs with mismatched IP addresses, "Href" attributes, link text, number of dots in domain names, domain name, email sender verification, etc [44]. There are also some simple keywords that the program will search for, such as "urgent", "update", "pause" and "commit"[44]. Their experimental results showed 99.7% accuracy, with the lowest false positive rate. About 0.06%. This process shows that this method is effective against phishing, as machine learning techniques can evolve as phishing attacks evolve [44].

- Phase 2: Detect Phishing

Attackers use sophisticated methods to identify potential phishing sites or evade malicious sites (or these sites) to ensure that phishing emails and websites reach vulnerable users [44]. Will do so. You will be asked to instruct the user (do not provide malicious information to emails or websites). Receive (and open) malicious emails. Many web browsers already have protection against phishing sites that use passive or active pointers. The active indicator displays a pop-up warning that the site is not considered rogue or secure, while the passive indicator. As expected, many users ignore it or, I'm not aware that passive and active indicators are more effective. However, some users trust that the site they are visiting is as expected because it was initially a trusted site [44]. Implementing a verification system on a trusted and secure site is helpful to counter this. If you look at the validation every time a user visits an actual website, you'll notice that fake websites don't have this validation. Providing certified identifiers and brands is eye-catching and helps ensure that users are in the right place.

- Phase 3: Factor Identification

We specify the factors based on the internal factors and external factors. Internal factors can be caused by the employee, and the external factors

1. Internal Factors
   The employee behavior and characteristics might be the factor in the leader becoming an email phishing victim, such as naivete, stress, unfocused, carelessness, ignorance, compassion, credulity, etc. In this case, only salespeople were affected because their job is selling and might share their contact or email to external.
2. External factors
   Deliberate actions of the company's business competitors Deliberate actions of unknown people and hoping to benefit from phishing carried out in the form of money or work from irresponsible people

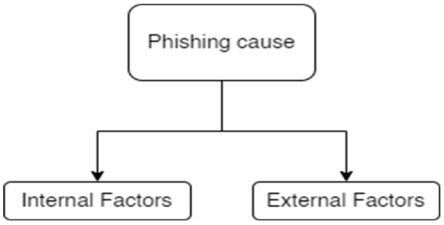

Fig. 8 Phishing cause factor

- Phase 4: Risk Identification

Risk assessment is the process of assessing how often a risk occurs or how significant the impact of a risk is. The fundamental aim of performing a risk analysis is to gauge the repercussions of a potential threat and ascertain the extent of the business's potential loss. The main results of the risk analysis are risk identification and the number of costs compared to the benefits to mitigate the risk of damage [44]. The initial stage is to assess the existing risks that can be seen from a business perspective or their impact on the company. After all the initial stages have been identified, it is time to provide possible mitigation steps to ensure that the risk can reduce the risk. This action is in the form of controls recommendations and priority steps to protect. Risk evaluation is used to maintain the continuity of the process to ensure that every action taken is appropriate. Usually, the company will look at the application, hardware, and other supporting factors.

- Phase 5: Awareness and training

This study offers insights into the significance of fostering awareness and delivering training on social engineering, which stands out as one of the most impactful strategies for minimizing the vulnerability to attacks. This solution can be by giving a relatively short training of about 3-5 minutes, by giving several tasks that they might do without disturbing their preparatory work. In addition, this tactic has also been used by the American Psychological Association, making it easy for them to ensure the security of data and email in the company. We also need to ensure that the division of roles is clearly and regularly defined. Ensuring that every procedure runs in harmony and is monitored. Awareness of users needs to be increased so that they do not fall into the trap of phishing. This phase is the leading solution discussed in detail in generating new ideas. Previous researchers have widely discussed this awareness. Many phishing training of the year large-scale is not against the present. In addition, more sophisticated phishing attacks depend on already participating users. In most cases, email phishing warnings or documentation will not work correctly. The user has a condition to ignore. I think they know emails like that how to protect yourself. Anti-phishing

solutions, such as creating quizzes or assessments that recap every month or using fun methods such as game creation or training system mail server, are recommended. Information Security Awareness (ISA) refers to a condition of consciousness where users are ideally dedicated to adhering to regulations, acknowledging potential risks, grasping the significance of their duties, and subsequently behaving in alignment with these principles. Despite the prevalence of information security breaches, particularly within knowledge-oriented establishments due to users not adhering to security protocols, it is imperative to implement proactive measures to preempt any adverse repercussions [21]. Therefore, the competent authorities or the commercial sector must follow appropriate principles to protect their privacy. These are data subject disclosure and approval processes, data subject explanation and notification purposes, data management and control, transparency and completeness of information, and preventing misunderstanding and misuse. Therefore, the existence of a network infrastructure for communication is very important, and the existence of a computer network is a standard set for the purpose of citizen satisfaction.

Raising public awareness involves creating private and public message campaigns about specific issues. This is an important part of developing community support for change in the informal and formal sectors to change knowledge and attitudes about certain aspects to be achieved based on needs and goals. and strategy. Therefore, security policies should be prioritized over other measures that address business processes and functional limitations in providing data services to customers.

D. Implement and Follow Up Solutions

Phishing is becoming more complicated to spot as a Cyber security expert. Meanwhile, phishing is more complex for attackers. Recent improvements in online security are universal. Phishing has become a more complicated victim of the new attack power. It is difficult for ordinary people to distinguish phishing activity from ordinary activity. We, large scale Phishing measure countermeasures integrate the proposed anti-phishing solution framework described in the previous section on servers of email providers such as Gmail, Yahoo, and Hotmail. The result is even people with no computer experience. The phishing risk is still protected at the main level. It will also be more efficient if the server is included in the Training system email service. Users get more education on how to protect the future. A very conscious community of users makes it difficult for scammers to launch successful attacks. Effective strategies for preventing phishing incidents are identified by conducting interviews with experts to impart knowledge to users. Specific safeguards to evade attacks and practical measures are deemed beneficial and contribute to enhancing the company's security. In this case, employees need to anticipate attacks, where employees need to check the personal data of the email sender such as information where they are placed, or their direct work, pay attention to the address/attachment contained in the email, check if they have the latest updates such as antivirus or other, it is necessary to identify advertisements. Misleading emails and then identifying potentially false data about themselves. Simultaneously, as a precautionary step following an attack, such as interacting with a suspicious link or opening an unfamiliar attachment, participants will modify their login information, initiate an antivirus scan, and enable the computer's Ethernet connection. The majority of respondents emphasized that receiving training should be considered a protective measure against phishing emails. In addition, other measures such as ensuring that security procedures are in place and that ISO 27001, NIST, or CIS policies and standards are fully implemented in the company.

Companies also need a security operations center (SOC) connected to their network or critical components to support IT security. SOC can be divided into two teams known as blue and red teams. In this context, the term "red team" refers to a collective acting in the role of an adversary or rival, offering security insights from this vantage point. On the other hand, the "blue team" comprises individuals tasked with scrutinizing information systems to ensure their security. They pinpoint vulnerabilities, assess the efficacy of each security measure, and ensure that it remains effective post-implementation. The Security Operations Center (SOC) aims to detect, analyze, and respond to cybersecurity incidents through a blend of comprehensive organizational solutions and technological procedures.

IV. CONCLUSION

The latest trend addresses a number of potential threats, such as phishing emails, which cause enormous and even financial damage to businesses. Despite implementing various preventive measures, the currently employed methods have not demonstrated their efficacy in countering this particular menace. Conversely, instances of phishing emails have surged dramatically. To tackle this escalating threat of phishing emails, there is a pressing need for more advanced and sophisticated phishing detection technology. The development of anti-phishing technology necessitates categorizing email phishing, factoring in its reliance on third-party services. Existing email content requires appropriate and quick action. Beyond technology, each employee's need for knowledge and curiosity about the dangers of phishing is a shared responsibility. Training or action training can help anticipate or as a means of early detection. Making sure there is a remedy is better than having to fix it. We need to realize that every action and behavior will affect the outcome, especially every decision making and accountability.

REFERENCES

[1] B. Cao, J. Zhao, Y. Gu, S. Fan, and P. Yang, "Security-Aware Industrial Wireless Sensor Network Deployment Optimization," *IEEE Trans. Ind. Informatics*, vol. 16, no. 8, pp. 5309–5316, 2020, doi: 10.1109/TII.2019.2961340.

[2] A. A. Al Shamsi, "Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE Effectiveness of Cyber Security Awareness Program for young children View project Sentiment Analysis for Arabic Dialects View project Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE," *Int. J. Inf. Technol. Lang. Stud.*, vol. 3, no. 2, pp. 8–29, 2019, doi: 10.13140/RG.2.2.28488.14083.

[3] M. Sas, G. Reniers, K. Ponnet, and W. Hardyns, "The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour," *Saf. Sci.*, vol. 144, p. 105447, 2021, doi: 10.1016/j.ssci.2021.105447.

[4] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and Information Security

Awareness," *Comput. Secur.*, vol. 88, p. 101640, 2020, doi: 10.1016/j.cose.2019.101640.
[5] H. Aldawood and G. Skinner, "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review," *Proc. 2018 IEEE Int. Conf. Teaching, Assessment, Learn. Eng. TALE 2018*, no. December, pp. 62–68, 2019, doi: 10.1109/TALE.2018.8615162.
[6] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Futur. Internet*, vol. 11, no. 4, 2019, doi: 10.3390/FI11040089.
[7] N. N. Pokrovskaia and S. O. Snisarenko, "Social engineering and digital technologies for the security of the social capital' development," *Proc. 2017 Int. Conf. "Quality Manag. Transp. Inf. Secur. Inf. Technol. IT QM IS 2017*, pp. 16–18, 2017, doi: 10.1109/ITMQIS.2017.8085750.
[8] A. M. Aroyo, F. Rea, G. Sandini, and A. Sciutti, "Trust and Social Engineering in Human Robot Interaction: Will a Robot Make You Disclose Sensitive Information, Conform to Its Recommendations or Gamble?," *IEEE Robot. Autom. Lett.*, vol. 3, no. 4, pp. 3701–3708, 2018, doi: 10.1109/LRA.2018.2856272.
[9] M. Chargo, "You've Been Hacked: How to Better Incentivize Corporations to Protect Consumers' Data Michael," *Tennessee J. Bus. Law*, vol. 20, pp. 6–23, 2004.
[10] J. Tan, W. X. Tee, A. Parsons, and A. Radlett, "Asean cyberthreat assessment 2021," *Interpol*, p. 5, 2021, [Online]. Available: https://www.interpol.int/content/download/16106/file/ASEAN Cyberthreat Assessment 2021 - final.pdf.
[11] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 82–97, Jan. 2022, doi: 10.1080/08874417.2020.1712269.
[12] G. Costantino, A. La Marra, F. Martinelli, and I. Matteucci, "CANDY: A social engineering attack to leak information from infotainment system," *IEEE Veh. Technol. Conf.*, vol. 2018-June, pp. 1–5, 2018, doi: 10.1109/VTCSpring.2018.8417879.
[13] A. Birajdar and T. N. N., "APPEARS Framework for evaluating Gamified Cyber Security Awareness Training," in *2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS)*, 2022, pp. 1–8, doi: 10.1109/IC3SIS54991.2022.9885399.
[14] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *J. Big Data*, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00318-5.
[15] A. Ključnikov, L. Mura, and D. Sklenár, "Information security management in smes: Factors of success," *Entrep. Sustain. Issues*, vol. 6, no. 4, pp. 2081–2094, 2019, doi: 10.9770/jesi.2019.6.4(37).
[16] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Comput. Secur.*, vol. 106, p. 102267, 2021, doi: 10.1016/j.cose.2021.102267.
[17] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: Systematic review," *Comput. Secur.*, vol. 99, p. 102030, 2020, doi: 10.1016/j.cose.2020.102030.
[18] B. Ghimire and D. B. Rawat, "Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8229–8249, 2022, doi: 10.1109/JIOT.2022.3150363.
[19] A. Corallo, M. Lazoi, and M. Lezzi, "Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts," *Comput. Ind.*, vol. 114, p. 103165, 2020, doi: 10.1016/j.compind.2019.103165.
[20] A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterp. Inf. Syst.*, vol. 16, no. 4, pp. 527–565, Apr. 2022, doi: 10.1080/17517575.2021.1896786.
[21] Y. A. Alsariera, V. E. Adeyemo, A. O. Balogun, and A. K. Alazzawi, "AI Meta-Learners and Extra-Trees Algorithm for the Detection of Phishing Websites," *IEEE Access*, vol. 8, pp. 142532–142542, 2020, doi: 10.1109/ACCESS.2020.3013699.
[22] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Front. Comput. Sci.*, vol. 3, no. March, pp. 1–23, 2021, doi: 10.3389/fcomp.2021.563060.
[23] R. Alabdan, "Phishing attacks survey: Types, vectors, and technical approaches," *Futur. Internet*, vol. 12, no. 10, pp. 1–39, 2020, doi: 10.3390/fi12100168.
[24] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommun. Syst.*, vol. 76, no. 1, pp. 139–154, 2021, doi: 10.1007/s11235-020-00733-2.
[25] R. Wash, "How Experts Detect Phishing Scam Emails," *Proc. ACM Human-Computer Interact.*, vol. 4, no. CSCW2, 2020, doi: 10.1145/3415231.
[26] J. Wu *et al.*, "Who Are the Phishers? Phishing Scam Detection on Ethereum via Network Embedding," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 52, no. 2, pp. 1156–1166, 2022, doi: 10.1109/TSMC.2020.3016821.
[27] G. Egozi, "Phishing Email Detection Using Robust NLP Techniques," *2018 IEEE Int. Conf. Data Min. Work.*, pp. 7–12, 2018, doi: 10.1109/ICDMW.2018.00009.
[28] P. Xia *et al.*, "Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange," *Proc. ACM Meas. Anal. Comput. Syst.*, vol. 5, no. 3, 2021, doi: 10.1145/3491051.
[29] M. A. Mendoza, "Cibersegurança ou segurança da informação? Explicando a diferença," 2017. https://www.welivesecurity.com/br/2017/01/17/ciberseguranca-ou-seguranca-da-informacao/.
[30] H. Ahmadian and A. Sabri, "Teknik Penyerangan Phishing Pada Social," vol. 2, no. 1, 2021.
[31] C. M. R. da Silva, E. L. Feitosa, and V. C. Garcia, "Heuristic-based strategy for Phishing prediction: A survey of URL-based approach," *Comput. Secur.*, vol. 88, p. 101613, 2020, doi: 10.1016/j.cose.2019.101613.
[32] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," *Comput. Secur.*, vol. 59, pp. 186–209, 2016, doi: 10.1016/j.cose.2016.03.004.
[33] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process," *IEEE Access*, vol. 9, pp. 44928–44949, 2021, doi: 10.1109/ACCESS.2021.3066383.
[34] P. L. Gallegos-Segovia, P. E. Vintimilla-Tapia, J. F. Bravo-Torres, I. F. Yuquilima-Albarado, V. M. Larios-Rosillo, and J. D. Jara-Saltos, "Social engineering as an attack vector for ransomware," *2017 Chil. Conf. Electr. Electron. Eng. Inf. Commun. Technol. CHILECON 2017 - Proc.*, vol. 2017-Janua, pp. 1–6, 2017, doi: 10.1109/CHILECON.2017.8229528.
[35] Zuhair, Hiba & Selamat, Ali & Salleh, Mazleena. (2016). Feature selection for phishing detection: A review of research. International Journal of Intelligent Systems Technologies and Applications. 15. 147. 10.1504/IJISTA.2016.076495.
[36] G. Varshney, M. Misra, and P. K. Atrey, "A survey and classi fi cation of web phishing detection schemes," 2016, doi: 10.1002/sec.
[37] S. Salloum, T. Gaber, S. Vadera, and K. Shaalan, "Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey," *Procedia Comput. Sci.*, vol. 189, pp. 19–28, 2021, doi: https://doi.org/10.1016/j.procs.2021.05.077.
[38] T. Lin *et al.*, "Susceptibility to Spear-Phishing Emails," *ACM Trans. Comput. Interact.*, vol. 26, no. 5, pp. 1–28, 2019, doi: 10.1145/3336141.
[39] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions," *SN Comput. Sci.*, vol. 2, no. 3, pp. 1–18, 2021, doi: 10.1007/s42979-021-00557-0.
[40] A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterp. Inf. Syst.*, vol. 00, no. 00, pp. 1–39, 2021, doi: 10.1080/17517575.2021.1896786.
[41] X. Chen, X. Liu, L. Zhang, and C. Tang, "Optimal Defense Strategy Selection for Spear-Phishing Attack Based on a Multistage Signaling Game," *IEEE Access*, vol. 7, pp. 19907–19921, 2019, doi: 10.1109/ACCESS.2019.2897724.
[42] I. Vayansky and S. Kumar, "Phishing – challenges and solutions," *Comput. Fraud Secur.*, vol. 2018, no. 1, pp. 15–20, 2018, doi: 10.1016/S1361-3723(18)30007-1.
[43] N. Farhana, M. Zaharon, and M. M. Ali, "Factors Affecting Awareness of Phishing Among Generation Y," *Asia-Pacific Manag. Account. J.*, no. April 2021, 2021, [Online]. Available: https://ir.uitm.edu.my/id/eprint/2861/.
[44] S. S. Lin, S. L. Shen, A. Zhou, and Y. S. Xu, "Risk Assessment and Management of Excavation System Based On Fuzzy Set Theory and Machine Learning Methods," *Autom. Constr.*, vol. 122, no. November 2020, p. 103490, 2021, doi: 10.1016/j.autcon.2020.103490.