Received:28 March 2025 | Revised: 14 April 2025 | Accepted: 28 April 2025
DOI: 10.62460/IJEASS/2025.031

REVIEW ARTICLE

Interdisciplinary Journal of Emerging and Social Sciences

A Model-Based Framework for Detecting and Preventing Phishing Attacks in Organizations using a GRC Approach

Fahim-ullah-Hisbani[1] and Asia Soomro[2]

[1]Department of Information Technology, Mehran University of Engineering and Technology, Jamshoro

[2]Department of Data Analysis, Mehran University of Engineering and Technology, Jamshoro

Correspondence:
fahim.hisbani888@gmail.com

Abstract

This study presents a new framework for detecting and preventing phishing attacks in organizations using a Governance, Risk, and Compliance (GRC) approach. The research looks at why phishing attacks succeed and proposes a three-layer defense system: Governance (creating anti-phishing policies), Risk Management (identifying vulnerable assets and people), and Compliance (tracking prevention efforts and reporting incidents). Unlike earlier models, the framework focuses on organizational policy development and employee vulnerability assessment alongside technical solutions. Using a design science approach, we developed this framework to help organizations build an anti-phishing culture that combines human awareness with technological protection.

KEYWORDS

Phishing detection; Cyber security framework; Social engineering; GRC model; Organizational security; Security policy; Risk assessment; Compliance monitoring

1 | INTRODUCTION

Nowadays, when everything is connected to the internet, new technologies have made security problems worse. Attacks using social engineering weaken the security of networks or systems and take over the system. Scammers fake a link in order to get private information like credit card numbers, user data, or login passwords. When people click on links they don't know or trust, they can be victims of social engineering scams like phishing. It could cost money, cause data loss, or reveal details about the system. People who are scammed don't know it's phishing until they click on links in a real phishing email that are harmful and compromise their computer or system's security. A lot of people send these kinds of links through email scams. The attacks happen when people aren't aware of phishing tactics, frameworks, and ways to stop them. It makes it more likely that phishing will work. In December 2024, more than 300,000 phishing attempts were recorded, according to the Phishing Activity Trends Report (2024) from APWG. Op Sec Security, a founding member of the APWG, told the group about the threats in different areas.

Many types of attacks happen in every industry and cost people and companies' money and damage their reputation (Deloitte, 2019). Attacks of social engineering are not sufficiently prevented. Current preventive strategies consist of campaigns, user-centric models, and user vulnerability models. Preventive efforts mostly center on persons, including themselves, in security sensor systems. It has to investigate cybersecurity under the direction of rules or acts for safe systems. Many models are suggested to stop these attacks. These models build on several approaches and distinct frameworks of social engineering attacks. Phishing has grown to be a serious problem in recent years, thanks to increased internet access. Attacks reveal patterns of demands for change in sensitive information, and login credentials are the most often used method to obtain data.

These demands come via emails, social media, games, SMS, and many more; inexperience with such attacks and carelessness raise the exposure to attacks. Phishing campaigns succeed primarily because of their more realistic and subtle means of persuading consumers to click the link. Fake emails fool the victims regarding personal information on usernames, passwords, etc. Phishing assaults seem to be honest and reasonable; hence, anyone might be a victim of them. Notwithstanding sophisticated anti-phishing methods, several elements contribute to the success of phishing attempts. This research addresses

the elements together with current models to investigate phishing methods in order to help in more successful prevention of future assaults. No matter how many firewalls, encryption, two-factor authentication, or phishing prevention measures a company has in place, if the person behind the keyboard falls for a phish, the organization will be hacked. Attackers employ convincing messages to get victims to divulge personal data or install dangerous programs on their machines.

Scammers create these emails in such a way as to pass for messages from a reputable source. Phishers target individuals instead of the systems since humans are regarded as the weakest link. Phishing delivers convincing messages using several methods, now including VOIP, SMS, instant messaging, social networking sites, multiplayer games, and email. Phishing attacks are becoming more regular and complicated by nature. Criminals also utilize "spear phishing," sending mass emails aimed at certain targets utilizing relevant contextual information in an attempt to attract more victims. Targeting top-level C executives, including CISOs, CTOs, CFO, or board members, whaling is another focused phishing attack. Aside from cloned web portals, attackers target two-factor authentication by cloning one-time passwords and creating a fake QR code, which may offer several discounts at grocery stores and home services stores in exchange for online payment. When scanned, it goes into the attacker's accounts.

Cyber criminals have also improved their techniques. (Bhardwaj and associates, 2020). Phishing is seriously compromising sensitive information, intellectual property, customer data, state secrets, and identity theft. On the surface, these attacks seem like a sort of spam. Phishing emails from hackers posing as hardware makers cost Google and Facebook more than $100 million in 2017. Fighting phishing attempts that try to profit from human errors is difficult since they take advantage of human errors. The restrictions on phishing reduction strategies have caused security failures in many enterprises, including reputable information security firms. Considering phishing as a primary concern for most businesses worldwide, it is crucial to know why phishing assaults are successful at the user level despite technological measures put in place (Khonji, Iraqi, and Jones, 2013a).

Following a conceptual model helps an organization create an anti-phishing culture for prevention and detection. The Phish Tank claims that phishing, usually conducted via email, is a fraudulent effort meant to obtain your personal data. Learning how to identify a phish will help you avoid phishing entirely. “Phishing is a sort of cybercrime when an individual impersonating a legitimate company solicits sensitive information from a target or targets through email, phone, or text message, aiming to get personally identifiable information, banking details, credit card information, and passwords. KnowBe4, 2021: “Phishing occurs when attackers endeavor to deceive users into performing erroneous actions, such as clicking a malicious link that downloads malware or redirecting them to a fraudulent website.” NCSC, 2018.

2. Literature Review

As Andress (2019) says, phishing is a type of social engineering attack that is used to get people to give up personal information or attack the system to fix bugs on the target system. Malicious actors disseminate harmful links through email, and clicking these links sends the user to a counterfeit website. These kinds of websites are made to get private information about people who visit them. These sites generally resemble reputable websites, like banking or social media platforms. All are identical to the official website of the targeted organization. Some contain content with substandard grammar and inappropriate domain names, while others may be exceedingly challenging to differentiate from authentic websites. To enhance the success rate, phishing assaults are often disseminated.

Numerous recipients get emails from phishers targeting specific corporations or organizations simultaneously, hence enhancing the likelihood of a greater success rate. Phishing is characterized by McAlaney and Hills (2020) as a social engineering tactic or a threat that poses a risk to cybersecurity. They assert that the expression of urgency or threat in emails or messages compels victims to respond promptly. Shaikh et al. (2017) characterize phishing as a significant cyber threat that exploits social engineering and technology to access internet users' financial information, resulting in billions of dollars in losses. Both definitions outlined above encompass email phishing techniques and their impact on victims.

However, this is not a comprehensive definition of phishing, as it encompasses several tactics such as email, messaging, and voice communication. Furthermore, some aspects of the criterion directly relate to the tactics utilized in email phishing. Khonji et al. (2013) define phishing as a form of cyber-attack that employs socially engineered communications transmitted through electronic communication channels to manipulate individuals into taking activities advantageous to the attacker. The definition delineates phishing as it pertains to electronic communication mediums, such as emails, texts, or websites.

3. Challenges of Phishing

Phishers have become more adept at creating forged websites that look identical to the intended destination, and have begun to include logos and

graphics in their phishing emails to make them appear more legitimate. Many hazardous, new, sophisticated phishing tactics use publicly accessible personal information to create credible and believable attempts that target victims directly. Social phishing and context-aware phishing are two types of assaults that take advantage of the vast quantity of publicly available data to make their schemes more effective. According to one study, victims are 4.5 times more likely to fall for a phishing effort if it comes from a close acquaintance or someone who knows them personally.(Vayansky and Kumar, 2018a)

To create a targeted campaign, spear-phishing requires some knowledge about the victims – their banking details, where they work, what sites they've recently bought from – and most of this information can be easily acquired by browsing profiles, blogs, and other websites. Some phishing attempts include malware such as worms or trojans in the emails they send, compromising the victim's computer security and providing another tool from which they may pick victims and launch attacks. Phishers have also begun to construct a psychology that plays on urgency, greed, or trust in their emails, when the fake websites have a real appearance and feel, even the most cautious and alert individuals might fall prey to their attacks.(Vayansky and Kumar, 2018a).By its very nature, phishing is widespread: the Anti-Phishing Working Group (APWG) discovered over 90,000 distinct phishing emails and over 130,000 unique phishing websites in the fourth quarter of 2009.

Because of a paucity of data from banks and other financial institutions, estimates for yearly monetary losses related to phishing range from $100 million to $3 billion for victims in the United States alone. Financial and financial services are the target of the majority of assaults, accounting for about 93 percent of all recorded attacks. (Vayansky and Kumar, 2018a). Phishing impacts individuals all around the world and is carried out on a worldwide scale, making it difficult to trace down and prosecute the perpetrators. Phishers have utilized a method known as 'rapid flux,' in which they use a wide pool of proxies and URLs to hide the real address of the phishing site. This makes it more difficult to ban the site, and it takes longer to locate the server. The attackers have also begun to create networks in which a separate individual carries out each component of the assault.

For example, someone skilled at creating forged websites may create a toolkit for other phishers to utilize, needing them simply to choose a site to duplicate and where to transmit the information. Users of the tools would then merely have to select victims and send emails. Surprisingly, up to a third of these toolkits would actually transport the stolen information to another location. In this approach, the creator of the tool has effectively hired unskilled phishers to perform all the effort, bear the blame, and gain no benefits. The genuine phisher would be able to avoid detection in this manner. (Vayansky and Kumar,2018a).

4. Theoretical Framework

This research grounds its GRC model for phishing prevention in Situational Crime Prevention Theory (Clarke, 1997), which argues that reducing opportunities for crime is more effective than addressing offender motivations. Applied to cybersecurity, this theory supports our multi-layered defence approach by increasing perceived effort (governance policies), increasing perceived risks (compliance monitoring), and reducing anticipated rewards (risk management). Additionally, Routine Activity Theory explains how phishing succeeds when motivated attackers encounter vulnerable targets in the absence of capable guardians, directly informing our framework's emphasis on identifying vulnerable assets and implementing protective controls. The Social Engineering Attack Framework (Mouton et al., 2016) explicitly addresses the psychological manipulation aspects of phishing, providing theoretical support for our approach to employee vulnerability assessment and training within the risk management layer. Together, these theories create a comprehensive foundation for understanding and combating phishing attacks at technical, organizational, and human levels.

5. Research Objectives:

- To understand the factors that are being used in phishing attacks against people in an organization.
- To develop and propose a practical anti-phishing conceptual framework that can be used as a guideline for preventing and detecting phishing attacks at an organizational level.

6. MATERIAL AND METHOD

This study employs a design science research (DSR) approach, as it is particularly well-suited for addressing complex organizational problems through the systematic creation and rigorous evaluation of innovative information technology artefacts, such as models and frameworks. Design science research emphasizes the development of prescriptive knowledge that not only advances theoretical understanding but also produces practical solutions capable of improving organizational performance (Peffers et al., 2007).

The choice of DSR is motivated by its iterative and problem-centric nature, enabling the research to move beyond descriptive and explanatory studies towards actionable solution design focused on real-world relevance and utility. This approach facilitates the

construction of a novel three-layered anti-phishing framework comprising Governance, Risk Management, and Compliance components that is intended to holistically address phishing vulnerabilities at both technical and human dimensions within organizational settings.

The research process follows key DSR phases: (1) problem identification and motivation, where the rising incidence and impacts of phishing attacks are thoroughly analyzed to define research objectives; (2) artifact design and development, in which the framework is conceptualized and operationalized based on a synthesis of existing knowledge and empirical insights; (3) demonstration, through the application of the framework within organizational contexts to solve the targeted cyber security problems; (4) rigorous evaluation, employing qualitative and quantitative methods such as case studies, simulated phishing exercises, and compliance audits to assess the artifact's effectiveness, efficiency, and adaptability; and (5) communication of results to both academic and practitioner audiences, ensuring the utility and transferability of findings (Peffers et al., 2007).

By adhering to the principles of rigor and relevance, this DSR methodology provides a structured pathway to iteratively refine the framework based on feedback and empirical evidence, thus ensuring scientific rigor while addressing the practical complexities of phishing attack prevention. This alignment with the core goals of design science research positions the study to generate impactful, evidence-based solutions that contribute both to scholarly knowledge and to enhanced organizational cyber security resilience (Van Aken, 2004; March & Smith, 1995).

Fig 1 below shows that phishing attacks are most likely to happen in the financial sector (36.65%), then in SAAS/webmail providers (21.5%). (Information on Phishing Trends for 2024).

7. Related models

7.1. Hybrid Model for Phishing Detection and Loss Computation

The model provides a series of tactics to assist the C-suite in making policy-level choices and framing organizational security policies in order to reduce losses as a result of phishing attempts.(*Phishing Detection and Loss Computation Hybrid Model: A Machine-learning Approach*, 2017) Companies that are routinely targeted by phishing attempts can benefit from a hybrid model such as the one depicted in the picture below. The hybrid model is made up of three modules. They are as follows:(*Phishing Detection and Loss Computation Hybrid Model: A Machine-learning Approach*, 2017).The use of risk analysis can be used to determine the likelihood that a projected URL will lead to a phishing attempt.

7.2. Ike Vayansky and Sathish Kumar Model:

Propose that there are three ways in which the solution to phishing can be approached.

Ike Vayansky and Sathish Kumar claim that there exist three ways in which it is possible to fight phishing attacks. The user can intercept phishing before its activation by blacklisting or blocking phishing websites or by filtering phishing emails. The former is implemented by observing the URLs and the sites they purport to be, either by human examination or by

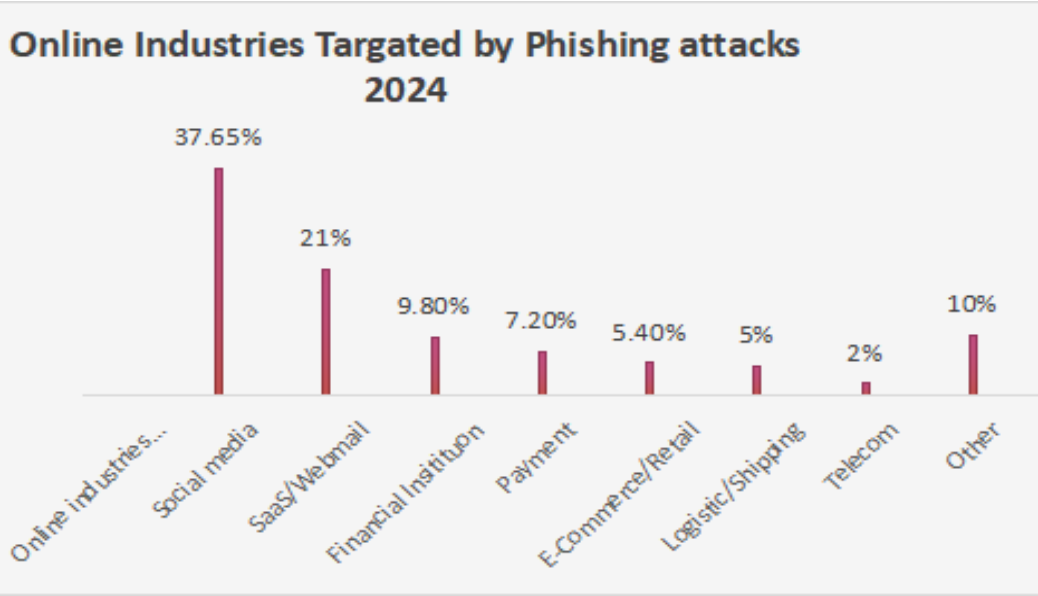

Fig. 1: Most targeted sectors of phishing attacks 2024.

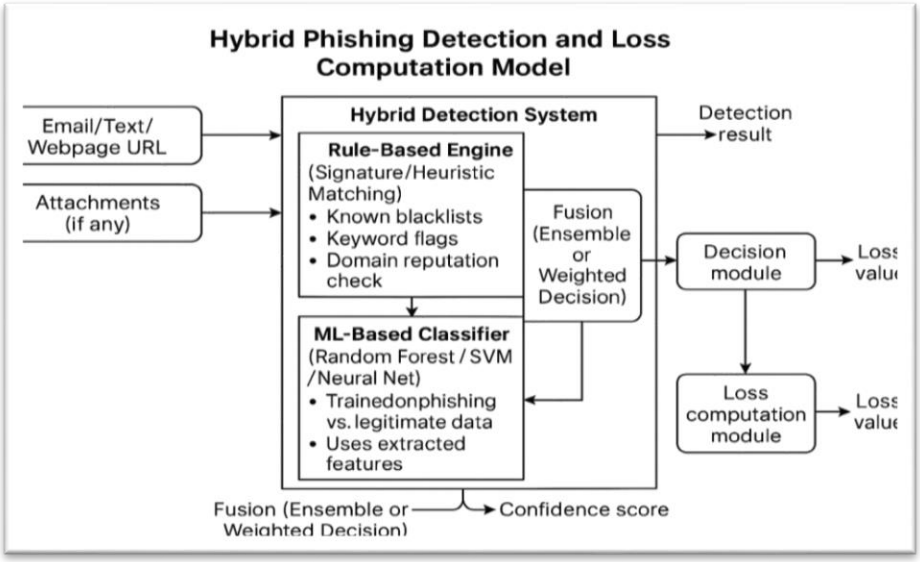

Fig. 2: Hybrid Phishing Detection and loss computation mode Adopted.

purely machine learning. To prevent phishing at the preventive level, that is, before it reaches the user, either blacklisting or blocking phishing websites or filtering phishing emails, it must be performed instantaneously. The first technique can be conducted either manually or automatically using machine learning algorithms and involves the process of assessing the URLs and the sites they purport to be associated with (Vayansky and Kumar, 2018a)It is possible to prevent phishing on the level of its prevention, i.e., prior to reaching the user, by blocking phishing websites, or by blocking phishing emails on their way to a user's email address. The former method can be done manually or automated with machine learning by analyzing the URLs and the websites they purport to represent, and is growing common. Most of the presently trainable generic phishing is general and fails to cover the more sophisticated types of phishing attacks; the training is also limited in that it requires the users to read and take the materials. Sending phishing warnings or education material via email is not effective in general because this has effectively trained most users to dismiss such mail and conclude that they know how to protect themselves in this case (Vayansky and Kumar, 2018c).

7.3. Proposed Model for Phishing Prevention and Detection

Governance, Risk, and Compliance as a Firewall for phishing prevention and detection in a company forms the foundation of the suggested approach. At the organizational level, this model can be utilized as a comprehensive guide to build anti-phishing culture and actions done for detection and prevention. Previous models lacked any justification for high-level anti-phishing rules and the classification and evaluation of assets, including the information assets and the people (which can be accomplished by means of social profiling). Furthermore, lacking in all the models discussed before is the risk-based approach offered by the GRC model.

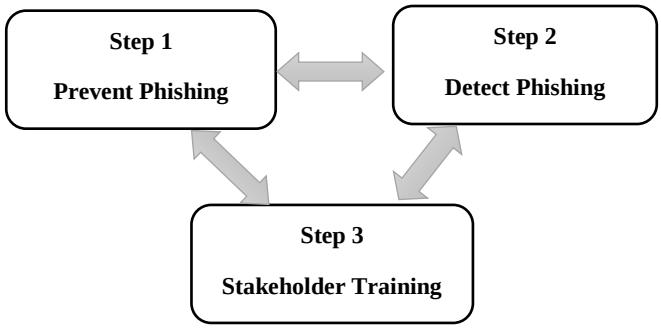

Fig. 3: Vayansky and Sathish Kumar Model:

According to literature, GRC is a system of people, processes, and technology that helps an organization to understand and prioritize stakeholder expectations; set business objectives that are consistent with values and risks; achieve objectives operating within legal, contractual, internal, social, and ethical constraints; provide relevant, reliable and timely information to suitable stakeholders; and maintain compliance with applicable laws and regulations; so enabling the measurement of performance and effectiveness of the organization. (Goos et al., 2010) Integrated GRC, sometimes referred to as GRC, is the cross-functional, extended enterprise capacity that, when used, produces performance grounded on sound principles and practices at several phases of an organization. An integrated GRC project is a transforming effort that will affect the company's operational emphasis as well as its strategic orientation.

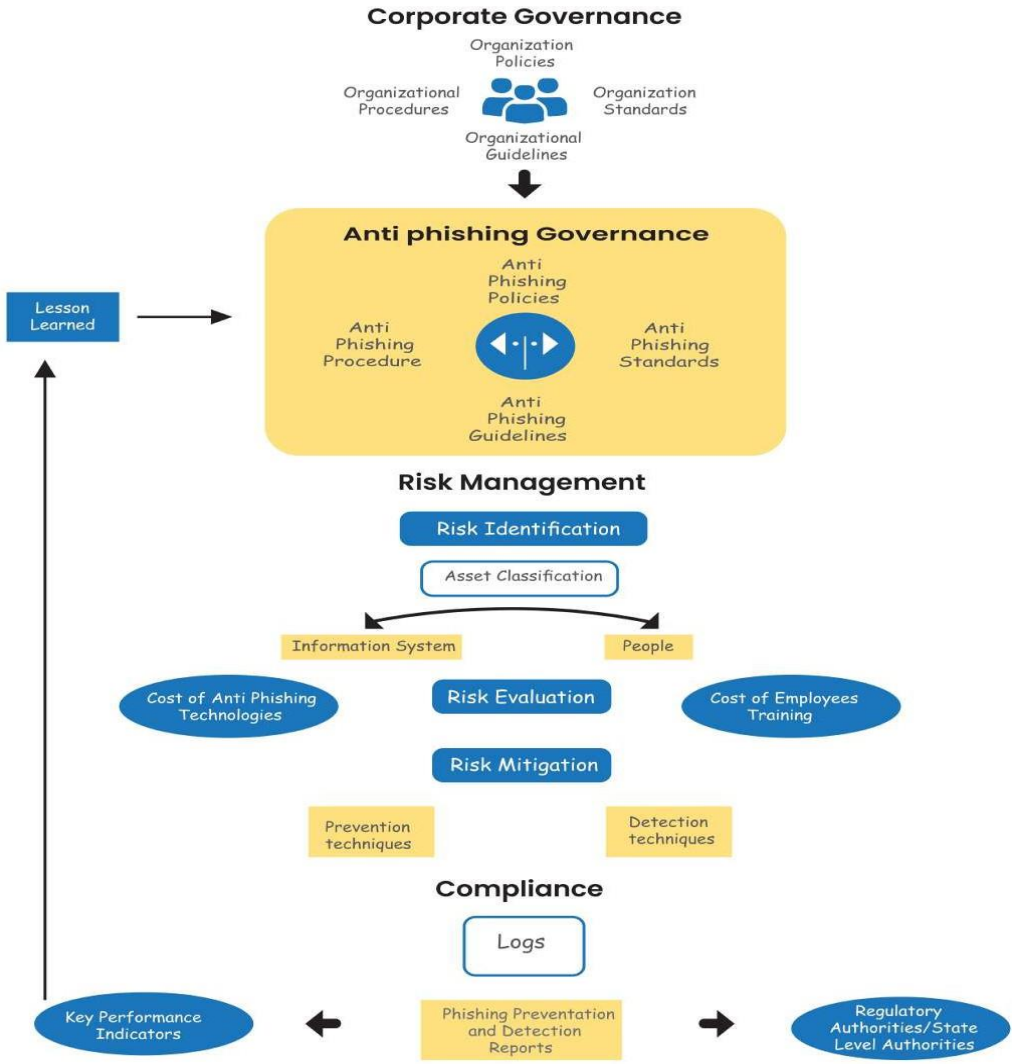

Fig. 4: GRC Pishing prevention and detection model (Author made).

7.4. Governance Firewall

Although phishing prevention and detection governance could be the first layer of defense, at this point, an organization should include the anti-phishing policies in their information security policies and may form a separate anti-phishing policy, as most phishing attackers target employees. Policies may also reflect a top management commitment at an organizational level and establish a basis for standards and practices.

7.5. Risk Management Firewall:

In the risk assessment stage, the first step is to list the assets, which include information systems, devices, and users. A phishing attack targets people through systems, and people are the weakest link in this case if they haven't been properly trained. So, it is suggested that social profiling of users could be done at this stage by estimating the amount of money that could be lost. This is because each asset in an organization has a different value, and most employees aren't trained enough to spot phishing attempts. Employees who are trained to spot and stop phishing attempts could be seen as a high-value asset. At the risk evaluation stage, loss estimation could be done by figuring out how much it will cost to train workers and set up new technologies, tools, and methods.

7.6. Compliance Firewall:

Phishing prevention and detection logs could be kept at this point to track essential performance indicators and how successfully anti-phishing tools and methods are stopping and spotting phishing attempts. Users should also be let to report the logged potential phishing attempts. Furthermore, these logs should produce a report that may be included in an anti-phishing policy, process, or guiding lesson learnt in a company. Should an entity be reporting, such as crime agencies, or if state-level norms and regulations apply, then so should it be.

8 | DISCUSSION

8.1. Limitations and Future Directions

Focus groups and phishing detection gamification models can be created from this model. Data analysis can be performed on the real data gathered from organizations to measure the effectiveness of tools and techniques.

9. Conclusion

Phishing attempts may appear to be spam on the surface. Still, they have the potential to cause significant losses in the form of identity theft, sensitive intellectual property, and consumer information.Cyber criminals have refined their strategies to include targeted attacks on specific individuals. Whaling is a sophisticated type of phishing assault that targets high-profile individuals. When compared to this, spear-phishing attacks are highly tailored and aimed at particular individuals within a company. Human nature allows phishing scammers to take advantage of people's natural tendency to overlook critical warning indications. It is mainly due to the application of persuasive concepts and scam techniques that modern phishing is so successful. People's interpretation of information and decision-making are known to be influenced by such principles, which are recognized to exist. In the end, the hybrid model for phishing detection and loss computation provided some of the foundations for the risk analysis of phishing attacks but focused on prevention techniques only does not cover the human aspects of detection, as compared to the GRC model is proposed because it covers the deficiencies of the above models as it serves as a guideline for developing an Anti-phishing culture of prevention and detection in an organization.

REFERENCES

Andress, J. (2019). Foundations of information security: a straightforward introduction. No Starch Press.

Bhardwaj, A. (2024). Cybercrime, Digital Terrorism, and 5G Paradigm: Attack Trends of the New Millennium. In 5G and Fiber Optics Security Technologies for Smart Grid Cyber Defense (pp. 1-27). IGI Global.

Clarke, S. (2006). Theory and practice: Psychoanalytic sociology as psycho-social studies. Sociology, 40(6), 1153-1169.

Khonji, M., & Iraqi, Y. (2018, December). Attributing authors of emirati tweets. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 206-212). IEEE.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186-209.

McAlaney, J., & Hills, P. J. (2020). Understanding phishing email processing and perceived trustworthiness through eye tracking. Frontiers in Psychology, 11, 1756.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of management information systems, 24(3), 45-77.

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cyber security. Computers & Security, 124, 102974.

Vayansky, I., & Kumar, S. (2018). Phishing–challenges and solutions. Computer Fraud & Security, 2018(1), 15-20.

Van Aken, J. E., & Romme, G. (2009). Reinventing the future: adding design science to the repertoire of organization and management studies. Organization Management Journal, 6(1), 5-12.