ISSN: 2182-2069 / E-ISSN: 2182-2077

Financial Institutions Phishing Attack Protection Measures

Wang Wei Ming[1*]

[1*]Department of Information Engineering, National Taitung University, Taiwan, Republic of China. as542514@gmail.com, https://orcid.org/0009-0005-7354-7749

Received: June 06, 2025; Revised: July 18, 2025; Accepted: August 14, 2025; Published: August 30, 2025

Abstract

In today's network environment, the risk of network security threats caused by protecting information assets or reducing network platforms includes the risk of network threats caused by individuals, enterprises and governments using online shared data, financial records, intellectual property rights and sensitive information. If proper protection is not taken, it is likely to be used maliciously. Phishing attacks have taken on different forms over time, and understanding the ongoing cybersecurity issues, the problem with phishing attacks depends on the human factor. This study focuses on how financial institutions can prevent phishing or cyber attacks, such as simulating the threat and severity of phishing incidents through cyber security assessment tools. identify security vulnerabilities, and improve network security awareness. Used to strengthen cyber security practices through phishing attack incidents. This project aims to familiarize financial institutions with the potential risks of phishing crises, which may involve information theft through email attacks or firewall blacklisting.

Keywords: Phishing, Cybersecurity, Blacklist, Information Security, Pharming.

1 Introduction

Digitalization has become quite common all over the world. The purpose of cyber security is to protect information systems, information networks, computer equipment and data from cyber threats (including theft, destruction and unauthorized access). However, with the advancement of global digitalization, the level of information security threats continues to increase, and the corresponding network threats have become more complex. If phishing attacks are targeting financial institutions, the main reason is that these institutions manage a large amount of personal data. Criminals often use phishing attacks to steal sensitive personal information from financial institutions. But another key factor is that financial institutions hold large amounts of money, which allows these phishers to take advantage of the opportunity to launch their attacks. Common phishing attacks often use ransomware attack methods, including delivery, infiltration, destruction and extortion.

Regarding ransomware, early detection methods have been conducted on the topic of ransomware for many years. Scholars have been constantly looking for methods to prevent ransomware attacks, but before that, the detection of ransomware attacks was mainly based on monitoring and identification mechanisms (Cen et al., 2024). The scholars described the ransomware workflow, including payment, network deployment, data destruction, and data disposal. Generally speaking, phishing or cyber-attacks

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 686-703.
DOI: *10.58346/JISIS.2025.I3.046*

*Corresponding author: Department of Information Engineering, National Taitung University, Taiwan, Republic of China.

are carried out based on Windows-based software, and the detection mechanisms at each stage are investigated (Moussaileb et al., 2021).

In addition, scholars have also proposed that cyber hackers use ransomware to analyze network vulnerabilities such as fingerprint recognition, propagation, commands, encrypted files, and locked operating systems, or more advanced hackers may threaten by deleting original files and ransom information (Hull et al., 2019). However, financial institutions are clearly at higher or even more serious risk of phishing attacks, second only to government agencies (Jamithireddy, 2025). Even if financial institutions take preventive measures to prevent phishing attacks, there are still problems such as network security vulnerabilities, which will enable attackers to effectively carry out network attacks (Ayeblo & Faraahi, 2015). For example, phishing usually involves sending deceptive information to trick individuals into revealing sensitive information

Over the past five or even ten years, as digitalization has become more popular around the world, phishing attacks have become more sophisticated and cunning, posing a major challenge to network security. Scholars (Taib et al., 2019) explored phishing attacks, emphasizing the psychological manipulation of deceiving individuals. Scholars found that enhanced authentication can be used to mitigate the effectiveness of phishing threats, providing an additional layer of security at the network level (Arora, 2024).

In addition, some researchers emphasized the need to implement encryption at a large scale and strong network security measures to deal with phishing threats in organizations.

Many scholars have proposed that ethical hacking, also known as penetration testing or white hat hacking, mainly involves the authorization to intentionally identify and exploit vulnerabilities (Aldawood & Skinner, 2018). When financial institutions become targets of phishing attacks, they are often attacked by ransomware. Scholars have proposed an investigation method for ransomware defense, focusing on multiple platforms, including personal computers, mobile devices, the Internet of Things (IoT), and cyber-physical system platforms (Oz et al., 2022). Scholars proposed a study based on machine learning technology for detecting ransomware software on personal computers. Because traditional antivirus software uses signature codes to identify malicious software, for example, it cannot detect newly emerged ransomware viruses (Deshmukh & Menon 2025). Because personal computer analysis and detection are used to prevent ransomware attacks, (Beaman et al., 2021) also used the same detection method, focusing on function calls such as application programming interfaces (APIs), file and directory operations, registry changes, entropy, strings, and network traffic.

To prevent ransomware attacks, detection at the operating system level based on APIs is critical (Ji, 2022). Ransomware detection features can be examined across multiple layers (i.e., attack surfaces), including the physical, hardware, firmware, virtual machine hypervisor, operating system, container, and application layers. If attackers gain privileged access to the operating system and successfully attack the detection mechanisms at the OS level, detecting ransomware becomes difficult due to advancements in modern operating systems and virtualization technologies, which hinder obtaining a full view of guest operating systems from the hypervisor (More & Tapaswi, 2014).

To protect financial institutions or organizations from ransomware attacks, additional protection layers are required to prevent privilege escalation and other evasive attacks at the operating system level. However, scholars have also suggested the imitation of benign application behavior at the OS level to evade machine learning-based ransomware detectors (Zhou et al., 2023). Moreover, many dynamic analysis solutions for ransomware detection use ransomware behavior features obtained at the OS level, including file and system activity (Kharaz et al., 2016; Scaife et al., 2016; Continella et al., 2016; Kharraz

& Kirda, 2017), network traffic (Cabaj et al., 2018; Cusack et al., 2018; Alhawi et al., 2018), and system logs (Roy & Chen, 2021).

Considering the complex attack surfaces and workflows of modern ransomware, a deep defense detection system can increase the likelihood of detecting ransomware attacks through sophisticated evasion techniques. This paper focuses on researching and discussing phishing attacks in financial institutions, such as ransomware attacks, and using firewall protection functions as a case study.

2 Related Work

Phishing attacks are the most common information security incidents. Hackers usually use these attacks to steal sensitive information, personal information, etc. This is a common means of cyber-attack. The main reason is that they hope to steal the public information or financial data of an organization through cyber-attacks. As mentioned above, there are many ways to attack cyberspace. Each approach has specific techniques and goals, and they often exploit human weaknesses and employ strategies of deception and organizational paralysis (Hijji & Alam, 2021). Information security incidents related to phishing attacks often exploit the above weaknesses to manipulate victims into revealing sensitive information or taking actions that compromise their security (Syafitri et al., 2022; Gupta et al., 2014; Kashif, 2019).

As mentioned above, the problem with phishing attacks is that hackers use deception to make phishing attacks successful, which emphasizes the attacker's level of trust in the individual or user. The sense of urgency or trust created by phishers can easily lead victims to disclose confidential information. These criminals often exploit people's trust in them and get users to click on malicious links, resulting in problems such as the leakage of sensitive data (Veksler et al., 2020; Fan et al., 2023). Regarding ransomware, it is mainly spread through emails, which is the most common form of cyber deception. The above criminals may send fraudulent emails impersonating government agencies, well-known organizations, or trusted entities (Mujtaba et al., 2017).

Problems with phishing attacks as mentioned above, hackers attack through malicious methods such as ransomware. Another problem is that firewall systems cannot effectively prevent phishing attacks from happening (Rishikesh et al., 2022). For example, malicious attachments or links are sent through emails, resulting in the theft of victim's device information and data. Hackers often use urgent or panic-inducing language to prompt victims to receive messages and take action. These hackers may also use caller ID spoofing to make the call look like it is from a legitimate source (Gupta et al., 2016). Through the above methods, attackers can trick victims into providing sensitive information and data.

For example, personal information, credit card information, or login credentials. This strategy may involve impersonating a senior executive or giving an urgent reason to disclose sensitive information. Although the possibility of financial institutions conducting phishing attacks via phone has decreased in recent years, some organizations should take precautions when handling sensitive information. Many scholars recommend that organizations should educate employees to prevent problems such as phone identification and phishing threats (Bubukayr & Almaiah, 2021). In addition, some attackers also send fraudulent text messages impersonating government organizations (Timko & Rahman, 2023).

Referring to Figure 1, a phishing attack email from "DBGE Bank" is clearly identified as a phishing attempt. There is no such bank as DBGE, and banks typically do not send such notifications to organizations (Darapour, 2016). The email contains a URL that is clearly a phishing link. In this study, the firewall has been configured to block phishing sites. For legitimate banks that are included in a whitelist, users will be able to access the websites as intended. However, if the user clicks on the phishing link, they may be redirected to a counterfeit website (Anderson & Moore, 2006; Habeeb, 2022). Additionally, sometimes these emails attempt to install malware on the recipient's device. If a user accidentally clicks on the provided link, they should be cautious, especially when prompted to provide personal or financial information. It is critical to verify the legitimacy of the sender's email and avoid clicking on links in such messages to mitigate the risk of fraud (Ferreira et al., 2015).

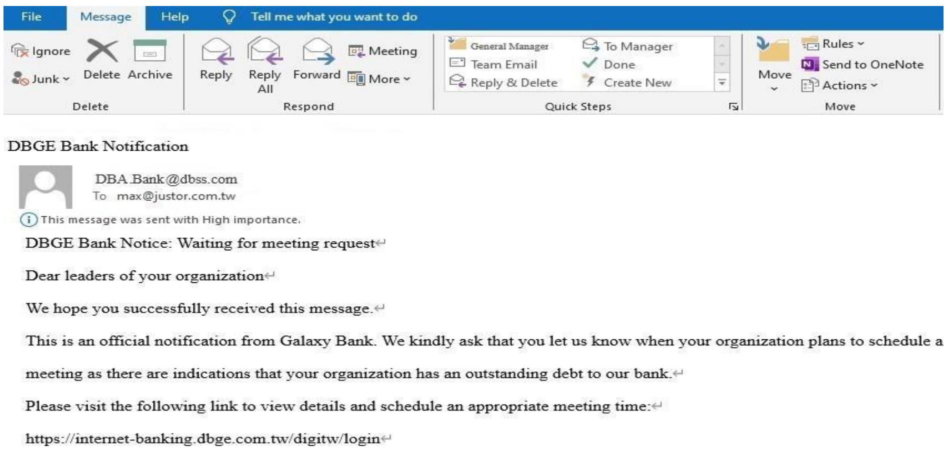

Figure 1: Phishing Attack Via Email

As shown in Figure 1, clicking on a phishing link can lead to a URL spoofing attack.URL spoofing is similar to phishing, where attackers exploit human weaknesses to take advantage of victims' Trust the given URL. URL spoofing attacks could trick victims into ransomware attacks Taking actions that harm their systems or provide an advantage to the attacker (Chen & Chen, 2019). in spite of No matter what form of phishing occurs, prevention is key. Phishing should be defined as Impersonating a trusted entity to obtain sensitive information (Sameen et al., 2020). Multiple studies it is suggested that when the software is repeatedly loaded, it can exacerbate phishing attacks by combining Multiple attack vectors, thereby increasing the effectiveness of attacks and the ability to evade detection (Taib et al.,2019). Scholars have suggested that the influence of cybercriminals is to increase the destructive power of phishing attacks by maximizing the power of attacks, mainly to target unsuspecting victims (Desolda et al., 2021).

Figure 2 shows the whitelist presented in the firewall list. Figure 2 shows that the website is not included in the whitelist, which prevents users from accessing the website. The problem in Figure 2 is that the website is not added to the whitelist but is blacklisted, so it is not trusted. Therefore, users cannot visit legitimate websites. To solve the phishing problem, it is necessary to configure the firewall correctly to ensure that trusted websites are included in the whitelist to prevent users from being blocked from accessing legitimate websites.

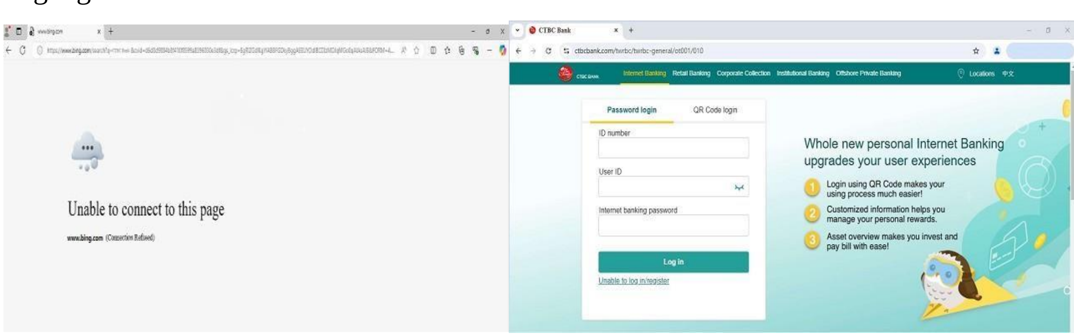

Figure 2: Whitelist Presented in the Firewall List

Figure 2, personnel from financial institutions can only access the screen on the left, while the screen on the right is displayed for websites that are not recognized as part of the financial institution's approved whitelist.

Through analytical methods to solve the problem of phishing attacks, this study emphasizes the importance of users in the problem of phishing attacks, because cyber-attacks lead to problems such as the leakage of sensitive data. This is probably because users have a low sense of crisis about cyber security, which further highlights the importance of cyber security awareness. Phishing criminals usually use this type of malicious behavior or sensitive information (Syafitri et al., 2022). Studies have also shown that phishing incidents usually send unknown links, causing personal and financial information to be leaked through cyber security loopholes (Fatima et al., 2019). Taking financial institutions as an example, implementing data encryption or credential verification to solve the problem and prevent phishing incidents is also possible, scholars have suggested that URL encryption and the use of high-performance firewalls can effectively reduce the risk of phishing (Sherry et al., 2015). There are also many literatures pointing out that in order to combat phishing attacks, organizations should actively prevent credential theft attacks, especially through active detection and response strategies.

Phishing attacks often involve fake login attempts, which has been highlighted in multiple related studies. In order to mitigate these risks, advanced detection technologies and measures must be introduced to deal with phishing attacks. Financial institutions and organizations should prioritize strengthening employees' information security awareness and reducing the risk of preventing phishing attacks.

3 Research Methodology

For financial institutions, phishing attacks are a potential risk. For example, the financial system administrator of a financial institution becomes the target of a cyber-attack and may become a victim, which will lead to serious financial risk consequences for the financial institution. Or as described above, for financial institutions, personal information issues have always been the most important issue for financial institutions. The same problem, if it is attacked by a phishing attack, will also lead to serious personal data leakage. The purpose of this study is to prevent phishing attacks through financial institutions. The study aims to evaluate the prevention and control of financial institution members against emails that may or may not be related, evaluate whether they have sufficient cyber security awareness, and whether they have taken necessary cyber security measures to prevent phishing attacks. In order to achieve this research goal, this study will simulate cyber security incidents within financial institutions to collect data, analyze phishing attack incidents through user credentials, and the purpose of the research experiment is to strengthen cyber security protection, improve information security awareness and prevention capabilities.

3.1 Firewall

Phishing attacks are relatively threatening to financial institutions. The main reason is probably due to firewall configuration issues. If the firewall system of a financial institution is unable to block URLs that are not approved by the financial institution, or is unable to block illegal URLs, this may expose the financial institution's system to phishing attacks. However, criminals often exploit system vulnerabilities to redirect users to seemingly legitimate websites, which are then used and deceived by criminals. These suspicious URLs are mostly used by phishing criminals to steal sensitive data, such as the personal information and login credentials mentioned above. Therefore, the firewall should be effectively configured to prevent the risk of phishing attacks.

This study aims to improve the network security of financial institutions by integrating the configuration performance of firewalls to prevent phishing attacks. The research method simulates a controlled phishing attack, as shown in Table 1. It examines the review and verification of email filtering rules. This filtering method is used to identify harmful and threatening emails or to intercept emails that may have the characteristics of phishing attacks. This method is used to filter suspicious emails or intercept threatening emails. This is a mechanism to prevent phishing attacks.

Next, during the firewall setup phase, the system will automatically identify and block emails with phishing intent to reduce the risk, as shown in Figure 2. This is to prevent suspicious emails from being clicked by financial institution personnel and to reduce the harm of phishing attacks.

In addition, this study also explores the risks associated with URLs during phishing attacks. The main reason for phishing attacks is that phishing criminals use malicious link URLs to deceive users into malicious URLs. For this type of malicious URL, when users are deceived by criminals and click on it, they may unsuspectingly leak user information to criminals. In order to reduce the risk, this study recommends restricting web pages, which means that only trusted and approved URLs can be allowed. Its purpose is to reduce the possibility of phishing attacks by restricting users from accessing unauthorized suspicious websites.

Table 1. illustrates the process of adding unknown emails to the blacklist during phishing attacks. This is to ensure that emails deemed suspicious by the system are permanently isolated. Financial institutions generally adopt strict network security protocols to restrict access to specific network resources and only allow access to legitimate websites and websites that require verification. Therefore, the motivation for adding unknown websites or emails to the firewall blacklist is to protect sensitive data.

Special emphasis is placed on the importance of network security defense mechanism protection system. Financial institutions need to process sensitive information such as personal information or financial data. In such an environment, the problem of being attacked by phishing is relatively high. Establishing an effective email filtering system can block highly threatening websites and protect network security. These all require the configuration of a firewall. Taking financial institutions as an example, it is crucial to reduce the risk of phishing attacks.

Table 1: Review Email Filtering List Configure Firewall Email Filtering Restrict Access to Suspicious Websites Update and Maintain Blacklist

Action or Configuration	**Description**
Review Email Filtering List	Review and verify the filtering system to flag phishing emails, preventing them from reaching the inbox.
Configure Firewall Email Filtering	Configure firewall settings to automatically flag and. block suspected phishing emails.
Restrict Access to Suspicious Websites	Configure firewall or network security settings to limit user access to unapproved websites, preventing URL spoofing attacks.
Update and Maintain Blacklist	Add identified phishing website URLs to the blacklist to prevent users from accessing them.

3.2 Email Testing

Through the experiment, the experiment method of using email is shown in Figure 1. The problem of phishing attacks is that the email is sent to the financial institution through an unknown or unsafe URL source. At the same time, this email is a ransomware email. The experimental company and account management issues of this study, so this experiment will receive emails suspected of potential threats. Warning signals are issued for the test emails of this study (including emails from unknown sources). The issues for the warning are as follows:

1. Emergency notice: The account has completed security check, please confirm login activity
2. Security Update: Important notice, please update your account credentials immediately
3. Abnormal alert: If you find suspicious login activities, please take immediate action.
4. System notification: You need to reset your password to ensure the security of your account
5. Measures taken: Unauthorized access to this account has been detected, please confirm
6. Security Warning: Account verification required
7. Transaction notification: There is an unprocessed transaction notification for this account.
8. Please confirm the payment activity.
9. Alert: Suspicious transaction activity has been detected on this account

The above-mentioned email test is used to evaluate the effectiveness of the firewall. It mainly detects whether the financial institution staff logs in to suspicious websites or uses suspicious accounts and abnormal logins. This evaluation mainly tests the effectiveness of the firewall. Through the occurrence of phishing incidents, the system administrator can immediately receive notification messages such as email notifications of the above-mentioned problems. In short, preventive measures should be taken, mainly to mitigate phishing attacks. Also tests employees' reaction and recognition abilities.

3.2.1 Email Detection

The email filtering system is closely related to the configuration of the firewall. The main reason is that the firewall's defense measures can effectively prevent phishing attacks. In order to improve performance, several key factors have been considered in the most accurate way to ensure the reliability and effectiveness of the research.

The key to email detection systems is that firewalls need to establish an effective system to enable emails to be effective in detection. During the process of phishing email simulation, when suspicious emails are sent, the firewall will immediately prioritize filtering these suspicious emails and limit them to continuous monitoring. In the face of phishing attacks, firewalls must be updated over a long period of time. As a systematic defense measure, these defense measures can be shown to reduce the risk of phishing attacks and effectively prevent the threat of malicious emails. Specifically, protecting the sensitive data of financial institutions and preventing employees from leaking or stealing data requires a firewall protection system. In other words, an effective email filtering system not only helps to identify illegal or harmful emails, but also can filter them based on the sender's address, content, and attachments. During the experimental simulation test, let the employees of financial institutions be familiar with common phishing attacks as a strategy to improve and identify suspicious emails and enhance network security awareness.

Regarding the research method, it will first be designed based on data from diverse sources to ensure the validity of the final results. The subjects will cover employees of multiple financial institutions, and the email filtering system will be tested according to the needs of different environments. The sample selection will be appropriate and reliable.

As digitalization becomes prevalent around the world, phishing attacks are also evolving rapidly. This study also emphasizes the need for continuous system updates. However, with the advancement of phishing and technology, regular updates of firewall defense tools such as blacklist and whitelist filtering systems are necessary to ensure that the firewall can protect the system and identify new types of attacks, thereby reducing vulnerabilities and risks. (Do this)

All tests are scientifically verified through repeated experiments, statistical analysis is used to ensure the stability of research results, and conclusions related to simulated phishing attacks are evaluated based on simulated test results. They are compared with existing network security measures to ensure the effectiveness of each research strategy. The test data results are based on repeatable experimental designs to improve data accuracy and reliability.

We use data from world-renowned security companies and threat sources as guidelines for developing defense strategies for phishing attacks. We integrate external blacklist and whitelist management professional resources to supplement internal testing data to ensure that research results are not only practical, but also provide feasible solutions.

In general, through multi-level testing and monitoring, this approach can verify that the firewall plays an effective defensive role in an actual phishing attack environment, and continuously adjust and optimize according to the research plan, using the reliability framework as a network security guarantee for the firewall's protection effectiveness in the face of phishing attacks by financial institutions. This approach can effectively protect the system data of financial institutions and the network security awareness of employees.

According to the above description of email detection, the purpose is to filter out URLs from non-whitelisted websites. This is done by Yao, who emphasizes that suspicious URLs can be blocked through firewall filtering to ensure that users do not click on non-whitelisted email links. The following steps are taken for email detection to prevent phishing attacks:

1. **Set up the Filtration System**
   - **Check firewall filter list**: Filter out potential threats through email filtering system rules, including keywords, sender addresses, subject lines or attachments.
   - **Filter malicious emails**: Set up the firewall's blacklist and whitelist, block emails from suspicious sources and add them to the blacklist.
2. **Set Blacklist and Whitelist Rules**
   - **Filtering rules through firewall**: Setting firewall rules can filter suspicious emails, and then filter employee emails after the emails filtered by the firewall.
   - **Malicious URL prevention**: Malicious URLs may cause users to click and may lead users to illegal websites, so firewalls should be set to block access to unauthorized websites.
3. **Manage Firewall Blacklist**
   - **Block suspicious accounts and websites**: Illegal websites and suspicious accounts should be added to the firewall blacklist to block possible phishing attacks and prevent potential threats from entering the internal network.
4. **Website Access Permissions**
   - **Limit access to suspicious websites:** Used to identify illegal websites, network access restrictions should be set to prevent employees from clicking on links by mistake.

- **Allow access to whitelisted URLs:** Set up a firewall whitelist to enhance the security of the network environment.

5. **Testing and Monitoring**

- **Test employees' cyber security**: Test whether financial institution employees can identify illegal websites or blacklisted accounts. This helps assess employee's cyber security awareness.
- **Monitor emails**: filter out emails, analyze and evaluate them, and adjust filtering rules based on the analysis results to enhance defense capabilities.

3.2.2 Reliability and Validity of the Research

1. **Data Diversity and Representation**

Through simulations conducted in cooperation with financial institutions, data samples from employees during the simulation process were collected. The samples were targeted at testing the filtering system of the firewall to ensure the validity of the research results.

2. **Continuous System Updates**

The firewall system in this study will be regularly updated and optimized to maintain the ability to respond to new attack strategies.

3. **Reproducibility and Scientific Rigor of Testing**

The research test results will be verified and compared multiple times, and statistical analysis will be performed after the samples are collected to ensure the stability and credibility of the research results.

4. **Third-Party Data Support**

Based on data from cyber threat intelligence sources released by global cyber security companies, blacklists and whitelists are established to ensure the foresight and effectiveness of defense measures.

3.2.3 Firewall Filtering Rules and Blacklist Management

Through the detection process, we can understand that in the configuration of the test firewall; in order to prevent the threat of phishing attacks, we must first set up firewall rules. This practice is used to filter malicious authentication provided by suspicious accounts. The firewall rules are used to intercept potential phishing emails as shown in Figure 3. Figure 3 illustrates how we configure the system's blacklist to block emails that are considered inappropriate. Financial institutions. Therefore, employees of financial institutions will not be able to access the website Blacklisted. However, a related problem arises: when a website is added to the blacklist, the corresponding IP address associated with the website will also be added to the blacklist filter list. As shown in Figure 4. Figure 4 shows that the restriction does not apply to restricted websites. Instead, they point to the IP addresses of financial institutions, which will not be able to access the blacklist. The website shown in Figure 3. This method is used to solve the problem of web page access restrictions. See Section 3.2.1 for details.

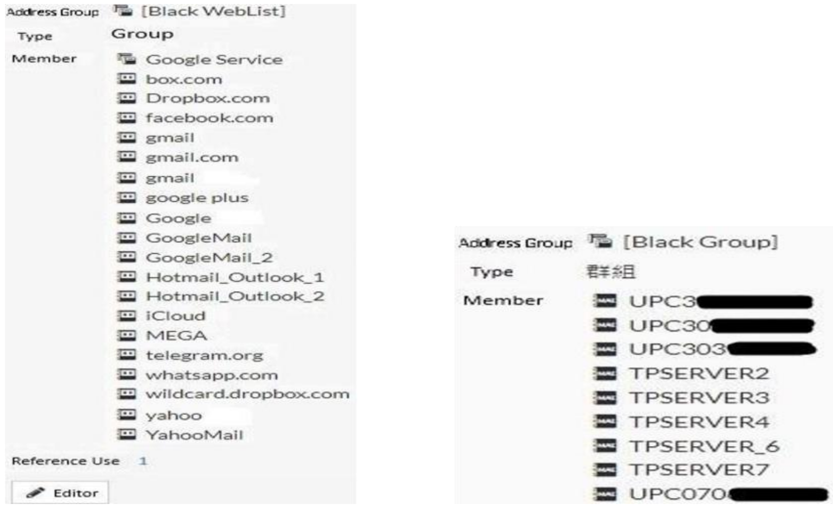

Figure 3: On the Far Left, Emphasizes that the Financial Institution is Unable to Access Specific Websites. Therefore, These Particular Websites are Added to the Blacklist to Prevent Personnel from Accessing Them; On the Far Right, Adds the Website to the Blacklist and Sets the IP Addresses of Financial Institution Personnel. The Primary Purpose Is to Block the Restricted Ips from Accessing the Blacklisted Website (IP Addresses Are Obscured)

3.2.4 Risk Assessment and Monitoring

After the aforementioned tests, this study will also focus on risk assessment to monitor and detect the responses of financial institution employees. This is due to the various causes of phishing attacks, such as email leaks or internal firewall issues within an organization. Therefore, the risk level of phishing attacks to financial institutions is still considered high. If the risk level is high, financial institutions are more likely to face consequences such as hacker attacks. Naturally, this is not limited to financial institutions; any organization seeks to minimize risk exposure. As a result, this study's email monitoring process also categorizes the risk levels of phishing attacks into three tiers: low, medium, and high, and tests them accordingly.

According to the 2023 Verizon Data Breach Investigations Report (DBIR), phishing remains one of the most common forms of cyberattack, accounting for more than 30% of all reported data breaches. This underscores the importance of having a comprehensive risk assessment protocol. The 2022 FBI Internet Crime Report highlights that 41% of phishing attacks targeted banks and financial services, showing the high frequency of such attacks in the financial sector. With the continuous evolution of phishing techniques, including spear-phishing and whaling targeting high-level executives, the risks faced by financial institutions have been significantly exacerbated.

As shown in Figure 4, if abnormal email activity occurs, such as a sudden irregular login to an employee's account, this event will be displayed in Figure 5. In this case, if such an event occurs, the firewall will immediately block the issue and notify the system administrator. The purpose of this approach is to monitor whether the employee account is accessed suspiciously. This method is used to protect the organization's email system, preventing unauthorized individuals from logging in and carrying out attacks such as ransomware. Monitoring of abnormal logins, especially those outside of work hours or from unusual locations, is crucial for early detection of phishing attacks. Financial institutions typically implement multi-factor authentication and behavioral analysis to enhance the effectiveness of their email systems and reduce the likelihood of successful phishing attacks.

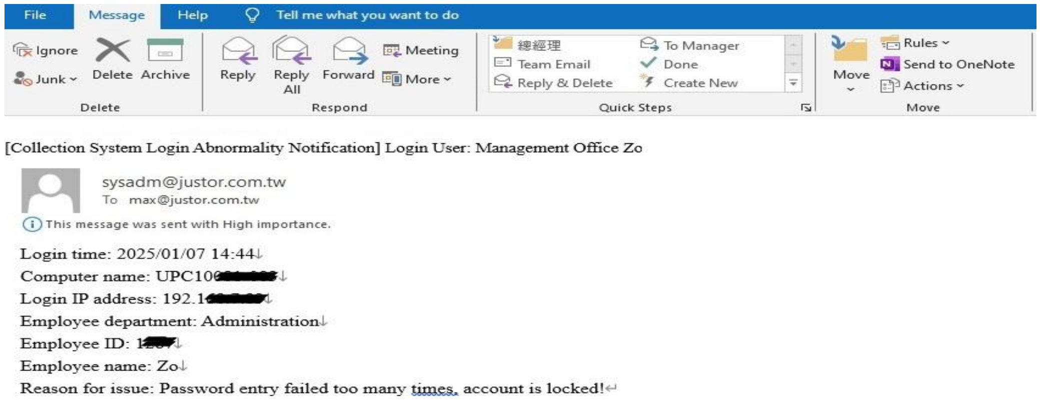

Figure 4: Shows that when there is Abnormal Login Activity on an Account, the Firewall will Detect it and Notify the System Administrator Via Email (IP addresses are obscured)

To address phishing attack incidents, it is critical to conduct a risk assessment, not only to identify the risk level but also to prevent such attacks from recurring. In this study, after discussions with cooperating financial institutions, a risk assessment table was developed specifically for financial institutions, as shown in Table 2. Table 2 outlines the steps that should be followed after an incident occurs, starting with identifying the incident's needs, causes, and other explanatory factors. Then, the phishing attack incident should be assessed. Relevant departments, such as the IT department, should evaluate the analysis after the incident, including the type of incident handling and the accounts used. "Accounts used" refers to administrator accounts, which are exclusively available for system administrators to repair compromised accounts affected by the phishing attack. Furthermore, evaluating the risk level of the incident is crucial, particularly emphasizing the need to assess the risk level after filling out Table 2. After completing the assessment, corrective measures should be implemented to prevent the recurrence of the incident. Financial institutions must adopt proactive measures when addressing phishing risks. The risk assessment process not only identifies vulnerabilities but also serves as a basis for improving organizational defenses. Lessons learned from each phishing event help reduce the frequency and severity of future attacks. Studies show that institutions with structured incident response plans and comprehensive employee training typically experience fewer successful phishing attacks. For example, organizations that continuously conduct phishing threat training report a 25% reduction in successful phishing attacks.

Table 2: Presents the Risk Assessment form to be Completed in the Event of a Network Attack.

Information Security Remediation Request Form	
Requirement, Reason and Explanation	□ Equipment Changes □ Equipment Changes □ Software Changes □ Email Configuration Changes Excluded □ Other Patch Descriptions
Phishing Attack Incident Evaluation, Review, Changes and Analysis	Treatment Type： □ Processing and Execution □ Remove Operator：_________ Operation Instructions： Risk Level: □Low □Medium □High User Account：

Table 2, Through the information security remediation request form, further assess the risk levels of phishing attacks. The risk assessment form developed in collaboration with the financial institution to determine how to handle issues that arise after a phishing attack occurs within the financial institution is shown in Table 2. For the risk assessment in Table 2, if the risk level is classified as high, the financial institution leadership must be notified. When it comes to information security, leadership is the ultimate decision maker. As shown in Table 2, when a phishing attack occurs, a series of procedures need to be handled. It is particularly emphasized that the purpose of these programs is to prevent and identify phishing attacks. Through cooperation with financial institutions in this study, we can understand that the threat to network security is not enough for the employees of financial institutions. We further understand that if financial institutions are attacked by phishing, there will be serious threats. By detecting phishing attacks on financial institutions and making an assessment within 24 hours, the assessment content shows that there is a possibility of financial institutions suffering significant financial or reputational losses, and this possibility is reduced by 70%. This highlights the importance of establishing an efficient and coordinated risk assessment and response framework to mitigate the impact of phishing attacks on financial institutions.

3.2.5 Enhance Network Security

Assess the risk of phishing attacks through vulnerability scanning. Its purpose is to enhance the network security capabilities of financial institutions. The main reason is that financial institutions frequently experience phishing attacks. A systematic approach is adopted to conduct vulnerability scanning and analyze the vulnerabilities existing in the internal domain account permissions of financial institutions. In response to the ever-changing phishing attacks, if the firewall cannot effectively block malicious URLs, it is very likely that the domain account and the entire system will face network security threats. Special attention should be paid to the vulnerability scanning technology that should be used for detection and repair. This approach is to enhance network security.

By using the Nessus Essentials tool to perform vulnerability scanning and conduct evaluations based on the experiment, the Nessus Essentials tool can accurately identify the potential network security risks of the financial institution's system. During the evaluation process, it can be learned that different IP addresses may be potential malicious websites. Through vulnerability scanning detection, suspicious activities can be learned. Based on the scan results, it can be evaluated that a certain IP address has abnormal traffic, indicating that the IP address may have the possibility of data being stolen by criminals, and immediate detailed analysis and response are required, as shown in Figure 5.

According to Figure 5, if abnormal behavior is detected for a specific IP address, it means that the IP may be at risk of phishing attacks and further investigation is required. If the IP frequently communicates with known phishing websites, it may have been exposed to phishing attacks and countermeasures need to be taken immediately. This response process will help to quickly identify phishing attacks and prevent further compromise of the financial institution’s internal systems. Additionally, according to the 2023 Verizon Data Breach Investigations Report, phishing remains one of the most common cyber-attacks, accounting for more than 30% of all reported data breaches. Additionally, according to the FBI’s 2022 Cybercrime Report, 41% of phishing attacks targeted the banking and financial services sectors, highlighting the high risks the financial industry faces in responding to phishing attacks.

Through the scanning process, each IP address will be subjected to a detailed risk assessment and classified accordingly based on the severity of the anomalies found in the scan results. For example, if the scan results show that certain IP addresses exhibit obvious abnormal behavior, such as frequently visiting suspicious websites or communicating with phishing email servers, these IPs will be marked as high risk and blocked immediately. Once the vulnerability scan confirms that there are no anomalies, the system will display a normal status, indicating that the IP address is not involved in any potential cyber-attacks or phishing incidents.

The goal is to promptly discover weaknesses in the internal networks of financial institutions through vulnerability scanning, and to strengthen the system based on the scanning results to reduce the success rate of phishing attacks. In addition, the research will also analyze abnormal traffic patterns and potential attack behaviors discovered during the scanning process to provide data support for subsequent mitigation measures. This approach will effectively enhance the ability of financial institutions to respond to cyber threats such as phishing attacks, and provide empirical evidence for building stronger cyber security defenses.

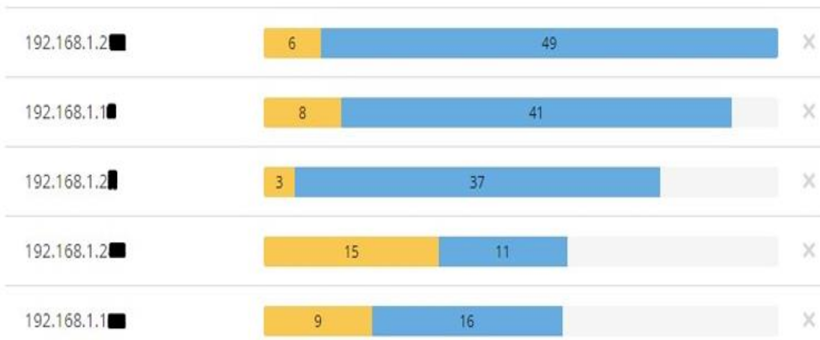

Figure 5: Vulnerability Scanning Sample Category Distribution, Yellow Indicates Unauthorized (Server Blocked)

4 Experimental Results

The experiment results show that this study implemented strict protective measures for the emails of financial institutions. The primary reason for this, as mentioned earlier, is that financial institutions are among the most vulnerable organizations to phishing attacks. This is because financial institutions hold a large amount of personal data, making them prime targets for phishing attackers seeking to acquire more personal information. Based on the experiment, it can be observed that the firewall settings were configured to successfully block emails from unknown sources, demonstrating the firewall’s ability to block malicious or suspicious emails. Additionally, this study used the firewall's blocking functionality to generate a data report, as shown in Figure 6. Since this study collaborated with a financial institution, the institution allowed us to generate the data related to the firewall's blocking of phishing attacks, as shown in Figure. 6

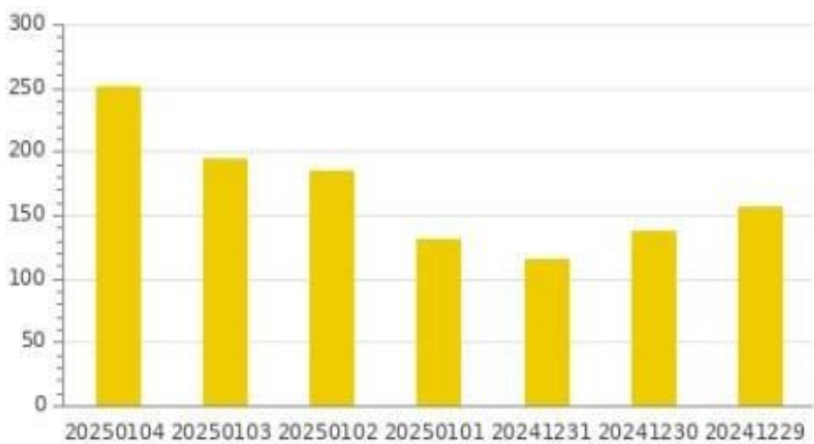

Figure 6: Statistics of the Daily Attack Blocking Frequency

From Figure 6, it can be observed that the firewall blocked a total of 1,169 phishing attacks. This indicates that the risk level of network attacks is relatively high. However, due to the firewall's blocking function, no phishing attacks occurred. The effectiveness of the firewall in blocking network attacks can be seen in Table 3.

Table 3: Shows the Data of the Firewall Blocking Phishing Attacks

Total Blocked Attacks	1169(Counts)
Total Blocked Attack Types	70
Total Blocked Ports	9
Total IP Addresses	Source IP: 276 Dest. IP: 6
Risk	Critical: 72 High: 84 Medium: 1013
Attack Direction	Incoming: 1169 Outgoing: 0

The experimental results reveal the situation of phishing attacks. Figure 6 shows the number of phishing attacks encountered daily, and the total of these occurrences is displayed in Table 3. It can be observed that despite the high frequency of phishing attacks, the firewall effectively blocked them.

Additionally, Table 3 shows that a risk assessment was conducted in this study. The results of the assessment are based on the number of phishing attacks occurring each day, which are categorized into risk levels according to the risk assessment criteria. This approach emphasizes the evaluation of the total number of phishing attacks for the week to determine the risk level. Therefore, from the perspective of this study, the direction of research can effectively prevent phishing attacks on financial institutions.

5 Discussion and Solutions to Cyber Security Issues for Financial Institutions

Through the above, it is particularly emphasized that the blacklist and whitelist mechanism required in the firewall filtering system is effective in preventing phishing attacks. For example, when the firewall successfully filters malicious websites or non-whitelisted email accounts, it is relatively important. Further understanding that if there is a need to evaluate different types of firewalls (such as content-based firewalls and behavior-based firewalls), firewalls will filter emails, including attachments, web page content, or malicious code by analyzing blacklist and whitelist mechanisms and can effectively block phishing attacks.

In addition, it is crucial to improve the awareness and identification ability of financial institutions' network systems and employees regarding network security. In particular, it is noted that IT personnel in general financial institutions have relatively high authority, which is also likely to be one of the reasons for phishing attacks. Therefore, it is necessary to further explore the effectiveness of employee education and simulated phishing attack tests in preventing actual attacks. Through the results of this study, we will explore how to measure the effectiveness of these measures and their contribution to the organization's defense capabilities.

Firewall filtering can indeed effectively block phishing attacks, but the risk of cyber attacks faced by financial institutions is still relatively high. This study emphasizes that financial institutions need to conduct comprehensive risk assessments when facing phishing attacks. For financial institutions, it is relatively important to identify potential phishing threats because of the threat of phishing attacks through emails. Such a risk identification process should be based on the analysis of past attacks, as well as industry trends and emerging attack methods. Therefore, financial institutions should conduct a detailed analysis of each risk identified, assess its likelihood and impact, and classify the risks into different levels, as shown in Table 2. If a comprehensive risk assessment is conducted, a multi-layer firewall defense system needs to be established to protect the financial institution's system from phishing attacks. However, large financial institutions have relatively more resources to prevent phishing attacks, but if it is a medium-sized financial institution today, it can be understood that medium-sized financial institutions have limited resources but network security is still difficult to conduct effective risk assessment.

Therefore, risk assessment is crucial for financial institutions because through risk assessment, institutions can identify and analyze potential risks and take appropriate preventive measures based on the severity of the risks. Whether it is a large bank or a small or medium-sized financial institution, establishing a standardized risk assessment process, regularly updating preventive measures, and combining multi-layered defense technologies with employee training are the keys to effectively managing phishing risks.

6 Conclusions

Based on the results of this study, we can understand the problem of phishing attacks faced by financial institutions. The preventive measures proposed based on the experimental results include firewall filtering. Risk assessment can be made for filtering. Through the assessment, we can understand that through the analysis of actual cases, we can find that firewalls can block suspicious emails to prevent the threat of phishing attacks, especially for high-risk financial institutions. Firewall filtering rules can reduce the potential harm of phishing attacks.

However, although firewalls can block phishing attacks, traditional firewall defenses can still cause phishing attacks because attackers often use human psychological weaknesses to deceive. This further emphasizes that risk assessment is effective in preventing phishing attacks because risk assessment can help financial institutions analyze potential threats and take countermeasures based on risk levels.

However, it should be emphasized that other forms of phishing attacks should be considered, such as fake websites, malicious links, etc. A thorough analysis of past related incidents can enable financial institutions to predict how to respond to potential phishing attacks. The results of this study show that the use of differentiating risk levels can be used to help financial institutions address risk issues and should prioritize high-risk attacks and take corresponding defensive measures.

In addition to firewall filtering, employee network security education and training is relatively important. Through the simulation of phishing attacks, we can understand the importance of network security to financial institutions. Risk assessment is carried out by identifying suspicious emails, and firewall filtering rules are formulated according to the severity of the risk. The risk assessment process should be regularly updated. Preventive measures and employee training and phishing threats are the key to effective phishing risk management. Cooperation with technology vendors and experts should be strengthened to continuously improve their defense capabilities. After all, cyber criminals can still use it to launch sophisticated attacks (Capuano et al., 2022).

References

[1] Aldawood, H., & Skinner, G. (2018, December). Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE)* (pp. 62-68). IEEE. https://doi.org/10.1109/TALE.2018.8615162

[2] Alhawi, O. M., Baldwin, J., & Dehghantanha, A. (2018). Leveraging machine learning techniques for windows ransomware network traffic detection. In *Cyber threat intelligence* (pp. 93-106). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-73951-9_5

[3] Anderson, R., & Moore, T. (2006). The economics of information security. *science*, *314*(5799), 610-613. https://doi.org/10.1126/science.1130992

[4] Arora, G. (2024). Desing of VLSI Architecture for a flexible testbed of Artificial Neural Network for training and testing on FPGA. *Journal of VLSI circuits and systems, 6*(1), 30-35. https://doi.org/10.31838/jvcs/06.01.05

[5] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333. https://doi.org/10.3390/electronics12061333

[6] Ayeblo, Y. N., & Faraahi, A. (2015). A Survey of the Solutions to Detect and Deal with File Injection Attacks in Web Sites through Access to Web Server Shared Resources. *International Academic Journal of Science and Engineering*, *2*(2), 234–248.

[7] Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & security*, *111*, https://doi.org/ 10.1016/j.cose.2021.102490

[8] Cabaj, K., Gregorczyk, M., & Mazurczyk, W. (2018). Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics. *Computers & Electrical Engineering*, *66*, 353-368. https://doi.org/10.1016/j.compeleceng.2017.10.012

[9] Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. *Ieee Access*, *10*, 93575-93600. https://doi.org/10.1109/ACCESS.2022.3204171

[10] Cen, M., Jiang, F., Qin, X., Jiang, Q., & Doss, R. (2024). Ransomware early detection: A survey. *Computer Networks*, *239*, 110138. https://doi.org/10.1016/j.comnet.2023.110138

[11] Chen, Y. H., & Chen, J. L. (2019). Ai@ ntiphish—machine learning mechanisms for cyber-phishing attack. *IEICE Transactions on Information and Systems*, *102*(5), 878-887. https://doi.org/10.1587/transinf.2018NTI0001

[12] Continella, A., Guagnelli, A., Zingaro, G., De Pasquale, G., Barenghi, A., Zanero, S., & Maggi, F. (2016, December). Shieldfs: a self-healing, ransomware-aware filesystem. In *Proceedings of the 32nd annual conference on computer security applications* (pp. 336-347). https://doi.org/ 10.1145/2991079.2991110

[13] Cusack, G., Michel, O., & Keller, E. (2018, March). Machine learning-based detection of ransomware using SDN. In *Proceedings of the 2018 ACM international workshop on security in software defined networks & network function virtualization* (pp. 1-6). https://doi.org/10.1145/3180465.3180467

[14] Darapour, M. (2016). The role of toxic assets in the formation of financial crisis (Case study: Iran central bank’s monetary system). *International Academic Journal of Organizational Behavior and Human Resource Management*, *3*(2), 1–7.

[15] Deshmukh, S., & Menon, A. (2025). Machine Learning in Malware Analysis and Prevention. In Essentials in Cyber Defence (pp. 74-89). Periodic Series in Multidisciplinary Studies.

[16] Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: a systematic literature review. *ACM Computing Surveys (CSUR)*, *54*(8), 1-35. https://doi.org/10.1145/3469886

[17] Fan, Y., Saeidi, M., Lai, K. K., Yang, J., Cai, X., & Chen, Y. (2023). Corruption and infrastructure development based on stochastic analysis. *Archives for Technical Sciences/Arhiv za Tehnicke Nauke*, (28). https://doi.org/10.59456/afts.2023.1528.011Y

[18] Fatima, R., Yasin, A., Liu, L., & Wang, J. (2019). How persuasive is a phishing email? A phishing game for phishing awareness. *Journal of Computer Security*, *27*(6), 581-612. https://doi.org/10.3233/JCS-181253

[19] Ferreira, A., Coventry, L., & Lenzini, G. (2015, July). Principles of persuasion in social engineering and their use in phishing. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 36-47). Cham: Springer International Publishing.

[20] Gupta, V., Sharma, P., & Gill, H. (2014). Wireless Data Routing with Security Keys. *International Journal of Communication and Computer Technologies (IJCCTS)*, *2*(2), 135-138.

[21] Habeeb, M. A. (2022). The Impact of Use of Expert Systems on Improving Effectiveness of Accounting Information Systems: Applied Study in Iraqi Commercial Banks. *International Academic Journal of Social Sciences, 9*(2), 131–144. https://doi.org/10.9756/IAJSS/V9I2/IAJSS0922

[22] Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions. *Ieee Access*, *9*, 7152-7169. https://doi.org/10.1109/ACCESS.2020.3048839

[23] Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science*, *8*(1), 1-22, 10.1186/s40163-019-0097-9

[24] Jamithireddy, N. S. (2025). Integrating decentralized finance (DeFi) protocols into SAP systems for automated payment processing. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *16*(2), 346–366. https://doi.org/10.58346/JOWUA.2025.I2.022

[25] Kashif, R. (2019). A compact circular polarized antenna for fixed communication applications. *National Journal of Antennas and Propagation*, *1*(1), 1-4. https://doi.org/10.31838/NJAP/01.01.01

[26] Khan, M.U., Wei, L., Ji, Y. (2022). BlueSky Ransomware: Fast Encryption via Multithreading. *Ransomware, Threat Research.*

[27] Kharaz, A., Arshad, S., Mulliner, C., Robertson, W., & Kirda, E. (2016). {UNVEIL}: A {Large-Scale}, automated approach to detecting ransomware. In *25th USENIX security symposium (USENIX Security 16)* (pp. 757-772).

[28] Kharraz, A., & Kirda, E. (2017, September). Redemption: Real-time protection against ransomware at end-hosts. In *International Symposium on Research in Attacks, Intrusions, and Defenses* (pp. 98-119). Cham: Springer International Publishing. 10.1007/978-3- 319-66332-6_5

[29] More, A., & Tapaswi, S. (2014). Virtual machine introspection: towards bridging the semantic gap. *Journal of Cloud Computing*, *3*(1), 16. https://doi.org/ 10.1186/s13677-014-0016-2

[30] Moussaileb, R., Cuppens, N., Lanet, J. L., & Bouder, H. L. (2021). A survey on windows-based ransomware taxonomy and detection mechanisms. *ACM Computing Surveys (CSUR)*, *54*(6), 1-36. https://doi.org/10.1145/3453153

[31] Mujtaba, G., Shuib, L., Raj, R. G., Majeed, N., & Al-Garadi, M. A. (2017). Email classification research trends: review and open issues. *IEEE access*, *5*, 9044-9064. https://doi.org/10.1109/ACCESS.2017.2702187

[32] Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys (CSUR)*, *54*(11s), 1-37. https://doi.org/10.1145/3514229

[33] Rishikesh, R., Tamilselvan, Y., & Sujai, S. (2022). Intrusion of Attacks in Puppet and Zombie Attacking and Defence Model Using BW-DDOS. *International Academic Journal of Innovative Research*, *9*(1), 13-19. https://doi.org/10.9756/IAJIR/V9I1/IAJIR0903

[34] Roy, K. C., & Chen, Q. (2021). Deepran: Attention-based bilstm and crf for ransomware early detection and classification. *Information Systems Frontiers*, *23*(2), 299-315. https://doi.org/10.1007/s10796-020-10017-4

[35] Sameen, M., Han, K., & Hwang, S. O. (2020). PhishHaven—An efficient real-time AI phishing URLs detection system. *Ieee Access*, *8*, 83425-83443. https://doi.org/10.1109/ACCESS.2020.2991403
[36] Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016, June). Cryptolock (and drop it): stopping ransomware attacks on user data. In *2016 IEEE 36th international conference on distributed computing systems (ICDCS)* (pp. 303-312). IEEE. https://doi.org/10.1109/ICDCS.2016.46
[37] Sherry, J., Lan, C., Popa, R. A., & Ratnasamy, S. (2015, August). Blindbox: Deep packet inspection over encrypted traffic. In *Proceedings of the 2015 ACM conference on special interest group on data communication* (pp. 213-226). https://doi.org/10.1145/2785956.2787502
[38] Syafitri, W., Shukur, Z., Asma'Mokhtar, U., Sulaiman, R., & Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. *IEEE access*, *10*, 39325-39343. https://doi.org/10.1109/ACCESS.2022.3162594
[39] Taib, R., Yu, K., Berkovsky, S., Wiggins, M., & Bayl-Smith, P. (2019, August). Social engineering and organizational dependencies in phishing attacks. In *IFIP conference on human-computer interaction* (pp. 564-584). Cham: Springer International Publishing.
[40] Veksler, V. D., Buchler, N., LaFleur, C. G., Yu, M. S., Lebiere, C., & Gonzalez, C. (2020). Cognitive models in cybersecurity: learning from expert analysts and predicting attacker behavior. *Frontiers in Psychology*, *11*, 1049. https://doi.org/10.3389/fpsyg.2020.01049
[41] Zhou et al., 2023 Zhou C., Guo L., Hou Y., Ma Z., Zhang Q., Wang M., Liu Z., Jiang Y. Limits of i/o-based ransomware detection: an imitation based attack2023 IEEE Symposium on Security and Privacy (SP), IEEE, San Francisco, CA, USA (2023), pp. 2584-2601, https://doi.org/10.1109/SP46215.2023.10179372

Author Biography

Wang Wei Ming, a researcher at National Taitung University, is currently a project researcher at National Kaohsiung Normal University. Obtained a master's degree from the Institute of Information Engineering at National Taitung University in 2023.