HONG KONG JOURNAL OF SOCIAL SCIENCES

香港社會科學學報

第一的第 57 期 (2021 春/夏) Vol. 57 Spring/Summer 2021

Phishing as Cyber Fraud: The Implications and Governance

Nur Farhana Mohd Zaharon[1], Mazurina Mohd Ali[2*]

[1] KYC Operations Analyst, Citigroup Transaction Services (M) Sdn. Bhd., Kuala Lumpur, Malaysia

[2] Faculty of Accountancy, Universiti Teknologi MARA Selangor, Puncak Alam Campus, 42300 Bandar Puncak Alam, Selangor, Malaysia

Received: May 25, 2021 ▪ Reviewed: June 23, 2021 ▪ Accepted: July 21, 2021 ▪ Published: August 30, 2021

Abstract:
Internet technology brings a revolutionary change in modern living and socio-economic transactions. The nature of high-speed Internet allows Internet users to become ignorant of their data and information transparency. This behavior gives rise to phishing attacks by cybercriminals. Cybercriminals are highly trained people including in performing social engineering tactics to deceive internet users. Therefore, Internet users must know about phishing. This paper aims to explore phishing as cyber fraud, including the implications of phishing attacks and the governance to prevent phishing attacks. This study benefits individuals, companies, the government, and the public to increase phishing awareness and mitigate phishing attacks.

Keywords: phishing, cyber fraud, risk, risk management, Internet, technology.

作为网络欺诈的网络钓鱼：影响和治理

摘要：
互联网技术给现代生活和社会经济交易带来了革命性的变化。高速互联网的特性使互联网用户对其数据和信息的透明度一无所知。这种行为会引起网络犯罪分子的网络钓鱼攻击。网络罪犯是训练有素的人，包括执行社会工程策略来欺骗互联网用户。因此，互联网用户必须了解网络钓鱼。本文旨在探讨作为网络欺诈的网络钓鱼，包括网络钓鱼攻击的影响和防止网络钓鱼攻击的治理。这项研究有利于个人、公司、政府和公众提高网络钓鱼意识并减轻网络钓鱼攻击。

关键词：网络钓鱼、网络欺诈、风险、风险管理、互联网、技术。

Corresponding Author: Mazurina Mohd Ali, Faculty of Accountancy, Universiti Teknologi MARA Selangor, Puncak Alam Campus, Selangor, Malaysia; email: mazurina@uitm.edu.my

1. Introduction

Internet technology brings a revolutionary change in modern living and socio-economic transactions such as in communication, shopping, commerce, networking, entertainment and becomes the source of data and information. People can facilitate it easily via digital devices such as laptops and smartphones (Arachchilage & Love, 2014). Due to this rapidly increasing revolution, people tend to rely more on internet sources. In recent years, the growth of Internet connectivity increased cyber fraud activities and encouraged people to commit fraud and victimize others (Kamruzzaman et al., 2016). Now, it becomes a major problem worldwide, and no countries are immune to it.

Fraud is generally known as a crime of using dishonest methods to gain something from others (Albrecht & Albrecht, 2004). On the other hand, cyber fraud is a fraud involved in Internet services or software connected to the Internet (Zahari et al., 2017). Phishing, e-mail scams, data breaches, lottery scams, love scams, and malware are examples of cyber fraud. Other types of cyber fraud include credit card fraud and internet auction fraud.

Nowadays, the nature of high-speed Internet allows internet users to become ignorant of their data and information transparency. Moreover, cybercriminals are highly trained people including in performing social engineering tactics on internet users. Krombholz et al. (2015) stated that social engineering uses deception to manipulate individuals to compromise information systems and divulge personal or private information that might be exploited fraudulently.

Instead of using technological attacks on networks, social engineers utilized human psychology techniques like influence and persuasion to persuade people to hand up their personal information. This human psychology is one of the reasons why consumers are more vulnerable to cyber fraud, particularly phishing attacks.

Phishing is a cyber-fraud. The fraudsters imitate someone from legitimate institutions to persuade people to provide sensitive information such as personal information, banking and credit card information, and passwords (Katkuri, 2018). Scammers generally contact the victims via e-mail, phone, or text messaging. The data is then utilized to access sensitive accounts, which can lead to identity theft and financial loss (Hanna et al., 2021). One victim, for example, receives an e-mail from the bank, and the victim has been asked to update the personal details and bank account number. However, the login pages are bogus, and the hackers take advantage of stealing the victim's information.

According to Ernst and Young's 2018-2019 Global Information Survey (van Kessel, 2018), phishing is the top cyber threat to organizations, with 22% of cases reported by malware with 20% cases and disruptive cyber-attacks with 13% cases. The United States (US)'s government warned their citizens about phishing texts or e-mails asking the citizens to donate and give charity to help the active and veteran military members to show their patriotism and kindness in conjunction with the US Independent Day on the 4th of July. However, the US government warned their citizens not to trust and click on the links (Special to the Times, 2020).

In 2010, CyberSecurity Malaysia reported 294 phishing websites, and most of them targeted local banks such as Maybank2U.com and Cimbclicks.com. CyberSecurity Malaysia is an agency incorporated under the supervision of the Ministry of Communications and Multimedia Malaysia and responsible for providing cybersecurity services and programs to reduce cybersecurity issues and strengthen Malaysia's cybersecurity. CyberSecurity Malaysia and the Malaysian Communications and Multimedia Commission (MCMC) are accountable for mitigating cybercrime (Malaysian Communications and Multimedia Commission, 2021).

Statistics from The Malaysia Computer Emergency Response Team (MyCERT) under CyberSecurity Malaysia revealed that cyber fraud has the highest number of incidents reported. Phishing includes in a cyber fraud category. In 2019, cyber fraud cases topped the list with 7,774 incidents reported, while intrusion reported 1,359 cases, and malicious codes reported 738 cases. In 2020, there are 4,906 cases reported from January until June 2020, and cyber fraud topped the list again. The second one is an intrusion that reported about 730 cases and malicious codes about 232 cases. However, there is no specific data on phishing incidents reported by MyCERT.

Table 1. Reported incidents based on general incident classification statistics for 2018, 2019, and 2020 (Malaysia Computer Emergency Response Team (MyCERT), 2021)

Incident	2020 (January - June 2020)	2019	2018
Cyber Fraud (Phishing is included in cyber fraud)	4,906	7,774	5,123
Intrusion	730	1,359	1,805
Malicious Codes	232	738	1,700

One scenario reported on the Inland Revenue Board Malaysia (IRBM) is a syndicate of fraudsters actively impersonating IRBM officers (Rahim, 2020). The victims received a phone call from the fake IRBM officers with similar IRBM contact numbers. The victims were accused of allegedly being involved in tax evasion and money laundering. The fictitious IRBM officials also threatened to freeze the bank account in violation of the Anti-Money Laundering, Terrorist Financing, and Proceeds of Unlawful Activities Act (AMLA). To unfreeze the bank account, the victims must pay the required amounts. On the other hand, the payments are made to the bank account, which IRBM does not handle.

Another scenario reported that Malaysia Airlines (MAS) received many screenshots of fares that are not consistent with its system. According to MAS, there is a fake website using the MAS name. This fake website can be discovered by searching in Google, and it displays incorrect fares. MAS urged the users to verify the correct URL, www.malaysiaairlines.com, before booking any flight tickets. Furthermore, the users can also utilize MAS mobile application to search or book flights and appointed agents (Malaysian Airlines, 2020).

Amid the Covid-19 pandemic in Malaysia and the movement control order (MCO), cybersecurity incidents increased by up to 82.5 percent (Meikeng, 2020). Between the commencement of the MCO on March 18, 2020, and the end of the year, 838 incidents were reported to CyberSecurity Malaysia, compared to 459 incidents in the same period last year. During the MCO, most incidents involved phishing and other forms of fraud. Fraudsters utilized Covid-19 themes through phishing e-mails to lure individuals and distribute fake news through numerous channels, including e-mail and a hacked unknown website.

Other than that, Malaysian policies recorded a 20% increase in bogus phone call cases during the MCO, with losses amounting to close to half a million (Nordin, 2020). The cases have increased to 34 cases compared with 28 cases, with recorded losses at RM 480,000 as of May 2020. The fraudsters would impersonate enforcement agencies such as the police and deceive them by saying they have a police record or a court case. To resolve the case, the victim must provide personal information and make payments. The fraudster was also able to create phone numbers that were identical to those used by law enforcement. The main difference is that instead of +60, the fraudster would generally utilize area codes such as +80, +90, and others, followed by agency numbers.

Furthermore, the IRBM has warned Malaysians not to be duped by scammers who send false text messages saying they have qualified for the Bantuan Prihatin Nasional (BPN) during the MCO (Yeoh, 2020). The bogus text messages received from personal phone numbers asked recipients to reply with their personal and financial information and promised that they would be paid within 24 hours (Figure 1). The IRBM has provided an example of legitimate text messages, which will be delivered from phone numbers such as 62000 or 63833 (Figure 2). Personal information, such as complete names and financial information, will never be requested in text messages.

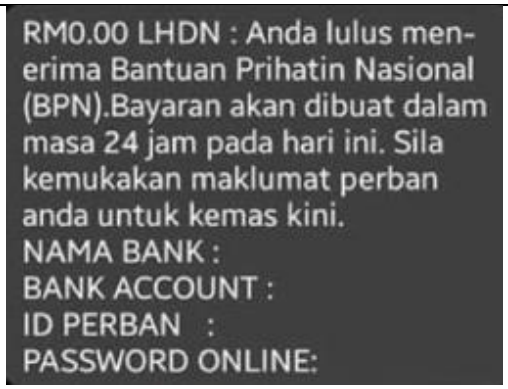

Figure 1. Example of a fake text message of Bantuan Prihatin Nasional (BPN) (Bernama, 2020)

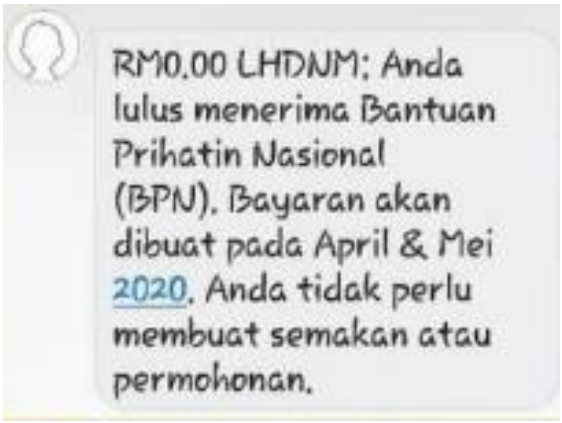

Figure 2. Example of the genuine text message by the Inland Revenue Board Malaysia (IRBM) (Yeoh, 2020)

The motivation of this study is to explore phishing as cyber fraud. Previous studies that explore phishing are mostly in the western and developed countries such as Australia. Most past studies looked at the strategies to combat phishing attacks (Maurya & Jain, 2020; McCombie & Pieprzyk, 2010). The fraudsters always develop new phishing techniques and take the opportunity in the current situation to attack their victims. Given many phishing cases reported in Malaysia, and in 2020, the phishing cases arise amidst the Covid-19 pandemic, it shows that this issue with the level of phishing awareness (pre-phishing) is still low. Not to mention the implications (post-phishing) and the governance to prevent it. Although there are studies on the implications and governance of cyber fraud, very little research exists on the implications and governance of phishing attacks within a Malaysian context. Therefore, this study will fill this gap.

The structure of this paper is as follows. The following section describes phishing as cyber fraud. Section 3 explains the implications of phishing attacks, followed by section 4 that explains the governance to prevent phishing attacks. The final section concludes the paper.

2. Phishing

In 1996, the term "phishing" was established based on an analogy in which fraudsters exploited telecommunication as a fishing hook to "phish" sensitive data such as usernames, passwords, and other personal information (Martino & Perramon, 2011).

According to Martino and Perramon (2011), the first two letters "ph" is thought to be derived from the term "phreaking," which means "hack into" telecommunication systems.

In the late 1990s, many fraudulent individuals registered with the America Online (AOL) network system website using bogus credit card data, which was the first phishing assault (Jain & Gupta, 2017). Gupta et al. (2017) stated an evolution of phishing from 1996 to 2014. In 1997, the media declared the change of a new attack called "phishing". Then, in 1998, the fraudsters started using messages and newsgroups to attack the victims, while in 1999, mass mailing was introduced and used to escalate the phishing attack. From 2000 until 2003, the fraudsters used URL, screen logger, instant messaging (IM), and internet relay chat (IRC) to attack the victims. Later, in 2006, the fraudsters firstly attack the victims via Voice over Internet Protocol (VoIP). In 2007, more than USD 3 billion was lost to phishing scams, and later in 2010, it was reported that Facebook gains more phishing attacks than Google. In 2012, about 6 million unique malware samples were identified, and in 2014, there were about 750,000 malicious e-mails sent using the Internet of Things (IoT) devices such as smartphones.

2.1. Types of Phishing

2.1.1. Spoofing E-Mail, Spear Phishing, and Whaling

One of the phishing attacks is spoofing e-mail. Spoofing e-mail is the creation of e-mail messages with a forged sender address (Romney & Steinbart, 2018). The e-mails seem like messages sent to the victims, and the contents in the e-mails trick the victims into opening the E-mail (Gupta et al., 2016). These spoofing e-mails can be easily achieved with a working Simple Mail Transfer Protocol (SMTP) server and mailing software like Outlook or Gmail (Chhabra & Bajwa, 2015). Once an e-mail message is composed, the fraudster or scammer can forge the fields within the message header, such as the FROM, REPLY-TO, and RETURN-PATH addresses (Sanchez & Duan, 2012). After the e-mail is sent, it will appear in the recipient's mailbox (Sanchez & Duan, 2012). As a result, spoofing e-mail may easily trick consumers into revealing information by reading or clicking on the e-mail.

In 2005, the term spear-phishing was first used (Gupta et al., 2017). Spear phishing's concept is similar to spoofing e-mail, where the fraudsters trick the victims into providing credential information via e-mail. However, spear phishing targets specific individuals or groups, while spoofing e-mail attacks random users (Chaudhry et al., 2016). For spear-phishing, the fraudster usually will do some research on the potential victims before attacking them. The same method has also been used to attack high-rank officers and prominent people, such as the senior executives of an organization and government officials called whaling. Whaling attack also aims to steal money or sensitive data of high-level officers for illegal purposes (Chaudhry et al., 2016). In these scenarios, the organization should be more aware of the e-mails that arrive in the organization's e-mail, mainly external e-mail messages. The fraudsters commonly use tactics using the display of the trusted people or organizations' names and send the messages via external e-mail addresses to trap the victims.

2.1.2. SMiShing

The other phishing attack is SMS phishing or SMiShing, which uses short messaging services (SMS) or text messages on mobile phones (Romney & Steinbart, 2018). SMiShing usually attacks the victims, such as bankers, system administrators, and law enforcement agencies, by sending text messages that impersonate the sources and a vital text message notifying the victims about information or account number having been stolen or frozen (Yeboah-Boateng & Amanor, 2014). In these situations, the fraudsters usually ask the victims to open the website or dial the phone number to verify the account information. The fraudsters typically deceive the victims by asking them to withdraw the money and send it to the fraudster or steal the victims' information by giving an attachment for the victims to download. The attachment usually contains a virus or malware which can hack the victims' phones, and the fraudster can access all information such as contacts, applications, and messages on the phones.

2.1.3. Vishing

As SMishing is a phishing attack via SMS or text messages, vishing is a phishing attack via phone call. The term "Vishing" is derived from the combination of "voice" and "phishing" (Romney & Steinbart, 2018). Vishing is an act of using telephone services to deceive the victims into surrendering private data and information to the fraudster (Yeboah-Boateng & Amanor, 2014). The victims are usually unaware of the fraudster's ability to use an advanced automated system to commit this kind of fraud. Also, Yeboah-Boateng and Amanor (2014) stated that vishing uses the practice of leveraging Voice over Internet Protocol or VoIP. This practice delivers voice communications and multimedia sessions over Internet Protocol (IP) networks to imitate trusted agencies such as banks and enforcement agencies, including police, customs, anti-corruption commission, and many more to deceive the victims (Yeboah-Boateng & Amanor, 2014). In this situation, victims usually follow all the instructions from the call, as they are confident that it is the actual calls from the trusted agencies.

2.1.4. Search Engine Phishing and Pharming

Search engine phishing is a type of phishing attack using bogus web pages. The fraudster will create fake web pages which offering cheap products and incredible deals and get them indexed by legitimate

search engines (Suganya, 2016). These bogus web pages usually will trigger upon a specific Google result page, as shown in Figure 3, and the online shoppers will click on those web pages. The online shoppers will provide their personal and confidential information such as address, ID number, bank account number, credit and debit card number. They believe they are accessing genuine web pages (Chaudhry et al., 2016). Other than search engine phishing, the fraudsters also used another method which is called pharming. The evolution of pharming started in 2004 (Gupta et al., 2017). The fraudsters will modify the host files or install the malicious codes in the Domain Name System (DNS) website (Chaudhry et al., 2016). As a result, the website link will return as a bogus website.

The users need to check the originality of the web pages before doing any transactions or providing any sensitive information. Based on the Cloudflare website (2021), an American web infrastructure and website-security company, HTTP stands for Hypertext Transfer Protocol, a protocol or prescribed order where the data is passed between the web browser and network. The S in HTTPS stands for 'Secure' as this website has a secure connection. As a result, the link with HTTPS is more secure than HTTP. A website that uses HTTP has HTTP:// in its weblink, while HTTPS has HTTPS://. Between June 2015 and June 2016, Google reported a 13% increase of HTTPS requests served (Finamore et al., 2017). HTTPS is valuable because it protects all communication and customer information and legitimizes any sites. On the online shopping website, the customers will be safer to shop at websites with HTTPS.

Other than that, the users also need to pay attention to hyperlinks or URLs. URL, which is known as Uniform Resource Locator, is the access web address. The URL of phishing websites looks similar to the original URL, which is why phishing websites have trapped many people. The fraudster will steal the users' information when the users provide sensitive information through phishing URLs (Suganya, 2016).

Furthermore, the users also need to check the content of the websites before doing any transactions or provide any sensitive information. The fraudsters create bogus websites similar to the actual websites to deceive web visitors and steal their personal information. Moreover, the logo and the appearance of legitimate websites are easy to copy.

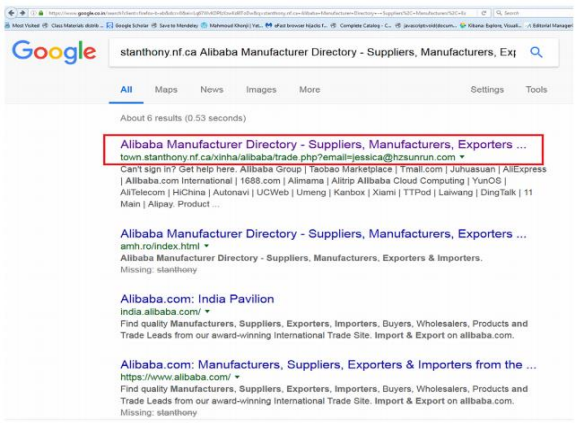

Figure 3. Example of phishing websites in Google result page (Rao & Pais, 2019)

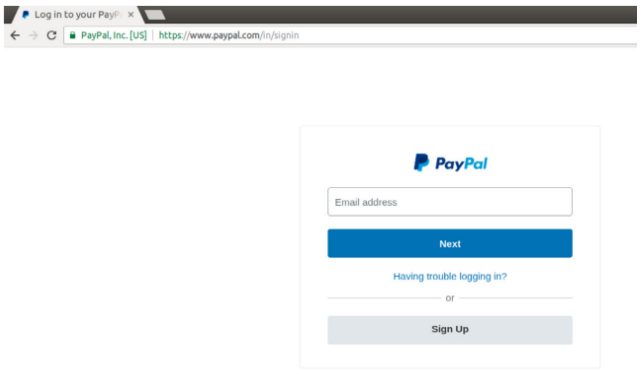

Figure 4. Example of a legitimate website (Rao & Pais, 2019)

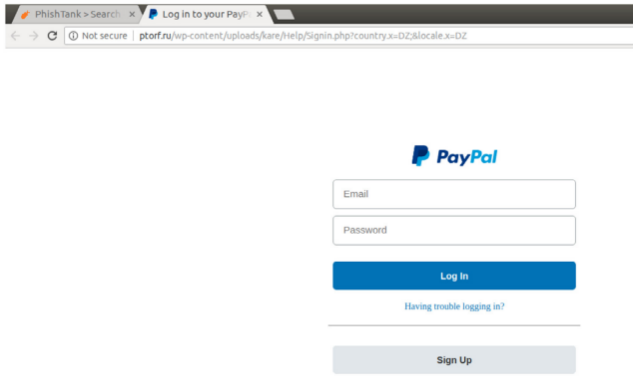

Figure 5. Example of a phishing website (Rao & Pais, 2019)

Figures 4 and 5 show the example of legitimate and phishing websites based on Rao and Pais (2019). It shows that phishing websites do not contain HTTPS in the URL. There are some differences between legitimate and phishing websites where there is a password box in the phishing website, while in a legitimate website, the users need to click 'Next' to key in the password. Furthermore, the font of 'Having trouble logging in?' is smaller, and there is no 'or' in-between 'Having trouble logging in?' and 'Sign Up' compared to legitimate websites. Other than these examples, some phishing websites contain fake logos, no contact information provided, and some sentence structure, grammar, and spelling errors. Other than that, the users shall check for the padlock or lock icon displayed in the web browser (Figure 6). The padlock or lock icon indicates the secure mode of communication in the web browser where the data is encrypted. This

icon will prevent other people from modifying the data of the users.

Figure 6. Example of the padlock icon in the web browser (Rao & Pais, 2019)

2.2. Statistics of Phishing around the World

PhishLabs is a cyber-security expert from the US, and they provide external intelligence, incident reports, and security awareness training to mitigate digital risks. Phishing Trends and Intelligence Report 2018 by PhishLabs states that the United States is the most popular choice for fraudsters and hosts 56% of all phishing infrastructure. After the United States, the following countries, where fraud is the most popular, are France and Germany, with about 4%, and Great Britain and Canada, with about 3%. Besides these countries, South and Southeast Asia countries are not excluded from fraudsters to host their infrastructure and show tremendous growth. Singapore has increased by about 88% in phishing infrastructure and volume, France - by about 82%, Ukraine - by about 70%, Indonesia - by about 40%, and Malaysia - by about 39%.

According to the Anti-Phishing Working Group (APWG)'s Phishing Activity Trends Report for the Second Quarter of 2018, the payment industry is the most targeted industry sector, accounting for roughly 36% of all phishing victims. After the payment business, the next most targeted industrial sector is a software as a service (SaaS) or webmail, accounting for about 21% of the total. Software as a Service (SaaS) is a service delivery approach for software. A third-party provider will host the application and rent IT solutions to the users and make it available for customers to purchase or develop over the Internet (Kim et al., 2016). Examples of SaaS are Google Apps, Amazon Web Services, and Dropbox. The financial institution sector accounts for approximately 16 percent of phishing attacks, and cloud storage or file hostings, such as Google Drive, Flickr, and Picasa, account for about 9 percent. Social media shows 4% of the most targeted industry or sector.

3. Implications of Phishing Attack

Several impacts occurred if the phishing attack is not mitigated. One of the effects is that it will lead to monetary losses as the fraudsters take the money and negatively impact the country's society and economic growth. Monetary costs are the funds or expenditures used for personal and family needs and the cost of purchasing material, production, services, and marketing in an organization. Monetary losses are the amount of money lost (Wardman, 2016). Monetary losses also include theft of valuable and sensitive information of customers, stakeholders and organizations, and computer troubleshooting costs (Kamruzzaman et al., 2016).

Other than that, the phishing attack can reduce the trust of the stakeholders and consumers for online activities. It also can damage the brand reputation of an organization. The brand is the foundation of every company's market capitalization. For example, suppose one organization has been attacked and encountered phishing websites under their brand. In that case, the legitimate websites will also be affected and blacklisted by the users for an extended period even though the phishing websites have been removed from the blacklisted domain (Mohammad et al., 2015). The users have lost their trust, and the organization needs to work hard to gain back confidence from the users.

Besides that, the impact of phishing is identity theft. Identity theft is one of the worst potential consequences of phishing which could cause massive financial loss, psychological and emotional impacts (Vučković et al., 2018). Identity theft is a type of fraud involving using other people's identities to steal money or gain other benefits (Romney & Steinbart, 2018). The fraudsters also can pretend or disguise to be the victims for any purpose. There was one case in the US in 1994 where a 12-year-old boy, Gabriel Jimenez's identity, was stolen. Her mother, Jeri Marks, first discovered the problem when her son, Gabriel Jimenez, has filed the taxes for work as a child model. Then, she found out an illegal immigrant stole and used her son's identity. Despite notifying the police, the Internal Revenue Service (IRS), and the Social Security Administration, the situation persisted. Even though Gabriel Jimenez had reached adulthood, the situation had worsened (Whitaker, 2007).

3.1. Implications for Individuals

Firstly, the individual or the users should be careful of social engineering techniques used by the fraudster to deceive the victims. The users should be suspicious when they receive calls, messages, or e-mails with a sense of excitement and panic, such as about winning a considerable sum of money, urgency, and obtaining a warrant from authority. When the users receive calls from the people who claim from authority organizations such as the Malaysian Anti-Corruption Commission (MACC) and the Royal Malaysia Police, the users should be calm and not panic.

The users can check the authorization or identity of the callers, such as full name, the organization name, location, organization branch, and many more. The users shall hang up the call if they realize it is a phishing attack, or the callers insist the users reveal their sensitive information such as username, passwords, bank account, and credit card details. Another option is the users can hang up the calls, claiming that they are from authority organizations without further asking for information and directly calling the organizations for confirmation. The users should not reveal any confidential information to other

people under any circumstances and should not deposit money to strangers when requested. Furthermore, the users should never allow the caller to control computers, smartphones, and tablets because the fraudsters might hack the devices to collect the information.

When users want to do online shopping or online banking, they should avoid phishing websites. When they search the website on the Google result page, they need to check whether there are multiple domains with the exact name on the Google result page because one of those websites might be a phishing website. The users should ensure the correct URL of the website. If the users are suspicious about the originality of the website, they can call several organizations directly on the website to ensure the originality. Phishing usually does not provide contact information, and phone numbers usually cannot be reached. Furthermore, the users should also check the website's grammar, spelling, and logo before doing any transaction or entering confidential information. The users should also ensure the website contains 'HTTPS in the URL and padlock icon to secure the data to avoid phishing threats.

Furthermore, the users can use the same application to handle online websites while taking e-mails messages. When users get e-mails or texts from firms demanding personal information such as passwords, identification numbers, security numbers, bank account, or credit card details, they should be cautious. Legitimate companies will never ask the users to verify or provide confidential information in unsolicited e-mail or messages. Besides, when the users receive the e-mails, they need to check the e-mail address, spelling, sentence structure, and grammar and see if it is intentionally misleading. The users can also call the company that sent the e-mail message if they doubt the origin of the e-mail received.

Based on the Cyber Security Awareness Alliance website, a Singapore Government Agency website, the users can hover over the hyperlink in the e-mail message before clicking on it. It is because a small window will appear to show where the link leads. The users should not click the hyperlink if the link does not match the company which sent the e-mail message and should not respond and download any attachment in the suspected phishing e-mails or messages. Furthermore, for office e-mail, the users should ensure whether the e-mail is from an external source since most phishing e-mails begin with messages from an external e-mail system. Then, the users can also report on phishing e-mails to the responsible team through their office e-mails.

Moreover, users need to be concerned about their password usage and anti-virus to secure and protect the data. The users should scan all removable drives before using them on the computer to avoid a virus attack. The users also should install and update the anti-virus software in electronic devices to protect their devices from virus attacks. They should not easily download any freeware on the Internet as some freeware might contain viruses that can harm the users' computers and devices.

For password usage, Kennedy et al. (2016) suggested that users should have good credential passwords requiring a length of 6 to 8 characters, consisting of uppercase, lowercase, numbers, and special characters. The passwords should be unique and do not contain familiar characters such as 123456, full name, and date of birth. Other than that, the passwords should be different for different applications to avoid the risk of a phishing attack. The fraudsters will access other accounts once they can detect the password if the users use the same passwords for different applications.

The users need to upgrade their phishing knowledge by reading phishing materials on the Internet, social media, and bank websites. At the same time, they also need to update themselves with the current news, primarily related to the phishing attack. It is because the fraudsters always upgrade their phishing techniques to deceive their victims. The users also should immediately report to the banks when there is a suspicious transaction in their bank account. Other than that, the user can write to MCMC whenever they encounter any phishing e-mails or sites. MCMC will immediately remove the phishing site to safeguard Malaysian Internet users from the attack. The users need to protect themselves against phishing threats.

3.2. Implications for Companies

All companies should also take some actions to enhance awareness among the employees and avoid phishing threats. Companies can conduct phishing assessments to increase employees' awareness about phishing. Phishing assessment is deceptive e-mails sent to employees within the companies to test the level of security awareness. These e-mails imitate phishing e-mails with social engineering where hyperlinks, open file attachments, and access to provide sensitive information are attached in these e-mails. Ikhsan and Ramli (2019) stated that phishing assessment gives knowledge and simulates real cases where the employees can safeguard themselves when facing real phishing e-mails in the future.

Furthermore, companies also need to provide regular training and programs to increase employees' security awareness. The companies can send standard information and knowledge of phishing through office e-mails and websites. At the same time, the companies can always provide the latest news and updates about phishing, especially on the current situation or method used in phishing to the employees. In addition, the companies also need to ensure the employees' anti-virus is constantly updated to secure and protect the data. Other than that, the corporations such as banks and e-commerce should provide relevant information about phishing to their customers in websites, applications, commercial and digital, or e-flyers to increase customer awareness, especially when the customers are handling online money transfers and e-commerce services.

For password usage, Kennedy et al. (2016) mentioned that other than having good credential passwords and use different passwords for different applications, the passwords also should be changed regularly to reduce the exposure to a phishing attack. In this situation, Kennedy et al. (2016) mentioned that a password expiration policy should be implemented in a certain period, such as the passwords should be changed every 90 days. Password expiration policy is also recommended by the National Institute of Standards and Technology (NIST). These recommendations can be implemented in companies and customer dealing institutions such as banks and e-commerce corporations to protect and secure employees and customers from phishing attacks.

3.3. Implications for Government

The government should take action to mitigate phishing attacks. The government agencies such as MCMC and CyberSecurity Malaysia shall conduct an awareness program to increase phishing awareness among the public. MCMC and CyberSecurity Malaysia can share information and current news about phishing on their official websites and social media such as Facebook, Instagram, Twitter, and many more. It is because people tend to use social media more to know the current issue and information.

Furthermore, the government agencies also shall use the media platform to do commercial and advertisement to give information about phishing. The platforms could include television, YouTube, Iflix, and the ad before the cinema begin. In commerce and advertising, the government agencies shall provide basic knowledge about phishing, the medium used for a phishing attack, how to avoid phishing attacks, and give information on how the public can make a report about phishing.

Also, the government agencies shall monitor the companies to ensure they provide relevant training and exercise to increase phishing awareness among the employees. Moreover, the government agencies can also introduce the platform to refresh the current updates and list fraud e-mails, websites, and phone numbers for the public to refer to. In Australia, Australia Competition and Consumer Commission (ACCC) has established a 'scamwatch' based on Figure 7 to provide information about scams to consumers and businesses. This website also provides the current news about fraud, reporting fraud, types of scams, and scam statistics. Malaysia can take this example to introduce a sole platform to give public citizens information on deception and cyber fraud.

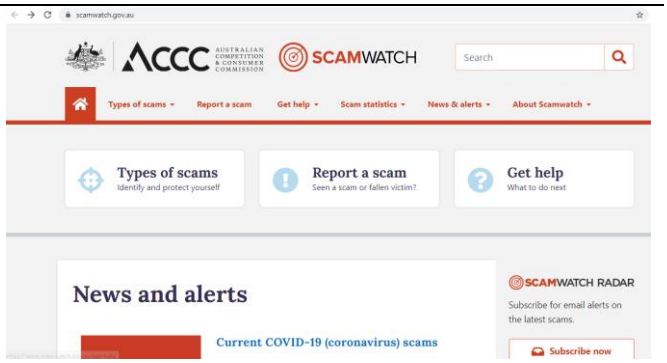

Figure 7. Australian scamwatch website (Australian Competition and Consumer Commission, 2021)

4. The Governances to Prevent Phishing Attack

In this era of technology, many companies adopt digital strategies at the forefront of their company agenda. However, cyber frauds such as phishing attacks are still being neglected. Understanding cyber risks and information security practices is an essential step to be taken by companies to prevent any cyber frauds, especially phishing attacks. Kazemi et al. (2012) and Hsu and Wang (2015) mentioned that top management consists of the board and senior management is responsible for implementing information security programs and risk management safeguard organizational assets. A survey done by Kankanhalli et al. (2003) on information security managers from various sectors showed that top management organizations with stronger support provide more preventive efforts than top management with weaker support. Sonnenschein et al. (2017) found that top management awareness is crucial for effective IT security management.

4.1. Capital Market

In Malaysia, Securities Commission Malaysia issued Guidelines on Management of Cyber Risk on October 31, 2016. This guideline applies to all capital market entities in Malaysia. The guidelines set out the board of directors' and management's roles and responsibilities in the oversight and management of cyber risk, cyber risk policies and procedures that capital market entities should develop and implement, requirements for managing cyber risk, and reporting requirements to the Securities Commission Malaysia (2016).

Securities Commission Malaysia (2016) emphasized that the board must provide surveillance to manage cyber risk as part of the general risk management framework of the capital entity. The board must ensure that the board's capital market's cyber risk policies and procedures are given to the board for approval. Management should ensure that the authorized cyber risk policies and procedures are followed. The boards must then evaluate the efficacy of cyber risk policies execution and ensure that policies and processes, such as performance indicators, are reviewed regularly. Furthermore, the boards also need to ensure adequate

resources to assign accountable, responsible persons to manage cyber risk. The boards also must ensure that management continues to encourage cyber resilience awareness at all levels of the organization. Additionally, boards must ensure that the impact of cyber risk is appropriately analyzed before performing new operations and that the board is kept up to date and informed of new or emerging trends and cyber threats.

Besides that, management also is responsible for implementing cyber risk policies and procedures. The policies and procedures must contain a clear explanation of the cyber risk tolerance, including the frequency and severity of cyber breaches, the maximum service downtime, the potential for negative media attention, and regulatory and financial consequences. The policies and procedures must also have the processes for identifying, detecting, assessing, and escalating cyber breaches for decision-making and requires third-party service providers to adhere to the entity's information security policy. Communication protocols, including reporting procedures, must be included in the rules and procedures during a cyber breach. The management also must periodically update and report any emerging cyber violation and its impact on the entity.

Furthermore, the management must also recommend to the board any appropriate strategies and measures to manage cyber risk, including prevention, detection, and recovery measures. The management also shall make necessary changes to existing policies and procedures for better cyber risk management. The preventive measures that can be implemented include deploying anti-virus and malware software to identify and isolate harmful code and create firewalls to eliminate weak points and prevent an attacker from obtaining access to a company's network. Furthermore, cyber incident detection measures include the following: (i) identifying cyber risk scenarios to which the business is most likely exposed, (ii) detecting capital market incidents, analyzing the effect of cyber risk occurrences, and (iii) determining an adequate reaction and communication strategy. When a cyber breach is discovered, it should be reported to an incident response team, management, and the board of directors. Furthermore, critical systems and services should be recovered within the entity's stated recovery time target for recovery methods. The company should create a complete business continuity and recovery strategy for the designs, operations, and services emerging from a cyber breach.

4.2. Financial Institution

Phishing attacks rely on social networking and electronic communication technology. For financial institutions, the Central Bank of Malaysia implemented risk management in technology (RMiT). The policy came into force on January 1, 2020. The board must create and approve a technological risk appetite that is matched with the financial institution's risk appetite requirement (Central Bank of Malaysia, 2020). The board should also monitor and assess how well the technology risk management framework (TRMF) and cyber resilience framework (CRF) are implemented.

Furthermore, the board must designate either a board-level committee with technology knowledge or a separate committee with technology experience to assist the board in providing oversight over technology-related issues. The board must ensure that the financial institution's IT and cybersecurity strategy plans are sufficient for at least three years. The board of directors must monitor the financial institution's technological risk by ensuring that the key performance indicators and risk indicators are in place.

Aside from that, the board audit committee is in charge of assessing and correcting the technological control gap and ensuring that technology audit scope, methods, and frequency are suitable.

In addition, senior management is accountable for ensuring that the financial institution's technology risk policy is implemented effectively. Senior management must incorporate the TRMF and CRF, which have been authorized by the board, into particular policies and processes that are in line with the approved risk appetite. Top management must form a cross-functional committee that comprises senior executives from both technology functions and core business divisions to be in charge of overseeing the strategic technology plan's execution, as well as the rules and procedures that go with it. This cross-functional group is also in charge of keeping the board up to date on important technological issues and approving any deviations from technology policy. Senior management must assign qualified personnel and resources to assist the efficient management of technology risk by maintaining resilient technology systems.

4.3. Government

Malaysian Administrative Modernization and Management Planning Unit or MAMPU has developed Cyber Security Framework for Public Sector or 'Rangka Kerja Keselamatan Siber Sektor Awam' (RAKKSSA) to provide information security guidelines to the government ministries and agencies to protect their data in digital technology (Masrek et al., 2019). There are eight major components of RAKKSSA (Malaysian Administrative Modernization and Management Planning, 2016). The first component is to identify where all government ministries should identify the roles and responsibilities of the governance structure at each level, the laws and regulations, assets to be protected, and the associated risks. The second component is protected in which to reduce the risks identified, the required security concepts, technology, procedures, and human skills must be developed. The third component is used to identify malicious assaults by identifying unusual patterns of use and network traffic.

The fourth component is to ensure that appropriate actions in response to these harmful assaults are taken and increase communications with stakeholders and the broader public. The fifth component, recovered,

concerns the capacity to recover from malicious assaults and system failures to maintain information availability. The sixth component is procured to ensure that security measures and requirements are followed throughout the system's lifespan, regardless of whether they were acquired through external acquisition or in-house development. This critical component covers procurement requirements, vendor management, resource footprint, system development life cycle, and more. A security audit is the eighth component. The audit and enforcement agencies' scope of audit and enforcement is defined by the eight components, which cut across all components.

5. Conclusion

This study adds in the literature about the implications of phishing attacks and the governance to prevent phishing attacks. In general, phishing could not be eliminated, but to some extent, it can be mitigated. Therefore, this study puts forth the importance of awareness and the implications of phishing to individuals, companies, and the government. This study highlights the importance of having a high level of understanding of phishing that will help to reduce the possibility of becoming the victims. Hence, some action and efforts to upgrade oneself about phishing knowledge are essential, especially in the world full of uncertainties that we live in today.

Acknowledgments

The study is supported by the Fundamental Research Grant Scheme (FRGS, Reference code: FRGS/1/2019/SS01/UITM/02/34) provided by the Ministry of Higher Education (MOHE) of Malaysia, and the authors thank the Ministry for its research support. The authors also would like to thank the Universiti Teknologi MARA Selangor, Kampus Puncak Alam for providing this opportunity.

References

[1] ALBRECHT, W.S., & ALBRECHT, C. (2004). *Fraud examination & prevention*. Mason, Ohio: Thomson/South-Western.

[2] ANTI-PHISHING WORKING GROUP. (2020). *Phishing Activity Trends Report: 2nd Quarter 2018. Unifying the Global Response to Cybercrime*. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q2_2018.pdf

[3] ARACHCHILAGE, N.A.G., & LOVE, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304-312. https://doi.org/10.1016/j.chb.2014.05.046

[4] AUSTRALIAN COMPETITION AND CONSUMER COMMISSION. (2021). *Home: Scamwatch.* Retrieved from https://www.scamwatch.gov.au/

[5] BERNAMA. (2020). *Bantuan Prihatin: LHDN nafi minta maklumat perbankan menerusi SMS bernama.* Sinar Harian. Retrieved from https://www.sinarharian.com.my/article/77055/KHAS/Covid-19/Bantuan-Prihatin-LHDN-nafi-minta-maklumat-perbankan-menerusi-SMS

[6] CENTRAL BANK OF MALAYSIA. (2020). *Risk Management in Technology (RMiT).* Retrieved from https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+%28RMiT%29.pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078

[7] CHAUDHRY, J.A., CHAUDHRY, S.A., & RITTENHOUSE, R.G. (2016). Phishing attacks and defenses. *International Journal of Security and Its Applications*, 10(1), 247-256. http://dx.doi.org/10.14257/ijsia.2016.10.1.23

[8] CHHABRA, G.S., & BAJWA, D.S. (2015). Review of E-mail System, Security Protocols and Email Forensics. *International Journal of Computer Science & Communication Networks*, 5(3), 201-211. Retrieved from https://www.researchgate.net/publication/286053691_Review_of_E-mail_System_Security_Protocols_and_Email_Forensics

[9] CLOUDFLARE. (2021). *What is HTTPS?* Retrieved from https://www.cloudflare.com/learning/ssl/what-is-https/

[10] FINAMORE, A., VARVELLO, M., & PAPAGIANNAKI, K. (2017). Mind the gap between HTTP and HTTPS in mobile networks. In KAAFAR, M., UHLIG, S., & AMANN, J. (eds.) *Passive and Active Measurement. PAM 2017. Lecture Notes in Computer Science,* Vol. 10176. Cham: Springer, pp. 217-228. https://doi.org/10.1007/978-3-319-54328-4_16

[11] GUPTA, B.B., TEWARI, A., JAIN, A.K., & AGRAWAL, D.P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, 28, 3629–3654. https://doi.org/10.1007/s00521-016-2275-y

[12] GUPTA, S., SINGHAL, A., & KAPOOR, A. (2016). A literature survey on social engineering attacks: phishing attack. *The International Conference on Computing, Communication and Automation*, Noida, India, 29-30 April 2016, pp. 537-540. https://doi.org/10.1109/CCAA.2016.7813778

[13] HANNA, K.T., FERGUSON, K., & BEAVER, K. (2021). *Data breach*. Search Security. Retrieved from https://searchsecurity.techtarget.com/definition/data-breach

[14] HSU, C., & WANG, T. (2015). Composition of the Top Management Team and Information Security Breaches. In CRUZ-CUNHA, M., & PORTELA, I. (eds.) *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*.

Hershey, Pennsylvania: IGI Global, pp. 116-134. http://doi:10.4018/978-1-4666-6324-4.ch008

[15] IKHSAN, M.G., & RAMLI, K. (2019). Measuring the information security awareness level of government employees through phishing assessment. *The 34th International Technical Conference on Circuits/Systems, Computers and Communications*, JeJu, Korea (South), 23-26 June 2019. https://doi.org/10.1109/ITC-CSCC.2019.8793292

[16] JAIN, A.K., & GUPTA, B.B. (2017). Phishing detection: Analysis of visual similarity-based approaches. *Security and Communication Networks*, 2017, 2017, 5421046. https://doi.org/10.1155/2017/5421046

[17] KAMRUZZAMAN, M., ISLAM, M.A., ISLAM, M.S., HOSSAIN, M.S., & HAKIM, M.A. (2016). Plight of youth perception on cyber crime in South Asia. *American Journal of Information Science and Computer Engineering*, 2(4), 22-28. Retrieved from http://files.aiscience.org/journal/article/html/70080067.html

[18] KANKANHALLI, A., TEO, H.H., TAN, B.C.Y., & WEI, K.K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2), 139-154. https://doi.org/10.1016/S0268-4012(02)00105-6

[19] KATKURI, S. (2018). Indian Cyber Law. *International Journal of Advanced Research and Development*, 3(1), 640-644. Retrieved from http://www.advancedjournal.com/archives/2018/vol3/issue1/3-1-158

[20] KAZEMI, M., KHAJOUEI, H., & NASRABADI, H. (2012). Evaluation of information security management system success factors: Case study of municipal organization. *African Journal of Business Management*, 6(14), 4982-4989. https://doi.org/10.5897/AJBM11.2323

[21] KENNEDY, L.Z., CHIASSON, S., & OORSCHOT, P.V. (2016). Revisiting password rules: Facilitating human management of passwords. *The APWG Symposium on Electronic Crime Research (eCrime)*, Toronto, Canada, 1-3 June 2016. https://doi.org/10.1109/ECRIME.2016.7487945

[22] KIM, S.H., JANG, S.Y., & YANG, K.H. (2016). Analysis of the determinants of software-as-a-service adoption in small businesses: risks, benefits, and organizational and environmental factors. *Journal of Small Business Management*, 55(2), 303-325. https://doi.org/10.1111/jsbm.12304

[23] KROMBHOLZ, K., HOBEL, H., HUBER, M., & WEIPPL, E. (2015). Advanced Social Engineering Attacks. *Journal of Information Security and Applications*, 22, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

[24] MALAYSIA COMPUTER EMERGENCY RESPONSE TEAM (MYCERT). (2021). *Incident statistics*. Retrieved from https://www.mycert.org.my/portal/statistics?id=b75e037d-6ee3-4d11-8169-66677d694932

[25] MALAYSIAN ADMINISTRATIVE MODERNIZATION AND MANAGEMENT PLANNING. (2016). *Rangka Kerja Keselamatan Siber Sektor Awam*. Retrieved from https://www.malaysia.gov.my/portal/content/30090?language=my

[26] MALAYSIAN AIRLINES. (2020). *Malaysia Airlines Cautions Customers of Fake Website*. Retrieved from https://www.malaysiaairlines.com/us/en/news-article/2020/malaysia-airlines-cautions-customers-fake-website.html

[27] MALAYSIAN COMMUNICATIONS AND MULTIMEDIA COMMISSION. (2021). *Phishing Attack*. Retrieved from https://www.mcmc.gov.my/en/faqs/phishing-attack

[28] MARTINO, A.S., & PERRAMON, X. (2011). Phishing Secrets: History, Effects, Countermeasures. *International Journal of Network Security*, 11(3), 163-171. Retrieved from https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.624.6627&rep=rep1&type=pdf

[29] MASREK, M.N., HARUN, Q.N., & RAMLI, I. (2019). The Role of Top Management in Information Security Practices. *The 6th International Conference on Education, Social Sciences and Humanities*, Istanbul, Turkey, 24-26 June 2019. Retrieved from https://www.researchgate.net/publication/338764650_THE_ROLE_OF_TOP_MANAGEMENT_IN_INFORMATION_SECURITY_PRACTICES

[30] MAURYA, S., & JAIN, A. (2020). Deep learning to combat phishing. *Journal of Statistics and Management Systems*, 23(6), 945-957. https://doi.org/10.1080/09720510.2020.1799496

[31] MCCOMBIE, S., & PIEPRZYK, J. (2010). Winning the phishing war: A strategy for Australia. *The 2nd Cybercrime and Trustworthy Computing Workshop*, Ballarat, Australia, 19-20 July 2010. https://doi.org/10.1109/CTC.2010.13

[32] MEIKENG, Y. (2020). *Cybersecurity cases rise by 82.5%*. The Star. Retrieved from https://www.thestar.com.my/news/focus/2020/04/12/cybersecurity-cases-rise-by-825

[33] MOHAMMAD, R.M., THABTAH, F., & MCCLUSKEYA, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review*, 17, 1-24. https://doi.org/10.1016/j.cosrev.2015.04.001

[34] NORDIN, R. (2020). *Cops record 20% increase in phone scams during MCO period*. The Star. Retrieved from https://www.thestar.com.my/news/nation/2020/05/19/cops-record-20-increase-in-phone-scams-during-mco-period

[35] PHISHLABS. (2018). *Phishing Trends and Intelligence Report 2018*. Retrieved from

https://www.phishlabs.com/whitepapers/2018-phishing-trends-intelligence-report/

[36] RAHIM, R. (2020). *IRB warns of fraudsters impersonating its officers in 'tax arrears' scam.* The Star. Retrieved from https://www.thestar.com.my/news/nation/2020/06/07/irb-warns-of-fraudsters-impersonating-its-officers-in-tax-arrears-scam

[37] RAO, S.R., & PAIS, A.R. (2019). Jail-Phish: An improved search engine-based phishing detection system. *Computers and Security*, 83, 246-267. https://doi.org/10.1016/j.cose.2019.02.011

[38] ROMNEY, M.B., & STEINBART, P.J. (2018). *Accounting Information Systems.* 14th ed. London: Pearson Education.

[39] SANCHEZ, F., & DUAN, Z. (2012). A sender-centric approach to detecting phishing e-mails. *The International Conference on Cyber Security*, Alexandria, Virginia, USA, 14-16 December 2012. https://doi.org/10.1109/CyberSecurity.2012.11

[40] SECURITIES COMMISSION MALAYSIA. (2016). *Guidelines on Management of Cyber Risk*. Retrieved from https://www.sc.com.my/api/documentms/download.ashx?id=9aaddb2e-aa13-409a-a47f-8d0124afd229

[41] SONNENSCHEIN, R., LOSKE, A., & BUXMANN, P. (2017). The Role of Top Managers' IT Security Awareness in Organizational IT Security Management. *The International Conference on Information Systems*, Seoul, South Korea, 10-13 December 2017.

[42] SPECIAL TO THE TIMES. (2020). *CBI issues alert about possible ID theft scams over 4th of July weekend.* The Fort Morgan Times. Retrieved from https://www.fortmorgantimes.com/2020/07/02/cbi-issues-alert-about-possible-scams-over-4th-of-july-weekend/

[43] SUGANYA, V. (2016). A review on phishing attacks and various anti phishing techniques. *International Journal of Computer Applications*, 139(1), 20-23. https://doi.org/10.5120/ijca2016909084

[44] VAN KESSEL, P. (2018). *Is cybersecurity about more than protection?* Retrieved from https://www.ey.com/en_gl/consulting/global-information-security-survey-2018-2019

[45] VUČKOVIĆ, Z., VUKMIROVIĆ, D., MILENKOVIĆ, M.J., RISTIĆ, S., & PRLJIĆ, K. (2018). Analyzing of e-commerce user behavior to detect identity theft. *Physica A: Statistical Mechanics and its Applications*, 511, 331-335. https://doi.org/10.1016/j.physa.2018.07.059

[46] WARDMAN, B. (2016). Assessing the gap: Measure the impact of phishing on an organization. *The 12th Annual ADFSL Conference on Digital Forensics, Security and Law*, Daytona Beach, Florida. Retrieved from https://commons.erau.edu/cgi/viewcontent.cgi?article=1366&context=adfsl

[47] WHITAKER, B. (2007). *Never too young to have your identity stolen.* The New York Times. Retrieved from https://www.nytimes.com/2007/07/21/business/21idtheft.html

[48] YEBOAH-BOATENG, E.O., & AMANOR, P.M. (2014). Phishing, SMiShing & Vishing: An assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, 5(4), 297-307. Retrieved from https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.682.2634&rep=rep1&type=pdf

[49] YEOH, A. (2020). *LHDN warns of SMS scam targeting Bantuan Prihatin Nasional recipients.* The Star. Retrieved from https://www.thestar.com.my/tech/tech-news/2020/04/03/lhdn-warns-of-sms-scam-targeting-bantuan-prihatin-nasional-recipients

[50] ZAHARI, A.I., BILLU, R., & SAID, J. (2017). *E-Commerce Fraud: An Investigation of Familiarity, Trust and Awareness Impact towards Online Fraud.* Retrieved from https://www.researchgate.net/publication/319311612_E-Commerce_Fraud_An_Investigation_of_Familiarity_Trust_and_Awareness_Impact_towards_Online_Fraud

参考文:

[1] ALBRECHT, W.S., & ALBRECHT, C. (2004)。**欺**诈检查和预防。俄亥俄州梅森：汤姆森/**西南**。

[2]**反网**络钓鱼工作组。(2020)。**网**络钓鱼活动趋势报告：2018 **年第二季度**。统一全球应对网络犯罪。取自 https://docs.apwg.org/reports/apwg_trends_report_q2_2018.pdf

[3] ARACHCHILAGE, N.A.G., & LOVE, S. (2014)。计算机用户的安全意识：避免网络钓鱼威胁的观点。人类行为中的计算机，38, 304-312。https://doi.org/10.1016/j.chb.2014.05.046

[4]**澳大利**亚竞争和消费者委员会。(2021)。**主**页：骗局。**取自** https://www.scamwatch.gov.au/

[5] 马来西亚。(2020)。爱心援助：LHDN 拒绝通过短信要求提供银行信息。**西**纳哈里安。取自 https://www.sinarharian.com.my/article/77055/KHAS/Covid-19/Bantuan-Prihatin-LHDN-nafi-minta-maklumat-perbankan-menerusi-SMS

[6] 马来西亚中央银行。(2020)。**技**术风险管理(米特)。**取自** https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+%28RMiT%29.pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592

[7] CHAUDHRY, J.A.、CHAUDHRY, S.A. 和 RITTENHOUSE, R.G. (2016)。网络钓鱼攻击和防御。国际安全杂志及其应用，10(1)，247-256。http://dx.doi.org/10.14257/ijsia.2016.10.1.23

[8] CHHABRA, G.S., & BAJWA, D.S. (2015)。审查电子邮件系统、安全协议和电子邮件取证。国际计算机科学与通信网络杂志，5(3)，201-211。取自 https://www.researchgate.net/publication/286053691_Review_of_E-mail_System_Security_Protocols_and_Email_Forensics

[9] 云耀。(2021)。什么是HTTPS？取自 https://www.cloudflare.com/learning/ssl/what-is-https/

[10] FINAMORE, A., VARVELLO, M., & PAPAGIANNAKI, K. (2017)。注意移动网络中 HTTP 和 HTTPS 之间的差距。在 KAAFAR, M., UHLIG, S., & AMANN, J. (编辑。) 被动和主动测量中。聚丙烯酰胺2017。计算机科学讲义，卷。 10176. 查姆：斯普林格，第 217-228 页。 https://doi.org/10.1007/978-3-319-54328-4_16

[11] GUPTA, B.B., TEWARI, A., JAIN, A.K., & AGRAWAL, D.P. (2017)。打击网络钓鱼攻击：最新技术和未来挑战。神经计算与应用，28, 3629–3654。https://doi.org/10.1007/s00521-016-2275-y

[12] GUPTA, S., SINGHAL, A., & KAPOOR, A. (2016)。关于社会工程攻击的文献调查：网络钓鱼攻击。计算、通信和自动化国际会议，印度诺伊达，2016 年 4 月 29-30 日，第 537-540 页。https://doi.org/10.1109/CCAA.2016.7813778

[13]汉娜，K.T.，弗格森，K.，和比弗，K.（2021）。数据泄露。搜索安全。取自 https://searchsecurity.techtarget.com/definition/data-breach

[14] HSU, C., & WANG, T. (2015)。最高管理团队的组成和信息安全漏洞。在 CRUZ-CUNHA, M., & PORTELA, I. (编辑。) 数字犯罪、网络空间安全和信息保障研究手册。宾夕法尼亚州赫尔希：IGI全球，第 116-134 页。http://doi:10.4018/978-1-4666-6324-4.ch008

[15] IKHSAN, M.G., & RAMLI, K. (2019)。通过网络钓鱼评估衡量政府工作人员的信息安全意识水平。第 34 届国际电路/系统、计算机和通信技术会议，韩国济州（南），2019 年 6 月 23-26 日。https://doi.org/10.1109/ITC-CSCC.2019.8793292

[16] JAIN, A.K., & GUPTA, B.B. (2017)。网络钓鱼检测：基于视觉相似性的方法分析。安全与通信网络，2017，2017，5421046。https://doi.org/10.1155/2017/5421046

[17] KAMRUZZAMAN, M., ISLAM, M.A., ISLAM, M.S., HOSSAIN, M.S., & HAKIM, M.A. (2016)。南亚青年对网络犯罪的认知困境。美国信息科学与计算机工程杂志，2(4)，22-28。取自 http://files.aiscience.org/journal/article/html/70080067.html

[18] KANKANHALLI, A., TEO, H.H., TAN, B.C.Y., & WEI, K.K. (2003)。信息系统安全有效性的综合研究。国际信息管理杂志，23（2），139-154。https://doi.org/10.1016/S0268-4012(02)00105-6

[19] KATKURI, S. (2018)。印度网络法。国际高级研究与开发杂志，3(1)，640-644。取自 http://www.advancedjournal.com/archives/2018/vol3/issue1/3-1-158

[20] KAZEMI, M., KHAJOUEI, H., & NASRABADI, H. (2012)。信息安全管理系统成功因素评估：市政组织案例研究。非洲商业管理杂志，6(14)，4982-4989。https://doi.org/10.5897/AJBM11.2323

[21] 肯尼迪, L.Z., CHIASSON, S., & OORSCHOT, P.V. (2016)。重新审视密码规则：促进密码的人工管理。亚太工作组电子犯罪研究研讨会(电子犯罪)，加拿大多伦多，2016 年 6 月 1 日至 3 日。https://doi.org/10.1109/ECRIME.2016.7487945

[22] KIM, S.H., JANG, S.Y., & YANG, K.H. (2016)。小型企业采用软件即服务的决定因素分析：风险、收益以及组织和环境因素。小企业管理杂志，55（2），303-325。https://doi.org/10.1111/jsbm.12304

[23] KROMBHOLZ, K., HOBEL, H., HUBER, M., & WEIPPL, E. (2015)。高级社会工程攻击。信息安全与应用杂志，22, 113-122。https://doi.org/10.1016/j.jisa.2014.09.005

[24] 马来西亚计算机紧急响应小组（MYCERT）。(2021)。事件统计。取自 https://www.mycert.org.my/portal/statistics?id=b75e037d-6ee3-4d11-8169-66677d694932

[25]马来西亚行政现代化和管理规划。(2016)。公共部门网络安全框架。取自 https://www.malaysia.gov.my/portal/content/30090?language=my

[26]马来西亚航空公司。(2020)。马航警告假网站客户。取自 https://www.malaysiaairlines.com/us/en/news-article/2020/malaysia-airlines-cautions-customers-fake-website.html

[27]马来西亚通信和多媒体委员会。(2021)。网络钓鱼攻击。取自 https://www.mcmc.gov.my/en/faqs/phishing-attack

[28] MARTINO, A.S., & PERRAMON, X. (2011)。网络钓鱼的秘密：历史、影响、对策。国际网络安全杂志，11(3)，163-171。取自 https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.624.6627&rep=rep1&type=pdf

[29] MASREK, M.N., HARUN, Q.N., & RAMLI, I. (2019)。最高管理层在信息安全实践中的作用。第六届教育、社会科学和人文国际会议，土耳其伊斯坦布尔，2019 年 6 月 24-26 日。检索自 https://www.researchgate.net/publication/338764650_THE_ROLE_OF_TOP_MANAGEMENT_IN_INFORMATION_SECURITY_PRACTICES

[30] MAURYA, S., & JAIN, A. (2020)。深度学习打击网络钓鱼。统计与管理系统杂志，23(6)，945-957。https://doi.org/10.1080/09720510.2020.1799496

[31] MCCOMBIE, S., & PIEPRZYK, J. (2010)。赢得网络钓鱼战争：澳大利亚的战略。第二届网络犯罪和可信计算研讨会，澳大利亚巴拉瑞特，2010 年 7 月 19-20 日。https://doi.org/10.1109/CTC.2010.13

[32] 梅肯，Y.（2020）。网络安全案件上升了82.5%。星。取自 https://www.thestar.com.my/news/focus/2020/04/12/cybersecurity-cases-rise-by-825

[33] 穆罕默德，R.M.，THABTAH，F.，& MCCLUSKEYA，L.（2015）。网络钓鱼网站方法的教程和批判性分析。计算机科学评论，17，1-24。https://doi.org/10.1016/j.cosrev.2015.04.001

[34] NORDIN, R. (2020)。在行动管制令期间，警察记录的电话诈骗增加了20%。星。取自 https://www.thestar.com.my/news/nation/2020/05/19/cops-record-20-increase-in-phone-scams-during-mco-period

[35] 钓鱼实验室。(2018)。2018 年网络钓鱼趋势和情报报告。检索自 https://www.phishlabs.com/whitepapers/2018-phishing-trends-intelligence-report/

[36] RAHIM, R. (2020)。税务局警告欺诈者在“欠税”骗局中冒充其官员。星。取自 https://www.thestar.com.my/news/nation/2020/06/07/irb-warns-of-fraudsters-impersonating-its-officers-in-tax-arrears-scam

[37] RAO, S.R. 和 PAIS, A.R. (2019)。网络钓鱼：改进的基于搜索引擎的网络钓鱼检测系统。计算机与安全，83，246-267。https://doi.org/10.1016/j.cose.2019.02.011

[38] 罗姆尼，MB 和斯坦巴特，P.J.（2018 年）。会计信息系统。第 14 版。伦敦：培生教育。

[39] SANCHEZ, F., & DUAN, Z. (2012)。一种以发件人为中心的检测网络钓鱼电子邮件的方法。网络安全国际会议，美国弗吉尼亚州亚历山大市，2012 年 12 月 14-16 日。https://doi.org/10.1109/CyberSecurity.2012.11

[40]马来西亚证券委员会。(2016)。网络风险管理指南。取自 https://www.sc.com.my/api/documentms/download.ashx?id=9aaddb2e-aa13-409a-a47f-8d0124afd229

[41] SONNENSCHEIN, R., LOSKE, A., & BUXMANN, P. (2017)。高层管理者的它安全意识在组织它安全管理中的作用。年国际信息系统会议，韩国首尔，2017 年 12 月 10-13 日。

[42] 特别的时代。(2020)。CBI 在 7 月 4 日周末发布有关可能的身份盗窃诈骗的警报。摩根堡时报。取自 https://www.fortmorgantimes.com/2020/07/02/cbi-issues-alert-about-possible-scams-over-4th-of-july-weekend/

[43] SUGANYA, V. (2016)。网络钓鱼攻击和各种反网络钓鱼技术综述。国际计算机应用杂志，139（1），20-23。https://doi.org/10.5120/ijca2016909084

[44] VAN KESSEL, P. (2018)。网络安全不仅仅是保护吗？取自 https://www.ey.com/en_gl/consulting/global-information-security-survey-2018-2019

[45] VUČKOVIĆ, Z., VUKMIROVIĆ, D., MILENKOVIĆ, M.J., RISTIĆ, S., & PRLJIĆ, K. (2018)。分析电子商务用户行为以检测身份盗用。物理一种：统计力学及其应用，511，331-335。https://doi.org/10.1016/j.physa.2018.07.059

[46]沃德曼，B.（2016）。评估差距：衡量网络钓鱼对组织的影响。第 12 届 ADFSL 年度数字取证、安全和法律会议，佛罗里达州代托纳比奇。取自 https://commons.erau.edu/cgi/viewcontent.cgi?article=1366&context=adfsl

[47]惠特克，B.（2007）。永远不要太年轻，以免您的身份被盗。纽约时报。取自 https://www.nytimes.com/2007/07/21/business/21idtheft.html

[48] YEBOAH-BOATENG, E.O., & AMANOR, P.M. (2014)。网络钓鱼、微信和威兴：对移动设备威胁的评估。计算和信息科学新趋势杂志，5(4)，297-307。取自 https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.682.2634&rep=rep1&type=pdf

[49] YEOH, A. (2020)。LHDN 警告针对国民党收件人的短信诈骗。星。取自 https://www.thestar.com.my/tech/tech-news/2020/04/03/lhdn-warns-of-sms-scam-targeting-bantuan-prihatin-nasional-recipients

[50] ZAHARI, A.I., BILLU, R., & SAID, J. (2017)。电子商务欺诈：对在线欺诈的熟悉度、信任度和意识影响的调查。取自 https://www.researchgate.net/publication/319311612_E-Commerce_Fraud_An_Investigation_of_Familiarity_Trust_and_Awareness_Impact_towards_Online_Fraud