Article

Phishing—A Cyber Fraud: The Types, Implications and Governance

International Journal of Educational Reform
2024, Vol. 33(1) 101–121

DOI: 10.1177/10567879221082966
journals.sagepub.com/home/ref

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

Abstract

Internet users are becoming ignorant with their data and the transparency of information due to the nature of high-speed internet today. Regrettably, internet users are deceived by engineering tactics performed by highly trained people, namely cybercriminals. Thus, in order to combat phishing attacks, internet users should be educated on security concerns, the influence of social engineering and anti-phishing knowledge. This paper presents a literature review of phishing, a type of cyber fraud, covering the types of phishing, the implications and governance. This study benefits the public to mitigate phishing attacks and increase phishing awareness.

Keywords

phishing, cyber fraud, internet, technology, interpretation, governance

Introduction

The internet has caused a revolution in modern living, and socio-economic transactions such as communication, shopping, commerce, networking, entertainment and is the source of data and information. People can access the internet easily via digital devices such as laptops and smartphones (Arachchilage & Love, 2014). Due to the rapidly increasing revolution, people rely heavily on internet sources. Recently,

[1]Faculty of Accountancy, Universiti Teknologi MARA Selangor, Kampus Puncak Alam, Selangor, Malaysia
[2]KYC Operations Analyst, Citigroup Transaction Services (M) Sdn. Bhd., Kuala Lumpur, Malaysia

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

internet connectivity growth has increased cyber fraud activities and encouraged people to commit fraud and victimise others (Kamruzzaman et al., 2016). The issue has become a significant problem globally, and no countries are immune to it.

Fraud is generally known as a crime of using dishonest methods to gain something from others. On the other hand, cyber fraud or internet fraud involves internet services usage or software with internet access (Zahari et al., 2017). Examples of cyber fraud are phishing, email scams, data breaches, lottery scams, love scams, Nigerian letter frauds, credit card frauds, investment schemes, malware business frauds, internet auction frauds and non-delivery merchandises.

Currently, internet users are ignorant of their data and information transparency due to high-speed internet. Highly trained people, such as cybercriminals, perform social engineering tactics to deceive ignorant internet users. Krombholz et al. (2015) denoted that social engineering uses deception to manipulate individuals to compromise information systems and steal personal or confidential information that could be utilised for fraudulent intentions. Instead of technical attacks on networks, social engineers use human psychology, such as influence and persuasion, to lure individuals into giving their confidential information to them. Human psychology is one reason why users are exposed to cyber fraud, especially phishing attacks.

Phishing is a form of cyber fraud. Fraudsters imitate themselves as someone from legitimate institutions to lure individuals into sharing sensitive data such as personal information, passwords and banking and credit card details (Katkuri, 2018). The fraudsters frequently contact their victims via text messages, telephone or email. The retrieved information is subsequently utilised to access vital accounts and cause financial loss and identity theft. For example, a victim receives an email from the bank and is asked to update the personal details and bank account number. Nevertheless, the login pages are bogus, and the hackers take advantage by stealing the victim's information.

Since 2016, phishing attack cases have increased to 1,220,523 cases. The Anti-Phishing Working Group (APWG) has confirmed that the cases have recorded the highest number since 2004 (Rao & Pais, 2019). The APWG is the international coalition unifying the global response to cybercrimes across industries, trade associations, government and law enforcement agencies and non-government organisations (NGOs). Rao and Pais (2019) also stated that the total loss from 450,000 phishing attacks amounted to USD 5.9 billion. The Kaspersky Lab's anti-phishing systems were triggered 154,957,897 times in 2016 compared to 2015, where the systems were activated about 148,395,446 times. These figures prove that phishing attempts continuously increase annually.

Ernst and Young's 2018–2019 Global Information Survey stated that phishing is the top cyber threat to organisations with 22% of reported cases, followed by malware with 20% cases and disruptive cyberattacks with 13% cases. The government of the United States of America (USA) warned its citizens about phishing texts or emails asking for donations and charity to help active and veteran military members to show their patriotism and kindness in conjunction with the USA Independent Day on the 4th of July.

The citizens were warned not to trust and click on the links (Special to The Times, 2020).

In 2010, CyberSecurity Malaysia reported 294 phishing websites, with most websites targeting local banks such as Maybank2U.com and Cimbclicks.com. CyberSecurity Malaysia is an incorporated agency supervised by the Ministry of Communications and Multimedia Malaysia. It is responsible for providing cybersecurity services and programmes to reduce cybersecurity issues and strengthen Malaysia's cybersecurity. CyberSecurity Malaysia and the Malaysian Communication and Multimedia Commission (MCMC) are accountable for mitigating cyber crimes.

Statistics from The Malaysia Computer Emergency Response Team (MyCERT) under CyberSecurity Malaysia revealed that the highest number of reported incidents involve cyber fraud. Phishing is included in the cyber fraud category. In 2021, reported cyber fraud cases topped the list with 7,098 incidents, followed by 1,410 intrusion cases and 648 malicious codes cases. In 2020, 7,593 cases were reported. Cyber fraud topped the list, followed by 1,444 intrusion cases and 593 malicious codes cases. Nevertheless, there is no specific data on phishing incidents reported by MyCERT. (Table 1)

A New Straits Times article on 21st November 2019 reported that a hairdresser suffered a RM 14,900 loss due to a phone call he received from an unknown individual. The unknown individual claimed to be calling from Malacca court and accused the hairdresser of being involved in money laundering activities. The call was later transferred to a Malacca policeman and then to an anti-money laundering officer (Rahim, 2019). The victim stated that he believed that the unknown individual called from a police station as he could hear people busily working in an office in the background. Besides, the victim fell for the claim as he had lost his identity card five years earlier and assumed that the card had been misused.

The same scenario happened to the Inland Revenue Board Malaysia (IRBM), where a fraudsters' syndicate actively impersonated IRBM officers (Rahim, 2020). The victims received a phone call from fake IRBM officers with similar IRBM contact numbers. The victims were accused of involving in money laundering and tax evasion activities. The fake IRBM officers threatened to freeze the victims' bank accounts under the Anti-Money Laundering, Terrorism Financing and Proceeds of Unlawful Activities Act (AMLA). The victims were ordered to make the required

Table 1. Reported Incidents Based on General Incident Classification Statistics for 2018, 2019, 2020 and 2021.

Incident	2021	2020	2019	2018
Cyber Fraud (including Phishing)	7,098	7,593	7,774	5,123
Intrusion	1,410	1,444	1,359	1,160
Malicious Codes	648	593	738	1,700

payments for their bank accounts to be unfrozen. However, the payments were transferred to bank accounts that IRBM does not own.

In addition to these cases, Malaysia Airlines (MAS) received numerous screenshots of fares inconsistent with its system. According to MAS, a fake website is operating under the name of MAS. This fake website can be discovered via Google search and displays incorrect fares. Thus, MAS urged its users to verify the correct URL, www.malaysiaairlines.com, before booking flight tickets. The users can also utilise the mobile application of MAS and appointed agents to search or book flights (Malaysian Airlines, 2020).

Cyber security incidents increased to 82.5% during the Movement Control Order (MCO) amid the Covid-19 pandemic in Malaysia (Meikeng, 2020). Since the implementation of MCO on 18th March 2020, 838 incidents have been reported to CyberSecurity Malaysia. In contrast, only 459 cases were reported within the same period of the previous year. Fraud cases, such as phishing, made up most cases reported during the MCO. Covid-19 themed phishing emails were used by the fraudsters to lure people and spread fake news through numerous sources such as compromised unrecognised websites and emails.

In addition, the Malaysian police recorded a 20% increase in bogus phone call cases during the MCO, with a loss of approximately close to half a million (Nordin, 2020). The cases increased to 34 cases compared to 28 cases, with losses recorded to be RM 480,000 as of May 2020. The fraudsters impersonate enforcement agencies such as the police and deceive the victims by accusing them of being listed in the police record or involved in a court case. The victim is required to share their personal details and pay money as case settlement. Besides, the fraudsters create phone numbers identical to the enforcement agencies to confuse the victims. They commonly use area codes such as +80, +90 and others, followed by the agency numbers instead of +60.

Malaysians have also been reminded by the IRBM to not fall for fraudsters who send fake text messages stating that the victims have qualified for Bantuan Prihatin Nasional (BPN) during the MCO (Yeoh, 2020). The fraudulent text messages sent through personal phone numbers prompted recipients to respond with their personal and banking information. The messages assured them that their payment would be received within 24 h. The IRBM has posted examples of genuine text messages, and the text messages will be sent from numbers, such as 62,000 or 63,833. The text messages will not request personal details, including full names and banking information. (Figures 1 and 2)

Based on the MyCERT statistics, the reported incidents of cyber fraud (including phishing) has topped the list from 2018 to 2020. Many phishing cases are reported in Malaysia, and in 2020, the phishing cases spiked amidst the Covid-19 pandemic. Unfortunately, the awareness level concerning this issue is still low and will worsen if this issue is not combated. The fraudsters are constantly developing new phishing techniques and take the opportunity in the current situation to attack their victims.

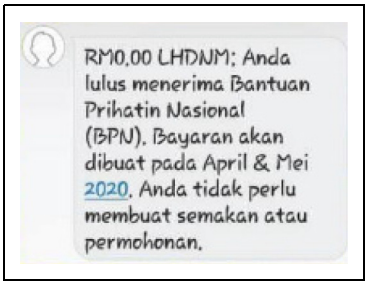

Figure 1. An example of a genuine text message by the IRBM.

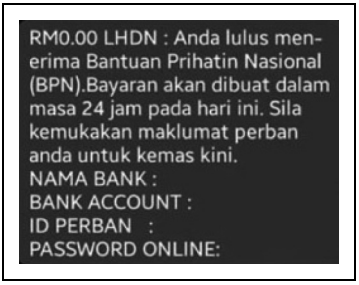

Figure 2. An example of a fake text message concerning BPN.

Literature Review

History of Phishing

The term "phishing" was coined in 1996 based on the analogy where fraudsters utilised telecommunication as a fishing hook to "phish" personal data, including passwords, usernames, and other confidential data (Martino & Perramon, 2011). Martino and Perramon (2011) also stated that the utilisation of the first two letters, "ph", are thought to have been formed from the term "phreaking", which means hack into telecommunications systems.

At the beginning of the 1990s, the first phishing attack began as numerous fraudulent users with fake credit card information registered with the America Online (AOL) network system website (Jain & Gupta, 2017). The bogus accounts were passed by AOL through a simple validity test that failed to verify the legitimacy of the credit card. The attackers managed to access the resources of the AOL system after the fake account was activated. Subsequently, AOL identified that the accounts and the credit cards were invalid after the billings were generated. Several AOL users' accounts were also hacked. An algorithm was then created by the attackers to generate random credit card numbers that can be used to open AOL accounts. The attackers

subsequently create an account and hack the users' accounts when the algorithm matches a real credit card number. The fake accounts were banned by AOL instantly.

After the incident, AOL took preventive measures by confirming the validity of credit cards and the identity of the account. Nevertheless, these hackers have used other methods, such as pretending to be AOL employees. The attackers sent messages to the users via AOL messenger to collect the AOL users personal information. Numerous users gave the attackers their passwords and other sensitive information. The attackers, pretending as AOL employees, directly sent the bills to the users' credit cards and the users needed to dispute the charges. However, after several months, no notice was given to the users (Rader & Rahman, 2013). This situation became a significant problem in 1996, and the word "phishing" was first posted in AOL. Subsequently, AOL alerted the users of the potential phishing abuse via their emails and messaging software.

Gupta et al. (2017) discussed the evolution of phishing from 1996 to 2014. In 1997, the media declared the new attack as "phishing". The fraudsters started using messages and newsgroups to attack the victims in the following year. Next, mass mailing was introduced and used to escalate the phishing attack in 1999. From 2000 to 2003, the fraudsters used Uniform Resource Locator (URL), screen logger, instant messaging (IM) and internet relay chat (IRC) to attack the victims. Later, in 2006, the fraudsters began attacking victims via Voice over Internet Protocol (VoIP). In 2007, loss involving phishing scams amounted to more than USD 3 billion, while in 2010, Facebook was reported to receive more phishing attacks than Google. Subsequently, approximately six million unique malware samples were identified in 2012, whereas 750,000 malicious emails were sent via the Internet of Things (IoT) devices such as smartphones in 2014.

Types of Phishing Attack

Spoofing Email, Spear-Phishing and Whaling. One of the phishing attacks is spoofing email. Emails created with a forged sender address is known as spoofing email. The emails appear to be messages sent to the victims, and the contents trick the victims into opening the email (Gupta et al., 2016). A functioning Simple Mail Transfer Protocol (SMTP) server and mailing software such as Gmail or Outlook make spoofing emails creation easily achievable. The scammer or fraudster can forge the message header fields such as the FROM, REPLY-TO and RETURN-PATH addresses immediately after an email message is created. The email with the entered address appears in the recipient's mailbox after being sent (Sanchez & Duan, 2012). No mechanism is provided by the SMTP to address the authentication process. Thus, spoofing email can easily manipulate the users to reveal their personal information by reading or clicking the email.

The term spear-phishing was first used in 2005 (Gupta et al., 2017). The spear-phishing concept is similar to spoofing email, where the fraudsters trick victims into providing credential information via email. However, spear-phishing

targets specific individuals or groups, while random users are attacked in spoofing email cases (Chaudhry et al., 2016). In spear-phishing, the fraudster will often research the potential victims before attacking them. The method has been used to attack high-rank officers and prominent figures, such as the senior executives of organisations and government officials. This attack is known as whaling and often aims to steal sensitive information or money from high ranking officers for illegal intentions (Chaudhry et al., 2016). In these scenarios, organisations should be more aware of emails that arrive in the organisations' email, mainly external email messages. The fraudsters commonly use the tactics by displaying the name of trusted individuals or organisations on the emails sent via external email addresses to trap the victims.

SMiShing. Another form of phishing attack that utilises text messages or short messaging services (SMS) is known as SMS phishing or SMiShing. In SMiShing, text messages are sent through impersonating the sources such as law enforcement agencies, bankers and system administrators to attack the victims. A vital text message informs the victims that their information or account number had been stolen or frozen (Yeboah-Boateng & Amanor, 2014). In these situations, the fraudsters usually ask the victims to visit the website or contact the provided phone number to verify the account information. The fraudsters typically deceive the victims by asking them to withdraw money and send it to the fraudster or steal their information by attaching an attachment for the victims to download. The attachment usually contains a virus or malware capable of hacking the victims' phones. Consequently, the fraudster can access all the victims' information such as contacts, applications and phone messages.

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". 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 often unaware of the fraudster's ability to utilise an advanced automated system to commit this type of fraud. In addition, Yeboah-Boateng and Amanor (2014) stated that vishing uses the practice of leveraging VoIP. This practice delivers multimedia sessions and voice communications over Internet Protocol (IP) networks to imitate trusted agencies, including banks, and enforcement agencies, such as police, customs, anti-corruption commission and others to deceive the victims. In this situation, victims usually will follow all the instructions from the call, as they are confident that the call is from the trusted agencies.

Search Engine Phishing and Pharming

Phishing attacks using bogus web pages are known as search engine phishing. Fake web pages that offer incredible deals and cheap products are created by fraudsters, and the sites are indexed by legitimate search engines (Suganya, 2016). These bogus

web pages will usually trigger a specific Google result page, as shown in Figure 3 (Rao & Pais, 2019), and online shoppers will click on those web pages. The shoppers will provide personal and confidential information such as address, ID number, bank account details, credit and debit card numbers. They believe they are accessing genuine web pages (Chaudhry et al., 2016). Besides search engine phishing, the fraudsters use another method, namely pharming. The evolution of pharming started in 2004 (Gupta et al., 2017). The fraudsters modify the host files or install malicious codes in the Domain Name System (DNS) of the website (Chaudhry et al., 2016). Resultantly, the website link will return as a bogus website.

Users must verify the originality of the web pages before performing any transactions or providing any sensitive information. The Cloudflare website, an American web infrastructure and website-security company, stated that HTTP refers to 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", indicating that the 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 a website that uses HTTPS has HTTPS://. Google reported a 13% increase of HTTPS requests served between June 2015 and June 2016 (Finamore et al., 2017).

Thus, HTTPS is valuable because it protects communication and customer information and legitimises sites. Customers will be safer when shopping online at websites with HTTPS. Besides, users must pay attention to hyperlinks or URLs. The URL, known as Uniform Resource Locator, is the access to the web address. The URL of phishing websites appears similar to the URL of the original website. The similarity has caused phishing websites to trap many people. The fraudster will steal the users' information when the users provide sensitive information through phishing URLs (Suganya, 2016).

Furthermore, the users must check the content of the websites before performing any transactions or providing any sensitive information. The fraudsters create

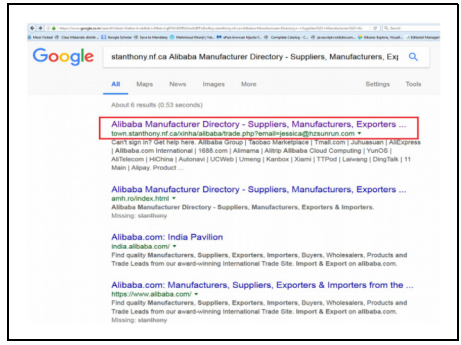

Figure 3. Example of phishing websites in google result page.

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.

Figures 4 and 5 show the examples of legitimate and phishing websites based on Rao and Pais (2019). The figures indicate that phishing websites do not contain HTTPS in the URL. Some differences exist between legitimate and phishing websites. For example, 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. The font of "Having trouble logging in?" is smaller, and there is no "or" in-between "Having trouble logging in?" and "Sign Up" in the phishing website compared to legitimate websites. Besides these examples, some phishing websites contain fake logos, no contact information, and sentence structure, grammar, and spelling errors. In addition, the users must check for the padlock or lock icon displayed in the web browser (Refer to Figure 6). The padlock or lock icon indicates the secure communication mode in the web browser where the data is encrypted. This icon will prevent other people from modifying the users' data.

Statistics of Phishing Around the World

PhishLabs is a cyber security expert from the USA who provides external intelligence, incident reports, and security awareness training to mitigate digital risks. Phishing Trends and Intelligence Report 2018 by PhishLabs states that the USA is the most popular choice for fraudsters and hosts 56% of all phishing infrastructure. France and Germany follow the ranking with approximately 4% and subsequently Great Britain and Canada, with 3%. Besides these countries, South Asia and Southeast Asia countries also host fraudsters' infrastructures and are showing tremendous growth. Singapore has increased its phishing infrastructure and volume by 88%. France increased by 82%, while Ukraine increased by 70%.

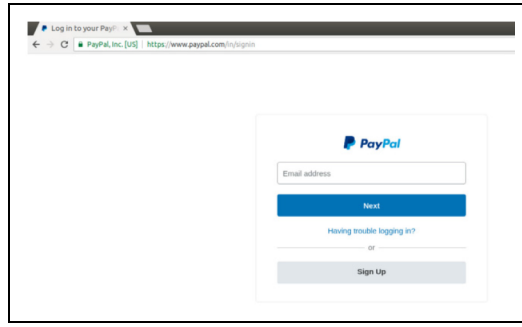

Figure 4. Example of a legitimate website (source: Rao & Pais, 2019).

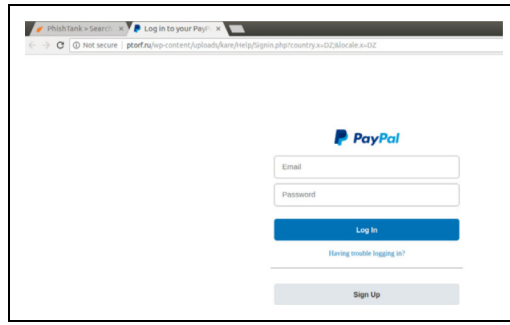

Figure 5. Example of a phishing website (source: Rao & Pais, 2019).

Figure 6. Example of the padlock icon in the web browser.

Additionally, Indonesia recorded a 40% increase, whereas Malaysia reported a 39% increase.

Based on the Phishing Activity Trends Report, Second Quarter of 2018 by APWG, the most targeted industry sector affected by phishing is the payment industry, which is about 36%. The second most targeted industry sector is the Software as a Services (SaaS) or Webmail with approximately 21%. The SaaS is a software distribution model of service. A third-party provider will host the application and rent information technology (IT) solutions to users and make them 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. Other industry sectors targeted by phishing attacks are financial institutions (16%) and cloud storage or file hosting such as Google Drive, Flickr and Picasa (9%). Social media make up 4% of the most targeted sector.

Impacts of Phishing Attack

Several impacts occur if phishing attacks are not mitigated. Phishing leads to monetary losses as the fraudsters steal money and negatively impact society and economic growth. Monetary costs are the funds or expenditures used for personal and family needs and purchasing material, production, services and marketing in an organisation. On the other hand, monetary losses are the amount of money lost (Wardman, 2016). They include theft of sensitive and valuable sensitive information concerning customers, stakeholders and the organisations and computer troubleshooting costs (Kamruzzaman et al., 2016).

The trust of consumers in online activities reduces due to phishing attacks. Phishing also damages an organisation's brand reputation. The brand is the foundation of every company's market capitalisation. For example, if an organisation is attacked and encounters phishing websites under their brand, the legitimate websites will also be affected. The organisation will be blocklisted by the users for an extended period, although the phishing websites have been removed from the blocked domain (Mohammad et al., 2015). The users lose their trust, and the organisation must work hard to gain confidence back from the users.

Identity theft is another impact of phishing and one of the worst potential consequences of phishing that could cause massive financial loss, psychological and emotional impacts (Vučković et al., 2018). Identity theft is a form of fraud where other people's identities are used to steal money or gain other benefits. The fraudsters can pretend or disguise to be victims for any purpose. For example, in 1994, a 12 years old boy from the USA, Gabriel Jimenez, had his identity stolen. His mother, Jeri Marks, first discovered the problem when her son, Gabriel Jimenez, had filed taxes for working as a child model. She later discovered that an illegal immigrant stole and used her son's identity. Although she has notified the police, the Internal Revenue Service (IRS) and the Social Security Administration, the problem continued. Although Gabriel Jimenez has reached adulthood, the situation has continued to worsen (Whitaker, 2007).

Implications

Implications for Individuals

Firstly, users must be careful with social engineering techniques used by fraudsters to deceive victims. The users should be suspicious when they receive calls, messages or emails with a sense of excitement such as winning a considerable sum of money or urgency and panic such as obtaining a warrant from authority. Importantly, the users should be calm and not panic if they receive calls from people claiming to be authorities, such as the Malaysian Anti-Corruption Commission (MACC) and the Royal Malaysia Police.

The users can check the authorisation or identity of the callers, such as full name, the organisation's name, location or branch where the callers called from and other details. The users should hang up the call if they realise 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. Additionally, the users can hang up the calls claiming to be from authority agencies without further asking for information and directly calling the organisations 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 devices such as computers, smartphones and tablets because the fraudsters might hack the devices to collect information.

Users performing online shopping or banking should take precautions to avoid phishing websites. They should check whether there are multiple domains with the exact name on the Google result page when searching for a website on Google because one of the websites might be phishing websites. The users should ensure the correct URL of the website. If the users are suspicious about the originality of the website, they can call the organisations directly to ensure the originality. Phishing websites usually do not provide contact information, and the provided phone numbers are often unreachable. Furthermore, the users should check the grammar, spelling and logo of the website before performing transactions or entering confidential information. The users should ensure that the website contains HTTPS in the URL and padlock icon to secure the data to avoid phishing threats.

Moreover, the users can use the same application to handle online websites while receiving emails. The users should be suspicious when they receive emails or messages requesting personal information such as passwords, security numbers, bank accounts or credit card numbers for companies. Legitimate companies will never ask the users to verify or provide confidential information in unsolicited emails or messages. When receiving emails, the users must check the email address, spelling, sentence structure and grammar to see if they are intentionally misleading. The users can call the company which sent the email if they doubt the originality of the email received.

According to the Cyber Security Awareness Alliance website, a Singapore government agency website, users can hover over the hyperlink in the email message before clicking on it. 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 emails and should not respond and download any attachment in the suspected phishing emails or messages. Furthermore, the users should ensure whether the email is from an external source for an office email since most phishing emails begin with messages from an external email system. They must report to the responsible team when they receive phishing emails through their office emails.

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

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

Thus, users must upgrade their phishing knowledge by reading phishing related materials on the internet, social media and bank websites. Concurrently, they also need to update themselves with the current news, primarily related to phishing attacks, because fraudsters constantly upgrade phishing techniques to deceive victims. The users should immediately report to the banks when there is a suspicious transaction in their bank account. They can also write to MCMC whenever they face phishing emails or sites. The phishing site will be immediately removed by MCMC to safeguard Malaysian internet users from the attack. Therefore, the users need to safeguard themselves to avoid phishing threats.

Implications for Companies

Companies should take necessary actions to enhance awareness among employees and avoid phishing threats. For example, companies can conduct phishing assessments to increase employees' awareness about phishing. Phishing assessment involves sending deceptive emails to employees within the companies to test their security awareness level. These emails imitate phishing emails with social engineering where hyperlinks, open file attachments and access to provide sensitive information are attached in these emails. Ikhsan and Ramli (2019) stated that phishing assessment provides knowledge and simulates real cases to employees where they can safeguard themselves when facing real phishing emails in the future.

Furthermore, companies must provide regular training and programmes to increase employees' security awareness. The companies can send standard information and phishing knowledge through office emails and websites. Simultaneously, the companies can always provide the latest news and updates about phishing, especially on the current situation or methods used in phishing to the employees. In addition, the companies must ensure that the employees' anti-virus is constantly updated to secure and protect data. Institutions dealing with customers such as banks and e-commerce corporations should provide relevant information about phishing to their customers in websites, applications, commercials and digitals, or e-flyers to increase customer awareness, especially when customers handle online money transfer and e-commerce services.

On the other hand, Kennedy et al. (2016) mentioned that besides having good credential passwords and using different passwords for different applications, the passwords should be changed regularly to reduce the exposure to phishing attacks. Kennedy et al. (2016) mentioned that a password expiration policy should be implemented after 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.

Implications for Government

The government should take action to mitigate phishing attacks. Government agencies such as MCMC and Cybersecurity Malaysia should conduct awareness programmes to increase phishing awareness among the public. Cybersecurity Malaysia and MCMC can share information and current news about phishing on their official websites and social media such as Facebook, Instagram, Twitter and other platforms. People tend to use social media to know the current issue and information.

Government agencies should use the media platform to display commercials and advertisements to provide information about phishing. The platforms could include television, YouTube, Iflix and the ads before movies are played in the cinema. The government agencies can provide basic knowledge about phishing, the medium used for a phishing attack, how to avoid phishing attacks and provide information on how the public can make a report about phishing through commercials and advertising.

The government agencies must monitor the companies to ensure they provide relevant training and exercise to increase phishing awareness among the employees. They can also introduce a platform to notify the current updates and listing of fraud emails, websites and phone numbers for the public to check. In Australia, Australia Competition and Consumer Commission (ACCC) has established a "Scamwatch" (Refer to Figure 7) to provide information about scams to consumers and businesses. This website also provides the latest news about fraud, reporting fraud, types of scams and scam statistics. Malaysia can emulate this example by introducing a platform to provide information on deception and cyber fraud to its citizens.

The Governances To Prevent Phishing Attack

In this technology era, many companies adopt digital strategies at the forefront of their company agenda. Nevertheless, cyber frauds, such as phishing attacks, are still being neglected. Understanding cyber risks and information security practices are essential for companies to prevent cyber fraud, especially phishing attacks. Kazemi et al. (2012) and Hsu and Wang (2014) mentioned that top management comprising the

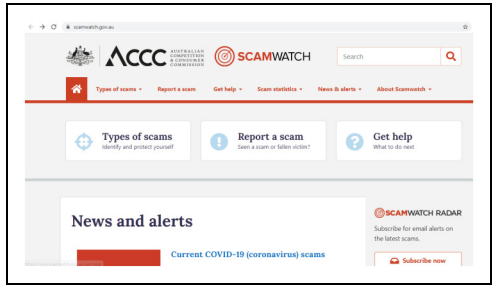

Figure 7. Australian scamwatch website.

board and senior management is responsible for implementing information security programmes and risk management to safeguard organisational assets. A survey by Kankanhalli et al. (2003) on information security managers from various sectors showed that organisations with stronger support from top management provide more preventive efforts than weaker top management support. Sonnenschein et al. (2017) discovered that top management awareness is vital for effective IT security management.

Board of Directors and Top Management

On 31st October 2016, the Guidelines on Management of Cyber Risk was issued by Securities Commission Malaysia. The guideline is applicable to all Malaysian capital market entities. The responsibilities and roles of the management and board of directors are listed in the guideline. The guideline covers the management and oversight of cyber risk, the development and implementation of policies and procedures by capital market entities, the requirements to manage cyber risk and reporting requirements to Securities Commission Malaysia (Securities Commission Malaysia, 2016).

The Securities Commission Malaysia (2016) emphasised 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 cyber risk policies and procedures of the capital market obtain the board's approval and verify that the management implements the approved cyber risk policies and procedures. Subsequently, the board must monitor the effectiveness of the implemented cyber risk policies and ensure that the policies and procedures are reviewed periodically, such as setting performance indicators.

Furthermore, the board must ensure adequate resources are available by assigning accountable and responsible individuals to manage cyber risk. The board is also responsible for ensuring that the management continuously promotes cyber resilience awareness at all organisational levels. In addition, the adequate assessment of cyber risk impact must be assured when new activities are undertaken. Similarly, the board must constantly be updated and aware of new or upcoming trends and impacts of cyber threats.

On the other hand, the management is responsible for implementing cyber risk policies and procedures. The policies and procedures must clearly describe cyber risk tolerance, including cyber breach occurrences and severities, potential negative media publicity, maximum service downtime, financial impact and potential regulatory. The policies and procedures must include processes for identifying, detecting, assessing, and reporting cyber breaches for decision-making and requirements for third-party service providers to comply with the organisation's information security policy. The policies and procedures must also contain communication procedures during the cyber breach event, including information to be reported, communication channels, reporting procedures, and the list of internal and external stakeholders. The

management must periodically update and report any emerging cyber breach and its impact on the organisation.

Furthermore, the management must also recommend suitable measures and strategies to the board, including prevention, detection and recovery measures, in managing cyber risk. The management should make necessary changes to existing policies and procedures for better cyber risk management. Implementable preventive measures include installing anti-virus software and malware programmes to identify and isolate malicious code and constructing firewalls to eliminate weak points to prevent attackers from obtaining access to an entity's network.

The detection measures of cyber incidents include identifying cyber risk scenarios that the entity is most likely to be exposed to, determining incidents in the capital market, assessing the impact of the cyber risk incidents, and establishing sufficient response and communication plans. Any form of cyber breach should be forwarded to the incident response team, management, and the board. In addition, the critical systems and services for recovery measures should be recovered within the targeted defined recovery time. The entity should implement comprehensive business continuity and recovery plans for the designs, services and operations caused by a cyber breach.

Financial Institution

Phishing attacks rely on social networking and electronic communication technology. The Risk Management in Technology (RMiT) has been implemented by the Central Bank of Malaysia for financial institutions since 1st January 2020. As per this policy, a technology risk appetite that aligns with the financial institution's risk appetite requirement must be established and approved by the board (Central Bank of Malaysia, 2020). The effective implementation of the cyber resilience framework (CRF) and technology risk management framework (TRMF) must be overseen and reviewed by the board.

A separate or an existing board-level committed with technological experience must be designated by the board for assistance in imparting oversight concerning technology-related matters. The sufficiency of the financial institution's cybersecurity strategic and IT plans that range no less than three years must be overseen by the board. The financial institution's technology risk must be monitored by the board to ensure that risk indicators and key performance indicators are in order. In addition, the board audit committee (BAC) is responsible for reviewing, addressing the technology control gap and ensuring appropriate technology audit scope, procedures and frequency of technology audits.

Besides, the senior management is responsible for assuring the effective implementation of the financial institution's technology risk policy. Board-approved CRF and TRMF must be implemented by the senior management into specific procedures and policies consistent with the approved risk appetite. A cross-functional committee including senior management from central business units and technology functions

must be established by the senior management to oversee the implementation of strategic technology plans and associated technology policies and procedures. This cross-functional committee is also responsible for promptly updating the board concerning key technology matters and approving deviations regarding technology-related policies. Senior management must assign competent staff and allocate resources to maintain robust technology systems to support the effective management of technology risk.

Government

Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) has developed Cyber Security Framework for Public Sector or "Rangka Kerja Keselamatan Siber Sektor Awam" (RAKKSSA) to provide information security guidelines to the ministries and government agencies to protect their data in digital technology (Masrek et al., 2019). There are eight major components of RAKKSSA (Malaysian Administrative Modernisation and Management Planning, 2016). The first component is to identify. The 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 protection, which necessitates the identification of the relevant security principles, technology, processes, and human skills to reduce the identified risks. The third component is detection, which represents detecting malicious attacks by recognising anomalies in usage and network traffic patterns.

Subsequently, responding to assure that responses to the malicious attacks are taken accordingly and improving communications with the stakeholders and the general public is the fourth component. Recovery, the fifth component, addresses the ability to recover damages resulting from system failures and malicious attacks to guarantee information availability. The sixth component is procurement to guarantee that security requirements and measures are implemented throughout the system's full lifespan, regardless of how the system was acquired, whether through in-house creation or external acquisition. The sixth component is essential and covers commissioning and decommissioning processes, procurement specifications, system disposal, system development life cycle, resource footprint, and vendor management. The security audit is the seventh component. The eighth component enforces cut across all the components to define the scope of auditing and enforcement undertaken by auditing and enforcement authorities.

Conclusion

This paper explored phishing by describing the history of phishing, the types of phishing, and the impact and implications. Phishing cannot be eliminated but can be mitigated to some extent. Mitigation efforts can be undertaken by developing awareness among individuals regardless of whether they were themselves or worked with any organisations. A high level of understanding of phishing will reduce the possibility

of becoming a victim. Hence, actions and efforts to upgrade phishing knowledge among individuals are essential, especially in the present world full of uncertainties.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Ministry of Higher Education, (grant number FRGS/1/2019/SS01/UITM/02/34).

ORCID iD


Mazurina Mohd Ali https://orcid.org/0000-0002-2877-3414

References

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*(September), 304–312. https://doi.org/10.1016/j.chb.2014.05.046

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. https://doi.org/10.14257/ijsia.2016.10.1.23

Finamore, A., Varvello, M., & Papagiannaki, K. (2017). Mind the gap between HTTP and HTTPS in mobile networks. International Conference on Passive and Active Network Measurement, pp. 217–228.

Guidelines on Management of Cyber Risk (2016). Securities Commission Malaysia.

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: State of the art and future challenges. *Neural Comput & Applic*, *28*, 3629–3654. https://doi.org/10.1007/s00521-016-2275-y

Gupta, S., & Singhal, A., & A. Kapoor (2016). A literature survey on social engineering attacks: phishing attack. 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, 2016, pp. 537–540.

Hsu, C., & Wang, T. (2014). Composition of the top management team and information security breaches. In M. M. CruzCunha (Ed.), *Handbook of research on digital crime, cyberspace security, and information assurance* (pp. 1436–1456). IGI Global.

Ikhsan, M. G., & Ramli, K. (2019). Measuring the information security awareness level of government employees through phishing assessment. 2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), JeJu, Korea (South), pp. 1–4.

Jain, A. K., & Gupta, B. B. (2017). Phishing detection: analysis of visual similarity based approaches. *Hindawi. Security and Communication Networks*, *2017*, 1–20. https://doi.org/10.1155/2017/5421046

Kamruzzaman, M., Islam, M. A., Islam, M. S., Hossain, M. S., & Hakim, M. A. (2016). Plight of youth perception on cybercrime in South Asia. *American Journal of Information Science and Computer Engineering*, *2*(4), 22–28.

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

Katkuri, S. (2018). Indian Cyber Law. *International Journal of Advanced Research and Development*, *3*(1), 640–644.

Kazemi, M., & Khajouei, H.,, & H Nasrabadi. (2012). Evaluation of information security management systems success factors: case of municipal organization. *African Journal of Business Management*, *6*(4), 4982–4989. https://doi.org/10.5897/AJBM11.2323

Kennedy, L. Z., Chiasson, S., & Oorschot, P. V. (2016). Revisiting password rules: Facilitating human management of passwords. 2016 APWG Symposium on Electronic Crime Research (eCrime).

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

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*(June), I13–I22. https://doi.org/10.1016/j.jisa.2014.09.005

Malaysia Airlines Cautions Customers of Fake Website. Malaysian Airlines, 11 June 2020, accessed August 2020 from https://www.malaysiaairlines.com/us/en/news-article/2020/malaysia-airlines-cautions-customers-fake-website.html

Martino, A. S., & Perramon, X. (2011). Phishing secrets: history, effects, and countermeasures. *International Journal of Network Security*, *12*(1), 37–45.

Masrek, M. N., Harun, Q. N., & Ramli, I. (2019). The Role of Top Management in Information Security Practices. Proceedings of SOCIOINT 2019- 6th International Conference on Education, Social Sciences and Humanities, 24–26 June 2019, Istanbul, Turkey.

Meikeng, Y. (2020). Cybersecurity cases rise by 82.5%. The Star. 12 April 2020. Accessed August 2020 from https://www.thestar.com.my/news/focus/2020/04/12/cybersecurity-cases-rise-by-825

Mohammad, R. M., Thabtah, F., & McCluskeya, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review*, *17*(August), 1–24. https://doi.org/10.1016/j.cosrev.2015.04.001

Nordin, R. (2020). Cops record 20% increase in phone scams during MCO period. The Star. 19 May 2020. Accessed August 2020 from https://www.thestar.com.my/news/nation/2020/05/19/cops-record-20-increase-in-phone-scams-during-mco-period

Rader, M., & Rahman, S. S. M. (2013). Exploring historical and emerging phishing techiniques and mitigating the associated security risks. *International Journal of Network Security & Its Applications (IJNSA)*, *5*(4), 23–41. https://doi.org/10.5121/ijnsa.2013.5402

Rahim, R. (2020). IRB warns of fraudsters impersonating its officers in "tax arrears" scam. The Star. 7 June 2020. Accessed August 2020 from https://www.thestar.com.my/news/nation/2020/06/07/irb-warns-of-fraudsters-impersonating-its-officers-in-tax-arrears-scam

Rahim, S. (2019). Hairdresser loses RM 14,900 in phone scam. New Straits Times. 21 November 2019. Accessed August 2020 from https://www.nst.com.my/news/nation/2019/11/540838/hairdresser-loses-rm14900-phone-scam

Rangka Kerja Keselamatan Siber Sektor Awam (2016). Malaysian Administrative Modernisation and Management Planning.

Rao, S. R., & Pais, A. R. (2019). Jail-Phish: An improved search engine-based phishing detection system. *Computers and Security*, *83*(June), 246–247. https://doi.org/10.1016/j.cose.2019.02.011

Risk Management in Technology (RMiT). (2020). Central Bank of Malaysia.

Sanchez, F., & Duan, Z. (2012). A sender-centric approach to detecting phishing emails. 2012 International Conference on Cyber Security, Washington, DC, 2012, pp. 32–39.

Sonnenschein, R., & Loske, A., & P. Buxmann (2017). The Role of Top Managers' IT Security Awareness in Organizational IT Security Management. Proceedings of the 2017 International Conference on Information Systems (ICIS2017).

Special to The Times (2020). CBI issues alert about possible ID theft scams over 4th of July weekend. The Fort Morgan Times. 2 July 2020. Accessed August 2020 from https://www.fortmorgantimes.com/2020/07/02/cbi-issues-alert-about-possible-scams-over-4th-of-july-weekend/

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

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*(1 December), 331–335. https://doi.org/10.1016/j.physa.2018.07.059

Wardman, B. (2016). Assessing the gap: Measure the impact of phishing on an organization. Annual ADFSL Conference on Digital Forensics, Security and Law, p. 2.

Whitaker, B. (2007). Never too young to have your identity stolen. The New York Times. 21 July 2007. Accessed August 2020 from https://www.nytimes.com/2007/07/21/business/21idtheft.html

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.

Yeoh, A. (2020). LHDN warns of SMS scam targeting Bantuan Prihatin Nasional recipients. The Star. 3 April 2020. Accessed August 2020 from https://www.thestar.com.my/tech/tech-news/2020/04/03/lhdn-warns-of-sms-scam-targeting-bantuan-prihatin-nasional-recipients

Zahari, A. I., Billu, R., & Said, J. (2017). E-Commerce Fraud: An Investigation of Familiarity, Trust and Awareness Impact towards Online Fraud.

Author biographies

Mazurina Mohd Ali is an associate professor at the Faculty of Accountancy, Universiti Teknologi MARA (UiTM) Selangor, Puncak Alam Campus. She is an associate member of Malaysian Institute of Accountants (MIA). Dr Mazurina teaches undergraduate and postgraduate students and supervises masters and doctoral students in her area of expertise. Her main research interest area is financial accounting and reporting, corporate sustainability, governance and risk.

Nur Farhana Mohd Zaharon is a Due Diligence Senior Specialist at Commerz Trade Services Sdn. Bhd. She graduated with a Bachelor's Degree of Civil Engineering with Honours in 2012. Later, she pursued a Master in Forensic Accounting and Financial Criminology and graduated in 2020. She also has an ICA certificate in anti-money laundering and sanction compliance. She has seven years of experience in anti-money laundering, due diligence, sanction compliance and fraud in banking, insurance and trade finance industry.