# Examining the Legal Responsibilities of Spear Phishing Attacks in Malaysia

Aleeya Fatinah Ahmad Fauzey[1] and Associate Professor Dr. Manique Cooray[2]

[1] Faculty of Law, Multimedia University, Melaka, Malaysia
[2] Faculty of Law, Multimedia University, Melaka, Malaysia
manique.cooray@mmu.edu.my

**Abstract.** Phishing is a form of a fraud that involves the use of deceptive e-mails, websites, and other online methods to steal personal data such as passwords, credit card numbers, and bank account information resulting in identity theft, financial fraud, and data breaches. Spear phishing in particular, is a type of phishing that targets a specific individual or organization. It is a form of social engineering that uses personalised e-mails or messages to trick the recipient into providing sensitive information or clicking on malicious links. While typically impersonating a trusted source, such as a colleague or a company, trust and confidence is built between the victim and the fraudster. Therefore, spear phishing is a serious threat to organizations and individuals. The objectives of this paper are to examine the relevant statutory provisions in Malaysia concerning spear phishing and evaluate the level of protection provided to individuals in the event of a personal data breach or misuse. The first section of the paper discusses the differences between phishing and spear phishing. The second section examines the legislative framework in Malaysia with reference to cases addressing such offences. The third section discusses the issues pertaining to liability and who should be held responsible in the event an individual's data is breached. Finally, based on the findings from the comparative study of the selected jurisdictions of Singapore and India for the comprehensive nature in addressing spear phishing the paper will put forth recommendations regarding the allocation of responsibility for spear phishing activities in Malaysia with a focus on the data protection laws as one of the ways in which Spear Phishing could be regulated.

**Keywords:** Phishing, Spear Phishing, Communications and Multimedia Act 1998, Penal Code (Malaysia), Personal Data Protection Act 2010.

## 1 Interpretation

General understanding of "phishing" can be defined as an attempt to induce an individual to reveal confidential information over an e-mail or the Internet in order for another person to steal their money. Phishers utilize a range of sophisticated methods to deceive innocent users, such as social engineering strategies and technology to send meticulously crafted e-mails that create the illusion of authenticity and deceive the recipients


Y. C. Adam and S. A. B. Samsudin (eds.), *Proceedings of the 3rd International Conference on Law and Digitalization 2023 (ICLD 2023)*, Advances in Social Science, Education and Humanities Research 791,
https://doi.org/10.2991/978-2-38476-154-8_6

(Hassan Y. A. Abutair, 2017). For instance, a phisher may send the victim an e-mail leading him to a counterfeit website designed to resemble a legitimate bank page. After that, the phisher can exploit any information the victim enters to deplete their bank accounts or perpetrate identity theft. Due to the multitude of techniques employed to conduct phishing attacks, the issues are extensive and cannot be resolved with a single solution. Phishing can also be categorized as a form of fraud. Fraud is defined as an unlawful or illicit deception carried out with the aim of acquiring money or other advantages.

Conversely, spear phishing is one of the tactics utilized in phishing attempts. The Cambridge Dictionary defines "spear phishing" as an act of sending fraudulent e-mails to extract confidential data from users towards specific individual or organization by mimicking a sender which the recipient knows. Once a user clicks on the link which can be found inside a phishing e-mail, it would then take the user to a malicious website that might download harmful data onto their computer. When the attachment is opened, malicious malware may execute posing a threat to the security of the host's computer. The attacker could launch activities that may compromise the security of the computer, and the network to which it is linked or any other data. Organizations are increasingly vulnerable to attackers that try to access their computer systems by using human behaviour (Sasse et al., 2001). One method to accomplish this is through targeted fraudulent e-mails that seek to deceive employees into opening hazardous links, downloading malicious attachments, transferring business funds, or disclosing sensitive information. This method is frequently referred to as spear phishing (Workman, 2008). As a result of this unlawful act, users' personal data is exposed and is no longer safeguarded.

The terms "phishing" and "spear phishing" do not have specific definitions. In the absence of interpretations to the meanings of these terms reference is made to the Computer Crimes Act 1997 ("CCA '97") (Act 563), Communications and Multimedia Act 1998 ("CMA '98") (Act 588) and the Penal Code of Malaysia (Act 574) to understand the elements of phishing and spear phishing as these legislative provisions address certain related cybercrimes.

### 1.1 Differences of Phishing and Spear Phishing

There are several differences between phishing and spear phishing that we need to distinguish in eliminating these crimes. Spear phishing is a concentrated kind of phishing that is specifically targeted at a certain group or person, whereas phishing is an exploratory attempt to acquire sensitive and secret information from a range of people. Phishing e-mails are sent to a relatively random group of recipients who are less likely to reply. In contrast, large companies or organizations and high-level corporate employees are typically the targets of spear phishing. Phishing attacks are mass produced and not personalized meanwhile spear phishing attacks are personalized for their targets and send out target specific e-mails.

The majority of phishing attackers are cybercriminals or expert hackers. The attackers for spear phishing, in contrast, tend to be professional malicious code distributors with expertise in social engineering and fraudulent transactions. An illustration of a phishing e-mail is one that appears to be from a reputable delivery service and claims that "Your package has been delayed, click here for details;" The user may visit a fake website where they are asked for their name, address, and social security number and if they click the link could result in the installation of malware on their computer. That information could be exploited for fraud or identity theft purposes, or it could be traded on the black market. As for the example of spear phishing e-mails, the user might get an e-mail from a co-worker, by stating "Hey, while you're in Chicago you've got to eat at Joe's Grill, check out their menu" and including a link, the attacker can insert malware into the victim's computer while they are browsing the menu.

### 1.2 Statistic of Phishing Crime by MCMC

Malaysia's merging communications and multimedia business is governed by the Malaysian Communication and Multimedia Commission ("MCMC"). A total of 5,802 complaints about fraud and scams were documented between January 2020 and June 2022 by the MCMC and were forwarded to the relevant authorities for follow-up action. In accordance with the CMA '98 the Commission also blocked a total of 1,826 phishing websites between January 2020 and May 2022. MCMC has prohibited 1.6 billion calls that are allegedly fraudulent attempts by collaborating with telecom network operators. Statistics indicate that there are presently 26.3 million Internet users in Malaysia, and this number is projected to increase to 30.77 million by 2025. The expansion of the Internet has created greater avenues for computer crimes in Malaysia.

## 2 Effect of Spear Phishing on Victims: A study

Fraudsters have the ability to expose economically sensitive information and carry out various espionage activities through the use of stolen data. Moreover, spear phishing attacks have the capability to employ malware to take control of computers, assemble them into extensive networks called botnets, and utilize these networks to launch denial-of-service attacks. One of the most famous data breach attacks with spear phishing was with Anthem, a healthcare insurer. They reached a $115 million settlement in class action. Over 78 million medical records were accessible due to a spear phishing attack-related data breach they experienced.

### 2.1 Legal Frameworks in Malaysia

The Computer Crimes Act of 1997 encompasses provisions that explicitly prohibit certain actions related to computer usage. First and foremost is unlawful access to computer data meaning that individuals are prohibited from accessing computer data without proper authorization or permission. Secondly, the Act criminalizes unauthorized access to computer systems with the intent to commit additional offenses. Thirdly, the

Act prohibits unauthorized modification and finally wrongful communication of certain data. According to section 3(1)(a) of CCA '97, anyone who intentionally and knowingly gains access to a computer without authorisation and causes it to do any action with the intention of accessing any software or data stored on the device is considered as doing the said act illegally. Section 4(1)(a) of the CCA '97 states a person violates this section if they do an act listed in section 3 with the intent to do something that violates the Penal Code's definitions of fraud, dishonesty, or injury. Section 24 of the Penal Code establishes that an act is deemed to have been carried out "dishonestly" if it was intended to result in wrongful gain for one person or wrongful loss for another, irrespective of whether the action leads to unlawful gain or loss. Section 25 of the Penal Code stipulates that an individual is considered to have committed fraud if they engage in an act with the intention to defraud, even if the act itself may not inherently be fraudulent in nature. Section 44 of the Penal Code refers to any wrongdoing that results in physical, mental, reputational, or material harm to a person. Moreover, Section 378 of the Penal Codes provides an interpretation of what amounts to theft. The section illustrates that any individual who moves movable property with the purpose of dishonestly removing it from another person's possession without that person's consent is said to have committed theft. Section 415 of the Penal Code acknowledges that the sole or primary motivation for deceiving someone is not a determining factor in establishing an offense. This section implies that the presence of deception, regardless of whether it was the only or primary motivation, can still lead to legal consequences. For instance, section 415 provides (a) fraud or dishonestly persuades the victim into giving their property or money to someone else or into allowing someone else to keep their property or money; or (b) willfully prompts someone who has been deceived to act in a way that they otherwise would not have if they had not been deceived, and whose actions or omissions hurt another person's body, mind, reputation, or property, is said to "cheat". Section 416 of Penal Code further provides if they intentionally pretend to be someone else, exchange one person for another, or represent that they or another person is someone other than they or that other person actually is, they are said to be "cheating by personation." The case of Pendakwa Raya v Vishnu Devarajan [2015] highlights the importance of not only having relevant legislation like the CCA '97 but also ensuring that effective prosecution is carried out with proper expertise and attention to procedural details. In this particular case, the accused was faced with multiple charges under sections 3 and 5 of the CCA '97, which are likely related to offenses such as unauthorized access to computer data and unauthorized alteration of computer data. The accused was found not guilty of every charge because of procedural flaws, technicalities, and the prosecution's apparent lack of expertise in prosecuting computer crimes. The court declared the accusations as defective. The case of Pendakwa Raya v Hasimah Binti Aziz [2017] highlights a specific scenario where an individual was charged under Section 4(1)(b) of the CCA '97 for allowing unauthorized access to her Maybank bank account and subsequently aiding a fraud against the complainant. The complainant was convinced to transfer money in order to pay costs for the release of a gift that was allegedly given by someone she knew from Facebook. The investigator discovered proof that the accused had given her ATM card to a Facebook acquaintance. He claimed that he was unable to open a bank account in Malaysia. The court found that it was clear

from the facts presented that both the plaintiff and the defendant were themselves victims of Internet scams. The accused was tricked into giving her PIN code, ATM card details, and account information. In other words, the CCA '97 and the provisions in the Penal Code can indeed apply to spear phishing, as spear phishing falls under the broader category of cybercrimes, theft and cheating. However, the application of the Act is questionable as spear phishing cases depends on various factors, including the jurisdiction, evidence gathering, and the ability to identify and apprehend the perpetrators.

The CM A '98 is another legal framework in Malaysia that can be applicable to spear phishing cases. While the CMA '98 primarily focuses on regulating communications and multimedia activities, it contains provisions that can be relevant to combatting spear phishing and addressing cybercrimes. Section 211(1) provides no individual using a content applications service or content applications service provider shall submit content that is indecent, obscene, false, threatening, or offensive in nature with the intention of agitating, abusing, threatening, or harassing any person. Section 233(1)(a) of CMA '98 states a person who (a) by means of any network facilities or network service or applications service knowingly (i) makes, creates or solicits; and (ii) makes any comment, request, suggestion, or other communication that is obscene, indecent, false, menacing, or offensive with the goal to irritate, abuse, threaten, or harass another person; commits an offence. The CMA '98 imposes sanctions on content producers who provide false information and who have been granted a licence, whereas section 233 is imposed on users of networks who act unlawfully. These are just a few examples of how the CMA '98 can be applied to spear phishing cases. The precise application and enforcement of the Act depend on the specific circumstances, evidence gathering, and legal procedures undertaken by relevant authorities.

## 2.2 Legal Frameworks in Singapore

Under section 3(1) of the Computer Misuse Act 1993, any individual who intentionally causes a computer to carry out a task in order to secure unauthorised access to a computer's data or programmes is committing an offence. For the first offence, an offender is subject to a fine of up to $5,000 or a term of up to two years in jail, or both. In Public Prosecutor v Muhammad Nuzaihan bin Kamal Luddin [1999], the accused was found to have, among other things, hacked into many of the victim's servers in order to get unauthorised access to the victim's server's computer files. The defendant was sentenced to two months in prison for violating section 3(1) of Computer Misuse Act 1993.

Section 4(1) of the Computer Misuse Act 1993 states it is unlawful to make a computer execute any function in order to get access to any software or information kept on a computer with the intent to commit a variety of offences, including those involving fraud or dishonesty. The following punishments are possible for those found guilty of such an offence: a fine not to exceed $50,000; a term of imprisonment not to exceed 10 years; or both. The penalties for fraud and identity theft are laid out in the Penal Code 1871. A person who cheats by pretending to be someone else, switching one person for another intentionally, or representing that they or another person is someone other than

who they or that other person really is guilty of an offence and, upon conviction, would be subject to a term of imprisonment of up to five years, a fine, or both, according to section 419 read with section 416 of the Penal Code. Despite the broad scope of this offence, it may also apply in a cyber setting. Furthermore, the Computer Misuse Act 1993's definition of "computer" is flexible. This can be seen in the case of Public Prosecutor v Muhammad Nuzaihan bin Kamal [2000]. The accused was found guilty of violating the Computer Misuse Act 1993 including the offences of unauthorised access to computer data and altering a computer's contents. In this instance, the "computers" were interpreted to extend to the "proxy servers," which were the subject of the case. The accused may be found not guilty if this matter were presented before a Malaysian court because the proxy server only serves as storage, which does not meet the conjunctive conditions under the definition of CCA '97 in the interpretation of a "computer."

## 2.3 Legal Frameworks in India

The Indian law addresses spear phishing and other cybercrimes under the provisions of the Information Technology Act, 2000 (IT Act) and its subsequent amendments. The IT Act is the primary legislation in India that deals with various aspects of electronic governance, digital signatures, data protection, and cybersecurity. Section 43 of the IT Act states that if any person without permission accesses or secures access to a computer system, computer network, or computer resource, they shall be liable to pay damages by way of compensation to the person affected. It primarily focuses on unauthorized access and the liability for damage caused. Section 66 of the IT Act does not specifically address punishment for phishing. However, there are provisions in the Act that can be applied to phishing offenses. Section 66C of the IT Act deals with identity theft and provides punishment for anyone who fraudulently or dishonestly uses the electronic signature, password, or any other unique identification feature of another person. If phishing involves the fraudulent use of someone else's identity or personal information, this section may be applicable. Additionally, Section 66D of the IT Act addresses cheating by personation using a computer resource. It imposes punishment on individuals who, by means of any communication device or computer resource, cheat by personating someone else. If phishing involves impersonation or deceitful actions, this section may be relevant. It's important to note that the application of these sections will depend on the specific circumstances of the phishing offense and the evidence provided.

## 2.4 Liability of the Company Towards Their Users

The Personal Data Protection Act 2010 ("PDPA 2010") governs the acquisition, use, disclosure, and retention of personal data concerning individuals in Malaysia (Act 709). The Act governs how personal data is handled in Malaysian business activities. The Act is implemented according to seven (7) fundamental principles: General Principle, the Notice and Choice Principle, the Disclosure Principle, the Security Principle, the Retention Principle, the Data Integrity Principle, and the Access Principle. Under the Act, failure to comply with any of the seven (7) principles might result in a fine of up

to RM300,000 or imprisonment not exceeding two years or to both. According to the Act the general, security, retention, and disclosure principles are those that businesses frequently violate. This was most likely prompted by concerns about having to pay for complying with the rules, particularly for the SME's owners.

The Personal Data Protection Standard 2015 (the "Standard 2015"), defines the following three (3) minimum obligatory principles that enterprises must closely adhere to: Data Integrity Principle, the Retention Principle, and the Security Principle. If found guilty of breaking these minimum mandatory principles a penalty of up to RM250,000 in fines, up to two years in prison, or both can be imposed. The aforementioned seven (7) core data protection principles must still be followed, nonetheless.

(a) Security Principle (Section 9 of PDPA)
A data user or processor must take all reasonable precautions when processing personal data to guard against loss, misuse, modification, unauthorised or accidental access or disclosure, change, or destruction. The user of the data must, however, obtain a sufficient guarantee from the provider of third-party services regarding those providers' security measures for the protection of the data and take all reasonable steps to ensure compliance with this principle in situations where data processing is carried out by an outside third party.

(b) Retention Principle (Section 10 of PDPA)
This principle states that a data subject's personal information should not be stored for any longer than is necessary to fulfil the purposes for which it is being processed. When the aforementioned goal has been accomplished, it is the data user's responsibility to take all practical steps to delete all personal data entirely. According to the details provided by various rules, different retention periods apply; for instance, information regarding employee payrolls must be kept for seven (7) years. In contrast, inactive personal data must be deleted within 24 months and if it has no legal significance, it must be done so within 14 days.

(c) Data Integrity Principle (Section 11 of PDPA)
According to this principle, data users are constantly required to take reasonable steps to ensure that the personal data they use is accurate, up to date, complete, and serves the intended purpose for which it was acquired and processed.

In the case of CIMB Bank Bhd v Roebuck Development Sdn Bhd (In Liquidation) & Ors [2021], the court held that the second defendant had a duty to maintain the confidentiality of any personal information it had collected throughout the course of its business activities because the third-party buyer had not given any kind of authorization. The court further determined that it would be illegal to disclose this information. This case clearly demonstrates the critical importance of consent when it comes to personal data or information.

These principles demonstrate how Malaysian law emphasises the company's responsibility for the user's data privacy. Even though the company has been a victim of phishing, that does not free them of liability for failing to safeguard their users from this cyberattack. Determining the responsibility for spear phishing in Malaysia involves considering multiple parties who may be held accountable under the existing legal framework. Spear phishing raises questions about the individuals or entities responsible for the offense and the potential liabilities they may face. The responsibility for spear phishing primarily lies with the individuals or groups who initiate and execute the fraudulent activities. These perpetrators, who design and send deceptive e-mails or messages, are responsible for initiating the phishing attacks and attempting to gain unauthorized access to sensitive information or carry out fraudulent activities. However, as discussed above in terms of the PDPA 2010 in addition to the perpetrators, other parties may also bear responsibility. This includes individuals or organizations that fail to implement adequate security measures to protect against phishing attacks, such as organizations that neglect to train their employees on recognizing and reporting phishing attempts or that have insufficient security protocols in place.

## 3 Rights of Victims for Breach of Data

The PDPA 2010 outlines the seven data protection principles to control and safeguard the processing of personal data. Any data user who violates one of the aforementioned principles is in violation of the PDPA 2010, which carries a maximum fine of RM 300,000 and/or a maximum sentence of two years in prison. Nevertheless, the PDPA 2010 solely applies to commercial transactions, and it does not apply to the Federal or State Governments. Individuals may file a complaint with the Personal Data Protection Commissioner if they believe that their personal information may have been handled in violation of any provision of the Act. There are several recommendations which can be offered to the victims. First, the complainant must file a complaint and request explanation from the relevant organisation. In order to allow the inquiry to proceed, the complainant may submit another complaint to the Commissioner of Personal Data Protection if they are still dissatisfied with the organization's answer and actions. By submitting a notice of appeal, the complainant may appeal the Commissioner's judgement to the Appeal Tribunal if they are still not satisfied.

### 3.1 Recommendations

To determine specific responsibilities and liabilities for spear phishing cases in Malaysia, a comprehensive analysis of the circumstances, evidence, and legal provisions is necessary. There is a need for the government to emphasise businesses for better protection of their cybersecurity. If spear phishing occurs because of their carelessness, these data will be exposed to risk. There are numerous methods the company could strengthen their cybersecurity in order to prevent this illegal act from occurring. One of the recommended measures to enhance security against spear phishing attacks is the activation of idle time log out by companies. Idle time log out is a security feature that

determines the duration of inactivity allowed before a user's session is automatically terminated by the server.Users will be asked to confirm that they are still using their account after a certain inactive time. They will be logged out if they do not reply. This guards against hackers using a logged-in machine that has been left unattended to access your system. For service providers, when staff frequently uses shared or portable devices while delivering the service and is distracted by face-to-face interactions, it can be especially pertinent. For servers that handle high-risk data, such as financial information, the Open Web Application Security Project advises implementing idle time out (2 to 5 minutes). It believes that low-risk servers may tolerate extended idle times (15 to 30 minutes).

In addition to activating idle time log out, securing databases and networks is another crucial step for companies to enhance protection against spear phishing attacks. This involves implementing measures such as firewall installation and data encryption. Confidential information could potentially be less vulnerable to cyberattacks. The information that is kept in the company databases needs to be carefully chosen. Databases are a great tool for businesses to have a centralised repository for data and documents, but this does not mean that all information should be kept there. Automatic backups of company data should be configured to happen once per day or once per week, depending on the level of activity inside the company.

Moreover, the employees should be able to discern between genuine notifications and bogus antivirus offers. The company needs to train its employees to recognise bogus antivirus warning signals and alert IT as soon as they notice anything odd (if necessary). The business must have a policy in place for the steps to be taken should an employee's computer become infected with a virus. Malware is a sneaky programme that can access data by infiltrating computers through the Internet, social media, email, attachments, and downloads. As a result, cybercriminals may be able to access passwords, client information, bank accounts, and other sensitive data.

In addition, the company needs to prioritize e-mail security. Most of the time, malware is distributed by e-mail. This platform is used by the vast majority of phishing scams. Despite the fact that businesses and individuals have long been aware of the inadequate security provided by default e-mail settings, the issue is usually ignored. If a security programme is not correctly optimised, it will not provide the defence a company requires. Email encryption, multifactor authentication, disabling auto-forwarding for all emails, using trustworthy WiFi networks, and trusted e-mail security software are all essential for effective e-mail security.

## 4 Conclusion

The Computer Crimes Act 1997 and the Communications and Multimedia Act 1998 serve as the primary legal frameworks in Malaysia that address cybercrimes, including spear phishing. In some cases, third parties, such as e-mail service providers or Internet

service providers, may also have a certain level of responsibility for spear phishing incidents. This could be due to factors such as inadequate security measures or failure to detect and block phishing attempts on their platforms. Though there are many other measures of addressing spear phishing such as cyber security enhancement, cyber court enforcement this paper has looked into the legislative means of regulating the problem.

Therefore, to conclude, it is submitted that there should be greater emphasis placed on ensuring that the company complies with the Personal Data Protection Act 2010 in order to defend its cybersecurity, since they would be in charge of handling the personal information of their users. Malaysian laws could also enhance the compensation provided to victims. Currently the provisions mainly focuses on the penalties towards punishing the company for non-compliance as their sensitive information has been put at danger and could be misused by phishers as such the remedies offered might not be adequate. We can take Indian law for example, where they expressly stated that if the company negligently handle their users' data, they have to be responsible in compensating the victims for the breach of data.

## References

1. Pendakwa Raya (Public Prosecutor) v Vishnu Devarajan [2015] Kuala Lumpur High Court Criminal Appeal No. 42(ORS)-60-07/2015 (available at: http://foongchengleong.com/judgements/Pendakwa%20Raya%20v%20Vishnu%20Devarajan.pdf)
2. Pendakwa Raya lwn Hasimah Binti Aziz [2017] Kuala Lumpur Criminal Sessions Court Criminal Sessions Court Case No. WA-62CY-052-08/2017)
3. Public Prosecutor v Muhammad Nuzaihan bin Kamal Luddin [1999] 3 SLR(R) 653
4. Public Prosecutor v Muhammad Nuzaihan bin Kamal [2000] 1 SLR 34
5. CIMB Bank Bhd v Roebuck Development Sdn Bhd & Ors [2021] MLJU 62
6. (MCMC Statistics) https://www.mcmc.gov.my/en/media/press-clippings/beware-of-lurking-scammers