Legal Limitations relating to the Application of Thai Computer-related Crime Act of B.E. 2560 to the case of "Phishing"

Kanathip Thongraweewong

Abstract

"Phishing" is one of the important cybercrimes in digital age. This article focused on the legal aspect of controlling and criminalizing of "Phishing" in the context of the Computer related Crime Act B.E. 2550 as amended in B.E. 2560. Although "phishing" was stipulated in the draft Bill as a reason of government for amending section 14 (1) in B.E.2560, the author argued that this law could partially cover the practice of "Phishing" due to the fact that main elements of section 14 (1) demonstrate several limitations. The element of "input false of distort data", for example, limits the application of this section to the practice of representing false pretense to human or deceiving person. Hence, it could hardly apply to "phishing" that aims at deceiving system or manipulating the automatic computation of computer system. By conducting a comparative analysis of section 14 (1) to cybercrime convention of Europe, certain EU member's laws and phishing laws of the U.S., the author proposes the amendment of section 14 (1) in order to comprehensively regulate the practice of "Phishing".

Keywords: Phishing, Computer crime, Computer fraud, Computer related crime Act.

[1]Associate Professor of law, Director of Digital law Institute
Kasam Bundit University 1761 Patanakarn Road, Suan Luang, Bangkok 10250
E-mail: kanathip@yahoo.com

Introduction

"Phishing" is one of the important cybercrimes in digital age. From legal perspective, law relating to phishing varies from country to country. As for Thai law, "Phishing" is appeared as one of the main reasons for amending section 14 (1) of the Computer related Crime Act B.E. 2560. Hence, this article will examine the application of this law to the case of phishing by comparing elements of section 14 (1) to international and foreign laws.

Definition and classification of Phishing

There is no universal accepted definition of phishing both in academic and legal perspectives, the meaning and scope of phishing varies. The general meaning involves sending of electronic mail by pretending to be any legitimate persons or organization inducing any users to the fake website in which they provide personal data to the phishers (Stephen, 2006) Fraudulent way of getting confidential information. Users receive official looking email that attempt to fool them into disclosing online passwords and other personal information (Singh, 2011). It can be viewed as a form of online identity theft (Melnick and Dunham, 2008) using social engineering technique in order to obtain personal data and credentials to financial account of victims (Anti-Phishing Working Group, 2018). The phisher usually utilize electronic channels including email, message to elicit personal data or obtain financial benefits to false pretense (Rasha et al, 2015). It can also be done in the context of mobile application.

As for the classification of Phishing, it can take many forms involving different methods. . Based on a classification of Jakobsson and Myers (Markus, 2007), "Phishing" can be classified into 5 types as follows; (1) Deceptive Phishing. The most common practice of this type is sending deceptive email in bulk with a "call to action" demanding the recipient click on a link. The "call to action"; for example, statement that the recipient's account is at risk and offering to enroll in anti-fraud program, a fictitious invoice for merchandise that the recipient did not order, a statement that there is a

problem with recipient's account and ask them to visit a website to correct such problem. (2) Malware based Phishing involves running malicious software on the user's machine. This type of phishing can take many forms including keyloggers and screen loggers which monitor data being input and send the data to phishing server, Web Trojan popping up over login screens to collect data. (3) DNS Based phishing (Pharming) that interferes with the integrity of the lookup process of a domain name including hosts file poisoning, polluting the user's DNS cache with incorrect information that will be used to direct the users to an incorrect location. (4) Content Injection phishing which refers to inserting malicious content into a legitimate site. Such content can redirect to other sites, install malware on a user's computer. (5) Man-in-the-Middle Phishing is a form of phishing in which the phisher positions himself between the user and legitimate site. Messages intended for the legitimate site are passed to the phisher instead.

In a legal perspective, each type of phishing could be considered for the application of criminal offences.

Legal approaches to criminalize "Phishing"

Based on the different methods and behavior of "Phishing", each country takes different approach to criminalize phishing. This paper found that there are 5 legal approaches to criminalize "Phishing" as follows;

Approach 1: Applying interception law to the case of phishing

Due to the fact that main objective of "Phishing" is to obtain data being transmitted, the law relates to data interception can be applied to general behavior of "Phishing". The example of country that applies this approach is section 202b of German Criminal Code which stipulates that "Whosoever unlawfully intercepts data not intended for him, for himself or another by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility, shall be liable to imprisonment not exceeding two years

or a fine, unless the offence incurs a more severe penalty under other provisions" However, this paper found major limitation of this approach in a case where criminals merely disseminate fake information such as imitated websites online but there have not yet been any victims providing data to such fake websites. The interception law could not be applied in such case since its element requires the act of "intercept". In addition, the scope of interception law does not cover the initial stage of sending email with a fake sources or false content in order to deceive the recipients

Approach 2: Applying computer related forgery law to the case of "Phishing"

Regarding to the Convention on Cybercrime, "Phishing" is not criminalized as specific offences but it can be regulated under the provision of computer related fraud in article 7 which stipulates that "...Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches..." The advantage of this approach relies on the fact that "Phishing" generally involves inauthentic data, e.g. uploading a websites that imitate sites of well-known organization to the internet. This approach can be found in several European countries e.g., Bulgaria, Belgium which enact domestic laws in accordance with the article 7 of cybercrime convention.

Approach 3: Applying Computer related fraud law to the case of "Phishing"

Contrarily to the law relating to computer related forgery which focuses on the "inauthentic of data", the main offence of computer related fraud is that criminals cause victim a loss of property. This approach can be found in article 8

of the cybercrime convention which states "...when committed intentionally and without right, the causing of a loss of property to another person by: (a) any input, alteration, deletion or suppression of computer data, or (b) any interference with the functioning of a computer system..." The main objective of "Phishing" is to obtain personal data and abuse it leading to the loss of victim's property. Thus, this law could generally be applied to "Phishing" The domestic laws using this approach are, for example, the criminal code of Canada (article 279a) can be applied to 'phishing website if it is created with a purpose of obtaining economic benefit. Moreover, several countries in Europe are observed to take this approach including Austria (Section 148a of Penal Act), Finland (Section 1, Chapter 36), Criminal Code (Rikoslaki, 1889) and Denmark (The criminal code, Article 279a).

Approach 4: Enacting specific law for "Phishing"

Instead of applying other laws, this approach involves enacting specific law designed in response particularly to behavior and technical aspect of phishing. The element includes relevant behavior such as creation of forged data, the collection of personal data. The example of this approach can be found in certain state laws of the United States as follows;

California enacted specific law referred to as "Anti-Phishing Act" (California Code, Business and Professions Code, Division 8 (Special Business Regulations), Chapter 33, Anti-Phishing Act of 2005, Section 22948.2) which states that "It shall be unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business".

New York enacted specific law referred to as Anti-phishing act of 2006 (New York Laws, GBS - General Business, Article 26 - (390 - 399-ZZZ) which states that "It is unlawful for any person, by means of a web page, electronic message, or other use of the internet to solicit, request or collect identifying

information by deceptively representing himself or herself, either directly or by implication, to be a business or a governmental entity and doing so without the authority or approval of such business or such governmental entity". The advantage of this approach is that it corresponds to the nature of crime and limits the scope of offence to the behavior of "phishing" without leaving opportunity for applying the elements to other behaviors which will be discussed in a case of Thai law.

Approach 5: Applying relevant laws to the case of "Phishing"

This approach involves the application of other laws which are not originally enacted with the purpose of controlling "Phishing". The federal laws of the U.S. and Canada can be classified to this approach. With regards to the United States, federal law provides no specific law of "Phishing". Thus, the relevant laws vary depending on the fact of each case. For example, if phishing involves the identity theft, the Identity Theft and Assumption Deterrence Act shall be applied. The sending of "Phishing" email could be regulated by Spam law. Malware based phishing shall be regulated under the Computer Fraud and Abuse Act (CFAA) (Joanna, 2011). As for Canada, there is no specific law on "Phishing" but the identity theft law can be applied to "Phishing" where the criminal "obtains another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence..." (Criminal Code, section 402). The main limitation of this approach is the variation of relevant laws which shall be considered as a case-by-case basis.

Thailand's Legal approaches to criminalize "Phishing"

This part will examine section 14 (1) in general and analyse it in the context of the five approaches.

1. Section 14 (1) of the Computer related crime Act B.E. as an offence relating to Phishing

The computer related crime Act B.E.2550 of Thailand provides no specific offence of "Phishing". However, the relevant provision can be found in section 14 which was originally enacted

since B.E. 2550 which states “Any person commits the following offenses shall be subject to imprisonment up to five years and a fine not exceeding one hundred thousand baht, or both” and the section 14 (1) states that “.... input into a computer system forged or false computer data in a manner that is likely to cause damage to other person or the public”. The broad elements of this first version lead to the application of this section to online communication of false or fake content which is not relevant to the computer related fraud, especially the online defamation where plaintiffs used the section in conjunction with criminal law (Section 326 and 328 of the criminal code). However, in certain case, court ruled that the intention of section 14 (1) is not intended for applying to online defamation which is already covered by criminal law (Judgment of provincial court of Phuket no. 2161/2557, no. 6564/2558).

Nevertheless, this section was amended in B.E. 2560 as part of the enactment of Computer Related Crime Act B.E.2560 and the new version states that “Any person commits the following offenses shall be subject to imprisonment up to five years and a fine not exceeding one hundred thousand baht, or both”. In addition, section 14 (1) states “.... input into a computer system forged, false or distorted computer data, with bad faith or fraudulent intention, in a manner that is likely to cause damage to the public, this section shall not be applied in a case of defamation”. According to the reason of government for the amendment of this section in B.E. 2560 which appears in the Letter of Prime Minister's Office to the National Legislative Assembly (26 April B.E. 2559), this section aims at “controlling computer fraud, forgery... including the creation of fake website to induce victim to provide personal data for criminal to use in abuse manner (Phishing) ...”. Hence, it is evident that one of the purposes of section 14 (1) is to criminalize Phishing. This section can be applied to phishing especially in case that perpetrator inputs forged or false computer data into computer system such as uploading fake website or sending email with untrue statement inducing victim to click a link to fake

websites. However, this law provides no general definition of "Phishing" and there are several limitations to apply this section to "Phishing" as discussed in the next topic.

2. Analyzing section 14 (1) in the context of the five approaches

According to the approaches discussed above, the part will make comparative analysis to the Thai law.

In opposition to cybercrime convention which separates computer fraud and computer forgery into 2 different offence, section 14 (1) combine the two offence into single one. However, the scope and elements of this section differ from computer fraud and forgery according to the convention and some other countries due to the fact that section 14 (1) covers mere act of posting fake story or fake news online without causing any financial or economic loss, in contrast to computer related fraud in article 8 of cybercrime convention which limits to action causing "loss of property". In addition, it has broader scope by not restricting to defraud of system. Hence, the author argues that the application of this section can be analogous to approach 2 and 3 with several limitations.

Although section 14 (1) reflects the intention to criminalize phishing, it is different from Approach 4 which covers specific action of inducing victim to provide personal data. The author argues that If the amendments of section 14 (1) in B.E. 2560 takes the approach 4, this section shall respond specifically to phishing and cover most methods of phishing without being able to include "fake news or story".

The limitations in application of the Computer related crime Act B.E. to the case of Phishing

In this part, section 14 (1) will be analyzed, in general and in context of the types of "Phishing", to indicate the legal limitations relating to the application of this section to the case of "Phishing".

1. The general analysis of section 14 (1)

In general, there are 2 main limitations in applying section 14 (1) to the case of phishing.

The problem relating to the element of "Input" Section 14 (1) limits

the scope of element merely to the action of "Input computer data into system". Although this element can cover the upload of forged website, fake email with a link to lure victim, it cannot be applied to the whole process of "Phishing" which comprises several sub-behaviors such as creating of fake webpage or application that look similar to the legitimate ones, building of fake electronic mail, intercepting of personal data and credentials of victims through fake website and using data derived from victim to commit other crimes online. Comparing to the laws in the second and third approach, the actions include not only "input" but also "alteration, deletion, or suppression of computer data". In addition, certain types of "Phishing" may not involve the "Input" of data, e.g. DNS Based phishing and Man-in-the-Middle Phishing.

The problem relating to the element of "false, forged, or distortive data", this element reflects the intention to regulate the computer related fraud. However, comparing to the law in second approach, the main element of computer related fraud offence in laws of several countries including Cybercrime convention demonstrate the narrowly written elements to include only defraud of system, i.e., automatic processing or computing of a computer system, not defraud targeting the perception of human. Thus, the false or fake of content which is understandable by human is irrelevant. Such laws focus on the actions affecting the functioning of system (Explanatory Report to the Council of Europe Convention on Cybercrime, No.86). Hence, the "false, forged or distortive data" in section 14 (1) could be regarded as the main limitation to the case of phishing, especially the types of phishing which does not involve true or false of content in context of human perception, e.g. Malware based Phishing DNS Based phishing.

2. The analysis of section 14 (1) in the context of types of Phishing

Based on each type of phishing, the limitation of applying section 14 (1) can be discussed as follows;

- *Deceptive Phishing*: The reasons for amending section 14 (1) reflect the purpose of controlling this type of

phishing where criminal sending electronic communication offering "call to action" According to element of section 14 (1), this type of phishing involves the inputting of "fake data" in two dimension. Firstly, the input of message luring victim with a "call to action" for example claiming that the account is at risk and ask to visit a website for entering new password. This message contains "fake content" under this section. Secondly, the creation of fake website as a target or destination is another input of "fake data" according to section 14 (1).

- *Malware based Phishing Contrary to "deceptive phishing"*: This type of phishing would not involve the creation of fake website or claiming to be legitimate entity because it uses malware to collect victim's data. The main element of section 14 (1) which limits to "inputting fake, false or distortive computer data" could not be applied to this case. Although the sending of malware can be considered as "input computer data", the malware itself is not "fake, false or distortive".

- *DNS Based phishing (Pharming)*: This type leads to the technically alteration affecting lookup process of a domain name with the main purpose of redirecting user to fake websites. It could be referred to as "phishing through port redirection [8]. According to section 14 (1), the redirection process could not be fall under the element of "input fake, false or distorted computer data". The truth or false aspects of content is irrelevant to port redirection attack. However, section 14 (1) could be applied merely in aspects of the destination sites provided that such sites are "fake, false of distortive".

- *Content Injection phishing*: The main practice of this type of phishing involves inserting malicious content into a legitimate site. Although the insertion of such content can be regarded as "inputting computer data", such content is actually a "code" which cannot be read or understood by plain perception of human. Thus it could not be considered as "fake, false or distortive" computer data in the context of section 14 (1).

- *Man-in-the-Middle*: The ultimate goal of attackers who use this method is similar to other types of phishing, i.e. obtaining personal data from victim. However, the main practice of this type involves the act of intercepting data by technical means, not inputting "false, fake or distortive data". In addition, there is not fake destination such as websites because it is the attackers themselves who collect user's data, not luring user to provide data.

Conclusions and Recommendations

Although "phishing" was stipulated as reason for amending section 14 (1) of the computer related crime Act, the author argued that this law could partially cover the practice of "Phishing" due to the fact that main elements of section 14 (1) demonstrate several limitations. The element of "input false, forged or distortive data", for example, limits the application of this section to the practice of representing false pretense to human or deceiving person. Hence, it could hardly be applied to "phishing" which aims at deceiving system or manipulating the automatic computation of computer system. By conducting a comparative analysis of section 14 (1) to international and foreign laws, the author proposes two alternative for amending of section 14 (1); firstly, taking approach 4 by referring to state laws of the U.S. as a model law and secondly, taking approach 2 by referring to article 8 of cybercrime convention as a model law.

References

Anti-Phishing Working Group. (2018). **Phishing Report**.

Jim Melnick and Ken Dunham. (2008). **Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet**. Auerbach Publications.

Joanna L Grama. (2011). **Legal Issues in Information Security**. Jones & Bartlett Learning, LLC.

Markus Jakobsson and Steven Myers. (2007). **Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity theft**. John Wiley and Sons Publication.

Rasha S El-Din, Paul Cairns, and John Clark. (2015). "The Human Factor in Mobile Phishing". In **New Threats and Countermeasures in Digital Crime and Cyber Terrorism**. edited by Maurice Dawson and Marwan Omar. IGI Global.

Rick Howard. (2010). **Cyber Fraud: Tactics, Techniques and Procedures**. CRC Press.

Stephen D. Fried. (2006). "Phishing : A New twist to an old game". in **Information Security Management Handbook**. edited by Harold F Tipton and Micki Krause. Taylor & Francis Group, LLC.

Yatindra Singh. (2011). **Cyber Laws: A Guide to Cyber Laws, Information Technology, Computer Software**. Universal law publishing Co.