International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.02, February 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Detailed Survey on Phishing Attack Techniques and Countermeasures in World Wide Online Banking

Dhachainee a/p Murugayah[1], Sivagami a/p Govindasamy[2]

[1,2]BSc (Hons) in Software Engineering, Asia Pacific University, Malaysia

ABSTRACT

While the internet is undoubtedly playingsophisticated part in one's life, the modus operandi of stealing bank user's financial credentials has also escalated enormously over the past years, which potentially causinga direct loss to the affected victims and respective banks. Although online banking system is being the primary target of the perpetrator, but the ways of attaining the sensitive information varies. Phishing is one of thecommon techniques that have been used to lure the victim to believe fraudulent emails and messages as legitimate sources from the bank, but in reality those requests are coming from the unauthorized individuals with the intention of stealing the financial data. As the result, security has become the major concern for both banks and the users of online banking system. Therefore, this paper explores the tactics that the attackers utilize to trick the users to fall for online banking fraud victimization and defence techniques that can be taken with the help of information security technologies to curb phishing attacks in online banking. This paper can be used as guidance for the public to create awareness with the intention of combating phishing baits.

Keywords: **Counter Attacks, Counter Measures, Phishing Techniques**

I.INTRODUCTION

Technology has been facing drastic changes from time to time as the world is moving towards digitization. Progression in the technology enables future driven internet services in a wide range of fields to ease the human life and enhance the productivity. As the number of internet users isrisingexponentially, Malaysia is also following the rapid advancement of the technology whilethe number of Malaysians that relying on the internet has been increasingas interneteases users to accomplish their chores in an efficient and effective manner. [1] holds the view that, the number of Malaysian internet users isgrowing steadily.[2]stated that, the penetration of the internet among Malaysians has continued to progress rapidly since the year 2000 whereby the internet users increased from 0.1 % to 37.9% from 1995 to 2005 in Malaysia. As reported by Malaysian Communication and Multimedia Commission, the internet penetration rate in Malaysia in the first quarter of 2014 was 20.1 million users, which is approximately 66.6% of the Malaysian population[2].

Banking field is not an exemption to this evolution of the internet as online banking is a great platform which provides ground breaking offer to bank. Online banking will not only escalate the capabilities of the bank in providing good services to their respective customers, but also assist the bank in terms of providing better and unique features to niche segments of their online banking which will expand their business models and diminish

the operational costs. As banks continue to be digitized, the vulnerability to phishing attacks has amplified drastically. It is not surprisingto anyone that villains will appear to steal whenever money is involved in it.

With high technological development, exploit tools which can be used to find the vulnerability in the server side of a system has become accessible for anyone who have little knowledge in Information Technology. These tools ease the fraudsters to conduct phishing attacks bymanipulating the vulnerability in online banking servers in order to attain confidential data from the server. In 2015, a graduate from a university located in south-western Nigeria detained with the sum of 2.4 million of Naira for hacking bank customers' account details for several years [3]. In Canada, two 14 year old high school students hacked the ATM machine of the one of the famous banks in Canada, Bank of Montreal by using an old ATM operator manual that discovered on the internet [4]. All these examples corroborate that a person with average computer knowledge or a person who can gain manual source from the internet is able to launch phishing attacks.

II.PHISHING

Phishing refers to social engineering attacks of attainingprivate information and credentials fraudulently from the victims by impersonating those requests that came from a well-established organization. Phishing is the major threat to the financial institutions in Malaysia especially to the bankers. As reported by[5], Malaysian Computer Emergency Response Team (MyCERT) stated the number of cybercrime attacks in Malaysia especially phishing has increased exponentially. Moreover, Malaysian Communications and Multimedia Commission express the view that, most of the phishing attacks in Malaysia targeted online banking users and deceive them to disclose their credentials [6].

Phishing is conducted by phishers who either will operate in solitude or in a structured crime circle. Phishers actively operate globally and targeting both the developed countries such as U.S and the developing countries like Malaysia. Although highest notorious phishing circle operates in countries like Russia and U.S yet solitary phisher can operate anywhere, including countries like Nigeria, which is still in the process of discovering the benefits of cyber technology. Deceiving the victims to reveal their valuable information which the phishers later use to get access to the victim's bank accounts, perform money transactions or even trick the victim to pay some amount immediately are the common denominators that the phishers use. There are uncountable ways the phishers can use to attain victims' credit or debit card details or even trick the victims to hand over some money. An e-mail with lucrative subject line is the most prolific way of phishing attacks. It lures the recipient to check the email and along this chain, the recipient enters the financial information on the bogus website which looks like a legitimate website believing they will get free discounts and door gifts.

Most of the online banking customers were susceptible and tend to provide their private financial information to the fraudsters due to the lack of knowledge and skills they acquired in terms of the security and safety of the online banking. Phishing mainly occurred due to the difficulties that the people are having in taking protective measures to safeguard their sensitive information against the phishing attacks. Awareness of the fraudulent

schemes and basic knowledge on applying protective measures is necessary for the entire online banking users to perform safe and secure transactions.

2.1 PHISHING IMPACT TO THE VICTIMS

The impact of the phishing attack is much more insidious than stealing the privacy of people. Surrendering sensitive information will cause substantial financial loss to the victim. Usually the phishes use pop-up messages, instant messages or spam as the techniques in the attempt of inducing the victims to disclose their confidential information, in this matter revolves around online banking information such as pin number, password, credit or debit card numbers and other private information. Revealing the sensitive information may ruin the victims' life and lead to lots of problems and financial losses. Once the phishers captured the personal information that submitted through bogus website, thephishers can create fake accounts and mishandle the account for criminal activities. As the consequences, it will prevent the owners from accessing their own profile or accounts. In some cases, the victims can be detained for using their accounts for illegal activities but in reality it was the phishers.

This act of compromising the security of the system via social engineering can be found in a junk email folder, anonymous messages with links or even in the advertisements on Facebook and Twitter which attempt to re-direct the users to bogus websites. MacEwan University in Canada unintentionally lost about $ 10 million after receiving fake emails that one of the school vendors would like to change their bank information where the staff of the university became prey by paying the money into the new bank account which did not received by the vendor [7]. Due to the enormous growth of phishing technology, people are at high risk of being victimized for the phishing baits. China, which consists of huge amount of internet users, has encountered phishing attack where 60 million online users were conned out for $5 billion by the bogus websites in China [8]. [9]Everyday 10,000 phishing websites have been created in China and 95% of those websites were auto-generated by the phishers or hackers. This kind of monetary losses reduces public confidence in using the internet to carry out transactions. From the survey conducted by[10]42% of the participants in this survey responded that their trust on the brand and reputation of the organization will be significantly declined if they receive phishing email claiming to be from the respective organization. It is clearly shown that people's trust and confidence on the online banking highly affected by phishing attack.

2.2 PHISHING IMPACT TO THE BANKS

The fact that the banking industry is being the main target of the phishers to use phishing in order to breach the security of the banks is inevitable. Although there are safety protocols that have been built in both internal and external banking system and websites, it is always the human elements that make errors and fail to detect the phishing attack results in loss of direct monetary to the banks. Apart from the direct monetary loss, the fragile bond of the trust that the bank earnedfrom their customers will shatter. When the bank loses its corporate image due to loss of faith in the reliability and security of its electronic resources among the people, the bank will commence to lose its customer base. Furthermore, banks spend millions of dollars to analyse the weaknesses,

enhance the recovery time and security of their existing system to avoid occurrence of disasters. However, this endeavour of the banks to strengthen the safety and security of their electronic communication methods will cause significant loss of money, time and resources. In the case of high level phishing attacks, issuing new credentials to the affected customers, account replacement loss and customer service expenses will cause indirect loss to the banking business.

Generally the stereotypical phishing attack comes in the form of email with some sort of statement to deceive the user to insert or update their personal or financial information. These phishing emails send to users in the guise of those emailsthat came from the legitimate bank. A regular person will more likely to consider the email that matching previous emails that came from the banks. This is due to the bad practice of the business that request sensitive information of the customers via email and provide links to access their business websites. This type of emails bewilders the customers and leads them more likely to fall prey tothe phishing attacks.A metal supply company which is based in Michigan sued Comerica Bank by claiming that the bank exposed its online customers to phishing baits after the company lost $ 550,000 from its bank account[11]. The metal supply company received an email with a link from the bank requested them to update security software of the bank, in reality those requests came from the phisher. Therefore, banks need to safeguard their credibility by enhancing their electronic communicate methods and use robust solution to secure their email gateway from security threats.

2.3 PHISHING IMPACT IN MALAYSIA

Phishing is the one of the type of cybercrime attempt that has enormously increased in Malaysia, especially in online banking due to its high return on investment even though a small number of people victimized in the attack. As reported by [12] 39 phishing cases were reported in 2013 involving total loss of US$56,156 (RM 178,700). However, [13]stated that, 872 phishing cases were reported in 2011 with the total loss of RM 3.29 million, followed by 264 cases in Malaysia with the total loss of US$377,090 (RM 1.2 million) in 2012. Even though there is a reduction in the number of reported phishing cases, phishing cases in online banking are still a notable cybercrime attack in Malaysia. This is because of the number of online banking users that have been escalating as performing online transactions is much convenient and comfortable for the users. This became an ample opportunity for the perpetrator to deceive the online banking users to steal their money. Apart from high number of online banking users, human carelessness is also a prominent factor for phishing. Malaysian Communication and Multimedia Commission (MCMC) have taken many actions to curb the expansion of phishing activities in Malaysia and shutting down the suspicious websites is one of the steps taken by MCMC. [14]Stated that, Malaysian Communication and Multimedia Commission (MCMC) have identified and taken down 2,611 websites that suspected to be involved in phishing activities until the year of 2012.

III. PHISHING TECHNIQUES

3.1 MAN-IN-THE-MIDDLE ATTACK

Man-in-the-middle abbreviated as MITMA is a form of phishing technique, in a sense it is like eavesdropping. This cyber-attack occurs when the communication between two parties over the internet intercepted by malicious people. This real-time phishing allows the criminals to commit fraud by stealing personal and financial credentials through accessing the internet bank session in real time. MITMA permits the phishers to bypass the authentication protocols of the bank. The phishers impersonate both parties by inserting themselves as a relay or proxy into the conversation session and sniff the information that is sent between both parties without their acquaintance. This attack can be occurred in any form of online communication such as web surfing, social media messages or email.

Phishers will not only eavesdrop the conversation, meanwhile they will also target all the information in the electronic devices. Phishers discovered the possible ways to execute MITM attacks over the years, which is facilitated by relatively cheap hacking tools that can be purchased via online by whoever have enough money to buy. [15]Anti-fraud unit of RSA, which is the security division of EMC discovered universal MITM Phishing Kit on sale in the online fraudster forum for phishing fraudsters to capture personal credentials of the victims in real-time. There are a few types of MITM attack that organization or people will most like to encounter:

3.2 EMAIL HIJACKING

Phishers utilize this tacticto sniff the personal or financial information by targeting several email accounts. Mostly they will target large organizations and banks where large amount of transaction will occur. Once the phishers get the accessibility to access the emails, they will silently monitor the email communication and make an attempt in the right situation. For example, the phishers will wait for the scenario where the customers send email to the firms that they will be paying the amount, by spoofing the email address of the firm the phishers will send their bank account number. As the result the customers will make the transaction to the phishers' account without realizing they became prey for the phishing attack.

3.3 WI-FI EAVESDROPPING

MITM attacks mostly thrive on Wi-Fi connection where the phisher sets up a Wi-Fi connection under a legitimate name to deceive the people. Once the people start to use the Wi-Fi connection and connect their electronic device with that Wi-Fi connection, the phishers will instantly get access to the electronic devices. They will steal all the important files and personal credentials of whoever connected with that Wi-Fi connection.

3.4 SESSION HIJACKING

When a user gets access to a website, the connection will be established between the electronic device of the user and the website. Phishers can hijack the session of the user with the website via many options. Stealing the

browser cookies is one of the options that the phisher uses in session hijacking. Cookies which store small piece of information such as user location, login credentials and online activity in order to ease and make the users convenient to perform web browsing could turn to be a dangerous tool for the users as phishers can easily access to the victims' accounts if they got to hold the victims' login cookies.

IV.LINK MANIPULATION

Link Manipulation is one of the techniques of phishing. In this technique, the phisher sends a link to a website. This link is a deceptive link and opens up the bogus website instead of the original website that the user would like to access. Link manipulation is a widely used technique for these phishing scams. However, many internet users are aware of these phishing scams. Thus, the users now know that there is no reason to click on links that seems suspicious that could save them from many issues later. There are some ways of link manipulation that phishers use to get the users to click on the deceptive links and steal their data.

4.1 USE OF SUB-DOMAINS

Sub domains are Internet domains which are part of primary domains. For example, Yahoo.com is the primary domain and Mail from Yahoo would be the sub domain as in mail.yahoo.com. The domains are unique and sub domains are not, thus no domain owner would be able to prevent anyone from using their name. The phishers use this way in where the sub domains would be reversed such as yahoo.mail.com and this reversing sub domain would lead the users to the phishing links. The users especially the non-technical users would not be able to identify the difference between these two. Thus, the users would be scammed. However, the users should always remember that the URL hierarchy goes from right to left.

4.2 HIDDEN URLS

This is the simplest way phishers use to scam the users. In this way, phishers just mask the true domain name in text. This is done by having words such as "Click the link" or "Subscribe" instead of the actual link or writes a deceptive link as an actual link. So it looks like an actual URL where users would trust and click on it. There is also another way of hiding the URL where the phishers would use shortening tool such as bit.ly. Users and businesses such as banks are all now on social media networks, this becomes an opportunity for the phishers to wide spread their scams. With the assistance of shortening tools, the phishers would be able to scam many users because users would not be able to identify the actual link.

4.3 MISSPELLED URLS

Another common way of link manipulation is when a phisher will use a domain which has difference in spellings of a popular domain. Some examples include facebok.com, google.com and so on. The users will get scammed as these domains would look like the actual domains. The phishers would then proceed in asking personal information of the users in where the users would not have any doubts on any of these domains. This

way is also called as the URL hijacking. This happens because of users who accidentally misspelled URLs and do not realise those typing mistakes.

Some of these phishing techniques would and have happened to many users in the past, present and could also happen in the future. However, the impact of these phishing techniques can only be seen in major issues that includes financial institutions. Some of the phishers send emails to bank customers using some general greetings such as Hello 'Bank Name' Customer. Usually, banks would always send emails to their customers by addressing them with specific one's names. This kind of attacks is launched in bulk as at least one user would fall for it. According to The Star Online 2014, there were RM581, 000 losses, 51 cases involving the credit card scams. Bukit Aman has imprisoned some 180 syndicate members for this kind of frauds over that year.

V.WEBSITE FORGERY

Another phishing technique that phishers use is website forgery. This is just that the phishers will develop another website copying an original one. This is definitely a harmful website where the users will have to lose their sensitive information such as account details, passwords and so on. There are some ways that phishers can use website forgery. One of the ways is cross-site scripting.

5.1 CROSS-SITE SCRIPTING

Cross-site scripting or XSS is an attack where phishers executes harmful computer scripts into an authentic website. In this way, the users are indirectly targeted. Instead, the phishers have created a loophole in the websites that are being accessed by the users. Thus, then the harmful scripts will be delivered to the users' browsers. The phishers can take advantage of the XSS that is present within ActiveX or VBScript or JavaScript that is commonly used by most of the websites. The process starts with the phishers inserting a script into a page accessed by the users. For the users to constantly access the website, the phishers would use link manipulation techniques. This is then continued by the phishers by directly inserting the data into the deceptive website. Then, the phishers would insert a string to the webpage and the browser would accept the string as part of the code and loads the webpage. Thus, the script is executed, and the users would not be aware of the whole scenario and continue to access the website with their information being stolen.

Some of these phishing techniques would and have happened to many users in the past, present and could also happen in the future. However, the impact of these phishing techniques can only be seen in major issues that includes financial institutions. The Unisys Security Index is a global study that measures the attitudes of customers on a wide range of issues that have relations to national, personal, financial and Internet security. The study surveyed 1000 adults in Malaysia during April 2017. From the results, Malaysia recorded the third highest level of concern and is higher than the global average. The results have stated that 87% of Malaysians are concerned about others misusing their personal information. 77% of Malaysians are concerned about computer and Internet security in terms of viruses, hacking and so on. Finally, 88% Malaysians are concerned about other people gaining access to or using their credit card details [16].

These are all because of some phishing scams that affected Malaysians in a large scale. In Nov 2017, a young woman was scammed by phishers where an official email was sent to her regarding her payments. Thus, she clicked on the link leading her to the fake CIMB Clicks where she entered all her personal information. Later, she received a message from the bank saying that she performed a transaction where all the money from her bank account has been transferred to someone she does not know. Luckily, a police complaint has been filed and part of her money has been retrieved [17].

VI. PREVENTION TECHNIQUES

There are many phishing cases that are reported by the users and there could be many more cases that are not reported or brought forward by the internet users. However, there are also many preventive techniques that could be practised by the users to evade these kinds of phishing scams as the impact to the users and the surrounding is very much higher. All these techniques that are stated below are simple techniques that could be easily cultivated by the users. The users should understand that they are the ones responsible for their own safety on the internet.

6.1 EMAIL

Since most of the phishing scams happens through the emails, the users should ensure that the emails that they are receiving are from the legitimate sources. Even the links that they are clicking should be only authentic websites and so on. This step can be easily practised by the users by constantly checking for red flags. Red flags would be strange email addresses or misspelled links. Obviously, the users should be aware that these kinds of links or websites would not be legitimate ones and ensure that they do not click on it or share any personal information through it.

6.2 SOFTWARE

Some other simple techniques that can be used are users should make good use of the security software that is widely available in the market. This includes antivirus, antispyware and firewall software. All this software could do great help to the users and their computers. Sometimes phishers might insert some harmful scripts in the web browsers. Thus, by updating the web browsers and enabling phishing filter would assist the users in removing the harmful scripts or at least lessen the impact on the computer.

6.3 PERSONAL INFORMATION

Everything could be done on the internet today. This includes banking, online shopping and so on. It is the users' responsibility to ensure that their personal information such as credit card number, address and so on to be safe. For this, the users can simply use diverse email address for different purposes. In this way, the impact would be less as different information would be accessed at various sites.

Phishing scams have the highest impact in relation to financial institutions which are banks. There are many cases around the world that involves phishing such as fraud, data stealing and so on. There are some simple techniques that can be used by the users to protect themselves on the internet especially relating to their bank matters.

6.4 ONLINE BANKING

The simplest technique that could be done by the users is to delete all cookies and history file after performing transactions of any kind. Users might not be aware of the cookies that could be present in their browsers. Some websites intentionally use cookies to receive the personal information of the users for their own research and stuff. However, without the users realising, there might be some cookies that could be harmful that just adopt the important, personal details of the users where the phishers would be able to use against the users. The users should also use virtual keyboard while accessing online banking. This is because some virus or harmful substance could be attached to the keyboard. Thus, when accessing, the virus or some harmful substance would be able to detect the finger movement and the phishers would be able to imitate the exact movement of the users and access their bank details [18].

VII.RECOMMENDATION

Since everything could be done on the internet, the phishing scams are getting better and better every day. This is not a favourable situation for the users as they would have to practice more preventive measures to avoid the scams. Some of the future techniques that the users should have to follow are listed below. It might be that now these techniques may seem unusable for current scenarios. However, in the future, these techniques would be surely utilised because of its effectiveness.

- Users should never place an online order based on an email offer. This means that some phishing scams involving online shopping may send out offers in emails. This could deceive users who are not aware of the phishing scams.
- Online banking should use fingerprint scanning for authentication for any users' transactions. This would ensure that the phishers would not be able to perform any transactions of any kinds without the users' fingerprint access.
- Financial institutions should also consider utilising single-use credit card numbers. The advantage of using these single-use credit card numbers is that once it is used, then any phishers would not be able to use the same number for illegal access.
- The government should also ensure the users' safety on the internet. However, the government is also in the stake of danger for the phishing scams. This is because the government would have much more confidential information that has to be taken care of. Thus, the government need to adapt many initiatives in ensuring that these scams decreases. For that, the government should enforce the law by upgrading to a stricter punishment towards phishers. This will make the perpetrators to think twice before performing a crime especially related to these scams.

IX.CONCLUSION

During the completion of this research, extensive research has been done in the areas of impact of phishing, phishing techniques and prevention methods. In the introduction, many problems that initiate phishers into phishing have been discussed. Problems are explained in detail and with much useful information. Then, some important and common phishing techniques are discussed in the next chapter. In this chapter, several phishing techniques are discussed in detail with some real-life incidents. If there is a problem, then there should be a solution. Thus, the preventive techniques are discussed in the followingchapter. There are some simple measures to be taken by the users to ensure safety and security in using internet especially while using online banking. The main intention of this research is to educate the users on the consequences of phishing attacks and simple preventive methods that can be taken to curb the expansion of phishing attack as there are many users who are still unaware of these phishing scams. Through this paper, the users would now be able to know the danger of phishing and the importance of following the preventive techniques as those techniques could truly assist them in the internet world. In a nutshell, phishing is a most notable cybercrime attack as it produces high profitability to the perpetrators. Phishing becomes the major threat to online banking in Malaysia as it involves high flow of money transaction. Although there is a reduction in the number of phishing attacks in Malaysia, further action need to be made to utterly halt this social engineering attack. High efforts need to be taken to educate the netizens and the banks are also need to safeguard their credibility by enhancing their electronic communicate methods and use robust solution to secure their email gateway from security threats. Phishing attack will not only affect the security of the technology in a country but also give direct impact on the economic and cultural progression of a country.

X.ACKNOWLEDGMENT

The authors would like to share gratitude to Mr Umapathy Eaganathan, Lecturer in Computing, Asia Pacific University, Malaysia for the constant support and motivation which helped us to participate in this International Conference and also for journal publication.

REFERENCES

[1] Daka Advisory., 2014. “Digital development in Malaysia – An analysis of cyber threats and Responses,” [Online], [Retrieved January 13, 2018].

[2] Muniandy, L. and Muniandy, B., 2012. “State of Cyber Security and the Factors Governing its Protection in Malaysia,” International Journal of Applied Science and Technology, (2)4, 106-112

[3] Nairametrics, 2015. *How A Student Hacked Into Bank Customers’ Accounts.* [Online] Available at: https://nairametrics.com/how-a-student-hacked-into-bank-customers-accounts/ [Accessed 14 January 2018].

[4] Paganini, P., 2014. *Two 14-year-old students hacked an ATM with impressive simplicity.* [Online] Available at: http://securityaffairs.co/wordpress/25616/hacking/2-14-year-old-hacked-atm.html [Accessed 14 January 2018].

[5] Zulhuda, S., 2012. The state of e-government security in Malaysia: reassessing the legal and regulatory framework on the threat of information theft.

[6] Malaysian Communications and Multimedia Commission, 2018. *Phishing Attack.* [Online] Available at: https://www.skmm.gov.my/faqs/phishing-attack/1-what-is-phishing [Accessed 14 January 2018].

[7] Abrams, A., 2017. *A Canadian University Just Lost $10M In an Email Phishing Scam* [Online] Available at: http://time.com/4924461/macewan-canadian-university-loses-10-million-email-phishing-scam/[Accessed 15 January 2018].

[8] Jiang, H., Zhang, D. and Yan, Z., 2013. A Classification Model for Detection of Chinese Phishing E-Business Websites. In *PACIS* (p. 152).

[9] Chen, P., Nikiforakis, N., Desmet, L. and Huygens, C., 2014, November. Security Analysis of the Chinese Web: How well is it protected?. In *Proceedings of the 2014 Workshop on Cyber Security Analytics, Intelligence and Automation* (pp. 3-9). ACM.

[10] Blanco Hache, A.C. and Ryder, N., 2011. 'Tis the season to (be jolly?) wise-up to online fraudsters. Criminals on the Web lurking to scam shoppers this Christmas: 1 a critical analysis of the United Kingdom's legislative provisions and policies to tackle online fraud. *Information & Communications Technology Law*, *20*(1), pp.35-56.

[11] Cassim, F., 2014. Addressing the spectre of phishing: are adequate measures in place to protect victims of phishing?. *Comparative and International Law Journal of Southern Africa*, *47*(3), pp.401-428.

[12] Singh, K., 2013. *Big dip in phishing attacks in Malaysia, but ,* Kuala Lumpur: Digital News Asia.

[13] Gerald Goh, Ling, N.T & Sara, A. et al., 2015. Phishing: A Growing Challenge for Internet Banking Providers in Malaysia. Communications of the IBIMA, 5, 132-142.

[14] The Star, 2013. *652 phishing sites taken down by MCMC so far.* [Online] Available at: https://www.thestar.com.my/news/nation/2013/07/02/652-phishing-sites-taken-down-by-mcmc-so-far/#6TSbB05LDVtSz4IG.99
[Accessed 16 January 2018].

[15] Leyden, J., 2007. *Man-in-the-Middle phishing kit netted.* [Online] Available at:https://www.theregister.co.uk/2007/01/12/phishing_kit/[Accessed 17 January 2018].

[16] Digital News Asia. 2018. *Asia's top Internet scams, and how to stay safe | Digital News Asia*. [ONLINE] Available at: https://www.digitalnewsasia.com/asia%E2%80%99s-top-internet-scams-and-how-stay-safe. [Accessed 17 January 2018].

[17] Tang Ruxyn. 2018. *A Woman Lost Most Of Her Money After Falling Prey To A "LHDN Tax Refund" Scam*. [ONLINE] Available at: http://says.com/my/news/lhdn-tax-refund-email-scam-syndicate. [Accessed 17 January 2018].

[18]InfoSec Resources. 2018. *Link Manipulation*. [ONLINE] Available at: http://resources.infosecinstitute.com/category/enterprise/phishing/phishing-tools-techniques/link-manipulation/#gref. [Accessed 17 January 2018]