Phishdentity: Leverage Website Favicon to Offset Phishing Website

Jeffrey Choo Soon Fatt

Master of Science
(Computer Science)
2015
Phishdentity: Leverage Website Favicon to Offset Phishing Website

Jeffrey Choo Soon Fatt

A thesis submitted
in fulfillment of the requirements for the degree of
Master of Science

Faculty of Computer Science and Information Technology
UNIVERSITI MALAYSIA SARAWAK
2015
# TABLE OF CONTENTS

LIST OF FIGURES ........................................................................................................ III
LIST OF TABLES ............................................................................................................... IV
GLOSSARY OF TERMS .................................................................................................. V
ABSTRACT ..................................................................................................................... VII
ABSTRAK ....................................................................................................................... VIII
LIST OF PUBLICATIONS .............................................................................................. IX
ACKNOWLEDGEMENTS ............................................................................................... X

## 1 Introduction ............................................................................................................ 1
  1.1. Background of Phishing ...................................................................................... 1
  1.2. Motivation .......................................................................................................... 2
  1.3. Case Study Scenario ......................................................................................... 3
  1.4. Research Problems ............................................................................................ 5
  1.5. Research Objectives .......................................................................................... 5
  1.6. Scope of Research ............................................................................................. 6
  1.7. Outline of the Thesis ........................................................................................ 6

## 2 Phishing Attacks and Prevention Studies .............................................................. 7
  2.1. Classification of Phishing Attacks ...................................................................... 7
    2.1.1. Phishing Vectors .......................................................................................... 7
    2.1.2. Phishing Techniques ................................................................................... 9
  2.2. Prevention of Phishing Attacks ......................................................................... 11
    2.2.1. Non-technical Approach .......................................................................... 12
    2.2.2. Technical Approach .................................................................................. 13
  2.3. Database ............................................................................................................ 14
    2.3.1. List-based Approach .................................................................................. 15
    2.3.2. Image-based Approach ............................................................................ 20
  2.4. Search Engine ................................................................................................... 23
    2.4.1. Website Ranking ....................................................................................... 24
    2.4.2. WHOIS .................................................................................................... 25
    2.4.3. Search Results ......................................................................................... 26
  2.5. Classifier ........................................................................................................... 28
  2.6. Summary ........................................................................................................... 30

## 3 Methodology and Detection Schemes ................................................................... 34
  3.1. Proposed Framework ....................................................................................... 34
  3.2. Website Favicon ............................................................................................... 36
  3.3. Google search by image .................................................................................. 38
  3.4. Proposed Feature Set One .............................................................................. 41
    3.4.1. Second-level Domain .............................................................................. 42
    3.4.2. Path in URL ............................................................................................. 43
3.4.3. Title and Snippet ................................................................. 44
3.4.4. Highlighted Text ................................................................. 44
3.4.5. Domain Name Amplification .................................................. 45
3.5. Proposed Feature Set Two .......................................................... 46
  3.5.1. Lexical Analysis ................................................................. 46
  3.5.2. Host-based Analysis ............................................................ 48
  3.5.3. Domain Analysis ................................................................. 50
3.6. Phishing Discovery and Detection Scheme ..................................... 52
  3.6.1. Identification of Phishing Websites ........................................ 53
  3.6.2. Identification of Phishing Websites with the Absence of Favicon .... 57
  3.6.3. Final Integrated Phishing Detection System ............................... 59

4 Experimental Results and Analysis .................................................. 62
  4.1. Prototype Implementation ....................................................... 62
  4.2. Data Collection ..................................................................... 63
  4.3. Experimental Outline .............................................................. 65
  4.4. Experiment 1 – Evaluation of Phishdentity on Google search by image API ........ 68
  4.5. Experiment 2 – Evaluation of Phishdentity on Search Results ............... 71
  4.6. Experiment 3 – Evaluation of Phishdentity with the Absence of Favicon ...... 76
  4.7. Experiment 4 – Evaluation of Final Phishdentity ................................ 80
  4.8. Limitations ........................................................................... 84

5 Conclusions and Future Work ........................................................... 86
  5.1. Conclusions ........................................................................... 86
  5.2. Research Contribution ............................................................ 88
  5.3. Future Work .......................................................................... 89

BIBLIOGRAPHY .............................................................................. 91
LIST OF FIGURES

Figure 1.1: Example of a phishing website. .............................................................. 2
Figure 1.2: Example of a phisher masquerades as a bank agent to deceive consumers. ....... 4

Figure 2.1: Vectors of phishing attacks. ................................................................. 9
Figure 2.2: Types of phishing techniques through the web ........................................... 11
Figure 2.3: Anti-phishing organization category ....................................................... 12
Figure 2.4: The general framework of technical phishing prevention approach ............... 14
Figure 2.5: The structure of the database used to store and retrieve data ..................... 15
Figure 2.6: A warning from Google Chrome browser is displayed to internet users attempting to access a confirmed phishing website. ......................................................... 18
Figure 2.7: Three types of information that can be retrieved by using a search engine ... 24
Figure 2.8: Classifier commonly used in website classification .................................... 29

Figure 3.1: Proposed framework of Phishdentity ...................................................... 36
Figure 3.2: Example of Google’s favicon displayed on the browser’s address bar and tab. ... 37
Figure 3.3: Example of Google search by image interface ......................................... 38
Figure 3.4: Example of Google search by image results when PayPal favicon is queried. ... 39
Figure 3.5: Code snippet of Google search by image API ......................................... 40
Figure 3.6: Architecture of the proposed feature set one ........................................... 41
Figure 3.7: Example of second-level domains ......................................................... 42
Figure 3.8: Example of a path ................................................................................. 43
Figure 3.9: Example of an entry with title and snippet in the search results .................. 44
Figure 3.10: Example of highlighted text on one of the entries in the search results ....... 45
Figure 3.11: Part of the phishing URL is hidden behind the browser’s address bar ......... 48
Figure 3.12: Example of WOT safety rating in the search results of Google ................. 51
Figure 3.13: Code snippet of WOT API ................................................................. 52
Figure 3.14: Phishing websites targeting PayPal website has a favicon ....................... 53
Figure 3.15: Flowchart of query website classification with the presence of favicon ....... 54
Figure 3.16: Flowchart of query website classification with the absence of favicon ....... 58

Figure 4.1: Categorization of Alexa top 500 global website ........................................ 64
Figure 4.2: Categorization of 500 phishing websites ................................................. 65
Figure 4.3: Example of a website using the default browser favicon ............................ 76
### LIST OF TABLES

Table 3.1: Ways in HTML used to access the favicon.................................................................37
Table 3.2: Calculating the frequency of unique terms in the second-level domain.......................43
Table 3.3: Calculating the frequency of unique terms in the path. ............................................43
Table 3.4: Calculating the frequency of unique terms in the title and snippet. ............................44
Table 3.5: Calculating the frequency of unique terms of the highlighted text. ............................45
Table 3.6: Changes in the total frequency of the first layer. ......................................................46
Table 3.7: Examples of dots in URL feature. .................................................................................48
Table 3.8: WOT rating of reputation. ..........................................................................................52
Table 3.9: Three examples of URLs after appended with `favicon.ico`. ......................................54
Table 3.10: Weight assigned to each feature in the first layer.....................................................56
Table 3.11: Weight assigned to each feature of module B............................................................58

Table 4.1: Hardware and software specification. ........................................................................63
Table 4.2: Collection of data from Alexa top 500 global websites and PhishTank.......................63
Table 4.3: Evaluation results of Phishdentity under different test beds........................................69
Table 4.4: Evaluation of Phishdentity based on different number of search entries. .................73
Table 4.5: Assessment for Phishdentity and additional approach for the availability of favicon .78
Table 4.6: Performance comparison between Final Phishdentity, CANTINA and GoldPhish.....82
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIWL</td>
<td>Automated Individual White-List</td>
</tr>
<tr>
<td>API</td>
<td>Application Program Interface</td>
</tr>
<tr>
<td>APWG</td>
<td>Anti-Phishing Working Group</td>
</tr>
<tr>
<td>CANTINA</td>
<td>Carnegie Mellon Anti-Phishing and Network Analysis Tool</td>
</tr>
<tr>
<td>CBIR</td>
<td>Content-Based Image Retrieval</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DOM</td>
<td>Document Object Model</td>
</tr>
<tr>
<td>FN</td>
<td>False Negative</td>
</tr>
<tr>
<td>FP</td>
<td>False Positive</td>
</tr>
<tr>
<td>HTML</td>
<td>Hypertext Markup Language</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>IDE</td>
<td>Integrated Development Environment</td>
</tr>
<tr>
<td>IM</td>
<td>Instant Messaging</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>KNN</td>
<td>K-Nearest Neighbor</td>
</tr>
<tr>
<td>LR</td>
<td>Logistic Regression</td>
</tr>
<tr>
<td>LUI</td>
<td>Login User Interface</td>
</tr>
<tr>
<td>LDA</td>
<td>Linear Discriminant Analysis</td>
</tr>
<tr>
<td>MODI</td>
<td>Microsoft Office Document Imaging</td>
</tr>
<tr>
<td>NB</td>
<td>Naïve Bayes</td>
</tr>
<tr>
<td>NPO</td>
<td>Nonprofit Organization</td>
</tr>
<tr>
<td>OCR</td>
<td>Optical Character Recognition</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest-Shamir-Adleman</td>
</tr>
<tr>
<td>SIFT</td>
<td>Scale-Invariant Feature Transform</td>
</tr>
<tr>
<td>SLD</td>
<td>Second-Level Domain</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SVM</td>
<td>Support Vector Machine</td>
</tr>
<tr>
<td>TF-IDF</td>
<td>Term Frequency-Inverse Document Frequency</td>
</tr>
<tr>
<td>TLD</td>
<td>Top-Level Domain</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>TN</td>
<td>True Negative</td>
</tr>
<tr>
<td>TP</td>
<td>True Positive</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>UT</td>
<td>Unique Term</td>
</tr>
<tr>
<td>W3</td>
<td>World Wide Web</td>
</tr>
<tr>
<td>W3C</td>
<td>World Wide Web Consortium</td>
</tr>
<tr>
<td>WHOIS</td>
<td>Who Is</td>
</tr>
<tr>
<td>WOT</td>
<td>Web Of Trust</td>
</tr>
<tr>
<td>XSS</td>
<td>Cross-Site Scripting</td>
</tr>
</tbody>
</table>
ABSTRACT

Phishing attack is a cybercrime which will result in severe financial losses to consumers and entrepreneurs. Typically, the phishers are fond of using fuzzy techniques during the creation of phishing websites. They obfuscate the victims by mimicking the appearance and content of the legitimate website. In addition, most of the websites are susceptible to the threat of phishing attacks, including financial institutions, social networks, e-commerce, airline websites and others. Phishers can easily earn the trust of the victim by impersonating as a consultant in the travel agency, booking flights and hotel reservations. Therefore, it is important to establish an intelligent gateway for browsers that can protect internet users from visiting malicious websites. In this thesis, we proposed an approach which is based on the website favicon to uncover the hidden identity of a website. We employ Google search by image engine to obtain the search results specific to the website favicon. Then, we perform feature extraction based on the search results to retrieve the website identity. Our identity retrieval technique involves an effective mathematical model in which it could be used to assist in retrieving the right identity from the many entries of the search results. In addition, we also proposed additional approach which is based on the URL to examine the legitimacy of a website. More precisely, we study the URL based on the lexical features, host-based features and domain features. Additional approach is very useful when the website under examination does not have a favicon. We have collected a total of 500 phishing websites from PhishTank and 500 of the legitimate websites from Alexa Top 500 Global Websites to verify the effectiveness of this approach. From the experimental results, our proposed technique has achieved 97.4% true positive with only 5.4% false positive. After combining with additional approach, our proposed technique is able to improve the false positives to 2.2%, while slightly reducing the accuracy of classifying phishing websites where we have achieved 97% true positive.
ABSTRAK

LIST OF PUBLICATIONS


ACKNOWLEDGEMENTS

This thesis would not have been possible without the assistance from many people who have given their support directly or indirectly. First and foremost, I would like to express my sincere gratitude to my main supervisor, Dr. Chiew Kang Leng for his expertise, support, and encouragement throughout the study. His patient instruction encouraged me to think in a more profound and pervasive way. I also want to give special thanks to my co-supervisor, Dr. Sze San Nah who always inspired me to undertake a thorough and in-depth analysis on the research. I would also like to thank my colleagues for so many great and nice discussions, which made my life here full of laughter. Last but not least, I am deeply grateful to my parents and siblings for their endless love, understanding, support and encouragement, which has accompanied me throughout my life.

The funding for this project is made possible through the research grant obtained from the Ministry of Higher Education, Malaysia under the Long Term Research Grant Scheme 2011 [LRGS grant no: JPT.S (BPKI)2000/09/01/015Jld.4(67)].
Chapter 1

Introduction

The advancement of information technology has brought new ways of interacting with people. In particular, the internet has opened up many opportunities for businesses to create new sales. However, this convenience also attracts the people with bad intention to take advantage of the shortcomings of the internet for illegal activities. Without proper protection, internet users will be exposed to different types of online fraud, such as phishing. As a result, internet users may suffer financial loss or disclosure of personal information to fraudsters. Eventually, internet users will lose confidence in using the internet and it will inhibit the growth in online business.

1.1. Background of Phishing

Phishing is defined as an act to deceive the recipients through a legitimate-looking email or a website in order to earn the trust and confidence of internet users to divulge their personal and financial information [9, 20, and 29]. With the advancement of information technology, many business agencies (i.e., tourism, hotel, airline, etc.) are able to take advantage of e-commerce, electronic payment, and social networking technologies into their business in order to increase sales. But, this creates an opportunity for phishers to masquerade into different types of services such as financial institutions, social networking, and e-commerce websites to gain illegal profits. Anti-Phishing Working Group (APWG) reported a total of 128,378 unique phishing websites detected in its second quarter of 2014 phishing activity trends report [1]. The report showed evidence that phishing activities are on the rise which revealed that existing anti-phishing technology is unable to fight phishing attacks efficiently.

The most common way to launch a phishing attack is through a combination of internet content from multiple sources or domain name confusion. Phishing websites can be done relatively quickly and requires little effort. This is because phishers simply clone the entire
website with some modifications in the input tags to collect personal information. The time of this process can be shortened by utilizing phishing kits [5], which are available on the black market. In addition, advancement of information technology helps phishers to develop more sophisticated phishing techniques to avert phishing detectors. Figure 1.1 shows an example of a phishing website masquerading as PayPal. There are two flaws identified in the address bar (as indicated by the red line box in Figure 1.1):

- The domain name is completely different than the original.
- It obfuscates the URL with HTTPS as part of the URL.

![Image of a phishing website](https://example.com/image.png)

**Figure 1.1:** Example of a phishing website.

Phishers are highly in favor of visual deception techniques to fool potential victims. It manipulates the perception of the victim through common images shown on the website. A sophisticated phishing websites usually will adopt iconic images of the targeted website including the website favicons with distinctive contents. More specifically, phishers have the ability to reproduce similar targeted websites by adjusting the structure of HTML, images, flash objects, or some other dynamic components. In other words, sophisticated phishing attacks can cause phishing detectors to produce false negative results. This course of action is known as a phishing page polymorphism.

### 1.2. Motivation

Since the advent of phishing in cybercrime over the past decade, it has caused tremendous financial losses to internet consumers and online businesses [2 – 3]. It also tarnishes the reputation and trust of the targeted company. If there is no countermeasure to prevent the occurrence of phishing attacks, then there will be more internet consumers become the
victims of phishing. Eventually, phishing will affect the economic growth of a country. Government and non-profit anti-phishing organizations provide many channels to help educate internet users when browsing the internet, especially when dealing with money transactions on the internet. However, internet users are still falling into the trap of phishing. In other words, alternative approaches need to be developed to detect and prevent phishing attacks. As a result, the computational approach is introduced to study the behavior of phishing and propose countermeasures to detect phishing activity. While there are many anti-phishing solutions available in the market, but none of the solutions are 100 percent effective without incurring false alarms to the targeted company. In addition, advances in information technology have provided opportunities for phishers to study the mechanism of anti-phishing and produce high profile phishing attacks [4].

Phishing activity trends have not diminished despite many efforts from different bodies. The severity of these attacks can be seen from the reports published as follows:

- According to the reports published [1 – 4], the statistics of phishing incidents around the world has increased dramatically. In Malaysia alone [4], a total of 1033 unique phishing websites are reported on the fourth quarter of 2013. It is a 7.4% increment compared to the third quarter of 2013.
- According to a report conducted by RSA [2], the Anti-Fraud Command Center has estimated that in the first half of 2012, the potential loss in global organization committed solely by phishing is $687 million.

In summary, the study of new anti-phishing solution is necessary to compensate for weaknesses in existing anti-phishing solutions and to detect undiscovered phishing techniques.

1.3. Case Study Scenario

Figure 1.2 shows the flow of phishing attacks. The attacks consist of five steps as follows:

- Step 1: Phisher identifies potential fraud from available resources on the internet. Phisher send fake email to thousands of victims by modifying the content and header of email.
Step 2: The victims receive the email and they have no doubt (possibly careless or limited knowledge in email header structure) about the content and address of email sender.

Step 3: The victims respond to the email and open up the link in which it directs the victims to a fake website. Then, the victims submit their confidential data by logging to the fake website.

Step 4: Phisher reviews the victims’ data and takes advantage of the leaked information. Phisher gains access to the victims’ respective bank website by using the stolen data.

Step 5: Phisher successfully transferred the money from the victims account into his own bank account.

Figure 1.2: Example of a phisher masquerades as a bank agent to deceive consumers.¹

It is nearly impossible to predict the occurrence of phishing attacks. For example, a tourist who wants to book a hotel and a flight ticket over the internet make payments by using internet banking has a very high possibility to be targeted by phishers. If he has limited knowledge of phishing attributes or inability to distinguish between a rogue website and a legitimate website, then it is likely that he will suffer a significant financial loss.

1.4. Research Problems

- Existing textual-based anti-phishing solutions are depending on the content of a webpage to classify the legitimacy of a website. However, these solutions are incompetent to classify image-based phishing website. Phisher can replace the textual contents with images to evade phishing detectors. Hence, more victims will fall into image-based phishing attacks.

- Some phishers create phishing website that is visually dissimilar (i.e., webpage layout) to the legitimate website to phish potential victims. They preserve iconic images from legitimate websites to convince victims that the current webpage is benign. Existing image-based phishing prevention techniques are insufficient to classify such phishing attacks. As a result, these phishing websites will be falsely classified as legitimate websites.

- Most of the existing anti-phishing solutions are unable to reveal the identity of targeted legitimate websites. Instead, they only notify the matching attributes of phishing. It can become a serious threat to internet users if existing anti-phishing solutions cannot identify the identity of new phishing website.

- Existing anti-phishing solutions have low detection speed to classify websites. The detection speed would only get worse for website with dynamic contents because the phishing detectors need to extract and process even more data.

1.5. Research Objectives

The primary objective of this research is to develop a new anti-phishing solution that can reveal the identity of a website and determine the legitimacy accordingly. To achieve that, the specific objectives of the research are defined as follows:

- To evaluate the effectiveness of using graphical elements to recognize the identity of the website.
- To investigate the use of search engines that could reveal the identity of the targeted website.
- To analyze the factors that delay the detection of phishing in the classification.
1.6. Scope of Research

There are varieties of anti-phishing topics to be explored and studied. However, the scope is defined in this research to ensure appropriate contributions are made within the allotted timeframe. Therefore, this research focuses on the detection of phishing websites. Other types of phishing attacks (e.g. email, voice over internet protocol, etc.) are beyond of the scope.

1.7. Outline of the Thesis

The remaining of the thesis is organized as follows:

- Literature review of existing anti-phishing solutions are presented in chapter two. This chapter describes the phishing vectors and phishing techniques used in the creation of phishing websites. Then, the chapter will review different solutions of existing techniques. The review also identifies the advantages and disadvantages of the existing techniques.
- Chapter three presents the methodology of our proposed technique. It describes the application of favicon in Google search by image engine. The chapter also examines additional approach in offsetting the missing favicon scenario. We also discuss in detail a scheme for detecting phishing websites, with or without the presence of a favicon.
- Chapter four presents the experimental results and analysis of the proposed technique. First, we introduce the tools needed to implement the experiment. Then, we explain the method used to collect the data (legitimate and phishing websites). Next, we perform a variety of experiments to assess the proposed technique. Specifically, we are interested to observe the performance of these features in respond to the availability of favicon in legitimate websites and phishing websites. Lastly, we discuss about the limitation imposed by the proposed technique.
- We conclude our work in chapter five, where we summarize all the work from chapter one to chapter four. Next, we describe the contribution of this research. Then, we discuss the direction of future work.
Chapter 2

Phishing Attacks and Prevention Studies

This chapter describes the classification of phishing attacks. The chapter also includes studies on the prevention of phishing attacks. We start by introducing various types of vectors used by phishers to carry out the attacks. Then, we describe the types of phishing that occur on the website. We also discuss some of the approaches taken by the government and non-profit organizations against phishing attacks. For the phishing prevention studies, we analyze current state-of-the-art phishing prevention methods based on the strengths and limitations. Finally, this chapter summarizes the advantages and disadvantages of each method of preventing phishing.

2.1. Classification of Phishing Attacks

Phishing attacks pose a significant risk to the entrepreneurs to develop their business. The severity of phishing attacks can be seen from the report published by APWG [1]. In short, existing anti-phishing solutions are less effective against phishing attacks. Consumer can lose confidence to perform online transactions if the number of phishing activity increased or remained. To cope with the phishing attacks, we review different number of vectors used by phishers to disseminate the attacks. Then, we also review phishing techniques commonly used on the web.

2.1.1. Phishing Vectors

Phishing techniques have evolved since the advancement of information technology. It offers opportunities for phishers to increase the complexity of attacks using web technology. In addition, the phisher can use this technology to victimize internet users from different countries. Although phishing goal is to harvest personal credentials for illegal activities, but it
requires a vector for phishers to launch an attack. Figure 2.1 shows different vectors used in the phishing attacks. In general, we can classify phishing vectors [6] according to the properties described as follows:

- **Spoofed email.** A falsified message was sent by a phisher requesting immediate action from the victims. Usually, the message is modified so that it looks professional and ordinary to the victims. The email could be asking the victims to change account information, update details and verify account information. Sometimes, the victims are asked to visit the embedded link in which it redirects the victims to the phishing website and harvest the credential information.

- **Instant messaging (IM).** A type of online chat in which they perform a real-time text transmission through the internet. Typically, the chat is insecure and free of speech. Phishers can embed high-profile malicious code into the message and distribute it to the entire group of users. The malicious code can lead victims to a phishing website to dig up personal information. It also can hijack the computers to steal information from the victims.

- **Phone and SMS.** Phishers falsify the message and deliver it to victim's phone number to harvest personal credentials. The message was designed to create a sense of urgency so that the victim will respond to the request immediately. Typically, the message contains a high reward if the victim reacts to it within the prescribed period. However, the leaked information is used by phishers for illegal activities rather than rewarding the victims as promised in the message.

- **Internet browser vulnerabilities.** An old browser (i.e., outdated version) carries a high risk of being targeted by phishers. This risk increases if users never perform updates to the browser. Victims of hijacked computers may not notice changes in the browser. In fact, infected browsers may leak the sensitive information during the transmission. The vulnerability is mostly occurred in the settings of ActiveX, HTML, images, Java, JavaScript, and other web technologies. For example, some websites require ActiveX enabled to view the content or perform certain tasks. Phishers take advantages of these vulnerabilities to steal information from the victims.
2.1.2. Phishing Techniques

In this section, we will discuss the techniques used in the creation of phishing websites. It is also based on the scope of the research. Nevertheless, phishers like to use different techniques when making bait, especially in phishing websites. This is because most of the casual internet users do not understand or lack of knowledge about security risks on the internet. They tend to follow all the instructions when surfing the web. Therefore, this group of internet users may become victims of phishing if their web browser is outdated or computer does not install anti-phishing software. Figure 2.2 shows the types of phishing techniques used to obfuscate victims on the internet.

- **Malware or Trojan.** Malware or Trojan is a malicious program that is designed to corrupt and steal confidential information directly from victims through computing devices [7]. Typically, the malicious program is delivered to the computing devices via a malicious link embedded in the e-mail. This program will install into the computing devices in an automated fashion without permission and notification once the victim has visited the link. Malicious programs can perform a range of activities such as recording keystrokes on the keyboard, capturing screenshots etc. Then, this piece of information will be sent to the phishers account. It can cause severe financial loss to the victim if the phishers use stolen information for illegal activities.

- **Flash-based.** Flash-based phishing website or Phlashing is a type of phishing technique that uses flash animation to develop the content of a spoof website [8]. It is different from the usual phishing website where the source code of flash animation is hidden from client web browser. Viewers are required to use flash decompiler to read
the source code. Phishers take advantage of this limitation to defeat phishing detectors that scan the textual content of a webpage to find the attributes of phishing. Thus, this phishing technique causes the textual-based phishing detectors to be less effective against flash-based phishing websites. This type of phishing website began to be seen in June 2006 and is becoming more common in late 2006.

- **Popup window.** This type of phishing technique opens another window on the foreground of a browser [9]. This technique will inherit some of the graphical elements of a window opened previously. It convinces internet users that the current window has a relationship with the previous window. However, the information submitted is sent to a different URL destination. Phishers often use this technique in the website to trick internet users. This technique has the potential to circumvent existing phishing detectors. This is because most phishing detectors do not analyze the popup window.

- **Link manipulation.** Link or hyperlink is a stream of text that connects the reader to another website or other parts of the document. This type of phishing technique makes changes to the hyperlink so that it looks similar to the target URL [10]. In addition, phishers are also fond of using the at-sign (@) or dash (-) symbol to mimic the original URL. Many internet users have been given advice by the financial sectors not to visit the suspicious URLs for transaction. This is because the technique is able to deceive victims who are not careful in surfing the internet. Therefore, it is important to verify the URL domain name before visiting.

- **Visual deception.** Visual deception is a type of phishing technique that resembles legitimate websites to create a spoof website [11]. It mimics the layout, components and images used. Usually, the victims of this attack cannot distinguish between the clone website and original website without comparing the original website domain name. In addition, visual deception technique can avoid phishing detector that analyzes the textual content of a website. Phishers take advantage of this limitation to deceive internet users who do not have the ability to detect clone website. This technique can cause serious financial losses to internet users if no countermeasure is proposed to detect this type of phishing websites.

- **URL obfuscation.** URL obfuscation has the same concept of link manipulation except the phishers make changes to the website URL [12]. In addition, phishers can hide the actual phishing URL from the browser address bar. They do so by using a long URL
to force the victim to focus only on the front of the URL. Therefore, the victim who cannot remember the website domain name is gullible by this technique.

- **Cross-site scripting**. Cross-site scripting or XSS is a type of phishing technique that injects malicious code (e.g., JavaScript) to the website to change the content [8]. Information submitted to this website will be sent to the phishers. This type of phishing attack possesses a high threat to both internet users and website owners. This is because the malicious code is not easily detected by phishing detectors. Conversely, phishing detector should do a scan on the website structure to detect changes in the code. In addition, detection of phishing can become complicated if phishers combine this technique with other phishing techniques to increase the complexity of the attacks.

![Diagram of phishing techniques through the web]

Figure 2.2: Types of phishing techniques through the web.

### 2.2. Prevention of Phishing Attacks

Phishing is a very complicated deception technique. It manipulates the perception of victims without acknowledging the stolen information. The deception techniques include URL manipulation, appearance impersonation, iconic images etc. In addition, the phisher can transform the layout of a website (e.g., textual content) into image-based to evade the detection. As a result, the high-profile phishing attack that integrates a variety of techniques can defeat the purpose of anti-phishing solution. Nevertheless, we will study a variety of anti-phishing solutions to identify the pros and cons. To do so, the non-technical approaches are reviewed, followed by the technical approaches.
2.2.1. Non-technical Approach

In order to fend off these attacks, government sector (i.e., United States of America) has put much effort [13] to strengthen the security on the web. This includes disseminating precaution guidelines through digital media, conducting discussion forums, educating consumers [14] and etc. However, these efforts did not meet the ideal expectations since there are still many internet users are victimized by phishers. Figure 2.3 shows the category of the anti-phishing organization. Phishing prevention approaches can be divided into non-technical and technical. Non-technical approach delivers information to internet users through various communication channels such as using posters, educational programs, campaigns, games, and etc. The aim is to educate and raise public awareness about phishing attacks. Meanwhile, the technical approach seeks to build greater security for web browsers and provide automated protection for internet users against phishing attacks when surfing the web.

Anti-Phishing Working Group (APWG) [1] and PhishTank [15] are two well-known nonprofit organizations (NPOs) that assist researchers and developers to battle against phishing attacks. They provide blacklist in the form of API for developers and researchers to test against their anti-phishing techniques. However, the provided data is not sufficient to capture the entire phishing activities as it depends on human interaction to report phishing attacks. Since the effectiveness of blacklist is depended on the up-to-date listing, new phishing website can easily escape from the blacklist until someone reports it to the NPO. For websites that are verified and proved deceptive, these NPOs will inform respective hosting to suspend the domain name. It is not uncommon that the reported case may in fact a false alarm and could cause harm to a newly launched legitimate website if anonymous mistakenly reports it to the NPO. This could damage a benign website in terms of reputation and trust.

![Organization Diagram]

Figure 2.3: Anti-phishing organization category.