UNIVERSITI MALAYSIA SARAWAK

UNIMAS

Faculty of Computer Science and Information Technology

PHISHING EMAIL DETECTION TECHNIQUE BY USING HYBRID FEATURES

Lew May Form

Bachelor of Computer Science with Honours
(Computational Science)
2014

PHISHING EMAIL DETECTION TECHNIQUE BY USING HYBRID FEATURES

LEW MAY FORM

This project is submitted in partial fulfillment of the
requirements for the degree of
Bachelor of Computer Science with Honours
(Computational Science)

Faculty Computer Science and Information Technology
UNIVERSITI MALAYSIA SARAWAK
2014

E-MEL PHISHING TEKNIK PENGESANAN DENGAN MENGGUNAKAN CIRI-CIRI HIBRID

,

LEW MAY FORM

Projek ini merupakan salah satu keperluan untuk
Ijazah Sarjana Muda Sains Komputer
(Sains Komputan)

Fakulti Sains Komputer dan Teknologi Maklumat
UNIVERSITI MALAYSIA SARAWAK
2014

UNIVERSITI MALAYSIA SARAWAK

THESIS STATUS ENDORSEMENT FORM

TITLE PHISHING EMAIL DETECTION TECHNIQUE BY USING HYBRID FEATURES

ACADEMIC SESSION: 2013 / 14

LEW MAY FORM
(CAPITAL LETTERS)

hereby agree that this Thesis* shall be kept at the Centre for Academic Information Services, Universiti Malaysia Sarawak, subject to the following terms and conditions:

1. The Thesis is solely owned by Universiti Malaysia Sarawak
2. The Centre for Academic Information Services is given full rights to produce copies for educational purposes only
3. The Centre for Academic Information Services is given full rights to do digitization in order to develop local content database
4. The Centre for Academic Information Services is given full rights to produce copies of this Thesis as part of its exchange item program between Higher Learning Institutions [or for the purpose of interlibrary loan between HLI]
5. ** Please tick (√)

□	CONFIDENTIAL	(Contains classified information bounded by the OFFICIAL SECRETS ACT 1972)
□	RESTRICTED	(Contains restricted information as dictated by the body or organization where the research was conducted)
☑	UNRESTRICTED	

Validated by

(AUTHOR'S SIGNATURE) (SUPERVISOR'S SIGNATURE)

Permanent Address

MLD 1921, Jalan Paya,
Bukit Batu, 81020
Kulaijaya, Johor.

Date: 27 /06 / 14

Date: 27.6.2014

Note * Thesis refers to PhD, Master, and Bachelor Degree

** For Confidential or Restricted materials, please attach relevant documents from relevant organizations / authorities

DECLARATION

I declare that this thesis entitled "Phishing Email Detection Technique by using Hybrid Features" is the result of my own research except as cited in the references. This project has no previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signature :

Author Name : LEW MAY FORM

Date : 27 /06 / 14

ACKNOWLEDGEMENT

First of all, I give thanks and deeply grateful to my supervisor, Professor Dr. Chiew Kang Leng who guides me and helping me to perform the Final Year Project. I am really thankful that he gave me the opportunity to familiarize myself with this project and applied the knowledge that I gain in this four years studies in UNIMAS. I was honored that he as my supervisor.

Besides that, I also give thank to all my family and friends who always encouraged me to do well and supported me during I facing problem and feel discourage along this project. I maybe could not finish this project on time if without their support.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURE TITLE **PAGE**

LIST OF TABLES

TABLE TITLE PAGE

ABSTRACT

Email provides convenience of communicating to such large number of people, especially for businessman. However, more attacks are launched to target electronic communication user in order to harvest credentials information from them for illegal purpose used. The most commonly phishing method is initialed by sending out email to user tends to make the user believe that they are communicating with trusted entity, and deceive them into providing personal information. Recently, there are a lot of research have been done to overcome the phishing emails problem. This project aim to design a phishing email detection technique and focus on feature selection. The proposed method contains content-based feature, URL-based feature and behavior-based feature, which total nine feature sets. The proposed method has been evaluated on a set of 500 phishing emails and 500 legitimate emails. The proposed method obtain overall accuracy 97.25% with 1% false negative rate and 5% false positive rate. The proposed method able to classify more accurately than the hybrid feature proposed by Hamid et al.. This evidence that two newly add on feature sets, hyperlink feature and return path feature are potential indicator. The quite promising result is motivated future work to mine the attacker behavior and explore more about behavior-based feature.

ABSTRAK

E-mel memudahkan komunikasi antara sebilangan besar orang, terutamanya peniaga. Walau bagaimanapun, banyak serangan yang dilancarkan menyasarkan pengguna komunikasi elecktronik untuk mendapatkan maklumat sensitif daripada mereka dan digunakan dalam aktiviti yang menyalahi undang-undang. Kaedah *phishing* yang paling biasa ialah menghandarkan e-mel kepada pengguna supaya memujuk pengguna percaya bahawa mereka berkomunikasi dengan entity dipercayai, seterusnya memperdayakan pengguna memberikan maklumat sensitif. Kebelakangan ini, terdapat banyak penyelidikan telah dilakukan untuk mengatasi masalah e-mel *phishing*. Projek ini bertujuan untuk menyediakan e-mel *phishing* teknik pengesanan dan memberi tumpuan kepada pemilihan ciri. Teknik yang dicadangkan dalam projek ini mengandungi sembilan ciri, iaitu ciri berasaskan kandungan, ciri berasaskan URL dan ciri berasaskan tingkah laku. Teknik yang dicadangkan telah dinilai dengan 500 e-mel *phishing* dan 500 e-mel yang sah. Teknik yang dicadangkan juga mencapaikan 97.25% ketepatan, 1% kadar negatif palsu dan 5% kadar positif palsu. Teknik yang dicadangkan dapat mengelaskan lebih tepat daripada ciri hibrid yang dicadangkan oleh Hamid et al.. Ini menyatakan bahawa dua set ciri yang baru tambah, ciri *hyperlink* dan ciri *return path* ialah berpotensi indikator. Keputusan tersebut bermotivasi kerja depan untuk melombong tingkah laku penyerang dan meneroka lebih lanjut mengenai ciri berasaskan langkah laku.

CHAPTER 1 INTRODUCTION

Email has provided large number of people convenience of communicating. However, Unsolicited Bulk Email (UBE) becomes a huge problem in recent years. More and more phishing emails are flooding in network world to steal consumers' personal data like financial account credentials. These phishing attacks can be sub-divided into two categories, which are deceptive phishing and malware-based phishing.

Deceptive phishing is a scheme that employs social engineering to design forged email claims purportedly originally from legitimate business or agencies, and send it to users. Subsequently, email will receive an embedded link which attempts to redirect the user to a counterfeit websites that are designed to fraudulently obtain personal financial data like credit card number, identity information and login credentials. Malware-based phishing is a technical subterfuge scheme that relies on malicious code or malware. It attempts to obtain the victim's online account information by detecting and using security holes in victim's computer or misdirect the user to a legitimate website but monitored by proxies.

Phishing activity is growing at an alarming rate. According to Anti-Phishing Work Group (APWG) phishing attack trends reports (2013), the number of phishing email reports submitted to APWG show substantially increase, from 28,897 unique phishing reports in December 2009 to 45,628 unique phishing reports in December 2012. Phishing email causes a serious threat to information security and internet privacy. Forrester Research claims that 20 percent of consumers refuse to open email or attachment even the email look legitimate, due to their loss of trust (Lawton, 2005). The bogus email always persuade users to provide their personal credentials in order to correct some alleged problem supposedly found with an account, else the particular account maybe suspended. It can lead to fraudulent changes against credit cards, withdrawals from bank accounts, or other undesirable effects. Some user's unfamiliarity with browser security indicators can be the victim in these cases. Since the phishers able to convince the users by create replica of a site that nearly identical to the original legitimate websites. According to McCall (2007), the Gartner survey estimated that phishing attacks costs businesses $3.2 billion in losses and 3.3 percent of consumers claim that they lost money because of email-based phishing attacks.

Many machine-learning techniques have been proposed in the literature to detect and filter phishing email. For example, phishing attack detection tools at the network level, encryption-based approaches, black listing and white listing approaches, multi classifiers algorithms approaches, models based features approaches, clustering approaches, hybrid system approaches and evolving connectionist system approaches. Each classifiers technique for phishing emails detection above is not sufficient enough to protect consumers from the threat. All existing approaches have their limitation on consumes memory, consumes time, weak detection of zero-day attack, less accuracy, higher cost and need feed continuously (Almomani, Gupta, Atawneh, Meulenberg, and Almomani, 2013). On the other hands, phishing has become more and more sophisticated because phishers always apply new tricks to defeat or bypass the filter set by current anti-phishing techniques.

Hence, a hybrid selection feature which combines URL-based, content-based and behavior-based features is proposed in this project. This hybrid selection feature focus on email header and body-based content. Behavior-based feature in phishing emails cannot be disguised by an attacker. Besides that, email header is globally unique identification which is not visible to most users, but is a useful indicator in determining phishing emails. The hybrid feature approach is expected can be effective to identify and classify the phishing emails through evaluation of attacker behaviors.

1.0 Problem Statement

Current email server systems cannot effectively authenticate the genuineness of incoming emails. Although there are many anti-phishing techniques have been proposed to solve the phishing email attacks problem, but the rapidly growing of phishing activity illustrate that existing anti-phishing techniques is insufficient to filter phishing emails. In additional, a number of attacks and techniques might be easily developed by phishers, the robustness of recently proposed anti-phishing attacks approaches are under challenge (Florêncio and Herley, 2006). High changing rate of attacks increase the difficulty of detecting and filtering phishing email attacks.

Phishers are more advance to overcome the challenge of existing anti-phishing techniques by introducing sophisticated techniques from time to time in order to break away from the checking and detection of phishing email filter. This look like a battle between the anti-phishing attacks and the phishing attacks, anti-phishing effort to detect and filter the phishing email attacks, at the same time phishing attacks try hard to bypass the phishing email filter. Unfortunately, the updating rate of filters always defeated by the changing rate of attacks, due to each recently proposed anti-phishing attacks approaches has weakness in handling phishing attacks. Therefore, a more effective anti-phishing approach is needed to protect users from email-based phishing attacks.

1.1 Objectives

The main objective of the project is to design a phishing email filtering technique. In order to achieve that, this project includes method:

i. To analyze the header information of phishing emails.

ii. To differentiate an emails as either phishing email or legitimate email.

1.2 Brief Methodology

The basic system components and general processing steps of the proposed phishing emails filter is divided into three processing phases. They are feature selection, classification, and evaluation of the classification result (as shown in figure 1.1).

During feature selection phase, a component of potential features is generated through review and analysis existing works. Besides that, a set of datasets that include phishing emails and ham emails are collected for testing and training purpose. The datasets will then be divided into testing and training datasets. Training datasets is used to train the classifier, while testing datasets is used to estimate the error rate of training classifier.

Next, the classification is performed using WEKA (Waikato Environment for Knowledge Analysis). Classifier is used to classify each dataset as either phishing email or legitimate email. Lastly, the classification result will be evaluated based on the accuracy, false positive and false negative rate.

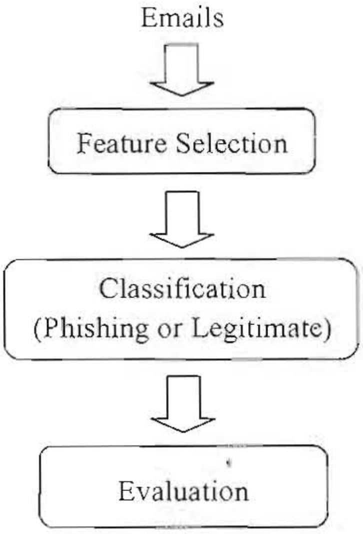


Figure 1.1: System Model

1.3 Scope

The proposed phishing attacks filtering technique will help user to identify the phishing emails more effectively. The datasets input of the proposed phishing attacks filtering technique is limited to emails.

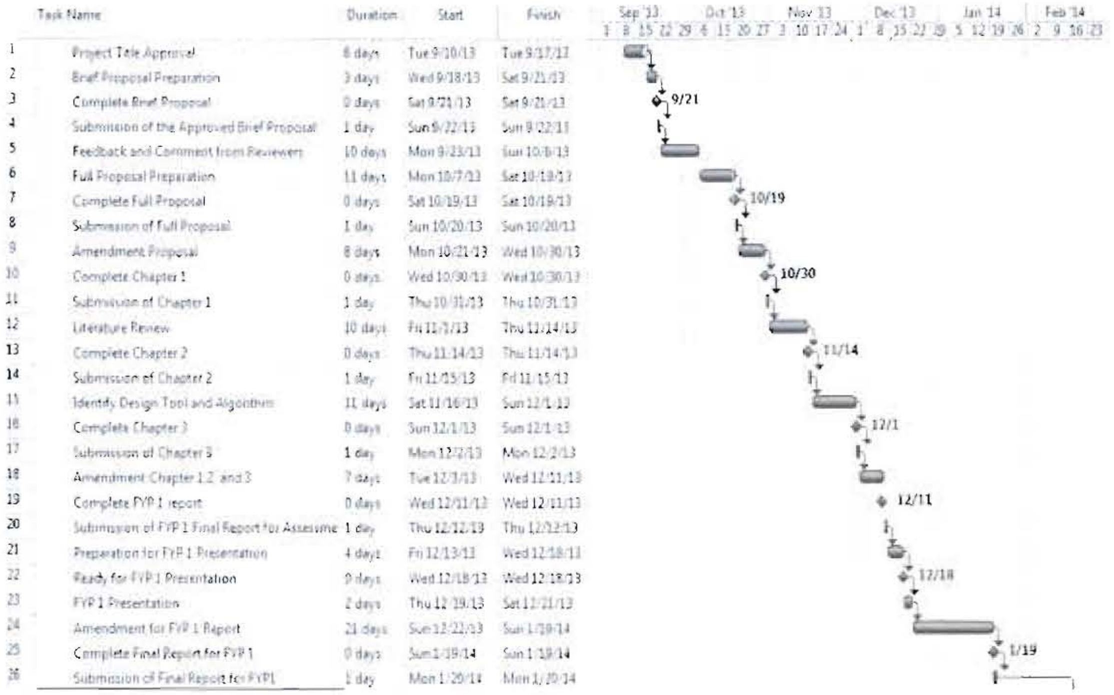
The scope of this project is focusing on deceptive email phishing detection, since deceptive phishing is one of the popular ways of phishing attacks. The main purpose of this project is feature selection. The phishing attacks filtering technique is identifying phishing email based on selected feature sets.

1.4 Significant of Project

More and more people are suffering from email-based phishing attacks over the past years, yet the problem still lacks of a better solution. Hybrid selection feature that evaluate the URL-based feature, content-based feature and behavioral feature can be a more effective way on filter phishing email attacks. Since behavioral feature cannot be disguised by an attacks by analyzing the email header information, like sender email and email's message-ID tags, this allow consideration on whether the sender send email from more than one domain message-ID or same domain message-ID is used by more than one sender be made. This approach is expected to be more helpful in identifying and classifying phishing emails.

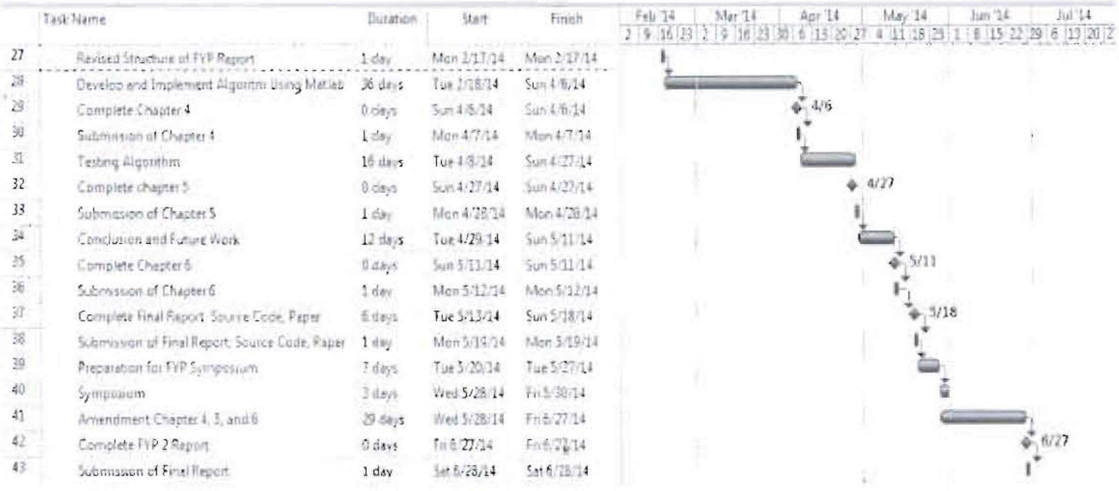
1.5 Project Schedule

The project schedule is used as guidance for the progression of the proposed project. In completing of this project, all progress will be done throughout first and second semester of the academic year of 2013/2014. Following are the Gantt chart for FYP 1 and FYP 2:



	Task Name	Duration	Start	Finish
1	Project Title Approval	6 days	Tue 9/10/13	Tue 9/17/13
2	Brief Proposal Preparation	3 days	Wed 9/18/13	Sat 9/21/13
3	Complete Brief Proposal	0 days	Sat 9/21/13	Sat 9/21/13
4	Submission of the Approved Brief Proposal	1 day	Sun 9/22/13	Sun 9/22/13
5	Feedback and Comment from Reviewers	10 days	Mon 9/23/13	Sun 10/6/13
6	Full Proposal Preparation	11 days	Mon 10/7/13	Sat 10/19/13
7	Complete Full Proposal	0 days	Sat 10/19/13	Sat 10/19/13
8	Submission of Full Proposal	1 day	Sun 10/20/13	Sun 10/20/13
9	Amendment Proposal	8 days	Mon 10/21/13	Wed 10/30/13
10	Complete Chapter 1	0 days	Wed 10/30/13	Wed 10/30/13
11	Submission of Chapter 1	1 day	Thu 10/31/13	Thu 10/31/13
12	Literature Review	10 days	Fri 11/1/13	Thu 11/14/13
13	Complete Chapter 2	0 days	Thu 11/14/13	Thu 11/14/13
14	Submission of Chapter 2	1 day	Fri 11/15/13	Fri 11/15/13
15	Identify Design Tool and Algorithm	11 days	Sat 11/16/13	Sun 12/1/13
16	Complete Chapter 3	0 days	Sun 12/1/13	Sun 12/1/13
17	Submission of Chapter 3	1 day	Mon 12/2/13	Mon 12/2/13
18	Amendment Chapter 1,2 and 3	7 days	Tue 12/3/13	Wed 12/11/13
19	Complete FYP 1 report	0 days	Wed 12/11/13	Wed 12/11/13
20	Submission of FYP 1 Final Report for Assessme	1 day	Thu 12/12/13	Thu 12/12/13
21	Preparation for FYP 1 Presentation	4 days	Fri 12/13/13	Wed 12/18/13
22	Ready for FYP 1 Presentation	0 days	Wed 12/18/13	Wed 12/18/13
23	FYP 1 Presentation	2 days	Thu 12/19/13	Sat 12/21/13
24	Amendment for FYP 1 Report	21 days	Sun 12/22/13	Sun 1/19/14
25	Complete Final Report for FYP 1	0 days	Sun 1/19/14	Sun 1/19/14
26	Submission of Final Report for FYP1	1 day	Mon 1/20/14	Mon 1/20/14

Figure 1.2: Gantt chart for FYP 1



	Task Name	Duration	Start	Finish
27	Revised Structure of FYP Report	1 day	Mon 2/17/14	Mon 2/17/14
28	Develop and Implement Algoritm Using Matlab	36 days	Tue 2/18/14	Sun 4/6/14
29	Complete Chapter 4	0 days	Sun 4/6/14	Sun 4/6/14
30	Submission of Chapter 4	1 day	Mon 4/7/14	Mon 4/7/14
31	Testing Algorithm	16 days	Tue 4/8/14	Sun 4/27/14
32	Complete chapter 5	0 days	Sun 4/27/14	Sun 4/27/14
33	Submission of Chapter 5	1 day	Mon 4/28/14	Mon 4/28/14
34	Conclusion and Future Work	12 days	Tue 4/29/14	Sun 5/11/14
35	Complete Chapter 6	0 days	Sun 5/11/14	Sun 5/11/14
36	Submission of Chapter 6	1 day	Mon 5/12/14	Mon 5/12/14
37	Complete Final Report, Source Code, Paper	6 days	Tue 5/13/14	Sun 5/18/14
38	Submission of Final Report, Source Code, Paper	1 day	Mon 5/19/14	Mon 5/19/14
39	Preparation for FYP Symposium	7 days	Tue 5/20/14	Tue 5/27/14
40	Symposium	3 days	Wed 5/28/14	Fri 5/30/14
41	Amendment Chapter 4, 5, and 6	29 days	Wed 5/28/14	Fri 6/27/14
42	Complete FYP 2 Report	0 days	Fri 6/27/14	Fri 6/27/14
43	Submission of Final Report	1 day	Sat 6/28/14	Sat 6/28/14

Figure 1.3: Gantt chart for FYP 2

1.6 Expected Outcome

The main outcome of this project is a working prototype of phishing email filtering which can be applied on existing emails server system. The proposed phishing email filtering technique has function to identify the origin of email whether it is phishing email or legitimate email. The filtering technique serves as security guard to protect users from phishing email attacks.

1.7 Project Outline

This project consists of six chapters. Chapter 1 introduce the project, it includes introduction to phishing emails attacks, problem statement, objectives, brief methodology, scope, significance of project, project schedule and expected outcome. Chapter 2 review the existing works, it includes details information about phishing emails life cycle, structure of phishing emails, difference between phishing and spam, related works and classifiers. Chapter 3 cover system design and methodology, it inclndes general framework of email filter, feature selection, classification, evaluation, flow chart and sequence diagram. Chapter 4 explains the project experimental setup, it includes description of implemented program files and feature extraction algorithm of each proposed feature sets. Chapter 5 analyze the classification results of the project, it includes datasets, datasets processing, performance metric and result analysis. Chapter 6 conclude the project, it includes contribution, limitation and future direction.

CHAPTER 2 LITERATURE REVIEW

2.0 Introduction

This chapter includes details of how phishers attack victim, what are the techniques that usually employed by phishers and how the anti-phishing techniques do works in order to detect the phishing attacks.

There are total 6 existing works have been review, including webpage level and emails level of existing anti-phishing techniques. Some discussion and comparison have been done based on each selected paper's proposed methodology and result outcome.

2.1 Phishing Emails Life Cycle

Process of phishing attack can be categorized into four stages, which are planning, attack, collection and identity theft. Please refer to Figure 2.1 for the phishing attack life cycle.

At planning and setup stage, the phishers compromise a host and installs a phishing website and mass-mailer in victim web server. After that, the phishers start to plan and target the potential victim by collecting their email addresses. At second stage, phishers start to attack by sending huge amount of phishing emails to potential victim. Those phishing emails always lure the victim through employed some phishing techniques. Please refer to Section 2.3 for further discussions of the structure of phishing emails. Normally, the phishing emails will persuade the users to provide their credential information, such as credit cards numbers, identity information or account login credentials in order to solve the issue. Some number of victims will trap in this kind of attack by providing requested information. If there are victims be spoofed and submits requested information, then the phishing process is at the third stage now, which is collection. The phishers will collect all the credential information from the victims. At the last stage, phishers used all collected data to do some illegal works, such as fraudulent charges against credit cards, withdrawals from bank accounts, or other undesirable effects.

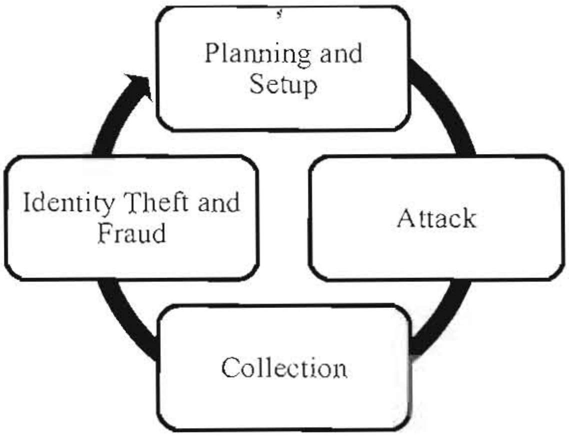


Figure 2.1: Phishing Attack Life Cycle

2.2 Spam versus Phishing

Spam emails are different from phishing emails. Spam emails is unsolicited emails that sent to user's email account adverting goods and services that user have not requested. While phishing emails is email that tries to trick user into giving their personal information, which is then used for illegal purpose without user's knowledge or permission. Therefore, spam filtering techniques may be a reference but is not suitable completely apply as phishing emails filtering techniques. Since the phishing techniques that employ by phishers is differ from the techniques that employ by spammer. Figure 2.2 illustrate the general framework of anti-phishing techniques.