Universiti Teknologi MARA

DETECTION PROCESS FOR ANTI-PHISHING

Redzuan Bin Nordin

Thesis is submitted in fulfillment of the requirements for

Bachelor of Science (Hons.)

Data Communication and Networking

Faculty of Computer and Mathematical Science

JULY 2013

ACKNOWLEDGEMENTS

TABLE OF CONTENT

CONTENTS   PAGE

ABSTRACT

Detection is about the detect the website whereby the website is original or phishing site. Phishing is associated with identity theft over the Internet by luring victims into false assumptions about trust relationships with websites. Data are only given out voluntarily from people in case of existing trust relationships. This project include detection and comparison process using pattern similarity, whereby it will compare the source code of the URL receive with the original source code whereby has been stored in the database. This method is important because it will ensure whether the phishing site or not. If it failed to detect, user will be easily to be a victim of the phishing site. Then if it detected the phishing site, it will pass the URL to the blacklist entry. Then it will inform the result to the user about the phishing site. In order to complete our project, we will use PHP language and mysql database. We also will develop it on the server so that we can avoid the process from being crashed. This is because of the research that we have done many anti-phishing before this implemented in the browser and have the highest probability to crash. Then, we hope our project can help the user from being fraud by the hacker or phisher.

CHAPTER 1

1.0 Introduction

This chapter describes the details of the background. As we know, this chapter one contains background of the project, problem statement, project aim and objective, project scope and significance as well as the outline if the thesis.

1.1 Background

Phishing is a technique to obtain the personal data for instances credit and debit card numbers, details of bank account and password in order to trick victim. Phishing also involves theft of identity or empty victim that checks and saves accounts. Nowadays, phishing is become more common and more advance than before this. Phishing is a form of cybercrime is growing rapidly. (Office of Information Technology, 2009).

Phisher tries to imposture as a trustworthy person or company and intended to cheat victims to expose their confidential data. The instant messaging is one of another communication to get confidential information. Phisher will create fake website that will attract people to use the fake website as the real one. After that, phisher will use all the data collected for the non-legitimate actions.

1.2 Problem Statement

Phishing is a combination of the words Fishing and Phreaking. Phreaking was a form of identity theft in the eighties and early nineties over the phone that was used to get free phone calls. Phishing instead is associated with identity theft over the Internet by luring victims into false assumptions about trust relationships with websites. Data is only given out voluntarily from people in case of existing trust