

ECE 1776 Project Proposal – Combating Phishing Websites

Introduction

There has been an increasing trend for criminals to use the Internet for fraudulent means. Phishing is one example where a criminal sends an unsolicited email to a user that appears to be from a trusted source, such as an online retailer or financial institution. The email redirects the user to a fraudulent website that is made to trick the user into believing they are at a legitimate website. The website prompts the user to supply credit card numbers, passwords, account information, or other personal data. This data is then harvested and either sold or used in a fraudulent way. According to estimates, 1.2 million users in the US suffered from phishing incidents causing losses of \$929 million (Kerstein 2005). Detecting fraudulent emails is important because an increase in phishing attacks will lead to further financial losses to both individuals and organizations. The motivation behind this project is to create a resilient and effective method to detect phishing websites.

Outline of the Proposed Solution

In order to automate the identification of possible phishing websites, the popular search engine, Google, will be used as an online reputation system that will help confirm if a website is fraudulent or legitimate. A Firefox extension will be created that will query the potential phishing website for keywords, the extension will use these keywords to query the reputation system and will compare the resulting top URL's with the URL of the possible phishing website. A phishing website will be identified if there is no match and this information will be communicated to the user via the Firefox extension.

Some interesting aspects regarding this implementation are:

- How to identify which websites we have to inspect?
- How to identify the keywords in the website?
- How high should the rank be to determine a legitimate website?
- What additional information sources can be used to identify a fraudulent website?
- Once a phishing website is identified, how can we inform the user?

The resulting implementation has to be easy to install, has to produce accurate identification, for example, avoid false-positives and false-negatives, and clearly inform the user about the potential dangers of visiting fraudulent websites. Also, using Google as a trusted source may not work as intended and having alternative methods to validate phishing websites may also be explored such as the WHOIS domain name search.

Related Work

Phishing is a recent problem, nevertheless due to its huge impact on the financial and on-line retailing sectors there are a comprehensive collection of related works. The list of the related works follow:

[1] Rachna Dhamija, et. al. Harvard University. *Why Phishing Work*.

This paper shows which malicious strategies are successful at deceiving general users and discards peripheral security indicators as a good approach to help users avoid these attacks. This paper gave us useful information related to effectively displaying and providing warnings to users.

[2] Parno Bryan, et. al. Carnegie Mellon University, *Phoolproof Phising Prevention*.

This paper discusses some design principles for anti-phishing tools and states that placing less reliance on the user during the authentication process will enhance security and eliminate many forms of fraud.

[3] Aaron Emigh, Radix Labs. *Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures*. <http://www.antiphishing.org/Phishing-dhs-report.pdf>

This paper discusses a wide variety of phishing attacks and countermeasures for the attacks.

[4] Wu, Min, Miller, Robert C., Garfinkel, Simson L. *Do Security Toolbars Actually Prevent Phishing Attacks?* CHI 2006. April 22-28, 2006.

This paper discusses why users get fooled by phishing attacks and the effectiveness of anti-phishing toolbars. Two user studies were conducted and the researchers found that actively interrupting a user with a pop-up message during a phishing attack is more effective than just a passive warning that is displayed in the browser toolbar.

[5] Google Toolbar <http://www.google.com/tools/firefox/safebrowsing/>

Google recently released a toolbar for Firefox that alerts the user if a webpage that he/she visits appears to be asking for personal or financial information under false pretense. Although this project looks similar, it does not provide any information about its implementation, measurements or effectiveness. Furthermore its approach to displaying information to the user is not very effective as shown in [1].

[6] Netcraft Toolbar <http://toolbar.netcraft.com/>

This toolbar prevents phishing attacks by using a centralized blacklist of current phishing URLs.

References

Kerstein, Paul, "How Can We Stop Phishing and Pharming Scams?", *CSO*, July 19, 2005.
<<http://www.csoonline.com/talkback/071905.html>>.