Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 49 (2015) 82 – 91

Procedia Computer Science

ICAC3'15

# AN IDEAL APPROACH FOR DETECTION AND PREVENTION OF PHISHING ATTACKS

Narendra. M. Shekokar, Chaitali Shah, Mrunal Mahajan,Shruti Rachh*

*D. J. Sanghvi College of Engineering, Vile Parle(W), Mumbai:400056, India*
*D. J. Sanghvi College of Engineering, Vile Parle(W), Mumbai:400056, India*
*D. J. Sanghvi College of Engineering, Vile Parle(W), Mumbai:400056, India*

**Abstract**

Phishing is a treacherous attempt to embezzle personal information such as bank account details, credit card information, social security number, employment details, and online shopping account passwords and so on from internet users. Phishing, or stealing of sensitive information on the web, has dealt a major blow to Internet security in recent times. These attacks use spurious emails or websites designed to fool users into divulging personal financial data by emulating the trusted brands of well-known banks, e-commerce and credit card companies.

In this paper, we propose a phishing detection and prevention approach combining URL-based and Webpage similarity based detection. URL-based phishing detection involves extraction of actual URL (to which the website is actually directed) and the visual URL (which is visible to the user). LinkGuard Algorithm is used to analyze the two URLs and finally depending on the result produced by the algorithm the procedure proceeds to the next phase. If phishing is not detected or Phishing possibility is predicted in URL-based detection, the algorithm proceeds to the visual similarity based detection. A novel technique to visually compare a suspicious page with the legitimate one is presented.



Peer-review under responsibility of organizing committee of the 4th International Conference on Advances in Computing, Communication and Control (ICAC3'15)

*Keywords:* Phishing; LinkGuard Algorithm;Discrete Cosine Transform (DCT)

## 1. Introduction

Phishing is an online deceitful activity wherein the objective of an attacker is to plagiarize a victim's sensitive information, such as online banking account details or social security number thus deceiving people into financial loss. Even though hoaxing people to make financial profit is an old idea, phishers have realized that social-engineering based attacks are easy to execute and highly profitable over the Internet.

* ShrutiRachh. Tel: +919757244133; Fax: -
E-mail Address: rachhshruts@gmail.com



Peer-review under responsibility of organizing committee of the 4th International Conference on Advances in Computing, Communication and Control (ICAC3'15)
doi:10.1016/j.procs.2015.04.230

A typical phishing attack may be based on several techniques, including exploiting browser vulnerabilities or performing man-in-the-middle attacks using a proxy. However, the most straightforward and widespread method includes setting up a web page that is similar to the one which is known to the user.

Therefore, although well known, phishing still poses a significant security threat and still a large number ofInternet users fall victim to this fraud. Furthermore, such attacks are not just causing troubles for Internet users, but also for companies that provide financial services online. This is because when users fall a prey to such phishing attacks, the organization providing the online service often suffers a loss in reputation as well as financial damage.

## 2. Phishing attack procedure and prevention methods

In this paper, we will consider methods to detect phishing that uses emails since phishers mostly use them to defraud the victims. The method is explained below:

*1)* Phishers set up a phony Web site which looks identical to the legitimate Web site, including page layouts, styles(font families, sizes and so on), key regions, setting up the web server and applying the DNS server name.
*2)* They send a huge number of fake emails to various users by spoofing as legitimate companies and organizations, trying to lure the potential victims to visit their Web sites.
*3)* Victims who receive such emails, opens them, clicks on the hyperlink in the email which leads them to fake website created by the phisher, wherein they give in their significant personal information such as bank account passwords, credit card details and so on.
*4)* Phishers embezzle such personal information and uses it for their own benefit such as stealing money from other people's accounts.

As per a study, it was found that 40% of the times, Internet users ignored browser-based cues such as the address bar and the security indicators. Some counterfeit websites are so similar to the legitimate websites that can fool even the most sophisticated users. As standard security indicators are not effective in preventing a large number of users from falling a victim to such phishing attacks, alternate approaches to avoid such attacks are needed.

## 3. Related Work

Phishing is a growing problem on the internet today for both consumers and businesses. One of the most common approaches for an attacker is to create a similar website in order to capture personal information from consumers. A malicious website may look identical to an online bank or other financial institution in order to capture passwords, social security numbers, account numbers, and other confidential information. A victim may not identify the malicious site until after the confidential information has been leaked.
Some of the approaches for phishing detection are:

### *3.1. Email-level approach*

This approach intends to amend the phishing attacksat the email level. The main concept is that when a spoofed email is not received by its victims, they cannot fall for the scam. Filters and content analysis techniques are often used to detectphishing emails before they can be delivered to users.For instance, by using training filters (e.g., Bayesianfilters), an enormous number of phishing emails can be thwarted.

In order to prevent spoofing of sender information in an email message, Microsoft and Yahoo have defined email authentication protocols (Sender ID and DomainKeys) that can be used to verify the credibility of a received email. If widely used, these solutions could help to prevent spam emails and, as a result, decrease the number of email-based phishing attacks.