Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.696 – 699

REVIEW ARTICLE

PHISHING WEBSITE DETECTION: A REVIEW

Feon Jaison[1], Seenia Francis[2]

[1]Department of Computer Science & Engineering, Jyothi Engineering College, Cheruthuruthy
[2]Assistant Professor, Department of Computer Science & Engineering, Jyothi Engineering College, Cheruthuruthy

Abstract—Phishing is an attempt to steal users' personal and financial information such as passwords, credit card numbers, through electronic communication such as e-mail and other messaging services. Attackers pretend to be from a organization which direct the users to a fake website that resembles a phishing website, which is then used to collect users personal information. Attackers can also trick users into downloading malicious codes or malware after they click on a link embedded in the email.

Various researches have been done for protecting the users from phishing attacks. They include firewalls, blacklisting certain domains and internet protocol (IP) addresses, spam filtering techniques, fake website detection, client side tool-bars and user education. Each of these existing techniques has some advantages and some disadvantages. The need to automatically discover a phishing target is an important problem for anti-phishing efforts. If we know the webpage which is considered as the target webpage, we can confirm which all are the phishing pages. It could help the owners to identify phishing attacks so that they can immediately take necessary counter measures.

Keywords-Phishing Website, Division Clustering Algorithm, Classifiers

Full Text: http://www.ijcsmc.com/docs/papers/February2014/V3I2201499a42.pdf