COMPARATIVE STUDY OF MACHINE LEARNING ALGORITHMS IN WEBSITE PHISHING DETECTION

ALMUKHAMMED KALYBAYEV

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

AUGUST 2013

I dedicate my thesis to my family. A special feeling of thankfulness to my loving wife, “Gaukhar” whose without her help and patience this work could not be done. To my parents whose words of inspiration and push for endurance ring in my ears.

ACKNOWLEDGEMENT

I would like to truly appreciate **Dr. Anazida Zainal** for taking the time out of her busy schedule to encourage and guide me through this project. Her deep knowledge and valuable experience inspired me and illuminated my path. Also for her great advices and technical points that she gave me with attractiveness.

Beside I should be appreciative of authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and creative area.

ABSTRACT

Harmful programs that are created to thieve user credentials have become a lot over the recent years, potentially leading to a loss of cash. The methods which are utilized by attackers to collect confidential information vary, when online banking systems continue to be the main goal of these attacks. Nowadays most widespread approach to protect against phishing attack is using blacklists in antiviruses and browser toolbars. Unfortunately, blacklist method fails in responding to newly emanating phishing attacks since registering new domain names has become easier, no comprehensive blacklist can ensure a perfect up-to-date database. Therefore it requires another approach to counter phishing attack which is more accurate and efficient than blacklist method. The purpose of this work is to evaluate and analyze the effectiveness of applying machine learning algorithms such as an Artificial Neural Network, Support Vector Machines and K-nearest Neighbor to website phishing detection. The datasets of phishing and non-phishing websites were gathered in order to train, test machine learning algorithm models, compare evaluative metrics of algorithms between each other. In addition, the final dataset was divided into three datasets with different ratios to see whether or not the trained models will show constant performance in testing results and whether these proportions have a good or bad influence on the ability of trained models to classify website. After all the analysis of the performance of each machine learning algorithm was made. This project suggests the Support Vector Machines algorithm as the best one to be used in phishing detection regardless of dataset proportion, because it showed almost the same performance throughout all test phases which is 98.5% on average.

ABSTRAK

Aplikasi merbahaya yang dicipta untuk mencuri maklumat sulit pengguna kini semakin bertambah dan berpotensi menyebabkan kerugian tunai. Sasaran utama adalah sistem kewangan dalam talian dan kaedah yang digunakan untuk mengumpul maklumat yang sensitif adalah berbeza. Pada masa kini, pendekatan yang paling meluas untuk berlindung daripada serangan pemalsuan adalah dengan menggunakan senarai hitam dalam antivirus dan bar alat pelayar. Malangnya, kaedah menyenarai hitam gagal untuk bertindak balas terhadap serangan pemalsuan baru yang bermula sejak pendaftaran nama domain baru menjadi lebih mudah, tiada senarai hitam yang komprehensif yang dapat memastikan pangkalan data yang terkini dan sempurna. Oleh itu, pendekatan lain diperlukan untuk menangani serangan pemalsuan dengan lebih tepat dan berkesan daripada kaedah senarai hitam. Tujuan kajian ini adalah untuk menilai dan menganalisa keberkesanan penggunaan algoritma pembelajaran mesin seperti ‘Artificial Neural Network’, ‘Support Vector Machines’ dan ‘K-nearest Neighbor’ dalam mengesan pemalsuan laman web. Dataset laman pemalsuan dan bukan pemalsuan telah dikumpul untuk melatih, menguji model algoritma pembelajaran mesin, membandingkan pestasi algoritma di antara satu sama lain. Di samping itu, dataset terakhir telah dibahagikan kepada tiga dataset dengan nisbah yang berbeza untuk melihat sama ada model yang terlatih itu akan menunjukkan prestasi yang berterusan dalam keputusan ujian dan sama ada kadar ini mempunyai pengaruh yang baik atau buruk kepada keupayaan model terlatih untuk mengklasifikasikan laman web. Setelah itu, kesemua analisis prestasi setiap algoritma pembelajaran mesin itu dilaksanakan. Projek ini mencadangkan algoritma ‘Support Vector Machines’ sebagai yang terbaik untuk digunakan dalam pengesanan pemalsuan tanpa mengira kadar dataset, kerana ia menunjukkan prestasi yang hampir sama sepanjang semua fasa ujian iaitu 98.5% secara purata.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ANN	Artificial Neural Network
APWG	Anti-Phishing Working Group
BART	Bayesian Additive Regression Trees
CCH	Contrast Context Histogram
DNS	Domain Name System
IDS	Intrusion Detection System
KNN	K-Nearest Neighbor
LPWA	Lucent Personalized Web Assistant
NB	Naïve Bayesian
SRD	Synchronized Random Dynamic Boundaries
SRP	Secure Remote Password protocol
SSL	Secure Socket Layer
SVM	Support Vector Machines
TCA	Trusted Credentials Area
URL	Unified Resource Locator

CHAPTER 1

INTRODUCTION

1.1 Introduction

The use of the Internet has grown in our usual live, a lot of services are now available online. This new business market offers many opportunities for service providers, including financial institutions. It should not surprise anyone that wherever money is involved, villains appear trying to steal it. The same applies to online financial systems. The surprising part is the recent increase in the number and the evolution of their techniques (Candid, 2005).

The main divider between the methods used is the point of attack. To simplify matters we can therefore categorize the attacks into three main groups: local, remote and hybrid attacks.

1. Local attacks happen on the victim's machine.
2. Remote attacks don't modify the machine but try to intercept or redirect the traffic of a session.
3. And hybrid attacks combine local and remote attacks and are the most powerful.

The most common remote attack against financial online services is phishing. An attacker sets up a copy of the web site they want to impersonate on a server they control. This copy includes some code from the original site. The set of used images can be gathered during a previous legitimate session. This makes it hard to trace the imposter in the server logs as no suspicious access is made. Next, the attacker sends emails to a large number of email accounts. The emails contain a convincing message that should trick the recipient into visiting the spoofed web site and revealing his log on credentials. Once the user enters his personal data into the spoofed web form the attacker saves the information and redirects the user to a fake error page or to the original web site.

Studies by the Anti-Phishing Working Group (APWG) have concluded that phishing attacks are likely to succeed with a chance of 5% on all message recipients. To lower the technical knowledge needed by users to perform these checks many solutions have been introduced. Most browsers nowadays will warn a user if they are about to visit a web site that uses an authentication string in the URL. There are many additional tools available. SpoofGuard for example, installs a toolbar that can perform the URL checks (Boneh *et al.*, 2005).

Phishing is an online identity theft in which an attacker uses fraudulent e-mails and bogus website in order to trick gullible customers into disclosing confidential information such as bank account information, website login information etc. (Topkara *et al.*, 2005).

In general, phishing is a relatively new internet crime. The ease of cloning a legitimate website to convince unsuspecting users has made phishing difficult to curtail. Mostly, an email with a redirecting website link is being sent to the user to update confidential information such as credit card, website login information and bank account information that belongs to the licit. As explained by Aburrous *et al.*, (2008), the complexity of understanding and analyzing phishing website is as a result of its involvement with technical problems and social. The main effect of phishing website is in the abuse of information through the compromise of user data which may harm victims in the form of financial losses or valuables. Phishing in comparison to other forms of internet threat such as hacking and virus is a fast growing internet crime. In the broad usage of the internet as a major form of communication, phishing can be implemented in different ways such as follows (Alnajim and Munro, 2009):

1. Email-to-email: when someone receives an email requesting sensitive information to be sent to the sender.
2. Email-to-website: when someone receives an email embedded with a phishing web address.
3. Website-to-website: when someone clicks on phishing website through a search engine or an online advert.
4. Browser-to-website: when someone misspelled a legitimate web address in a browser and then referred to a phishing website that has a semantic similarity to the legitimate web address.

Different types of anti-phishing measures are being used to prevent phishing, such as, Anti-Phishing Working Group is an industry group, which formulates phishing reports from different online incident resources and makes it available to its paying members (RSA, 2006). Meanwhile, anti-phishing measures have been implemented as additional extension or toolbars for browsers, as features embedded in browsers, and as part of website login operation. Many of this toolbars have been used in the detection of phishing. Garera *et al.*, (2007) proposed Spoof Guard which warns users of phishing website. This tool makes use of URL, images, domain name and link to evaluate the spoof likelihood.

Lucent Personalized Web Assistant (LPWA) is a tool that guards against identity theft to protect user’s personal information (Gabber *et al.*, 1999; Kristol *et al.*, 1998). It uses a function to define user variables such as email address, username and password for each server visited by the user. Ross *et al.*, (2005) proposed a similar approach in PwdHash.

R. Dhamija and J. D. Tygar (2005) proposed Dynamic Security Skins, which is another type of browser-based anti-phishing technique. This solution was implemented based on their previous work on Human Interactive Proofs (Dhamija and Tygar, 2005), which employs distinguishing features between legitimate and spoofed web sites by human. Dynamic Security Skins ensures identity verification of a remote server by humans, but is hard to spoof by attackers (Dhamija and Tygar, 2005). Furthermore, the tool uses a client-side password on the browser window with a Secure Remote Password protocol (SRP) for verification based authentication protocol. In addition, an image which is shared as a secret between the browser and the user ensures better security against spoofing. This secured image is either chosen by the user or as a result of random assignment and also, during each transaction, the image is being regenerated by the server and used in creating the browser skin. As a verification measure for the server, the user has to visually verify the authenticity of the image. In exceptional cases when the user login from an untrusted computer, the tool will not be able to guarantee security. Furthermore, it does not guard against malware and trusts the browser's security during the SRP authentication.

Herzberg and Gbara (2004) introduced TrustBar which is a third party certification solution against phishing. The authors proposed creating a Trusted Credentials Area (TCA). The TCA controls a significant area, located at the top of every browser window, and large enough to contain highly visible logos and other graphical icons for credentials identifying a legitimate page. While their solution does not rely on complex security factors, it does not prevent against spoofing attacks. Specifically, since the logos of websites do not change, they can be used by an attacker to create a look alike TCA in an untrusted web page.

Due to the ever increasing phishing websites springing up by the day, it is becoming increasingly difficult to track and block them as attackers are coming up with innovative methods every day to entice unsuspecting users into divulging their personal information (Garera *et al.*, 2007).

1.2 Problem Background

In today's financial world phishing is becoming the most dangerous and ubiquitous threat to the financial subjects, who deal with money transactions using their information technology systems. As a new type of cyber security threat, phishing websites appear frequently in recent years, which have led to great harm in online financial services and data security (Zhuang *et al*., 2012). The main targets of this type of threat are banks with their internet-banking systems. The development of the Internet for commerce and in particular the arrival of internet-banking systems gave birth to phishing. The technical nature of the internet has made copying a legitimate website a very simple exercise. Once this is done it is simple to direct internet-bank users to these copies of internet-banks using alert e-mails or malware, and convincing them to enter their internet-banking credentials. Then the same techniques were used in legitimate web infrastructure after capturing credentials.

With the growth of malware in the late 1990s and early 2000s, the ease by which millions of computers connected to the Internet could be quickly compromised was understood. However, these early efforts such as "Melissa" in 1999, "I Love You" and "Slammer" in 2001, were about announcing themselves and gaining credit for their writers rather than any primary profit motive. However, the new malware starting in 2003 would use the same types of system vulnerabilities, but remain hidden and capture account credentials and would ultimately become an even more effective phishing method.

Globally, phishing and related cybercrime is responsible for annual losses of billions money. Ultimately, simple users of internet-banking systems suffer from successfully committing phishing attacks. Sometimes banks refund the clients loses, but not in all cases. Also, in many cases banks who become victims of phishing attacks do not desire to publish these facts and make them available to the public because of fear to lose customers. That is why the thought that real statistics of annual losses from phishing are more than we know becomes obvious.

Most researchers have worked on increasing the accuracy of website phishing detection through multiple techniques. Several classifiers such as Linear Regression, K-Nearest Neighbor, C5.0, Naïve Bayes, Support Vector Machines (SVM), and Artificial Neural Network amongst others have been used to train datasets in identifying phishing websites. These classifiers can be classified into two techniques; either probabilistic or machine learning. Based on these algorithms, several problems regarding phishing website detection have been solved by different researchers. Some of these algorithms were evaluated using four metrics, Precision, Recall, F1-Score, and Accuracy.

Some studies have applied K-Nearest Neighbor (KNN) for phishing website classification. KNN classifier is a non-parametric classification algorithm. One of the characteristic of this classifier is that it generalizes whenever it is required to classify an instance. This has the effect of ensuring that no information is lost a scan happen with the other eager learning techniques (Toolan and Carthy, 2009). In addition, previous researches have shown that KNN can achieve accurate results, and sometimes more accurate than those of the symbolic classifiers. It was shown in a study carried out by Kim and Huh (2011) that KNN classifier achieved 99% detection rate. This result was better than that which was obtained from Naïve Bayesian (NB), and Support Vector Machines (SVM). Also, since the performance of KNN is primarily determined by the choice of K, they tried to find the best K by varying it from 1 to 5; and found that KNN performs best when K = 1. This as well, helped in the high accuracy of KNN compared to other classifiers.

Meanwhile, Artificial Neural Network (ANN) is another popular machine learning technique. It consists of a collection of processing elements that are highly interconnected and transform a set of inputs to a set of desired outputs. The major disadvantage is the time it takes for parameter selection and network learning. On the other hand, previous researches have shown that ANN can achieve very accurate results compared to other learning classification techniques. In a research carried out by Basnet *et al*., (2008), it was shown that Artificial Neural Network achieved an accuracy of 97.99%.

1.3 Problem Statement

Although, a lot of techniques and approaches have been designed and are being deployed the offenders are still able to overcome applied countermeasures. Typically, phishing detection methods use human verified URL blacklists. However, blacklist is frail in terms of newly appearing phishing websites and cannot identify phishing website in case of spear-phishing, when the attacker intentionally try to cause harm to particular victim. Also, the blacklist-based method is inefficient in responding to emanating phishing attacks since registering new domain names has become easier, no comprehensive blacklist can ensure a perfect up-to-date database. Possibility of “Zero day attacks” always exists. Thus, exploiting webpage features via machine learning techniques is more preferable, because this method does not have problems of blacklist approach mentioned above and does not rely on any databases are made by human. In addition, the machine learning classification technique should perform with consistent accuracy.

1.4 Purpose of Study

The purpose of this work is to evaluate and analyze the effectiveness of applying major machine learning algorithms to website phishing detection. In the future works the results of this analysis might be used to design applicable IDS.

1.5 Project Objectives

There are four objectives for this project. They are:

1. To train, test and evaluate Artificial Neural Network algorithm performance to detect phishing websites with the dataset.

2. To train, test and evaluate K-Nearest Neighbour algorithm performance to detect phishing websites with the dataset.
3. To train, test and evaluate Support Vector Machines algorithm performance to detect phishing websites with the dataset.
4. To compare and analyze the results of machine learning approaches testing.

1.6 Project Scope

The scopes of this research are as follows:

1. The dataset will be obtained from phishtank (www.phishtank.com)
2. The dataset will be used to evaluate the performance of Artificial Neural Networks (ANN), K-Nearest Neighbor (KNN) and Support Vector Machines (SVM).
3. The results of precision, recall, F1-score and accuracy of the three algorithms will be compared.
4. WEKA as a popular suite of machine learning will be used to train and test algorithms.

1.7 Significance of Study

Nowadays, there is an increasing need to detect phishing websites due to the adverse effect they can have on their victims. Lots of work has been done on website phishing detection using several techniques to achieve the same goal. This study evaluates the performance of some algorithms: ANN, KNN and SVM algorithms as regards to detection accuracy and false alarms by studying each of them individually and investigate to show which is more suitable to be used in phishing detection.

1.8 Organization of Report

The thesis is organized as follows and consists of 6 chapters. Chapter one describes the introduction, background of the study, the scope of the study and its primary objectives. The second chapter reviews available and related literature and current state of website phishing detection. Chapter three introduces the study methodology along with the appropriate framework for the study. Chapter 4 describes data preprocessing phases and creation of usable datasets for the purposes of this Project. Chapter 5 deals with training, testing and evaluation of chosen machine learning classifiers. And finally, Chapter 6 is about conclusion and recommendations for future work.

REFERENCES

A.P.W.G. (2010). Global phishing survey: Domain name use and trends in 2h2010.

Abbasi, A., and Chen, H. (2007). *Detecting Fake Escrow Websites Using Rich Fraud Cues and Kernel Based Methods.* Paper presented at the Proceedings of the 17th Workshop on Information Technologies and Systems.

Abbasi, A., and Chen, H. (2009a). A comparison of fraud cues and classification methods for fake escrow website detection. *Information Technology and Management, 10*(2), 83-101.

Abbasi, A., and Chen, H. (2009b). A comparison of tools for detecting fake websites. *Computer, 42*(10), 78-86.

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker Jr, J. F. (2010). Detecting fake websites: The contribution of statistical learning theory. *MIS Quarterly, 34*(3), 435.

Aburrous, M., Hossain, M. A., Thabatah, F., and Dahal, K. (2008). *Intelligent phishing website detection system using fuzzy techniques.* Paper presented at the Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on.

Afroz, S., and Greenstadt, R. (2009). Phishzoo: An automated web phishing detection approach based on profiling and fuzzy matching: Technical Report DU-CS-09-03, Drexel University.

Afroz, S., and Greenstadt, R. (2011). *Phishzoo: Detecting phishing websites by looking at them.* Paper presented at the Semantic Computing (ICSC), 2011 Fifth IEEE International Conference on.

Airoldi, E., and Malin, B. (2004). *Data mining challenges for electronic safety: the case of fraudulent intent detection in e-mails.* Paper presented at the Proceedings of the workshop on privacy and security aspects of data mining.

Alnajim, A., and Munro, M. (2009). *An Approach to the Implementation of the Anti-Phishing Tool for Phishing Websites Detection.* Paper presented at the Intelligent Networking and Collaborative Systems, 2009. INCOS'09. International Conference on.

Atighetchi, M., and Pal, P. (2009). *Attribute-based prevention of phishing attacks.* Paper presented at the Network Computing and Applications, 2009. NCA 2009. Eighth IEEE International Symposium on.

Basnet, R., Mukkamala, S., and Sung, A. (2008). Detection of phishing attacks: A machine learning approach. *Soft Computing Applications in Industry*, 373-383.

Berend, D., and Paroush, J. (1998). When is Condorcet's Jury Theorem valid? *Social Choice and Welfare, 15*(4), 481-488.

Chen, J., and Guo, C. (2006). *Online detection and prevention of phishing attacks.* Paper presented at the Communications and Networking in China, 2006. ChinaCom'06. First International Conference on.

Chen, K. T., Chen, J. Y., Huang, C. R., and Chen, C. S. (2009). Fighting phishing with discriminative keypoint features. *Internet Computing, IEEE, 13*(3), 56-63.

Chou, N., Ledesma, R., Teraguchi, Y., Boneh, D., and Mitchell, J. C. (2004). *Client-side defense against web-based identity theft.* Paper presented at the 11th Annual Network and Distributed System Security Symposium (NDSS’04).

Chua, C. E. H., and Wareham, J. (2004). Fighting internet auction fraud: An assessment and proposal. *Computer, 37*(10), 31-37.

Close, T. (2009). Waterken YURL: trust management for humans (2003). *Last visit on May, 30*.

Dhamija, R., and Tygar, J. (2005). Phish and hips: Human interactive proofs to detect phishing attacks. *Human Interactive Proofs*, 69-83.

Dhamija, R., and Tygar, J. D. (2005). *The battle against phishing: Dynamic security skins.* Paper presented at the ACM International Conference Proceeding Series.

Dhamija, R., Tygar, J. D., and Hearst, M. (2006). *Why phishing works.* Paper presented at the Proceedings of the SIGCHI conference on Human Factors in computing systems.

Dinev, T. (2006). Why spoofing is serious internet fraud. *Communications of the ACM, 49*(10), 76-82.

Dunlop, M., Groat, S., and Shelly, D. (2010). *GoldPhish: Using Images for Content-Based Phishing Analysis.* Paper presented at the Internet Monitoring and Protection (ICIMP), 2010 Fifth International Conference on.

Elkan, C. (2007). Evaluating Classifiers.

Fahmy, H. M. A., and Ghoneim, S. A. (2011). *PhishBlock: A hybrid anti-phishing tool.* Paper presented at the Communications, Computing and Control Applications (CCCA), 2011 International Conference on.

Fette, I., Sadeh, N., and Tomasic, A. (2007). *Learning to detect phishing emails.* Paper presented at the Proceedings of the 16th international conference on World Wide Web.

Fu, A. Y., Wenyin, L., and Deng, X. (2006). Detecting phishing web pages with visual similarity assessment based on earth mover's distance (EMD). *Dependable and Secure Computing, IEEE Transactions on, 3*(4), 301-311.

Gabber, E., Gibbons, P. B., Kristol, D. M., Matias, Y., and Mayer, A. (1999). Consistent, yet anonymous, Web access with LPWA. *Communications of the ACM, 42*(2), 42-47.

Garera, S., Provos, N., Chew, M., and Rubin, A. D. (2007). *A framework for detection and measurement of phishing attacks.* Paper presented at the Proceedings of the 2007 ACM workshop on Recurring malcode.

Gaurav., Madhuresh., M., and Anurag., J. (2012). Anti-Phishing Techniques: A Review. *International Journal of Engineering Research and Applications (IJERA), 2*(2), 350-355.

Hariharan, P., Asgharpour, F., and Camp, L. J. (2007). *Nettrust—recommendation system for embedding trust in a virtual realm.* Paper presented at the Proceedings of the ACM Conference on Recommender Systems.

Herzberg, A., and Gbara, A. (2004). Trustbar: Protecting (even naive) web users from spoofing and phishing attacks. *Computer Science Department Bar Ilan University, 6*.

Herzberg, A., and Jbara, A. (2008). Security and identification indicators for browsers against spoofing and phishing attacks. *ACM Transactions on Internet Technology (TOIT), 8*(4), 1-36.

Jamieson, R., Wee Land, L. P., Winchester, D., Stephens, G., Steel, A., Maurushat, A., and Sarre, R. (2012). Addressing identity crime in crime management information systems: Definitions, classification, and empirics. *Computer Law & Security Review, 28*(4), 381-395.

Ji, C., and Ma, S. (1997). Combinations of weak classifiers. *Neural Networks, IEEE Transactions on, 8*(1), 32-42.

Kim, H., and Huh, J. (2011). Detecting DNS-poisoning-based phishing attacks from their network performance characteristics. *Electronics Letters, 47*(11), 656-658.

Kittler, J., Hatef, M., Duin, R. P. W., and Matas, J. (1998). On combining classifiers. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 20*(3), 226-239.

Kristol, D. M., Gabber, E., Gibbons, P. B., Matias, Y., and Mayer, A. (1998). Design and implementation of the Lucent Personalized Web Assistant (LPWA). *Submitted for publication*.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., and Nunge, E. (2007). *Protecting people from phishing: the design and evaluation of an embedded training email system.* Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems.

Lam, L., and Suen, S. (1997). Application of majority voting to pattern recognition: An analysis of its behavior and performance. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, 27*(5), 553-568.

Levy, E. (2004). Criminals become tech savvy. *Security and Privacy, IEEE, 2*(2), 65-68.

Li, L., and Helenius, M. (2007). Usability evaluation of anti-phishing toolbars. *Journal in Computer Virology, 3*(2), 163-184.

Liu, G., Qiu, B., and Wenyin, L. (2010). *Automatic Detection of Phishing Target from Phishing Webpage.* Paper presented at the Pattern Recognition (ICPR), 2010 20th International Conference on.

Liu, W., Deng, X., Huang, G., and Fu, A. Y. (2006). An antiphishing strategy based on visual similarity assessment. *Internet Computing, IEEE, 10*(2), 58-65.

Ma, J., Saul, L. K., Savage, S., and Voelker, G. M. (2009). *Identifying suspicious URLs: an application of large-scale online learning.* Paper presented at the Proceedings of the 26th Annual International Conference on Machine Learning.

Martin, A., Anutthamaa, N., Sathyavathy, M., Francois, M. M. S., and Venkatesan, D. V. P. (2011). A Framework for Predicting Phishing Websites Using Neural Networks. *arXiv preprint arXiv:1109.1074*.

Miyamoto, D., Hazeyama, H., and Kadobayashi, Y. (2005). SPS: a simple filtering algorithm to thwart phishing attacks. *Technologies for Advanced Heterogeneous Networks*, 195-209.

Miyamoto, D., Hazeyama, H., and Kadobayashi, Y. (2007). *A proposal of the AdaBoost-based detection of phishing sites.* Paper presented at the Proceedings of the Joint Workshop on Information Security.

Moore, T., and Clayton, R. (2007). *Examining the impact of website take-down on phishing.* Paper presented at the Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit.

Parker, J. (1995). *Voting methods for multiple autonomous agents.* Paper presented at the Intelligent Information Systems, 1995. ANZIIS-95. Proceedings of the Third Australian and New Zealand Conference on.

Provos, N., McClain, J., and Wang, K. (2006). *Search worms.* Paper presented at the Proceedings of the 4th ACM workshop on Recurring malcode.

Rahman, A., Alam, H., and Fairhurst, M. (2002). Multiple classifier combination for character recognition: Revisiting the majority voting system and its variations. *Document Analysis Systems V*, 167-178.

Rokach, L. (2010). Ensemble-based classifiers. *Artificial Intelligence Review, 33*(1), 1-39.

Ronda, T., Saroiu, S., and Wolman, A. (2008). *Itrustpage: a user-assisted anti-phishing tool.* Paper presented at the ACM SIGOPS Operating Systems Review.

Ross, B., Jackson, C., Miyake, N., Boneh, D., and Mitchell, J. C. (2005). *A browser plug-in solution to the unique password problem.* Paper presented at the Proceedings of the 14th Usenix Security Symposium.

RSA. (2006). Phishing special report: What we can expect for 2007.

Ruta, D., and Gabrys, B. (2000). An overview of classifier fusion methods. *Computing and Information systems, 7*(1), 1-10.

Saberi, A., Vahidi, M., and Bidgoli, B. M. (2007). *Learn to Detect Phishing Scams Using Learning and Ensemble Methods.* Paper presented at the Web Intelligence and Intelligent Agent Technology Workshops, 2007 IEEE/WIC/ACM International Conferences on.

Schneider, F., Provos, N., Moll, R., Chew, M., and Rakowski, B. (2007). Phishing Protection Design Documentation.

See Ng, G., and Singh, H. (1998). Democracy in pattern classifications: combinations of votes from various pattern classifiers. *Artificial intelligence in engineering, 12*(3), 189-204.

Shreeram, V., Suban, M., Shanthi, P., and Manjula, K. (2010). *Anti-phishing detection of phishing attacks using genetic algorithm.* Paper presented at the Communication Control and Computing Technologies (ICCCCT), 2010 IEEE International Conference on.

Stajniak, A., Szostakowski, J., and Skoneczny, S. (1997). *Mixed neural-traditional classifier for character recognition.* Paper presented at the Advanced Imaging and Network Technologies.

Suen, C. Y., Nadal, C., Legault, R., Mai, T. A., and Lam, L. (1992). Computer recognition of unconstrained handwritten numerals. *Proceedings of the IEEE, 80*(7), 1162-1180.

Todhunter, I. (1865). *History of the Mathematical Theory of Probability from the time of Pascal to that of Laplace*: Macmillan and Company.

Toolan, F., and Carthy, J. (2009). *Phishing detection using classifier ensembles.* Paper presented at the eCrime Researchers Summit, 2009. eCRIME'09.

Topkara, M., Kamra, A., Atallah, M., and Nita-Rotaru, C. (2005). Viwid: Visible watermarking based defense against phishing. *Digital Watermarking*, 470-483.

Tout, H., and Hafner, W. (2009). *Phishpin: An identity-based anti-phishing approach.* Paper presented at the Computational Science and Engineering, 2009. CSE'09. International Conference on.

Whittaker, C., Ryner, B., and Nazif, M. (2010). Large-scale automatic classification of phishing pages. *Proc. of 17th NDSS.*

Willis, P. (2009). Fake anti-virus software catches 43 million users' credit cards. *Digital J.*

Wu, M., Miller, R. C., and Garfinkel, S. L. (2006). *Do security toolbars actually prevent phishing attacks* Paper presented at the Proceedings of the SIGCHI conference on Human Factors in computing systems.

Xiang, G., and Hong, J. I. (2009). *A hybrid phish detection approach by identity discovery and keywords retrieval.* Paper presented at the Proceedings of the 18th international conference on World wide web.

Ye, Z. E., Smith, S., and Anthony, D. (2005). Trusted paths for browsers. *ACM Transactions on Information and System Security (TISSEC), 8*(2), 153-186.

Zdziarski, J., Yang, W., and Judge, P. (2006). *Approaches to Phishing Identification using Match and Probabilistic Digital Fingerprinting Techniques.* Paper presented at the Proceedings of the MIT Spam Conference.

Zhang, J., Ou, Y., Li, D., and Xin, Y. (2012). A Prior-based Transfer Learning Method for the Phishing Detection. *Journal of Networks*, *7*(8), 1201-1207.

Zhang, Y., Egelman, S., Cranor, L., and Hong, J. (2006). *Finding phish: Evaluating anti-phishing tools*.

Zhang, Y., Hong, J. I., and Cranor, L. F. (2007). *Cantina: a content-based approach to detecting phishing web sites.* Paper presented at the Proceedings of the 16th international conference on World Wide Web.

Zhuang, W., Jiang, Q., and Xiong, T. (2012). *An Intelligent Anti-phishing Strategy Model for Phishing Website Detection.* Paper presented at the Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference.