SECURITY ALERT FRAMEWORK USING DYNAMIC TWEET-BASED FEATURES FOR PHISHING DETECTION ON TWITTER

LIEW SEOW WOOI

FSKTM 2019 44

SECURITY ALERT FRAMEWORK USING DYNAMIC TWEET-BASED FEATURES FOR PHISHING DETECTION ON TWITTER

By

LIEW SEOW WOOI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

May 2019

DEDICATION

To my dearest parents ***Liew Soon*** *and* ***Fong Kun Tai***
To my supportive and caring wife ***Chia Gah Wai***
To my lovely and cute daughter ***Liew Zhe Yie***
To all my family members for their intangible encouragements and advices

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

SECURITY ALERT FRAMEWORK USING DYNAMIC TWEET-BASED FEATURES FOR PHISHING DETECTION ON TWITTER

By

LIEW SEOW WOOI

May 2019

Chairman : Associate Professor Nor Fazlida Mohd Sani, PhD
Faculty : Computer Science and Information Technology

Phishing is a form of social engineering crime that deceives victims by directing them to a fake website where their personal credentials are collected eventually for further unlawful activities. Traditionally, phishing attacks target email, but now they have reached to Online Social Networks (OSNs) like Twitter. The challenging differences between the phishing attacks on email and Twitter are that Twitter disseminates vast information and is difficult to be detected unlike email. Many phishing detection methods, ranging from blacklists, heuristics and visual similarity to machine learning are used to detect phishing attacks for spam emails, machine learning approaches achieve the best phishing email detection results. However, it is observed that there are only a few machine learning solutions to detect phishing attacks on OSNs are being proposed and implemented. Phishing detection method of machine learning has been used to classify tweets on Twitter but the number of classification features used and the one achieving the highest phishing tweet detection accuracy of 94.56% (Random Forest) is still considered high. In addition, many phishing tweet detection researchers included tweet-based features to train the classification model for detection but such an approach could decrease the accuracy of detection systems as claimed by spam detection researchers. On another note, the efficiency of response time to alert users on Twitter is an important factor as well. However, the maximum response time achieved by the existing solutions is still considered high and the one claimed achieving the lowest maximum response time of 0.501 seconds is deemed inadequate.

The above mentioned problems are the motivation of this research; where it is vital to propose a security alert framework using dynamic tweet-based features for phishing detection on Twitter. This framework is divided into three phases which are classification model of phishing detection, detection algorithm of phishing tweet detection and security alert mechanism of phishing tweet detection. The best phishing classification features and machine learning technique are identified in order to produce and generate a classification model. This model is then embedded into the detection algorithm together with the inclusion of dynamic tweet-based features which are not as part of the features used to train a classification model for phishing tweet detection. Subsequently, the security alert mechanism is formulated by integrating with the detection algorithm to alert Twitter users.

The overall result significantly indicates that a novel security alert framework using dynamic tweet-based features for phishing detection on Twitter has been formulated. In addition, the result proved that the phishing detection accuracy has been improved to 94.75% with a reduced number of phishing classification features (11), phishing tweet detection accuracy on Twitter has been enhanced with the inclusion of dynamic tweet-based features as add-on filtering features (achieving 95.83% accuracy) and phishing tweet detection efficiency has been improved (with faster response time of 0.425 seconds). As a conclusion, this security alert framework has achieved its objective, is the only framework that provides phishing tweet detection security alert to prompt Twitter users to the best of our knowledge.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

KERANGKA AMARAN KESELAMATAN MENGGUNAKAN CIRI-CIRI BERASASKAN TWEET DINAMIK UNTUK PENGESANAN *PHISHING* ATAS TWITTER

Oleh

LIEW SEOW WOOI

Mei 2019

Pengerusi : Professor Madya Nor Fazlida Mohd Sani, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Memancing data (*Phishing*) ialah sejenis jenayah kejuruteraan sosial yang memperdaya mangsanya dengan mengarah mereka ke satu laman web palsu yang mana tauliah peribadi mereka akhirnya dikumpul untuk aktiviti menyalahi undang-undang yang seterusnya. Secara tradisi serangan *phishing* mensasar e-mel, tetapi sekarang mereka telah sampai kepada Talian Rangkaian Sosial (OSN) seperti Twitter. Perbezaan yang mencabar antara serangan phishing dalam emel dengan Twitter ialah Twitter menyebar maklumat yang pelbagai dan sukar untuk dikesan berbanding emel. Banyak cara pengesanan *phishing* terdiri daripada senarai hitam, heuristik, persamaan visual dan pembelajaran mesin digunakan untuk mengesan serangan *phishing* bagi e-mel spam, pendekatan pembelajaran mesin mencapai keputusan pengesanan e-mel *phishing* yang terbaik. Walau bagaimanapun, didapati hanya terdapat sedikit penyelesaian pembelajaran mesin untuk mengesan serangan phishing ke atas OSN yang telah dicadang dan diimplimentasi. Kaedah pengesanan *phishing* pembelajaran mesin telah digunakan untuk mengkelas tweet atas Twitter tetapi bilangan ciri pengkelasan yang digunakan dan salah satu pengesanan tweet *phishing* yang mencapai ketepatan tertinggi 94.56% (Hutan Rawak), masih dianggap tinggi. Selain itu, ramai penyelidik pengesanan tweet *phishing* memasukkan ciri-ciri berasaskan tweet untuk melatih model pengkelasan bagi pengesanan tetapi pendekatan tersebut boleh mengurangkan ketepatan sistem pengesanan sepertimana didakwa oleh penyelidik pengesanan spam. Di samping itu, kecekapan masa balasan untuk amaran pengguna atas Twitter adalah faktor penting juga. Tetapi, masa balasan maksimum yang dicapai oleh penyelesaian yang sedia ada adalah masih dianggap tinggi dan salah satu didakwa mencapai masa balasan maksimum paling rendah iaitu 0.501 saat dipercayai belum memadai.

Masalah-masalah yang dinyatakan di atas menjadi motivasi bagi penyelidikan ini; yang mana penting untuk mencadangkan satu kerangka amaran keselamatan menggunakan ciri-ciri berasaskan tweet dinamik untuk pengesanan *phishing* atas Twitter. Kerangka ini dibahagikan kepada tiga fasa iaitu model pengkelasan pengesanan *phishing*, algoritma pengesanan tweet *phishing* dan mekanisme amaran keselamatan pengesanan tweet *phishing*. Ciri-ciri terbaik pengkelasan *phishing* dan teknik pembelajaran mesin dikenalpasti untuk menghasilkan dan menjana satu model pengkelasan. Model tersebut kemudian dibenam dalam algoritma pengesanan bersama dengan ciri-ciri berasaskan tweet dinamik yang dimasukkan bukan sebagai sebahagian ciri-ciri untuk melatih model pengkelasan bagi pengesanan tweet *phishing*. Seterusnya, mekanisme amaran keselamatan dirumuskan dengan mengintegrasikan algoritma pengesanan untuk amaran pengguna Twitter.

Keputusan keseluruhan menunjukkan dengan signifikan bahawa satu kerangka amaran keselamatan yang baharu menggunakan ciri-ciri berasaskan tweet dinamik untuk pengesanan *phishing* atas Twitter telah dirumuskan. Selain itu, keputusan tersebut membuktikan bahawa ketepatan pengesanan *phishing* telah ditingkatkan menjadi 94.75% dengan mengurangkan bilangan nombor ciri-ciri pengkelasan *phishing* (11), ketepatan pengesanan tweet *phishing* atas Twitter telah ditingkatkan lagi dengan ciri-ciri berasaskan tweet dinamik dimasukkan sebagai ciri-ciri penapis tambahan (hingga ketepatan mencapai 95.83%) dan kecekapan pengesanan tweet *phishing* telah ditingkatkan (masa balasan cepat 0.425 saat). Sebagai kesimpulan, kerangka amaran keselamatan ini telah mencapai objektifnya, setakat yang diketahui merupakan satu-satu kerangka yang menyediakan amaran keselamatan pengesanan tweet *phishing* kepada pengguna Twitter.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my most gratitude and deepest appreciation to my supervisor, Associate Professor Dr. Nor Fazlida Mohd Sani for her continuous advice, support and encouragement throughout the entire period of my PhD study.

Furthermore, I would like to thank my co-supervisors, Associate Professor Dr. Razali Yaakob, Dr. Mohd. Taufik Abdullah and Dr. Mohd Yunus Sharum for their valuable input and feedbacks on my research work.

I would like to extend my thanks to the staff of the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia for their general help and assistance.

Last but not least, many thanks go to my family members, specially my wife, for giving me continual motivation and psychological support to complete this research and thesis. I also need to acknowledge with much appreciation the support of numerous parties, who had kindly helped me in the research and production of this thesis.

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software

Signature: ________________________ Date: __________________

Name and Matric No.: Liew Seow Wooi GS43835

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
API	Application Programming Interface
APWG	Anti-Phishing Working Group
CCH	Contrast Context Histogram
CFS	Correlation-based Feature Selection
CPU	Central Processing Unit
CSS	Cascading Style Sheets
CSV	Comma-Separated Values
DT	Decision Tree
DNS	Domain Name Service
FN	False Negative
FP	False Positive
FTP	File Transfer Protocol
GTR	Google Toolbar Rank
GUI	Graphical User Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPs	Hypertext Transfer Protocol with Secure Sockets Layer
IE	Internet Explorer
IP	Internet Protocol
IT	Information Technology
IDE	Integrated Development Environment
IoT	Internet of Things

JDK	Java Development Kit
KNN	K-Nearest Neighbors
LR	Logistic Regression
LAN	Local Area Network
MLP	Multilayer Perceptron
MITM	Man-in-the–middle
MyWOT	Web of Trust
NB	Naive Bayes
OSN	Online Social Network
PC	Personal Computer
PTI	Phishing Trends & Intelligence
RF	Random Forest
RT	ReTweet
SFH	Server Form Handler
SMO	Sequential Minimal Optimization
SQL	Structured Query Language
SSL	Secure Sockets Layer
SVM	Support Vector Machine
SaaS	Software-as-a-Service
TN	True Negative
TP	True Positive
TLD	Top-Level Domain
TF-IDF	Term Frequency-Inverse Document Frequency
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol

CHAPTER 1

INTRODUCTION

1.1 Introduction

Today, Information Technology (IT) has undoubtedly become a prominent part of our daily lives as it is used widely by everyone and serves as a backbone for industries to do business globally. It has grown rapidly and has been convenient to everyone in many ways. However, IT also results and increases security challenges for us to protect our information securely especially from social engineering attacks.

Social engineering is an art of getting users to compromise information systems (Krombholz et al., 2015) and is a form of information gathering involving human intervention that breaches security without one realising that he or she has been manipulated. Social engineering can also be interpreted as a method of launching attacks against information and information systems (Janczewski & Fu, 2010), is regarded as “people hacking” (Hasle et al, 2005) and is referred to as information systems penetration through the use of social methods. There are two types of social engineering approaches. One is human or non-technology based and the other is computer or technology based (Gulati, 2003; Maan & Sharma, 2012; Greitzer, 2014).

Phishing is a most significant computer or technology based social engineering attack; one of the most common and serious threats over the Internet (Gupta et al, 2016). Basically, it is a form of social engineering crime called “Semantic Attack” and is generally known as online identity theft that deceives victims by directing them to a fake website looks alike to the legitimate (Arachchilage & Love, 2013; Arachchilage & Love, 2014; Arachchilage et al., 2016) where their personal credentials are collected.

Phishing attacks traditionally target email which serves as the primary vector (Wilcox & Bhattacharya, 2015), but today, they have reached into the popular Online Social Networks (OSNs) such as Twitter, Facebook, Myspace, etc. (Aggarwal et al., 2012; Wilcox & Bhattacharya, 2015). Aaron & Rasmussen (2017) reported that social networking is the third industry (19%) targeted by phishing attacks after the industries of e-commerce (30%) and financial institutions (25%) in their 2016 statistic of Anti-Phishing Working Group (APWG) Global Phishing Survey: Trends and Domain Name Use. In addition to that, Proofpoint stated that social media phishing attacks increased 500% from the beginning of 2016 to the end of 2016 in their Q4 2016 & Year In Review : Threat Summary report. The report also stated about the angler phishing that intercepts customer support channels on social media with the purpose of stealing customers’ credentials. APWG highlighted in their survey that OSNs have become significant platforms where phishers launch phishing attacks. In addition to APWG’s survey, Amato et al. (2017) pointed out that OSNs have also become a primary interest area for cutting-edge cybersecurity applications due to its increasing popularity and the variety of data its interaction models allow for. Furthermore, Calabresi (2017) highlighted that ten thousand employees (Twitter users) in the Department of Defense, U. S. were targeted by a phishing attack with “expertly tailored messages” in March 2017 Time Magazine.

From the review studies, it was revealed that many Online Social Networks’ (OSNs)’ users are still unaware of phishing attacks that are happen in OSN platforms; this could cause severe harm to the users, both in the virtual and real world. With present OSN platforms, especially Twitter, phishers have started using it to spread phishing attacks due to its vast information dissemination and its difficulty to be detected unlike email because of it spreads fast in the network, has short content size and uses short Uniform Resource Locators (URLs) (Aggarwal et al., 2012; Nair & Prema, 2014). In addition, Twitter is an important source where people share information. Twitter is subject to attack by many malicious users due to its popularity makes it on attacked target (Lee & Kim, 2013). Therefore, it is important to build an effective phishing detection mechanisms for every OSN to protect its users (Aggarwal et al., 2012; Nair & Prema, 2014; Sharma et al., 2014) from being tricked by such phishing attacks.

Machine learning method has been used for phishing detection and the Random Forest (RF) machine learning technique is claimed to achieve the highest phishing detection accuracy by several researchers (Akinyelu & Adewumi, 2014; Basnet et al., 2014; Sananse & Sarode, 2015). In addition, it is claimed to be the best machine learning technique that gives the highest accuracy for phishing tweet detection on Twitter (Aggarwal et al., 2012; Sharma et al., 2014).

Despite there are many phishing detection solutions using machine learning techniques that were proposed on Twitter, such as RF, Decision Tree (DT), Naive Bayes (NB), etc., it is evident that there is still room for improving the phishing detection accuracy with the reduction number of classification features in the machine learning classification, enhancing the phishing tweet detection accuracy on Twitter with a new approach to include the dynamic tweet-based features which are not as part of the features used to train the classification model for phishing detection, and improving the phishing tweet detection efficiency with fast response time.

1.2 Problem Statement

Online Social Networks (OSNs) are among the most common means of social engineering attacks. The risks to such networks are expected to increase in future because the users’ posted information are valuable elements to OSN providers who encourage users to reveal and share more personal information (Algarni et al., 2013). In view of this, they highlighted that effective countermeasures should be deployed in order to mitigate such attacks.

Many phishing detection methods ranging from blacklists, heuristics and visual similarity to machine learning are used to detect phishing attacks for spam emails; in which the best phishing detection results are obtained using machine learning (Akinyelu & Adewumi, 2014). Despite machine learning approaches achieve the best phishing email detection results, it is observed that there are only a few machine learning solutions to detect phishing attacks on Online Social Networks (OSNs) are being proposed and implemented.

Phishing detection method of machine learning has been used to classify tweets on Twitter and the machine learning technique of Random Forest (RF) has been claimed to be the one achieving the highest phishing tweet detection accuracy of 94.56% with more than 11 classification features (Sharma et al., 2014). The number of classification features used to achieve such detection accuracy is considered high and shall be reduced. In addition to the number of classification features, Twitter specific features are also important features for phishing tweet detection on Twitter.

Spam detection studies on Twitter usually involve machine learning classification techniques and these studies highlight the use of important Twitter specific features for spam detection (Aggarwal et al., 2012). Hence, this implies that Twitter specific features or tweet-based features are important features used to classify tweets posted on Twitter specifically. Existing machine learning solutions including the one achieving the highest accuracy of 94.56% (Sharma et al., 2014) to detect phishing on Twitter, included tweet-based features to train a classification model. Nevertheless, such features related to followers and friends are dynamic Twitter data presented only at each time users tweet (Wood, 2015) and varied over time which could decrease the accuracy for detection systems (Shigang Liu et al., 2016; Chao Chen et al., 2017). Therefore, a new approach to include the dynamic tweet-based features which are not as part of the features used to train a classification model for phishing tweet detection shall be proposed. In addition to the new approach for enhancing phishing tweet detection, the efficiency in term of response time for detecting phishing tweet is vital.

Aggarwal et al. (2012), Nair & Prema (2014) and Sharma et al. (2014) pointed out that building effective phishing detection mechanisms for every OSN to protect its users is important because phishing attacks cause the leak of personal information and the loss of huge money. As such, this implies that the efficiency of response time to alert users especially on Twitter about phishing is an important factor. However, the maximum response time achieved by the existing solutions is still considered high and the one claimed achieving the lowest maximum response time of 0.501 seconds (Sharma et al., 2014) is deemed to be inadequate and shall be improved with a new security alert solution for Twitter users.

1.3 Research Objectives

The main objective of this research is to propose a security alert framework using dynamic tweet-based features for phishing detection on Twitter. To achieve this main objective, the specific objectives as follows are set for the research.

i. To propose a classification model with reduced number of classification features to improve the accuracy of phishing detection.

ii. To propose a detection algorithm with dynamic tweet-based features to enhance the accuracy of phishing tweet detection on Twitter.

iii. To propose a security alert mechanism with fast response time to improve the efficiency of phishing tweet detection.

1.4 Research Scope

The scope of this research focuses on machine learning of phishing tweet detection on Twitter and more specifically, formulates a security alert framework with the improvement of phishing detection accuracy, enhancement of phishing tweet detection accuracy on Twitter, and improvement of phishing tweet detection efficiency.

Deceptive phishing is a highly common phishing attack type as its attack tactic used is simple. It has to be tackled dynamically because it is a major problem in instant messengers (Ali & Rajamani , 2012) and Online Social Networks (OSNs). Basically, deceptive phishing deceives victims by directing them to a fake website where their personal credentials are collected eventually for further unlawful activities. As such, it is being selected as the main focus of this research.

Twitter is selected among all the other OSNs for this research because it is the fastest growing (McCord & Chuah, 2011; Kumar R & Kumar, 2012) and an immensely popular OSN that only provides micro-blogging to people to post 140 characters short messages called “Tweets” (Wang, 2010; McCord & Chuah, 2011; Aggarwal et al., 2012; Lee & Kim, 2013; Nair & Prema, 2014; Sharma et al., 2014). In addition, it is a popular medium used by phishers to spread phishing attacks due to its vast information dissemination and its difficulty to be detected unlike email because of it spreads fast in the network, has short content size and uses short Uniform Resource Locators (URLs) (Aggarwal et al., 2012; Sharma et al., 2014).

The following Figure 1.1 shows the summary of the research area towards the research scope.

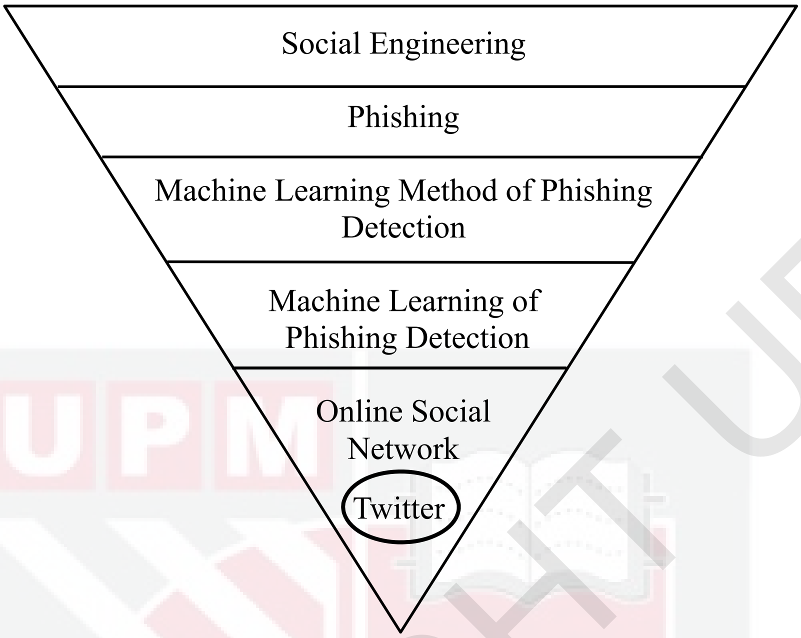
Social Engineering
Phishing
Machine Learning Method of Phishing Detection
Machine Learning of Phishing Detection
Online Social Network
Twitter

Figure 1.1 : Summary of Research Area towards Research Scope

Generally, the formulated security alert framework is based on the general phishing tweet detection adopted by a number of researchers (Aggarwal et al., 2012; Nair & Prema, 2014; Sharma et al., 2014). This framework comprises three phases namely classification model of phishing detection, detection algorithm of phishing tweet detection and security alert mechanism of phishing tweet detection.

In the classification model of phishing detection phase, an evaluation of classification accuracy using six machine learning techniques of Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Random Forest (RF), Decision Tree (DT), Logistic Regression (LR) and Sequential Minimal Optimization (SMO) which is claimed as the best machine learning techniques by the respective researchers (Toolan & Carthy, 2009; Fahmy & Ghoneim, 2011; Aggarwal et al., 2012; Zhang & Wang, 2012; Lakshmi & Vijaya MS, 2012; James et al., 2013; Akinyelu & Adewumi, 2014; Basnet et al., 2014; Sharma et al., 2014; Akanbi et al., 2015; Aydin & Baykal, 2015; Sananse & Sarode, 2015) is conducted. The evaluation also used the training dataset collected from Sharma et al. (2014), the possible extracted phishing classification features, ten fold cross-validation and the accuracy of 94.56% (targeted baseline) achieved by Sharma et al. (2014) on the same training dataset. To identify the best machine learning technique, standard information retrieval metrics namely accuracy, precision and recall, and a Confusion Matrix are used. The purpose of such evaluation is to determine the best machine learning technique with the best phishing classification features in order to produce and generate a classification model. This model is then embedded into a proposed detection algorithm together with the inclusion of dynamic tweet-based features using a new approach in the detection algorithm of phishing tweet detection phase. Subsequently, in the security alert mechanism of phishing tweet detection phase, a proposed security alert mechanism is formulated to integrate with the proposed detection algorithm to improve the efficiency of the phishing tweet detection response time for alerting users on Twitter.

This research also includes on experimental study to analyse the phishing detection accuracy comparison between the produced and generated classification model (with reduced number of classification features) and 94.56% achieved by Sharma et al. (2014), the phishing tweet detection accuracy on Twitter comparison between the formulated detection algorithm (with dynamic tweet-based features) and the Web Framework (Sharma et al., 2014), and the phishing tweet detection efficiency comparison between the formulated security alert mechanism (with fast response time) and the Web Framework (Sharma et al., 2014).

The research is delimited to two main components covering analysis and identification of problem, and formation of security alert framework. They will be discussed further in the following chapters and sections.

1.5 Research Contributions

The main contribution of this research is to formulate a security alert framework using dynamic tweet-based features for phishing detection on Twitter, with specific contributions as follows:

i. A classification model with reduced number of classification features improving the phishing detection accuracy.

ii. A detection algorithm with dynamic tweet-based features enhancing the phishing tweet detection accuracy on Twitter.

iii. A security alert mechanism with fast response time improving the phishing tweet detection efficiency.

1.6 Thesis Organisation

The remaining of this thesis is organised in the following manner:

Chapter 2 discusses the aspects that were covered in the literature review. It starts off with a discussion of the fundamentals of social engineering, covering its trends, approaches and types. Then, it talks about phishing, covering topics such as trends, types, attacks platforms and detection methods (such as blacklists, heuristics, visual similarity and machine learning). Thereafter, it is followed by an in-depth discussion on phishing detection method of machine learning, covering machine learning techniques such as Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Random Forest (RF), Decision Tree (DT), Logistic Regression (LR), Sequential Minimal Optimization (SMO), Naive Bayes (NB) and Multilayer Perceptron (MLP), and machine learning classification features for phishing detection, discussions on related works in machine learning of phishing tweet detection on Twitter covering machine learning technique of RF, general phishing tweet detection framework and existing problems of phishing tweet detection on Twitter in term of number of classification features, dynamic tweet-based features (Twitter data) and response time. This chapter ends with the discussions on the differences between the research work and existing works.

Chapter 3 explains about the methodology adopted for this research. It highlights two main components covering four phases. The first component is analysis and identification of problem (Phase 1) where potential problems for the research are explored and research objectives are formed. The second component, on the other hand, is about the formulation of security alert framework comprising classification model of phishing detection (Phase 2), detection algorithm of phishing tweet detection (Phase 3), and security alert mechanism of phishing tweet detection (Phase 4). The second component is the core component for this research where final targeted research objectives and research contributions are to be achieved eventually. In this chapter, the details of all phases are explained.

Chapter 4 presents the classification model of phishing detection. Security alert framework and its details focusing particularly on classification model are explained. In addition, this chapter discusses and explains the classification model design including its flowchart of production and generation, and experimental design, and its experimental results and discussion.

Chapter 5 presents the detection algorithm of phishing tweet detection. Similar to Chapter 4, security alert framework and its details focusing particularly on detection algorithm are explained. In addition, this chapter discusses and explains the detection algorithm design including its flowchart and experimental design, and its experimental results and discussion.

Chapter 6 presents the security alert mechanism of phishing tweet detection. Similar to Chapter 4 and Chapter 5, security alert framework and its details focusing particularly on security alert mechanism are explained. In addition, this chapter discusses and explains the security alert mechanism design including its flowchart and experimental design, and its experimental results and discussion.

Chapter 7 summarises the research along with the overall conclusion. In addition to the conclusion, future works are discussed in this chapter. This chapter is a last chapter for this thesis.

REFERENCES

Aaron, G., & Rasmussen, R. (2017). *APWG - Global Phishing Survey: Trends And Domain Name Use in 2016*. Retrieved from https://docs.apwg.org/reports/APWG_Global_Phishing_Report_2015-2016.pdf

Abdelhamid, N., Thabtah, F., & Faculty, H. A. (2017). Phishing Detection: A Recent Intelligent Machine Learning Comparison Based On Models Content And Features. *IEEE*, 72–77.

Aggarwal, A., Rajadesingan, A., & Kumaraguru, P. (2012). PhishAri: Automatic Realtime Phishing Detection On Twitter. *ECrime Researchers Summit, ECrime*, 1–12. https://doi.org/10.1109/eCrime.2012.6489521

Akanbi, O. A., Amiri, I. S., & Fazeldehkordi, E. (2015). *A Machine-Learning Approach To Phishing Detection And Defense*. https://doi.org/10.1016/B978-0-12-802927-5.00002-2

Akinyelu, A. A., & Adewumi, A. O. (2014). Classification Of Phishing Email Using Random Forest Machine Learning Technique. *Journal of Applied Mathematics*, *2014*. https://doi.org/10.1155/2014/425731

Al-Garadi, M. A., Varathan, K. D., & Ravana, S. D. (2016). Cybercrime Detection In Online Communications: The Experimental Case Of Cyberbullying Detection In The Twitter Network. *Computers in Human Behavior*, *63*, 433–443. https://doi.org/10.1016/j.chb.2016.05.051

Al-janabi, M., Quincey, E. De, & Andras, P. (2017). Using Supervised Machine Learning Algorithms To Detect Suspicious URLs In Online Social Networks. *2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 1104–1111.

Al-Zoubi, A. M., Alqatawna, J., & Faris, H. (2017). Spam Profile Detection In Social Networks Based On Public Features. *2017 8th International Conference on Information and Communication Systems (ICICS)*, 130–135. https://doi.org/10.1109/IACS.2017.7921959

Alexandre Kowalczyk - SVM. (n.d.). Support Vector Machine Tutorial. Retrieved May 15, 2016, from https://www.svm-tutorial.com/2017/02/svms-overview-support-vector-machines/

Algarni, A., Xu, Y., Chan, T., & Tian, Y.-C. (2013). Social Engineering In Social Networking Sites: Affect-Based Model. *The 8th International Conference for Internet Technology and Secured Transactions*, 508–515.

Ali, M. M., & Rajamani, L. (2012). APD: ARM Deceptive Phishing Detector System Phishing Detection In Instant Messengers Using Data Mining Approach. *Communications in Computer and Information Science*, 490–502. https://doi.org/10.1007/978-3-642-29219-4_56

Alkhateeb, F., Manasrah, A. M., & Bsoul, A. A. R. (2012). Bank Web Sites Phishing Detection And Notification System Based On Semantic Web Technologies. *International Journal of Security and Its Applications*, *6*(4), 53–66.

Amato, F., Castiglione, A., Santo, A. De, Moscato, V., Picariello, A., Persia, F., & Sperli, G. (2017). Recognizing Human Behaviours In Online Social Networks. *Computers & Security*. https://doi.org/10.1016/j.cose.2017.06.002

Anti-Phishing Working Group (APWG). (n.d.). Retrieved May 1, 2016, from http://www.antiphishing.org/

Arachchilage, N. A. G., & Love, S. (2013). A Game Design Framework For Avoiding Phishing Attacks. *Computers in Human Behavior*, *29*(3), 706–714. https://doi.org/10.1016/j.chb.2012.12.018

Arachchilage, N. A. G., & Love, S. (2014). Security Awareness Of Computer Users: A Phishing Threat Avoidance Perspective. *Computers in Human Behavior*, *38*, 304–312. Retrieved from http://dx.doi.org/10.1016/j.chb.2014.05.046

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing Threat Avoidance Behaviour: An Empirical Investigation. *Computers in Human Behavior*, *60*, 185–197. https://doi.org/10.1016/j.chb.2016.02.065

Aydin, M., & Baykal, N. (2015). Feature Extraction And Classification Phishing Websites Based On URL. *2015 IEEE Conference on Communications and NetworkSecurity, CNS 2015*, 769–770. https://doi.org/10.1109/CNS.2015.7346927

Basnet, R. B., Sung, A. H., & Liu, Q. (2014). Learning To Detect Phishing URLs. *IJRET: International Journal of Research in Engineering and Technology*, *3*(6), 11–24. https://doi.org/10.1109/ICMLA.2012.104

Benevenuto, F., Magno, G., Rodrigues, T., & Almeida, V. (2010). Detecting Spammers On Twitter. *Collaboration, Electronic Messaging, Anti-Abuse and Spam Conference (CEAS)*, *6*, 12. https://doi.org/10.1.1.297.5340

Bezuidenhout, M., Mouton, F., & Venter, H. S. (2010). Social Engineering Attack Detection Model: SEADM. *Information Security for South Africa*, 1–8.

Bhakta, R., & Harris, I. G. (2015). Semantic Analysis Of Dialogs To Detect Social Engineering Attacks. *Proceedings of the 2015 IEEE 9th International Conference on Semantic Computing, IEEE ICSC 2015*, 424–427. https://doi.org/10.1109/ICOSC.2015.7050843

Calabresi, M. (2017). Time Magazine - Inside Russia's Social Media War On America. Retrieved November 16, 2017, from http://time.com/4783932/inside-russia-social-media-war-america/

Chawla, M., & Chouhan, S. S. (2014). A Survey Of Phishing Attack Techniques. *International Journal of Computer Applications*, *93*(3), 1–4.

Chao Chen, Wang, Y., Zhang, J., Xiang, Y., Zhou, W., & Min, G. (2017). Statistical Features-Based Real-Time Detection Of Drifted Twitter Spam. *IEEE Transactions on Information Forensics and Security*, *12*(4), 914–925. https://doi.org/10.1109/TIFS.2016.2621888

Chiew, K. L., Chang, E. H., Sze, S. N., & Tiong, W. K. (2015). Utilisation Of Website Logo For Phishing Detection. *Computers and Security*, *54*, 16–26. https://doi.org/10.1016/j.cose.2015.07.006

Chitrey, A., Singh, D., Bag, M., & Singh, V. (2012). A Comprehensive Study Of Social Engineering Based Attacks In India To Develop A Conceptual Model. *International Journal of Information & Network Security (IJINS)*, *1*(2), 45–53. Retrieved from http://iaesjournal.com/online/index.php/

Computer Associates. (n.d.). Types Of Phishing Attacks. Retrieved May 1, 2016, from http://www.pcworld.com/article/135293/article.html

Cook, D. L., Gurbani, V. K., & Daniluk, M. (2008). Phishwish: A Stateless Phishing Filter Using Minimal Rules. *FC*, 182–186. https://doi.org/10.1007/978-3-540-85230-8_15

Coronges, K., Dodge, R., Mukina, C., Radwick, Z., Shevchik, J., & Rovira, E. (2012). The Influences Of Social Networks On Phishing Vulnerability. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2366–2373. https://doi.org/10.1109/HICSS.2012.657

Cuzzocrea, A., Martinelli, F., & Mercaldo, F. (2018). Applying Machine Learning Techniques To Detect And Analyze Web Phishing Attacks. A*ssociation for Computing Machinery*, 355–359. https://doi.org/10.1145/3282373.3282422

Dadkhah, M., Sutikno, T., Jazi, M. D., & Stiawan, D. (2015). An Introduction To Journal Phishings And Their Detection Approach. *Telkomnika (Telecommunication Computing Electronics and Control)*, *13*(2), 373–380. https://doi.org/10.12928/TELKOMNIKA.v13i2.1436

Dash, M., & Liu, H. (1997). Feature Selection For Classification. *Intelligent Data Analysis*, *1*(3), 131–156. https://doi.org/10.3233/IDA-1997-1302

Davinson, N., & Sillence, E. (2010). It Won't Happen To Me: Promoting Secure Behaviour Among Internet Users. *Computers in Human Behavior*, *26*(6), 1739–1747. https://doi.org/10.1016/j.chb.2010.06.023

Devmane, M. A., & Rana, N. K. (2014). Detection And Prevention Of Profile Cloning In Online Social Networks. *International Conference on Recent Advances and Innovations in Engineering, ICRAIE 2014*. https://doi.org/10.1109/ICRAIE.2014.6909237

Ebubekir Buber, O. D., & Ozgur Koray Sahingoz. (2017). Feature Selections For The Machine Learning Based Detection Of Phishing Websites. *IDAP 2017 - International Artificial Intelligence and Data Processing Symposium*. https://doi.org/10.1109/IDAP.2017.8090317

Fahmy, H., & Ghoneim, S. (2011). PhishBlock: A Hybrid Anti-Phishing Tool. *2011 International Conference on Communications, Computing and Control Applications, CCCA 2011*, 2–6. https://doi.org/10.1109/CCCA.2011.6031523

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online Social Networks: Threats And Solutions. *IEEE Communication Surveys & Tutorials Online*, *16*(4), 2019–2036. https://doi.org/10.1109/COMST.2014.2321628

Frauenstein, E. D., & Flowerday, S. V. (2016). Social Network Phishing: Becoming Habituated To Clicks And Ignorant To Threats? *2016 Information Security for South Africa - Proceedings of the 2016 ISSA Conference*, 98–105. https://doi.org/10.1109/ISSA.2016.7802935

Fu, A. Y., Wenyin, L., & Deng, X. (2006). Detecting Phishing Web Pages With Visual Similarity Assessment Based On Earth Mover's Distance (EMD). *IEEE Transactions on Dependable and Secure Computing*, *3*(4), 301–311. https://doi.org/10.1109/TDSC.2006.50

Gang Liu, Qiu, B., & Wenyin, L. (2010). Automatic Detection Of Phishing Target From Phishing Webpage. *Proceedings - International Conference on Pattern Recognition*, 4153–4156. https://doi.org/10.1109/ICPR.2010.1010

Gonzalez, J. J., Sarriegi, J. M., & Gurrutxaga, A. (2006). A Framework For Conceptualizing Social Engineering Attacks. *CRITIS*, 79–90. https://doi.org/10.1007/11962977_7

Google Safe Browsing. (n.d.). Retrieved May 15, 2016, from https://safebrowsing.google.com/

Gowtham, R., & Krishnamurthi, I. (2014). A Comprehensive And Efficacious Architecture For Detecting Phishing Webpages. *Computers and Security*, *40*, 23–37. https://doi.org/10.1016/j.cose.2013.10.004

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis Of Unintentional Insider Threats Deriving From Social Engineering Exploits. *Proceedings - IEEE Symposium on Security and Privacy*, 236–250. https://doi.org/10.1109/SPW.2014.39

Gulati, R. (2003). The Threat Of Social Engineering And Your Defense Against It. *Information Security*, 1–15. Retrieved from https://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2017). Defending Against Phishing Attacks: Taxonomy Of Methods, Current Issues And Future Directions. *Telecommunication Systems*. https://doi.org/10.1007/s11235-017-0334-z

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2016). Fighting Against Phishing Attacks: State Of The Art And Future Challenges. *Neural Computing and Applications*, 1–26. https://doi.org/10.1007/s00521-016-2275-y

Hara, M., Yamada, A., & Miyake, Y. (2009). Visual Similarity-Based Phishing Detection Without Victim Site Information. *2009 IEEE Symposium on Computational Intelligence in Cyber Security, CICS 2009 - Proceedings*. https://doi.org/10.1109/CICYBS.2009.4925087

Hasle, H., Kristiansen, Y., Kintel, K., & Snekkenes, E. (2005). Measuring Resistance To Social Engineering. *Information Security Practice and Experience*, 132–143. https://doi.org/10.1007/978-3-540-31979-5_12

Heikkinen, S. (2006). Social Engineering In The World Of Emerging Communication Technologies. *Proceedings of Wireless World Research Forum*, 1–10.

Hira, Z. M., & Gillies, D. F. (2015). A Review Of Feature Selection And Feature Extraction Methods Applied On Microarray Data. *Advances in Bioinformatics*, *2015*(1). https://doi.org/10.1155/2015/198363

Hodzic, A., Kevric, J., & Karadag, A. (2016). Comparison Of Machine Learning Techniques In Phishig Website Classification. *ICESoS 2016 - Proceedings Book*, 249–256. Retrieved from http://eprints.ibu.edu.ba/3308/1/Adnan Hodzic Jasmin Kevric and Adem Karadag.pdf

Huan Liu & Yu, L. (2005). Toward Integrating Feature Selection Algorithms For Classification And Clustering. *IEEE Transactions on Knowledge and Data Engineering*, *17*(4), 491–502. https://doi.org/10.1109/TKDE.2005.66

Huang, H., Tan, J., & Liu, L. (2009). Countermeasure Techniques For Deceptive Phishing Attack. *2009 International Conference on New Trends in Information and Service Science*, 636–641. https://doi.org/10.1109/NISS.2009.80

Huu Hieu Nguyen, & Duc Thai Nguyen. (2016). Machine Learning Based Phishing Web Sites Detection. *Lecture Notes in Electrical Engineering,* 371, 123–131. https://doi.org/10.1007/978-3-319-27247-4_11

InnovateUs. (n.d.). What Are The Different Types Of Phishing Attacks? Retrieved May 1, 2016, from http://www.innovateus.net/science/what-are-different-types-phishing-attacks

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social Phishing. *Communications of the ACM*, *50*(10), 94–100. https://doi.org/10.1145/1290958.1290968

Jain, A. K., & Gupta, B. B. (2018). Towards Detection Of Phishing Websites On Client-Side Using Machine Learning Based Approach. *Telecommunication Systems,* 68(4), 687–700. https://doi.org/10.1007/s11235-017-0414-0

James, J., L., S., & Thomas, C. (2013). Detection Of Phishing URLs Using Machine Learning Techniques. *2013 International Conference on Control Communication and Computing, ICCC 2013*, 304–309. https://doi.org/10.1109/ICCC.2013.6731669

Janczewski, L. J., & Fu, L. (Rene). (2010). Social Engineering-Based Attacks: Model And New Zealand Perspective. *Proceedings of the International Multiconference on Computer Science and Information Technology*, 847–853.

Jeeva, S. C., & Rajsingh, E. B. (2017). Phishing URL Detection-Based Feature Selection To Classifiers. *International Journal of Electronic Security and Digital Forensics*, 9(2), 116. https://doi.org/10.1504/ijesdf.2017.083979

Joshi, Y., Saklikar, S., Das, D., & Saha, S. (2008). PhishGuard: A Browser Plug-In For Protection From Phishing. *IMSAA'08 - 2nd International Conference on Internet Multimedia Services Architecture and Application*, 1–6. https://doi.org/10.1109/IMSAA.2008.4753929

Junger, M., Montoya, L., & Overink, F.-J. (2017). Priming And Warnings Are Not Effective To Prevent Social Engineering Attacks. *Computers in Human Behavior*, *66*, 75–87. https://doi.org/10.1016/j.chb.2016.09.012

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing Detection: A Literature Survey. *IEEE Communications Surveys and Tutorials*, *15*(4), 2091–2121. https://doi.org/10.1109/SURV.2013.032213.00009

Khonji, M., Jones, A., & Iraqi, Y. (2011). A Novel Phishing Classification Based On URLFeatures. *2011 IEEE GCC Conference and Exhibition, GCC 2011*, 221–224. https://doi.org/10.1109/IEEEGCC.2011.5752505

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced Social Engineering Attacks. *Journal of Information Security and Applications*, *22*, 113–122. Retrieved from https://pdfs.semanticscholar.org/3266/f05e2e5e785cbab72d2e378059ecc62ef706.pdf

Kuan-Ta Chen, Chen, J.-Y., Huang, C.-R., & Chen, C.-S. (2009). Fighting Phishing With Discriminative Keypoint Features Of Webpages. *IEEE Internet Computing*, *13*(3), 56–63. https://doi.org/10.1109/MIC.2009.59

Kuan-Ta Chen, Huang, C.-R., Chen, C.-S., & Chen, J.-Y. (2009). Fighting Phishing With Discriminative Keypoint Features. *IEEE Internet Computing*, *13*(3), 56–63. https://doi.org/10.1109/MIC.2009.59

Kulkarni, S. S., Tomar, M., Mittal, A., Arondekar, S., & Nayakawadi, A. (2015). Survey On Phishing Attacks. *International Journal of Advanced Research in Computer Science and Software Engineering*, *5*(2), 501–504.

Kumar R, A., & Kumar, S. (2012). Twitter Spamming: Techniques And Defence Approaches. *International Journal of Applied Engineering Research*, *7*(11), 2077–2081.

Kwak, H., Lee, C., Park, H., & Moon, S. (2010). What Is Twitter, A Social Network Or A News Media? *The International World Wide Web Conference Committee (IW3C2)*, 1–10. https://doi.org/10.1145/1772690.1772751

Lakshmi V, S., & Vijaya MS. (2012). Efficient Prediction Of Phishing Websites Using Supervised Learning Algorithms. *Procedia Engineering*, *30*(2011), 798–805. https://doi.org/10.1016/j.proeng.2012.01.930

Lee, S., & Kim, J. (2013). Warningbird: A Near Real-Time Detection System For Suspicious URLs In Twitter Stream. *IEEE Transactions on Dependable and Secure Computing*, *10*(3), 183–195. https://doi.org/10.1109/TDSC.2013.3

Maan, P. S., & Sharma, M. (2012). Social Engineering: A Partial Technical Attack. *IJCSI International Journal of Computer Science*, *9*(2), 557–559. Retrieved from http://www.ijcsi.org/papers/IJCSI-9-2-3-557-559.pdf

Mandal, M., & Mukhopadhyay, A. (2013). An Improved Minimum Redundancy Maximum Relevance Approach For Feature Selection In Gene Expression Data. *Procedia Technology*, *10*, 20–27. https://doi.org/10.1016/j.protcy.2013.12.332

Marchal, S., Francois, J., State, R., & Engel, T. (2014). PhishStorm: Detecting Phishing With Streaming Analytics. *IEEE Transactions on Network and Service Management*, *11*(4), 458–471. https://doi.org/10.1109/TNSM.2014.2377295

Mataracioglu, T., & Ozkan, S. (2011). User Awareness Measurement Through Social Engineering. *ArXiv E-Prints*, 1–7. Retrieved from http://arxiv.org/abs/1108.2149

MATLAB. (n.d.). Retrieved October 1, 2016, from https://uk.mathworks.com/products/matlab.html

Maurer, M.-E., & Herzner, D. (2012). Using Visual Website Similarity For Phishing Detection And Reporting. *Proceedings of the 2012 ACM Annual Conference Extended Abstracts on Human Factors in Computing Systems Extended Abstracts - CHI EA '12*, 1625. https://doi.org/10.1145/2212776.2223683

Mazher, N., Ashraf, I., & Altaf, A. (2013). Which Web Browser Work Best For Detecting Phishing. *ICICT 2013 - Proceedings of the 2013 5th International Conference on Information and Communication Technologies: Using Technology to Create a Better World*. https://doi.org/10.1109/ICICT.2013.6732784

McCord, M., & Chuah, M. (2011). Spam Detection On Twitter Using Traditional Classifiers. *ATC*, 175–186. https://doi.org/10.1007/978-3-642-23496-5_13

Meda, C., Bisio, F., Gastaldo, P., & Diten, R. Z. (2014). Machine Learning Techniques Applied To Twitter Spammers Detection. *Recent Advances in Electrical and Electronic Engineering*, 177–182.

Medvet, E., Kirda, E., & Kruegel, C. (2008). Visual-Similarity-Based Phishing Detection. *Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks - SecureComm '08*, 1. https://doi.org/10.1145/1460877.1460905

Meister, E., & Biermann, E. (2008). Implementation Of A Socially Engineered Worm To Increase Information Security Awareness. *Proceedings - 3rd International Conference on Broadband Communications, Informatics and Biomedical Applications, BroadCom 2008*, 343–350. https://doi.org/10.1109/BROADCOM.2008.68

Mohammad, R. M., Thabtah, F., & Mccluskey, L. (2013). Phishing Websites Features. *IEEE*.

Moreno-Fernandez, M. M., Blanco, F., Garaizar, P., & Matute, H. (2017). Fishing For Phishers. Improving Internet Users' Sensitivity To Visual Deception Cues To Prevent Electronic Fraud. *Computers in Human Behavior*, *69*, 421–436. https://doi.org/10.1016/j.chb.2016.12.044

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social Engineering Attack Framework. *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference*. https://doi.org/10.1109/ISSA.2014.6950510

Nagy, J., & Pecho, P. (2009). Social Networks Security. *Proceedings - 2009 3rd International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2009*, 321–325. https://doi.org/10.1109/SECURWARE.2009.56

Nair, M. C., & Prema, S. (2014). A Distributed System For Detecting Phishing In Twitter Stream. *International Journal of Engineering Science and Innoavtive Technology (IJESIT)*, *3*(2), 151–158.

Nigerianspam. (n.d.). Phishing Attacks - Types Of Phishing Attacks. Retrieved May 1, 2016, from http://www.nigerianspam.com/Phishing-Types.html

Nyamsuren, E., & Choi, H.-J. (2007). Preventing Social Engineering In Ubiquitous Environment. *Future Generation Communication and Networking (FGCN 2007)*, 573–577. https://doi.org/10.1109/FGCN.2007.185

Ola Soder - KNN. (n.d.). KNN Classifiers 1. What Is A KNN Cassifier? Retrieved May 15, 2016, from http://www.fon.hum.uva.nl/praat/manual/kNN_classifiers_1__What_is_a_kNN_classifier_.html

Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2016). Identification And Evaluation Of Discriminative Lexical Features Of Malware URL For Real-Time Classification. *Proceedings - 6th International Conference on Computer and Communication Engineering: Innovative Technologies to Serve Humanity, ICCCE 2016*, 90–95. https://doi.org/10.1109/ICCCE.2016.31

Phishing Trends & Intelligence (PTI) report. (2017). *PhishLabs - 2017 Phishing Trends &amp; Intelligence Report: Hacking Tthe Human*. Retrieved from https://pages.phishlabs.com/rs/130-BFB-942/images/2017 PhishLabs Phishing and Threat Intelligence Report.pdf

PhishLabs. (n.d.). Retrieved October 26, 2017, from https://www.phishlabs.com/

PhishTank. (n.d.). Retrieved May 15, 2016, from https://www.phishtank.com/

Prakash, P., Kumar, M., Kompella, R. R., & Gupta, M. (2010). PhishNet: Predictive Blacklisting To Detect Phishing Attacks. *Proceedings - IEEE INFOCOM*. https://doi.org/10.1109/INFCOM.2010.5462216

Proofpoint. (n.d.). Retrieved October 26, 2017, from https://www.proofpoint.com/us

Q4 2016 & Year In Review : Threat Summary report. (2017). *Proofpoint - Q4 2016 & Year In Review: Threat Summary*. Retrieved from https://www.proofpoint.com/sites/default/files/proofpoint_q4_threat_report-final- cm.pdf

Sadeghian, A., Zamani, M., & Shanmugam, B. (2013). Security Threats In Online Social Networks. *2013 International Conference on Informatics and Creative Multimedia*, 254–258. https://doi.org/10.1109/ICICM.2013.50

Sananse, B. E., & Sarode, T. K. (2015). Phishing URL Detection: A Machine Learning And Web Mining-Based Approach. *International Journal of Computer Applications*, *123*(13), 46–50.

Serafettin Senturk, E. Y. K., & Sogukpmar, I. (2017). Email Phishing Detection And Prevention By Using Data Mining Techniques. *2nd International Conference on Computer Science and Engineering, UBMK 2017*, 707–712. https://doi.org/10.1109/UBMK.2017.8093510

Sharifi, M., & Siadati, S. H. (2008). A Phishing Sites Blacklist Generator. *AICCSA 08 - 6th IEEE/ACS International Conference on Computer Systems and Applications*, 840–843. https://doi.org/10.1109/AICCSA.2008.4493625

Sharma, N., Sharma, N., Tiwari, V., Chahar, S., & Maheshwari, S. (2014). Real-Time Detection Of Phishing Tweets. *Fourth International Conference on Computer Science, Engineering and Applications*, 215–227. https://doi.org/10.5121/csit.2014.4727

Shekokar, N. M., Shah, C., Mahajan, M., & Rachh, S. (2015). An Ideal Approach For Detection And Prevention Of Phishing Attacks. *Procedia Computer Science*, *49*(1), 82–91. https://doi.org/10.1016/j.procs.2015.04.230

Sheng, S., Wardman, B., Warner, G., Cranor, L. F., Hong, J., & Zhang, C. (2009). An Empirical Analysis Of Phishing Blacklists. *The 6th Conference in Email and Anti-Spam, Ser. CEAS'09*. Retrieved from http://repository.cmu.edu/hcii%5Cnhttp://repository.cmu.edu/hcii/282

Shigang Liu, Wang, Y., Zhang, J., Chen, C., & Xiang, Y. (2017). Addressing The Class Imbalance Problem In Twitter Spam Detection Using Ensemble Learning. *Computers & Security*, *69*, 35–49. https://doi.org/10.1016/j.cose.2016.12.004

Shigang Liu, Zhang, J., & Xiang, Y. (2016). Statistical Detection Of Online Drifting Twitter Spam. *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security - ASIA CCS '16*, 1–10. https://doi.org/10.1145/2897845.2897928

Silic, M., & Back, A. (2016). The Dark Side Of Social Networking Sites: Understanding Phishing Risks. *Computers in Human Behavior*, *60*, 35–43. https://doi.org/10.1016/j.chb.2016.02.050

Skymind - MLP. (n.d.). Multilayer Perceptrons. Retrieved May 15, 2016, from https://deeplearning4j.org/multilayerperceptron

Statistics Solutions - LR. (n.d.). What Is Logistic Regression? Retrieved May 15, 2016, from http://www.statisticssolutions.com/what-is-logistic-regression/

Sunil, A. N. V., & Sardana, A. (2012). A PageRank Based Detection Technique For Phishing Web Sites. *2012 IEEE Symposium on Computers and Informatics, ISCI 2012*, 58–63. https://doi.org/10.1109/ISCI.2012.6222667

Sureshkumar M.E, Palanisamy, S., & Sowmiya.R.A, S. (2013). Data Isolation And Protection In Online Social Networks. *2013 International Conference on Information Communication and Embedded Systems, ICICES 2013*, 150–155. https://doi.org/10.1109/ICICES.2013.6508228

Tang, J., Alelyani, S., & Liu, H. (2014). Feature Selection For Classification: A Review. *Data Classification: Algorithms and Applications*, 37–64. https://doi.org/10.1.1.409.5195

Toolan, F., & Carthy, J. (2009). Phishing Detection Using Classifier Ensembles. *2009 ECrime Researchers Summit, ECRIME '09*. https://doi.org/10.1109/ECRIME.2009.5342607

Tout, H., & Hafner, W. (2009). Phishpin: An Identity-Based Anti-Phishing Approach. *Proceedings - 12th IEEE International Conference on Computational Science and Engineering, CSE 2009*, *3*, 347–352. https://doi.org/10.1109/CSE.2009.306

Usha, M., & Deepika, P. (2014). Phishing - A Challenge In The Internet. *International Journal of Computer Science and Information Technologies*, *5*(1), 260–263.

Varshney, G., Misra, M., & Atrey, P. K. (2016). A Phish Detector Using Lightweight Search Features. *Computers and Security*, *62*, 213–228. https://doi.org/10.1016/j.cose.2016.08.003

Vasek, M., Wadleigh, J., & Moore, T. (2015). Hacking Is Not Random: A Case-Control Study Of Webserver Compromise Risk. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 206--219. https://doi.org/10.7910/DVN/25608

Wang, A. H. (2010). Don't Following Me: Spam Detection In Twitter. *Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference, 2010*.

Web of Trust (MyWOT). (n.d.). Retrieved May 15, 2016, from https://www.mywot.com/

WEKA's Documentary. (n.d.). Retrieved January 25, 2017, from http://weka.sourceforge.net/doc.dev/index-all.html

WEKA. (n.d.). Retrieved January 25, 2017, from https://www.cs.waikato.ac.nz/ml/weka/

Wenyin, L., Liu, G., Qiu, B., & Quan, X. (2012). Antiphishing Through Phishing Target Discovery. *IEEE Internet Computing*, *16*(2), 52–60. https://doi.org/10.1109/MIC.2011.103

Wikipedia - DT. (n.d.). Decision Tree Learning (DT). Retrieved May 15, 2016, from https://en.wikipedia.org/wiki/Decision_tree_learning

Wikipedia - KNN. (n.d.). K-Nearest Neighbors Algorithm (KNN). Retrieved May 15, 2016, from https://en.wikipedia.org/wiki/K-nearest_neighbors_algorithm

Wikipedia - LR. (n.d.). Logistic Regression (LR). Retrieved May 15, 2016, from https://en.wikipedia.org/wiki/Logistic_regression

Wikipedia - MLP. (n.d.). Multilayer Perceptron (MLP). Retrieved May 15, 2016, from https://en.wikipedia.org/wiki/Multilayer_perceptron

Wikipedia - NB. (n.d.). Naive Bayes Classifier (NB). Retrieved May 15, 2016, from https://en.wikipedia.org/wiki/Naive_Bayes_classifier

Wikipedia - RF. (n.d.). Random Forest (RF). Retrieved May 15, 2016, from https://en.wikipedia.org/wiki/Random_forest

Wikipedia - SMO. (n.d.). Sequential Minimal Optimization (SMO). Retrieved May 15, 2016, from https://en.wikipedia.org/wiki/Sequential_minimal_optimization

Wikipedia - SVM. (n.d.). Support Vector Machine (SVM). Retrieved May 15, 2016, from https://en.wikipedia.org/wiki/Support_vector_machine

Wilcox, H., & Bhattacharya, M. (2015). Countering Social Engineering Through Social Media: An Enterprise Security Perspective. *ICCCI*, 54–64. https://doi.org/10.1007/978-3-319-24306-1_6

Wood, I. (2015). A Case Study Of Collecting Dynamic Social Data: The Pro-Ana Twitter Community. *Australian Journal of Intelligent Information Processing Systems*.

You Chen, Li, Y., Cheng, X.-Q., & Guo, L. (2006). Survey And Taxonomy Of Feature Selection Algorithms In Intrusion Detection System. *Information Security and Cryptology*, *4318*, 153–167. https://doi.org/10.1007/11937807_13

Yu, W. D., Nargundkar, S., & Tiruthani, N. (2009). PhishCatch - A Phishing Detection Tool. *2009 33rd Annual IEEE International Computer Software and Applications Conference*, *2*, 451–456. https://doi.org/10.1109/COMPSAC.2009.175

Yuan, H., Chen, X., Li, Y., Yang, Z., & Liu, W. (2018). Detecting Phishing Websites And Targets Based On URLs And Webpage Links. *Proceedings - International Conference on Pattern Recognition*, 2018–Augus, 3669–3674. https://doi.org/10.1109/ICPR.2018.8546262

Yue, Z., Hong, J., & Cranor, L. (2007). Cantina: A Content-Based Approach To Detecting Phishing Web Sites. *International Conference on World Wide Web*, 639–648. https://doi.org/10.1145/1242572.1242659

Zareapoor, M., & Seeja, K. R. (2015). Text Mining For Phishing E-mail Detection. *Advances in Intelligent Systems and Computing*, 65–71. https://doi.org/10.1007/978-81-322-2012-1_8

Zhang, J., & Wang, Y. (2012). A Real-Time Automatic Detection Of Phishing URLs. *Proceedings of 2nd International Conference on Computer Science and Network Technology, ICCSNT 2012*, 1212–1216. https://doi.org/10.1109/ICCSNT.2012.6526142

Zhao, Z., Morstatter, F., Sharma, S., Alelyani, S., Anand, A., & Liu, H. (2010). Advancing Feature Selection Research − ASU Feature Selection Repository. *ASU Feature Selection Repository Arizona State University*, 1–28. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.642.5862&rep=rep1&type=pdf

Zuhair, H., Selamat, A., & Salleh, M. (2016). Feature Selection For Phishing Detection: A Review Of Research. *Int. J. Intelligent Systems Technologies and Applications*, *15*(2). https://doi.org/10.1504/IJISTA.2016.076495