Middle-East Journal of Scientific Research 24 (Techniques and Algorithms in Emerging Technologies): 92-97, 2016
ISSN 1990-9233;
© IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.TAET23327

Cybercrime Risk and Cyber Security on Online Service Avoidance

[1]D. Muthusankar, [2]B. Kalaavathi and [3]M. Deepa

[1]Assistant Professor, CSE, K.S.Rangasamy College of Technology, Namakkal- 637215, Tamil Nadu, India
[*]Professor, CSE, K.S.R Institute for Engineering and Technology, Namakkal- 637215, Tamil Nadu, India
[*]P.G Scholar, CSE, K.S.Rangasamy College of Technology, Namakkal- 637215, Tamil Nadu, India

Abstract: Cybercrime is growing constantly and many people have been victims of hacking, theft, identity theft and malicious software. One of the best ways to avoid becoming a victim of Internet crime and protecting your sensitive information is available through the use of impenetrable security by means of a uniform system of software and hardware for the authentication of information that is sent or accessed over the Internet. It includes the control over the physical access to the hardware. The proposed work is a cost-effective model that builds on the technology acceptance research and findings from the criminology to identify use factor that internet users' intention to online services. To suspect that the avoidance of online banking, shopping and online social networking by internet crime victimization and media information. The distinct effects are provide by the perceived risk of Internet crime and moderated by the confidence of users online. In the proposed system software can be extended in order to prevent the high-tech crime and cyber-terrorism and they spread horror by the rapid provision of information by the information security to collect internet users and the increase of the safety awareness of all banks and companies today their business online, there are millions of users who use the Internet to conduct online banking transactions.

Key words: Cybercrime, Structural Equation Modeling · Online Services Avoidances · Cyber Security · Perceived Risk of Cybercrime · Phishing

INTRODUCTION

Web Mining is the claim of data mining techniques to discover patterns from the World Wide Web. Cybercrime is growing constantly and many people have been victims of hacking, theft, identity theft and malicious software. One of the best ways to avoid becoming a victim of Internet crime and protecting your sensitive information is available through the use of impenetrable security by means of a uniform system of software and hardware for the authentication of data that is sent or call up over the Internet. Computer security, also known as the cyber security or IT [1] security is the protection of information systems from theft or damage to the Hardware, the software and the information about you, as well as from any interruption or misdirection of the services they provide. It includes the control over the physical access to the hardware, as well as for protection against loss of network access, data and code of the injection system and through misconduct of operators, whether intentional or accidental, through you tricked by way of derogation from secure processes. It is a proactive detection of gaps in the security of computer systems which can be exploited by those who are for information warfare to seek entry in critical to change system, destroy or hold the government to blackmail by threatening to damage sensitive information infrastructure.

Online services have become an important part of our lives, because they make it possible to always and everywhere access to information. Obviously, these services are useful not only for Internet users, but also essential for financial organizations, because they help to reduce operating costs. Unfortunately the usefulness of online services overshadowed the start of the large-scale phishing attacks against Internet users. In online surveys are not prepared to many people a real anstors because of concern about privacy. Thus the anonymity is important for Online News Collection [2]. Existing system will develop a model that explains the effects of cybercrime on the prevention of online services show how cyber-crime creates the perceived risk [3] and how this risk is hesitant to use online user services. Test the model with a

Corresponding Author: D. Muthusankar, CSE, K.S.Rangasamy College of Technology, Namakkal- 637215, Tamil Nadu, India.

secondary analysis of the Eurobarometer 2012 Cyber Security Report (CSR), a representative of the pan-European survey on the public awareness of cybercrime. Then use Structural Equation Modeling Test seven hypotheses for three main online services, specifically: online banking [4], shopping and online social networking.

Related Work: Synthesize work from different field, to explain how cybercrime reduces online participation. Building on technology acceptance models to explain what factors influence the intention to use online services. Then, review the criminology literature to investigate qualifications of perceived crime risk and draw analogies to cybercrime. Finally, review existing work on the social effects of cyber-crime [5].

V. Venkatesh *et al.*, (2003), "User acceptance of information technology: Toward a unified view" This Models, clearing up the acceptance of new technologies, have been of interest in IS research since the first commercial use of computers. Several models have been introduced to measure the influence of different factors on the individual intention to use a new technology [6]. To focus on studies applying acceptance models in the context of general online services, online banking, online shopping and online social networking (OSN).

Davis *et al.*, (1989), the original TAM is shown in Figure 1. A person's recognition of a technology is hypothesized to be determined by his or her voluntary intentions towards using the technology. The purpose, in turn, is resolute by the person's attitude towards the use of the technology and his or her awareness of its usefulness. Attitudes are formed from the beliefs a person holds about the use of the technology [7]. The first belief, PU (perceived Usefulness) is the user's "subjective probability that using an exact request system will increase his or her job routine within an organizational context.

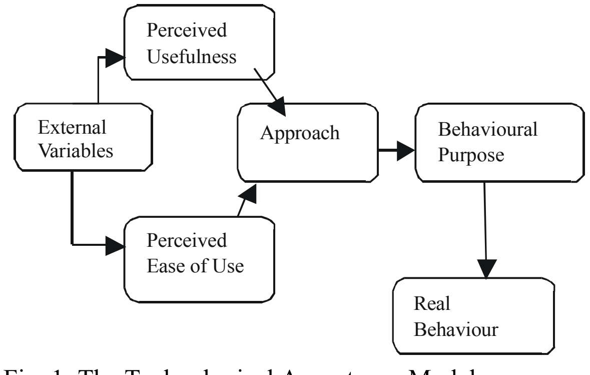

Fig. 1: The Technological Acceptance Model

K.F. Ferraro *et al*., (1987), "The measurement of fear of crime". While the former section explains how perceived risk negatively influence the society by making users hesitate to use online services, this section sheds light on how people's risk perception of crime is formed. Fear of crime is multidimensional in nature consisting of two distinct components [8]. First, the rather rational risk perception, which is often operationalized as a product of the probability of victimization and the severity of the crime. And second, fear as a rather emotional feeling of being unsafe. The two constructs are highly interrelated and the effects button them are still unclear.

J. Clough *et al.*, (2010), "Principles of cybercrime". The information capabilities of the Internet change the nature of crimes, as they provide cyber criminals with simple, cost effective and repeatable means of conducting rapid global-scale attacks, while remaining anonymous or inaccessible for law enforcement [9]. To consider consumer-oriented cybercrime, i.e., cybercriminal attacks that potentially harm Internet users, as they have the biggest effect on online service adoption.

C. Whittaker *et al.*, (2013), describe the design and performance characteristics of a scalable machine learning classifier that has been used in maintaining Google's phishing blacklist automatically [10]. Their proprietary classifier analyzes millions of pages per day, the examination of the URL and the content of a site to determine whether a site is phishing. Your system classifies sites of end-users and URLs of spam filtering Gmail presented collected. Although some URL -based functions are similar, we propose some new features and evaluate our approach with publicly available machine learning algorithms and public records. Unlike their approach, we do not use proprietary and page content based features.

Zhang *et al.*, (2007), present CANTINA, content-based approach to distinguish phishing websites, based on the TF-IDF in order retrieval algorithm and the Robust Hyperlinks algorithm [11]. By using a weighted sum of 8 features (4 content-related, 3 lexical and 1 WHOIS-related) they show that the CANTINA can capture about 95% of phishing sites correctly. The aim of our approach is to download the actual web pages and therefore the potential risk from the analysis of the harmful content on the user's system to reduce.

Jayshree Hajgude *et al.*, (2013), proposed a technique where they considered the advantages of blacklist, white list and heuristic technique for increasing accuracy and reducing false positive rate. In heuristic technique people are using textual analysis and URL

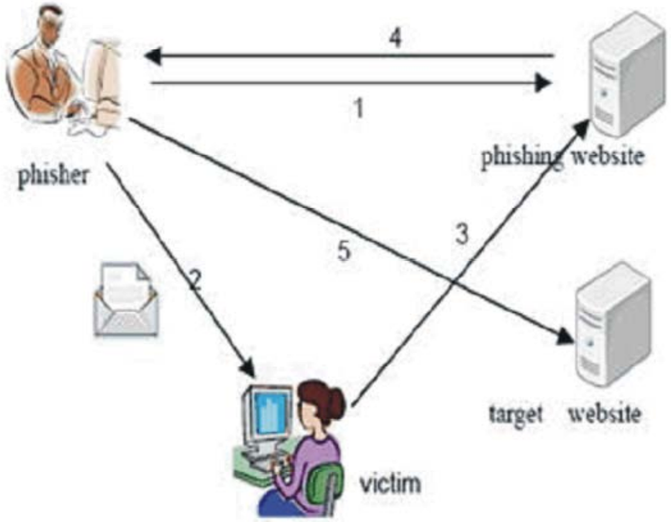

Fig. 2: Procedure of Phishing Attacks

analysis of e-mail. Since most of the phishing mails have similar contents, in proposed method increased the performance by analyzing textual contents of mail and lexical URL analysis. This technique detects phishing mail if DNS in actual link is present in blacklist [12].

Overview of Project: This phishing attack is done in different way and also much type of attacks is available but the common procedure is same for all type of attacks. Procedure of Phishing Attacks.

Phishing attack procedure is depicted in Figure 2. Following steps are involved in phishing attack [13].

- Phishers set up a faked Web site which looks accurately like the legitimate Web site, including setting up the web server, applying the DNS server name and making the web pages similar to the destination Website, etc.
- Send large quantity of spoofed e-mails to target users in the name of those legitimate companies and groups, trying to convince the prospective victims to visit their Web sites.
- Receivers obtain the e-mail, open it, click the spoofed hyperlink in the e-mail and input the required information.
- The personal information is transmitted from a phishing server to the phisher.
- Phishers steal the personal data and perform their fraud such as transferring money from the wounded.

The phisher uses the personality information of the victim to the goal website and impersonates the victim’s individuality to gain the illegal financial benefits. The e-mail directs the user to visit a Web site where they are asked to bring up-to-date personal information, such as passwords, credit card details and bank account numbers.

Proposed Work: In the planned work to reduce the risk and the improvement of the Usability user's online service by creating the Phish tank. The phish tank is the web service database for Phishing websites. It gives some regular service to the API Developer. Use heuristic methodology for the automatic classification of phishing URLs as potentially in nature. This method can be used to prevent a phishing attack either by masking the potential phishing URLS or by notification to the user about the potential threat. Since the focus is on the URL itself, this approach can be applied anywhere that a URL can be embedded, e.g. in e-mails, Web sites, chat, just to name a few [14, 15].

To improve the safety of the user Auto Responder email is implemented to send the message to the person who had sent threaten message. The key board typing words will be monitored to detect threaten words. As soon as threat words and any other worm deducted, an massage will be send to admin with ip address, time date, threat words with related sentences and the same will be sent by e mail to the person who had sent that threaten message. Here we are using check reader for sending automated emails. By using this we can check how many emails are bounced and track the warning message and check whether email is viewed by the sender or not.

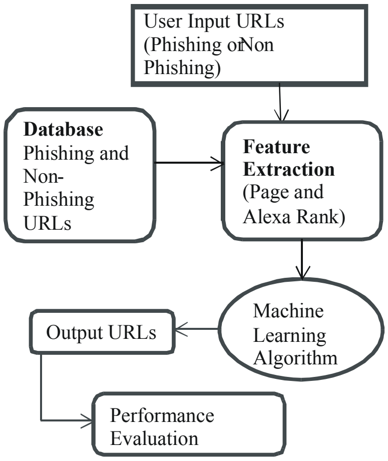
User Input URLs (Phishing or Non Phishing)
Database Phishing and Non-Phishing URLs
Feature Extraction (Page and Alexa Rank)
Machine Learning Algorithm
Output URLs
Performance Evaluation

Fig. 3: The Phishing URL Detection Framework

The Phishing URL Detection Framework: In this Figure 3, it describes the URL detection framework. In this the user gives the URL as an input this may be phishing URL or legitimate URL [16].

The database contains the both phishing and legitimate URLs the feature extraction extract the user input by the use of database and page or Alexa ranking. After this extraction the Machine learning algorithm is applied to the URL, then the output URL is displayed where the URL is legitimate or phishing.

The Phishing Email Detection Framework: In this Figure 4, procedure for detection of Email phishing.

- Sender creating the messages, its send to the check reader.
- Check reader checks the messages, if there is no worm is detected then the message will be send to the receiver.
- If there is any worm is detected then it is blocked then the message and the sender information will send to the Admin.
- Admin will send the warning message to the sender. The admin also monitor the warning message is read by the sender or not.

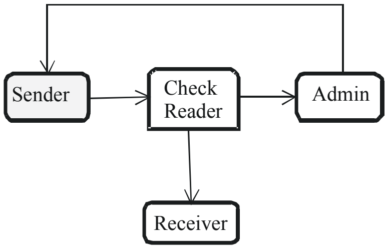

Fig. 4: The Phishing Email Detection Framework

Methods and Algorithms: Suggest a heuristic-based approach for classifying phishing URLs with the URLs only to information. Then treat the problem of detecting phishing URLs as a binary taxonomy problem with phishing URLs. First, phishing and legitimate sites will be collected to build the dataset. Then apply different machine learning algorithms to build models of training data. Thereafter, the two algorithms are used as follows:

- Random Forest algorithm, one of the most efficient machine learning algorithm in order to build prototypes of training data from the pairs of values and functions class labels. The prototypes are then separate set of test data and the data instance of the predicted class is compared with the actual data class.
- Content-based algorithm, (work on the publicly available data on the URLs), which focuses on the essentials, to distinguish phishing sites, legitimate.

Data Sets: For experiments, collect the data from various credible sources that are also used by Y. Zhang *et al*. [11] and many others. Collect the non-phishing URLs from two open data sources: Yahoo! directory and DMOZ Open Directory Project. Then use a Yahoo's server redirection service, *http://random.yahoo.com/bin/ryl*, which at random selects a web link from Yahoo directory and redirects browser to that page. In order to cover wider URL structures and also made a list of URLs of most commonly phished targets (using statistics of top targets from Phish Tank). Then crawled those URLs, parsed the retrieved HTML contents and harvest the hyperlinks within to also use as non-phishing URLs. These additional links are assumed to be benign, as they extracted from a legitimate source. Use these sources and call it Yahoo record. These URLs were collected between September 15, 2010 and October 31, 2010. The extra source of legitimate URLs, DMOZ, is a directory whose entries are vetted manually by editors. Use non-phishing URLs from this source and call it DMOZ data set.

Proposed Work Schemes

User Profiling: In the Top domain, user profiling is the process of gathering information specific to each visitor, either clearly or absolutely a user profile includes demographic information about the user, her interests and even her behavior when browsing a Top site. This information is exploited in order to customize the content and structure of a Top site to the visitor's specific and individual needs.

Phishing Search Engine: This module makes interface button background API Store, Its send sequence request to online phish verifier. The main dataset files are silently updates in the background of the engine. The module are gets some standard request to the port finder XML file. The XML parser works background to get result in the front of user.

API with Phish Tank: The phish tank is the top service database for phishing top pages. It gives some regular service to the API developer. To made a link button the phish tank server to the search engine. The phish tank top databases are store the top spam percentage, user comments and rank in hosting. The databases are simply categories from phish site. The maser suggested phisher are published by the user in phish tank.

Bank Administrator Login: Bank login an administrator can add money to customer account they can add new customer and all administrator related activities. This module made the bank report generation easier with very few clicks. Aesthetic report view makes the user to analyze the data easier.

Customer or User Login: This module is used to secure each PHP page with the login session data. If the session data is not found the page will redirect to not_loggedin.php where user needs to login credentials (i.e., Username or email and password) to login. If the login is successful it redirects to the corresponding page. If the user logged-in is in group of admin it redirects to admin dashboard and gives the full functionality to the software. User login customer can manage accounts they can transfer money and much more.

Hacker Terminal: This terminal was designed by hackers where they can develop by defacing the source code of the top site and creating their terminal. This module specifies when this key board typing words will be monitored when threat words will be deducted. As soon as threat words and any other worm, deducted message will be sent to admin with IP address, time date, threat words with related sentences and same will be sent by e mail. This module prevents the unnecessary upload of worm files or any other virus files which creates damage to the system.

Threatens Keywords and Files (Folder.htt, Desktop.ini): This module specifies when this key board typing words will be monitored when threat words will be deducted. As soon as threat words and any other worm, deducted massage will be send to admin with ip address, time date, threat words with related sentences and same will be sent by e mail. This component prevents the unnecessary upload of worm files or any other virus files which creates damage to the system.

CONCLUSION

This project offers a solution for the problem of phishing sites and URLs with Page Ranking and Phish Tank based function for random forest algorithm. It has been demonstrated that by applying -based Web Mining heuristic methodology on Random Forest and Content based algorithm. This system also offers a solution to the problem of the threat to the mail and bad words. Because the Internet is the unique situation in relation to the geography and identity, E-mail alert is required for the Internet to govern itself. So take advantage of the developments in technology and the increased efficiency of the operation in the report handling.

In future work, plan to develop a framework using this approach and deploy it for a large-scale real-world test.

REFERENCES

1. Erik Brynjolfsson, 2001. “The Contribution of Information Technology to Consumer Welfare”. “Information Systems Research”, 7(3).
2. Erik, Brynjolfsson Michael D. Smith, 2003. “Consumer Surplus in the Digital Economy: Estimating the Value of Increased Product Variety at Online Booksellers”. “Management Science”, 49(11): 1580-1596.
3. Fred D. Davis, 1989. “Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology” 13(3): 319-340.
4. Payam Hanafizadeh, 2013. “A Systematic Review of Internet Banking Adoption”. “Telematics and Informatics, 31: 492-510.
5. Ross, Anderson and Chris Barton, 2011. “Measuring the Cost of Cybercrime”. 23(5): 23-80.
6. Viswanath Venkatesh and Michael G. Morris, 2003. “User Acceptance of Information Technology: Toward a Unified View1”. “MIS Quarterly”, 27(3): 425-478.
7. Davis, F., R.P. Bagozzi and P.R. Warshaw, 1989. “User acceptance of computer technology: a comparison of two theoretical models”, Management Science, 35(8): 982-1003.

8. Ferraro, K.F. and R. La Grange, 1987. “The measurement of fear of crime,” Social. Inq., pp: 70-101.
9. Clough, J., 2010. “Principles of cybercrime”. Cambridge University Press.
10. Whittaker, C., B. Ryner and M. Nazif, 2010. Large-scale automatic classification of phishing pages, In: Proc. 17th Annual Network and Distributed System Security Symposium, NDSS?10, San Diego, CA, USA.
11. Zhang, Y., J. Hong and L. Cranor, 2007. CANTINA: a content-based approach to detecting phishing web sites, In: Proc. 16th Int. Conf. World Wide Web, WWW?07, Banff, Alberta, Canada, pp: 639-648.
12. Jayshree Hajgude and Dr. Lata Ragha, 2013. “Performance Evaluation of Phish Mail Guard: Phishing Mail Detection Technique by using Textual and URL analysis”, Int. J. on Recent Trends in Engineering and Technology, 8(1).
13. Joby James, L. Sandhya and Ciza Thomas, 2013. “Detection Of Phishing URLs Using Machine Learning Techniques”, International Conference on Control Communication and Computing (ICCC).
14. Paul A. Pavlou, 2003. “Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model”. “International Journal of Electronic Commerce”, 7(3): 69-103.
15. Li, Y.H. and J.W. Huang, 2009. “Applying theory of perceived risk and technology acceptance model in the online shopping channel, ” World Acad. Sci. Eng. Technol., pp: 53-76.
16. Weifeng, Zhang and Hua Lu, 2013. “Web Phishing Detection Based on Page Spatial Layout Similarity”. “Informatics”, 37: 231-244.