International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

A Survey on Credit Card Fraud based on Phishing Attack

S. Asha
M.E Student, S.A Engineering College,
Chennai, India

C. Bala Krishnan
Associate Professor, S.A Engineering College,
Chennai, India

ABSTRACT

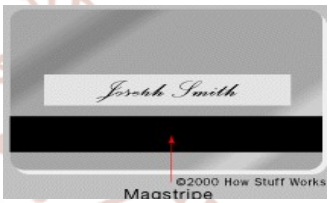
Credit card fraud is a comprehensive term for theft and fraud committed using or involving a payment card, such as a credit card or debit card. Credit card fraud occurs when customers give their credit card details to unfamiliar individuals or when cards are lost or stolen or when mail is diverted from the intentional recipient and taken by criminals or when the sensitive information such as account number associated with the card stolen. In this paper, we summarize about the phishing attack in brief through which the credit card frauds can occur during online shopping.

Keywords: *Fraud Detection, Phishing email, Authentication*

I. INTRODUCTION

Credit card fraud is a comprehensive term for theft and fraud committed using or involving a payment card, such as a credit card or debit card. A credit card is an instalment card issued to clients (cardholders) to empower the cardholder to pay a shipper for merchandise and enterprises, in view of the cardholder's guarantee to the third-party entity to pay them for the amount so paid in addition to other concurred charges.

A credit card is a thin plastic card, usually 3-1/8 inches by 2-1/8 inches in size and it contains identification information such as a signature or picture and approves the individual named on it to do purchase for which he will be charged periodically.



There is a stripe present at the back of the credit card. This is known as Magnetic Stripe which is made up of tiny iron based magnetic particles in a plastic like film.

1. Phishing Attack:

Phishing attack is the endeavor to obtain sensitive information such as username, passwords or credit card details such as account number, often for malicious reasons, by disguising as a reliable entity in an electronic communication. Phishing attack is carried out by email spoofing and it often directs users to enter password at a fake website whose look and feel are identical to that of the legitimate website. The only difference between the fake and the legitimate website is the url of the website.

2. Causes for Phishing attack:

There are several causes for the phishing attack to occur. They are

- Deceptive emails
- Susceptibility in browsers
- Limited use of digital signature
- Lack of user responsiveness
- Susceptibility in applications
- No Strong authentication present at bank side as well as at financial institution website

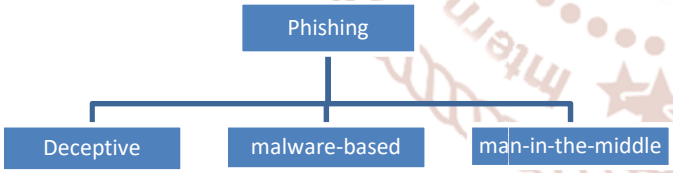
3. Effects of Phishing:

There are several effects that occur due to phishing attack.

- Financial loss to the banking and the financial institution
- Internet Fraud
- Identity theft
- Erosion of public trust in the internet
- Difficulties in law enforcement
- Investigations

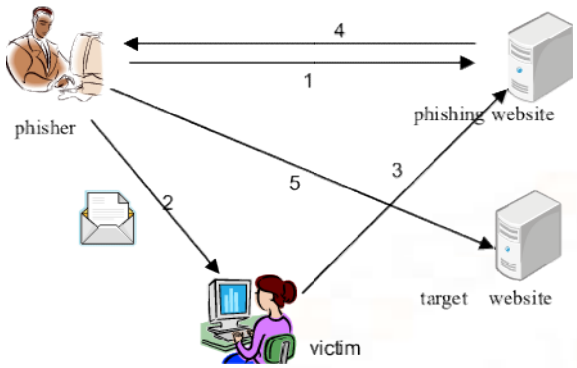
4. Types of Phishing Attack:

Phishing attack comes in many different shapes and forms. The reason for phishing attack also varies. There are different types of phishing attack.



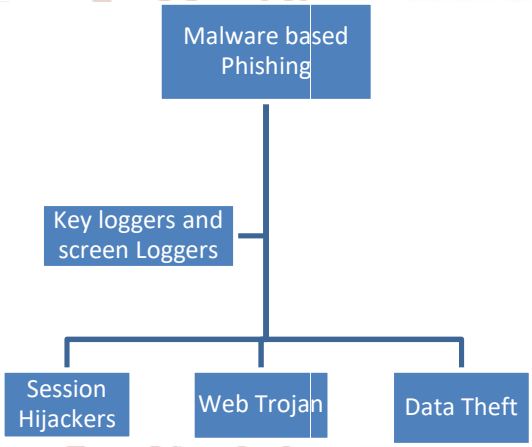
Deceptive Phishing:

Deceptive Phishing is the most common phishing attack that occurs through email. Phisher sends bulk of emails to the user and command them to click on the link given below. Phishers invitation to take action contains devastating data about the recipient's account. Phisher then collects confidential information given by the user.



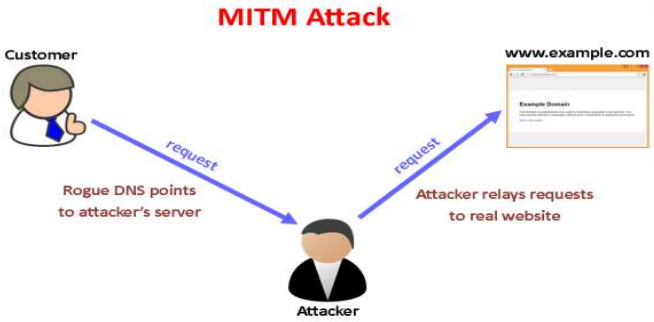
Malware based Phishing:

This type of phishing attack takes place by running malicious software on the client machine. This phishing attack takes place due to social engineering or security vulnerabilities. Exploiting the security vulnerabilities by injecting worms and viruses are another form of malware based phishing. There are various form of malware based phishing.



Man-in-the -Middle Phishing:

In this type of phishing attack, the phisher is present between the user and the legitimate site. This attack supports both HTTP as well as HTTPS Connection. This attack can be made successful by directing the customer to proxy server rather than the real server.



II. Related Work

A. Protecting user against phishing using Antiphishing

AntiPhishing is used to avoid users from using fraudulent web sites which in turn may lead to phishing attack. Here, AntiPhishing traces the sensitive information to be filled by the user and alerts the user whenever he/she is attempting to share his/her information to a untrusted web site. The much effective elucidation for this is cultivating the users to approach only for trusted websites. However, this approach is unrealistic. Anyhow, the user may get tricked. Hence, it becomes mandatory for the associates to present such explanations to overcome the problem of phishing. Widely accepted alternatives are based on the creepy websites for the identification of "clones" and maintenance of records of phishing websites which are in hit list.

B. Learning to Detect Phishing Emails

An alternative for detecting these attacks is a relevant process of reliability of machine on a trait intended for the reflection of the besieged deception of user by means of electronic communication. This approach can be used in the detection of phishing websites, or the text messages sent through emails that are used for trapping the victims. Approximately, 800 phishing mails and 7,000 nonphishing mails are traced till date and are detected accurately over 95% of them along with the categorization on the basis of 0.09% of the genuine emails. We can just wrap up with the methods for identifying the deception, along with the progressing nature of attacks.

C. Phishing detection system for e-banking using fuzzy data mining

Phishing websites, mainly used for e-banking services, are very complex and dynamic to be identified and classified. Due to the involvement of various ambiguities in the detection, certain crucial data mining techniques may prove an effective means in keeping the e-commerce websites safe since it deals with considering various quality factors rather than exact values. In this paper, an effective approach to overcome the "fuzziness" in the e-banking phishing website assessment is used an intelligent resilient and effective model for detecting e-banking phishing websites is put forth. The applied model is based on fuzzy logics along with data mining algorithms to consider various effective factors of the e-banking phishing website.

D. Collaborative Detection of Fast Flux Phishing Domains

Here, two approaches are defined to find correlation of evidences from multiple servers of DNS and multiple suspects of FF domain. Real life examples can be used to prove that our correlation approaches expedite the detection of the FF domain, which are based on an analytical model which can quantify various DNS queries that are required to verify a FF domain. It also shows implementation of correlation schemes on a huge level by using a distributed model, that is more scalable as compared to a centralized one, is publish N subscribe correlation model known as LARSID. In deduction, it is quite difficult to detect the FF domains in a accurate and timely manner, as the screen of proxies is used to shield the FF Mother ship. A theoretical approach is used to analyze the problem of FF detection by calculating the number of DNS queries required to get back a certain amount of unique IP addresses.

E. A Prior-based Transfer Learning Method for the Phishing Detection:

A logistic regression is the root of a priority based transferrable learning method, which is presented here for our classifier of statistical machine learning. It is used for the detection of the phishing websites depending on our selected characteristics of the URLs. Due to the divergence in the allocation of the features in the distinct phishing areas, multiple models are proposed for different regions. It is almost impractical to gather enough data from a new area to restore the detection model and use the transfer learning algorithm for adjusting the existing model. An appropriate way for phishing detection is to use our URL based method. To cope with all the prerequisites of failure of detecting characteristics, we have to adopt the transferring method to generate a more effective model. Comparative study of the classifiers' model-based features is shown in the below table.

CLASSIFIERS MODELS _ BASED FEATURES APPROACHES

Contribution Summary	Mechanism	Algorithm
Structural Features	The prototype implementation sit between(MTA) and (MUA)	Low level or recall measurements -Work with fixed number of features
Training Smart Screen	Uses the feedback data from the users of Microsoft.	Bayestan statistics100.000 email attributes
Semantic Ontology concept. Text classification of phishing emails using a heuristic way	Model works in 5 steps	Semantic ontology concepts by (TFV) Methods, Information Gain (IG), Nave Baayes algorithm classifier
PHONEY: Mimicking user response	PHONEY Technique is installed between a user's MTA and MUA	PHONEY Mimicking user response
Study the statistical filtering or phishing emailsl	Trained a classifier by features obtained based on Dynamic Markov chain and class topic models	Dynamic Markov chain and class topic models

III. CONCLUSION

Phishing attack cannot be solved with a solitary solution. It is a hazardous situation in which Phishers always try to come up with brand new modes of manipulating the consumers. Online customers should embrace regular risk scrutiny to detect the recent techniques which may head to a thriving Phishing assault. In order to find safer ways, user must be aware about the dangers of advanced malware which are taking place nowadays. Further contribution is done in detecting the identity theft and the phishing mails.

References

[1]. "Protecting Users against Phishing Attacks with Anti Phish" Engin Kirda and Christopher Kruegel Technical University of Vienna

[2]. "Learning to Detect Phishing Emails" Ian Fette School of Computer Science Carnegie Mellon University Pittsburgh, PA, 15213, USA icf@cs.cmu.edu Norman Sadeh School of Computer Science Carnegie Mellon University Pittsburgh, PA, 15213, USA Anthony Tomasic School of Computer Science Carnegie Mellon University Pittsburgh, PA, 15213, USA

[3]. Modeling and Preventing Phishing Attacks by Markus Jakobsson, Phishing detection system for e - banking using fuzzy data mining by Aburrous, M. ; Dept. of Comput., Univ. of Bradford, Bradford, UK ; Hossain, M.A. ; Dahal, K. ; Thabatah, F.

[4] M. Chandrasekaran, et al.," Phishing email detection based on structural properties", in New York State Cyber Security Conference (NYS) , Albany, NY ," 2006

[5] P. R. a. D. L. Ganger, "Gone phishing: Evaluating anti-phishing tools for windows. Technical report," September 2006

[6] M. Bazarganigilani,"Phishing E-Mail Detection Using Ontology Concept and Nave Bayes Algorithm," International Journal of Research and Reviews in Computer Science, vol. 2, no.2, 2011.

[7] M. Chandrasekaran, et al., "Phoney: Mimicking user response to detect phishing attacks," in: Symposium on World of Wireless, Mobile and Multimedia Networks, IEEE Computer Society, 2006, pp. 668-672

[8] I. Fette, et al., "Learning to detect phishing emails," in Proc. 16th International World Wide Web Conference (WWW 2007), ACM Press, New York, NY, USA, May 2007, pp. 649-656

[9] A. Bergholz, et al.,"Improved phishing detection using model-based features," in Proc. Conference on Email and Anti-Spam (CEAS). Mountain View Conf, CA, Aug 2008

[10] L. Ma, et al.,"Detecting phishing emails using hybrid features, "IEEE Conf, 2009, pp. 493-497