IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Special Issue-14, May 2019 E-ISSN: 2347-2693

Detection of E-Banking Phishing Websites

N. Saivikas Reddy[1*], Vinay Kumar M[2].

[1,2]Department of C and IT, Reva University, Bengaluru, India

[*]*Corresponding Author: vikasnikku98@gmail.com, Tel.: +91-8152072354*

DOI: https://doi.org/10.26438/ijcse/v7si14.4952 | Available online at: www.ijcseonline.org

***Abstract*—** The term Phishing refers to a fraudulent technique of stealing people's private data .The main aim of phishing attack is to steal consumer private data by provoking them to enter their details in the portals which are sent by the attacker. These portals resembles with the original website portal and provokes the users to enter their data like username and password, bank account details and other sensible information .The main goal of this paper is to perform research on the machine learning data techniques to detect the phishing attacks and to assist the police in handling the complicated phishing activities.

***Keywords*—** Phishing, criminal technique, associative classification algorithms

I. INTRODUCTION

The word Phishing is derived from "fishing" which means an activity of provoking the users to visit the websites sent by the attacker and make them enter their data such as login details, bank details etc.

This sensitive information is further used for bank transactions, theft activities, demanding money from the users etc.

There will be multiple phishers in a complete phishing attack. The first kind of phishers are called as "mailers" who sends many fake mails to the users which directs the users to fake websites. The second category phishers are those who set ups the phishing websites which provokes the users to enter their sensitive data and these type of phishers are called as "collectors". The third type of phishers are called as "cashers" who collects the confidential data provided by the users and users it for other activities. The most commonly used mechanism for phishing is to send fraudulent emails to the users which prompts the users to visit the link provided in the email and enter their sensitive information. The websites links send by the attackers seems to be original websites and provokes them to use those websites. Attackers will get the bank account details by stating like your credit card /debit card has been blocked or by stating like the users will get cashbacks if they pay their bills through the link provided in the email. Attacks which are not involving in getting users details are not considered as phishing. As per the records women are being targeted more when compared with men, and ages between 18-35 have been an active target for the attackers. Band spoofing or carding are the synonyms of phishing. Phishers will make use of each account for identity theft or money laundering etc. In September 2003, a banker reported a phishing attack on a bank for the first time.

Phishers targets are banks, financial institutions, social media and gaming sites. The first attack of phishing is failed but it gave a rise of these attacks in the future.

II. PHISHING ATTACKS

Beyond Phishing thorough email the attackers are using different techniques which are as follows

1.The attack in which the attacker copies the contents of the original email and sends a fraudulent email to the user by changing the links is called as "clone phishing".

2.The second type of phishing in which the attacker targets only the specific group of people like people working in the same organisation, this type of attack is known as "spear phishing".

3.In this attack the phisher sends the message asking the users to compliant about their issues to a phone number, this type of attack is called as "phone phishing" attack. As Voice over I is easy to manipulate with the traditional phone equipment, this attack becomes a good choice for the attackers.

The attacker can also perform web spoofing which means the attacker will forge the website to look like as an original website and provokes the users to enter their sensitive information. Modern internet browsers have the built in mechanisms to warn about these kind of websites but these warnings are neglected by careless users. To forge the website one has to just copy the front end code and requires little bit of programming to transfer input data into a file database. Once the website is created now the task is to make the users visit them, this is mostly done by using emails or by sending messages. Phishers will make use of blind drop server to store the data.

Phishers can use malware to collect the data such as screenshots, program activity. Malware send the collected data to the phishers through IRC channel, by email etc. Phishing is also done through pdf documents.

The term Pharming is defined as an attack which is intended to direct the users to fake internet hosts. DNS cache poisoning is the common method used for pharming. In this method the DNS records are manipulated. Domain Hijacking is another type of pharming attack in which the domain name is changed without the permission of the authorized persons, once it is done getting back the domain records to the original owner is more difficult. Domain hijacking is done in many ways such as tricking the users to enter their details by displaying fake phishing websites, Data breaching of domain registrar, they claim themselves to be authorized persons and asks the users details to verify them. By contacting the domain registrar technical support department and explain the situation is the fastest way of recovering the domain name. By contacting ICANN which resolves domain name disputes.

Content injection is a technique in which the attacker changes a part of the legal website which generally redirects The users outside the legal website and provokes to enter the details. Trojan Horse malware gives unauthorized access to the accounts.

III. PREVENTIVE MEASURES

1.It is advisable to enter the website link manually in the search bar rather copying the link from the sources.
2.Usage of Firewalls. Firewall is of two kinds one is desktop firewall which is a software kind and the other is network firewall which is hardware type. It is suggested to use both kinds of firewall to ensure maximum protection.
3.Update the browser regularly and focus on getting information about the advancements in phishing attacks.
4.It is advisable to change the passwords frequently and to save the passwords in any browser.
5.If you are not about the website security then it is better if you don't click the website link.
6.Try to contact the company or organisation directly if the message seems to be fraudulent.
7.Domain hijacking can be prevented by many ways such as using two-way authentication, by registering in a good domain name company, by using a strong password, by enabling WHOIS protection, by changing the passwords periodically and by keeping the domain records updated.
8.Malware can be detected by security products but they are not guarantee to protect completely.
9.If the name of the sender's email address doesn't match with the domain name, then don't open the link or any document.
10.Beware of signatures missing.
11.Use different passwords for different accounts.
12.Cross verify the bank transactions periodically.
13.Enable SMS alerts for all transactions done by using cards.
14.If you find any unexpected attachments for the emails, it is better to not to go for it.
15.Dont open any link unless you are completely aware of what you are doing.
16.Before visiting the website check the digital certificate.
17.Enter the sensitive information only in the portals which starts with HTTPS but not HTTP. Here S stands for secure.
18.If you doubt about phishing emails then search for the name of the sender in the internet, the attacker might have used the same method earlier.

As the attackers are finding new ways for phishing it is advisable to follow the above mentioned measures and constantly update the knowledge on cybersecurity.

IV. RELATED WORK

Detection of E-banking Phishing Websites-Problems with existing system:
1. Detects and block the phishing Websites in time.
2. Enhances the security of the websites.
Features of Proposed system:
1. The classification algorithm in data mining is used in this system.
2.Based on characteristics like website domain names," URL" the phishing websites can be detected.
3.This system can be used to do payment online securely

V. METHODOLOGY

1.Check if website contains special characters such as "@,-,&".
2. Check ranks of the websites)
- if<100000 score will be less
- if>200000 score is more

4.Check whether website is registered in DNS server using http://www.whois.com/whois/ Calculate age of website by checking the registration date and expiry date (if age less than 6 months then phishy)
5.if it contains many subdomains then may be phishing
6.The website is said to be fake if the score is less than the limit.

VI. MODULES AND THEIR DESCRIPTION

This system is having 6 Modules:
1. **Registration**

2. **Login**
3. **Add to Blacklist**
4. **Check Website**
5. **Feedback**
6. **Change Password**

Description:

1. **Registration:**
   - A visitor can register himself to the website to access it.
2. **Login:**
   - After registering, user and admin will input their credentials to login into the system.
3. **Adding to the Blacklist:**
   - The website can be blacklisted by the admin provided if they prove to be malicious.
4. **Checking of website:**
   - By entering the "URL" the user can check whether the website is blacklisted or not.
5. **Comments:**
   - Users can comment about the system functionalities.
6. **Change of Password:**
   - Change of password because of security reasons can be done by admin.

VII. ADVANTAGES

1.To maintain good relationships with the customer this system can be used.
2.This system can be used to make complete transaction process securely.
3.Users can make payments online by using this system.

The disadvantage is that if there is no internet, then this system will not work.

VIII. SYSTEM IMPLEMENTATION

❖ **Hardware Requirements:**

- Dual Core Processor Based Computer
- 1GB-Ram
- 50 GB Hard Disk
- Internet Connection

❖ **Software Requirements:**

1.Windows XP, Windows 7(ultimate & enterprise)
2.Visual studio 2010.
3.SQL Server 2008.

IX. FEASIBILITY REPORT

People often purchases the products online and makes their payment through online. In order to detect the e-banking phishing websites our system uses a classification datamining algorithm. The e-banking phishing websites may be detected by few important characteristics like Uniform Resource Locator and Domain Identity, security etc.
The term Feasibility Study means to determine whether the system proposed is feasible in terms of Technical, Economical and Operational.

❖ Technical Feasibility

This system is developed in .Net Framework with the use of C#. This application will be an online application and it can be accessed by using (Personal Computers, Laptop).

The proposed system is said to be technically feasible if the needed technologies are readily available.

Our system is technically possible as a result of, all the technology needed for our system is readily available.

Operating System:
Windows XP, 7(ultimate & enterprise)
Languages:
Asp.Net with C# (.Net 2010)
Database System:
MS-SQL Server 2008
Documentation Tool:
MS - Word 2013

❖ Economic Feasibility

The term economic feasibility is defined as a cost analysis mechanism to determine the validity of the proposed system. Our system is economically feasible because there is no need of additional investments. The cost of complete studying of the system, the cost of the materials and machinery, the maintenance cost are to be considered. The new system is said to be economically feasible only if there are more benefits in terms of cost and maintenance for the new system when compared with the old system.

Operational Feasibility

The term operational feasibility is the measure of solving problems using new proposed mechanisms. The method has to completely satisfy the users requirements.

X. TESTING

All the components of the system have to work properly and should produce desired outputs. The systems are said to be tested successfully tested after performing various types of tests.

1.Unit testing is the stage where all the modules are tested separately. This test is performed during programming stage itself. Unit testing is used to verify the accuracy of each unit. Unit is defined as the smallest part for testing in a software. By performing the unit testing one can make the process

agile, it also gives the documentation about the system, debugging process can be made simpler with unit test.

2.In Integration testing all the modules are integrated and tested. This test is performed to find the interaction faults between the modules. Some types of integration tests are top-down, bottom-up, big-bang, layer integration, back bone integration.

3.In system testing a series of tests are performed on the completely integrated system. System testing is performed as either functional requirements or system requirements. This test is intended to test beyond the requirements.

4.In validation testing the software is tested whether it meets the specific requirements as required by the client. IV&V know for carrying out the validation test as a third party.

5.In output testing phase, the system is tested whether the system produces desired outputs as needed by the clients.

XI. COMPARISION

1) Effeciency (Time): It is not so easy to find whether the website is malicious or not in time.Our proposed system is relatively faster in finding the phishing websites.

2) Security:Our proposed system provides better secuirty for the users data while surfing the websites as our system detects the phishing websites on time.

3) Ease of use:Our proposed system can be used with ease to find phishing websites.

XII. OUTCOME OF THE PROPOSED SYSTEM

The system provides a secure module to register and login for the users and accepts all the valid URLs and validate their authenticity and the users are alerted for the malicious websites and thus prevents the user landing into trouble by allowing access to hackers. The system also provides means to surf the internet through valid websites as the added feature.

XIII. CONCLUSION

Phishing is not new but a serious threat to today's world. Attackers are employing new methods to perform phishing, it has to be noted that no method has valid proof that it will protect from phishing. It is required to keep the browsers and antivirus software up to date to protect from phishing. Though no method can guarantee complete protection, it is better to try these. This system is developed in .Net Framework with the use of C#. This application will be an online application and it can be accessed by using (Personal Computers, Laptop). Now a days phishing is done through malware as well which makes it more challenges' for the cybersecurity experts

REFERENCES

[1] Abdulghani Ali Ahmed, Nurul Amirah Abdullah, "*Real Time detection of phishing websites".In the proceedings of the* 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON 2016),USA,pp. 2-5,2016.

[2] Stuart McClure, "*Hacking Exposed*", McGraw-Hill Education,pp. 28-45, 2012.

[3] Christopher Atikins,"Phishing attacks:Advanced Attack Techniques", CreateSpace Independent Publishing Platform,pp. 55-75,2018.

[4] Dr.Radha D,"Study on Phishing attacks and antiphishing tools" International Research Journal of Engineering and Technology (IRJET),Vol 3,Issuse.1,pp.1-4,2016.

[5] Himani T,"A survey paper on Phishing detection" International Journal of Advanced Research in Computer Science,Vol 5,pp 1-4,2016.

