ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

A Survey on Preventing of Phishing Attack

Pooja Dhake[1], Pratiksha Paithankar[2], Vidya More[3]

B. Tech Student, Dept. of CSE, Sandip University, Nashik, India[1]

B. Tech Student, Dept. of CSE, Sandip University, Nashik, India [2]

Asst. Professor, Dept. of CSE, Sandip University, Nashik, India [3]

ABSTRACT: Nowadays, security of the confidential, personal or financial information or data of the organization or an individual become a serious issue. "Phishing is the process in which the hacker target to the victim system and attempt to get personal or financial information or data". Phishing is the Cybercrime attack. The existing system detects phishing attacks from the black list as well as the website which are not present in the list that perform phishing. The website which performed phishing is later added in the black list. This system works on the algorithm called as 'Link Guard Algorithm', which words on character based so it can detect known Phishing attack. In this paper, we assume that how to prevent computers, Smartphone, tablets and laptop's from the Phishing attacks and to overcome the disadvantages of previous paper. Provide tips for preventing phishing attack.

KEYWORDS:Blacklist, Link guard algorithm, phishing attack, Cybercrime attack.

I. INTRODUCTION

Today all management or organization is using the internet for distributing the message so the communication must be secured. Nowadays phishing attack is become major issue in network security is needed to prevent information from this attack. The phishing is perform for gaining data, information, personal details through the dummy website, spamming. Phishing is used to steal the commercial information by targeted system. Few illegal hackers doing the Cybercriminal activity by committing scam or fraud. The purpose or goal behind the phishing is data money or personal information retrieve through the fake website. The technique to avoid phishing from dummy website is deleted that dummy website real time malicious URL.

II. LITERATURE REVIEW

According to the literature review the link guard is the previous system. Link guard algorithm is a tool that use character based anti-phishing approach. This technique used for detecting phishing site to the exact domain name server (DNS). To overcome these disadvantages of link guard algorithm the next technique is Microsoft Smart Screen Filter. This is plug-in tool developed for internet explorer (IE6). In this method the blacklist need to update regularly that's why the next technique is developed that is Netcraft. Netcraft is the anti-phishing browser extension in which is displays information about site, domain registration date. In the Netcraft technique user can override the warning displayed by Netcraft. So the later technique is developed that is Passpet. Passpet allows changing the password for individual site.

III. EXISTING SYSTEM

The existing system of phishing is "Link Guard Algorithm" in which Link Guard is the main component of Link Guard Algorithm is best compared to SHA. SHA is a Secure Hash Algorithm that is cryptography hash function.
It is design by National Security Agency. Link guard algorithm works on analysing the difference between real links and visual links. On the trusted site it calculated the similarities of URL; it consists of some important system like:

- Communication

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

- Database
- Analyzer
- Alerted
- Logger

Description of above components:

- **Communication:**

The input process can collect and sent to analyzer.

- **Database:**

Stores the input URL's.

- **Alerted:**

The analyzer sends a warning message as soon as it receives or gain from the alerts to the users. The analyzer receives the reaction of the users.

- **Logger:**

All the information stored.

- **Analyzer:**

Anayzer is the most

Blocked Diagram of Link guard algorithm:

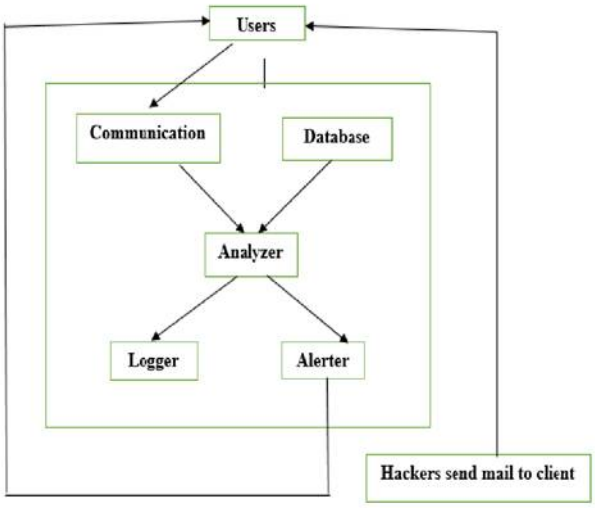

Fig 1: Diagram for Link Guard Algorithm

TYPES OF PHISHING ATTACK

There are seven types of phishing attack:

- Deceptive phishing
- Malware based phishing
- System reconfiguration
- Data theft
- Spear spoofing
- Clone spoofing

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

- Email spoofing

Description of above phishing attacks:

- **Deceptive Phishing:**

The meaning of this phishing is the important information stealing using directly communicates but nowadays the mostly used method is 'Deceptive message'. This process is send the text message to the victim that concerns about the need of verify the account details of users, unfavourable changes in account, fake account that the pure or innocent may fall in their trap.

- **Malware Based Phishing:**

This refers to scams that include running malicious software on the user's computer or PC's. Malware can be as attachment, downloadable file from the web site for a particular issue for large or medium business, which are not able to keep their software update.

- **System Reconfiguration:**

Change the setting on a user's computer for malicious purpose. Ex: of this attack is a bank website URL may be changed from "bankofxyz.com" to "bancofxyz.com".

- **Data Theft:**

Unsecured computers often contain subset of confidential information stored on secured server. Certainly computer or PC's are used to access such server and can more easily adjustable. Data theft is used to business spying or espionage.

- **Spear Spoofing:**

Phishing directly attempt at specific individuals have been decided spear phishing. Attacker gains the information to the targeted system to increase their probability of success.

- **Clone Phishing:**

It is a type of attack in which the legal or lawful or legitimate users delivered the mail that contains the attachment or link. This attachment or link replaced with the malicious code that sends from the email address spoofed to appear the original sender.

- **Email Spoofing:**

Email spoofing is the email activity in that the sender address and other emails title or header are altered through the email originated from the various sources.

VARIOUS PHISHING TECHNIQUE USED BY THE ATTACKER

- Embedding a link as an email that a card to change or redirect your employee to unsecure website that ask for personal or confidential information.
- Installing Trojan via malicious email attachment or links that contains harmful code or information.
- Spoofing the sender address in an email to appear as ahonourable or respectable or reputable source and ask for personal information.
- Attempting to obtain company information via the telephone or mobile phone by the role of a known company vender.

PREVENTION OF PHISHING ATTACK

- **Encrypt Data:**

Attacker are on the gyration or prowl for any type of company held data are lying around, such as bank chores or routing digits to employee social security numbers. If your company is holding on the important data, then this data need to ensure encrypted. Make your information keep safe or protected using 'full-disk encryption' tool. This feature requires some additional attention. Because the encryption only active the big screen or scenario when a login is not use. This means that attacker away from the computer like during the lunch break, in order to attack a system with malicious code or viruses. To capable your computer automatically log out after 10 minutes without use.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

- **Always verify a websites security:**

Even if you have installed anti-phishing toolbar, you need to verify the site security when ever ask to personal or confidential information. Always make sure the website URL begins with "https" and look the closed lock icon on the address bar.

- **Be alert of pop-ups:**

Pop-ups window can passes a legal or lawful or legitimate component of a website. However pop-ups are usually phishing attempts. The most browsers can allows the block pop-ups.

- **Check your account regularly:**

If you have not used any online account for several months don't assume that your account is secure. In order to prevent bank phishing and credit card phishing personally check your account or statement regularly.

- **Use firewall:**

Firewall act like buffers between your computer and outside intruders. You can use two different type of firewall that is desktop firewall, network firewall. First option is a type of software. The second option is a type of hardware when it is used together, they reduce the odds of phisher in filtrating your computer.

- **Never give out personal information:**

Never share your personal or financial or sensitive information over the internet. Make the habit of check the address of that website. Most of the phishing emails will directly go to pages where entries for financial or confidential or personal information are required. Never sends an email with confidential information to anyone.

- **Use Antivirus software:**

There are many reasons to use an antivirus software. The anti-spyware and firewalls setting are used to prevent phishing attacks and user update the program regularly. The antivirus always scans every file which comes from internet to your computer or PC's.

- **Never click on links included in emails:**

Do not click on hyperlinks attached in the email. As it might directly it go to a fake website. The website directly copy or type into browser.

WHY SHOULD CARE ABOUT PHISHING

By email, hacker use phishing to gains yours personal or financial or confidential information. It is a common way for the hacker to impersonate faithful person our company in an attempt to collect enough information to theft your identity. This email can also include hyperlinks that can contain malware code that can affect your computer system when clicked on. Hackers are very cultured or sophisticated this days and can easily set up fake website that gain your information without you realize it too late.

Eg: A hacker can send circulate you a link it is look or view as like real link but "bogus" website, ask for information like name, address, telephone number, and bank account details that they are used for personal use.

WHAT TO DO?

Delete the emails or text message that ask you to provide personal information (credit card and bank account details etc.). Legal companies doesn't ask for this information via email or text message.

The message may appear from organization they might threaten to close your account or take other action if you don't respond.

Don't reply or call phone numbers provided in that message either this messages direct you to spoof sites that look real but whose motive is to gain your personal information.

Some scammer ask for the phone number to update your account.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

REPORT PHISHING EMAILS

Forward phishing emails to spam@uce.gov and to the company, bank or organization part in the email. You also may report phishing email to reportphishing@antiphishing.org. The anti-phishing working group, a group of ISP's security vendors, financial institution and law enforcement agencies, and uses this reports to fight phishing.

If you might have been tricked by a phishing email:

- File a report with the Federal Trade Commission at www.ftc.gov/complaint
- Visit or meeting the FTC's identity or familiarity larceny website. Victims of phishing could become victims of identity; there are steps you can take to minimize your risk.

IV. CONCLUSION

Phishing is the big problem in the social media. Phishing is problem that cannot solved with new ideas or ways of attacking the user. This paper discuss about what is phishing, types of phishing, why should care about phishing, what to do when phishing is performed and where to report about phishing.

REFERENCES

1. suganya-2016-ijca-909084.pdf: a review of phishing attack and various anti-phishing techniques
2. Prevention-model-for-phishing-attack-in-webapplication-using-linkgaurd-algorithm.pdf: Prevention Model for Phishing Attack in Web application using Link Guard Algorithm.
3. IJEDRCP1403012.pdf: preventing phishing attacks using anti-phishing prevention technique.
4. IJARCCE50.pdf: a literature survey on phishing attack technique.
5. E01432836.pdf: intelligent phishing website detection and prevention system by using link guard algorithm.
6. ACS10143.May2014.04.pdf: review of phishing detection technique.
7. 34_A Survey.pdf: a survey on phishing detection and prevention technique.
8. 10.1.1.679.3229. Pdf: a survey on phishing attack techniques.
9. 10.1.1.429.3444. Pdf: A survey paper on phishing attack.