ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Phishing Techniques and Preventive Measures - A Review

Aeshwarya , Suman kumari

PG Student, Department Of Computer Science, K.L. Mehta Dayanand College, MDU, Faridabad, Haryana, India

PG Student, Department Of Computer Science, K.L. Mehta Dayanand College, MDU, Faridabad, Haryana, India

ABSTRACT: Phishing is a malicious activity of cyber criminals or fraudsters to gain personal information of the people to harm them. Such type of malicious activities are growing very fast because of the increase in number of Internet users today. It is a type of cyber crime which affects the people on a large scale. In this paper we have discussed the phishing, it's types and the ways to prevent this malicious activity. Many Anti-Phishing techniques have developed today to stop such type of practices but still it occurs. Some tips are given to identify phishing attacks. Phishing scams could be easily identified if a little attention is given and people on internet are made aware of them.

KEYWORDS: phishing scams, email, fraudsters

I. INTRODUCTION

With the increase in the number of people on internet, some frauds are also increasing day by day. Digitalization has made the our work easy as we don't need to go anywhere. Our smart phone or computer has become our wallet to get everything in just one click. On the other hand, malicious activities are also increasing to make us fool and gaining their access to our wallet. Cyber attacks have made it difficult to work safely on the internet. One of them is Phishing attack.

Phishing could be defined as an activity by criminals whose aim is to gain our personal information such as password, pin, etc. A small link or pop-up window is sent to us which we open and it asks for our personal information to enter there. There are such kinds of people on the internet who always waits for someone to enter their personal information. This information is used by those criminals to fulfill their malicious needs. This practice is common these days due to which many frauds occurs. Criminals find this method to be an easy way to make people fool and commit crime in which they are not caught. Phishing attack is the most easy one to commit crime. It can be the deceptive one, content injection, malware based, data theft, search engine, web Trojans, session Hijacking, key or DNS based.

According to Internet Records, the first time that the term “Phishing” was used & recorded was on January 2, 1996. This occurred in a Usenet newsgroup called Ao Hell. Some other recent cases are :

- Google Docs Warning : a quick warning was given that if there's an email in your inbox asking you to open a Google Docs from someone and you don't know who its is don't open it. It's probably a Phishing email.
- The income tax department, Mumbai has received thousands of complaints from tax payers duped of several crores of rupees by Phishing scamsters. The department has received several thousand of complaints from disgruntled tax payers, specially from small towns and remote areas.
- Massive Phishing attack targets Millions of Gmail users in 2017.

II . DIFFERENT TECHNIQUES OF PHISHING

Some common Phishing techniques can be as follows:

1. Deceptive Phishing

- It is the most common technique by which fraudsters attempt to steal people's personal information or login credentials. It frequently uses threats to scare users so that the users necessarily provide their information.

2. Spear Phishing

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

- It's goal is same as that of the Deceptive Phishing. In this fraudsters customize their attack emails with the target's name, position, company, work phone number and other information to trick the recipient into believing that they have any connection with the sender.

3. CEO Fraud

- In this type of attack, target can be anyone in an organization. Fraudsters attempt to harpoon an executive and steal their login credentials

4. Pharming

- This is a method to attack which stems from DNS cache poisoning. Under this attack, a pharmer targets a DNS server and changes the IP address associated with an alphabetical website name.

5. Dropbox Phishing

- Millions of people use Dropbox everyday to back up access and share their files. Attackers try to capitalize on the platform's popularity by targeting users with Phishing emails.

6. Google Docs Phishing

- Google Drive supports Documents, spreadsheets, presentations, photos and even entire websites.This technique targets Google Drive similar to the way they prey upon Dropbox users. In this method fake login pages are created.

III. LITERATURE REVIEW

Most of the time, Phishing scams happens through email. Hackers spoof the email address of any legitimate website or authority to send phishing scam email. Users are convinced to believe that the email has been sent by legitimate website. At the time users open that email and enter their personal information, their information is gained by the criminals and then those criminals forward that email to others in your contact list.

To put phishing page in a URL, you need to have two things

- ❏ Domain
- ❏ Web Hosting

An undetectable page is created and sent through email or message.

How the Phishing scams are created :

1. Create a page with gmail, Facebook or any other platform.
2. Set URL as legitimate one.
3. Send that link with an attractive or scary message through email or message which makes the users to open that.
4. Wait for the users response. This is all done.
5. When the user enter any data it shows it in your web database.

Tips to identify the Phishing scams:

- Spelling and bad grammar
  - Professional companies have a staff of editors that will not allow a mass email with such mistakes to go out to its users.
- Links in email
  - Rest your mouse(but don't click) on the address matches the link that was typed in the message.
- Threats
  - Cyber criminals often use threats that your security has been compromised to scare users.
- Spoofing popular websites or companies
  - Cyber criminals use web addresses of well known companies but are slightly altered.

These tips are helpful in identifying such type of practices which could harm any person or organisation at large scale. Many websites are estimated which contains such links. We have to be very aware about them. While any transaction, shopping, banking, social sites communication, etc. on internet, a proper attention is needed otherwise it's result could be dangerous.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

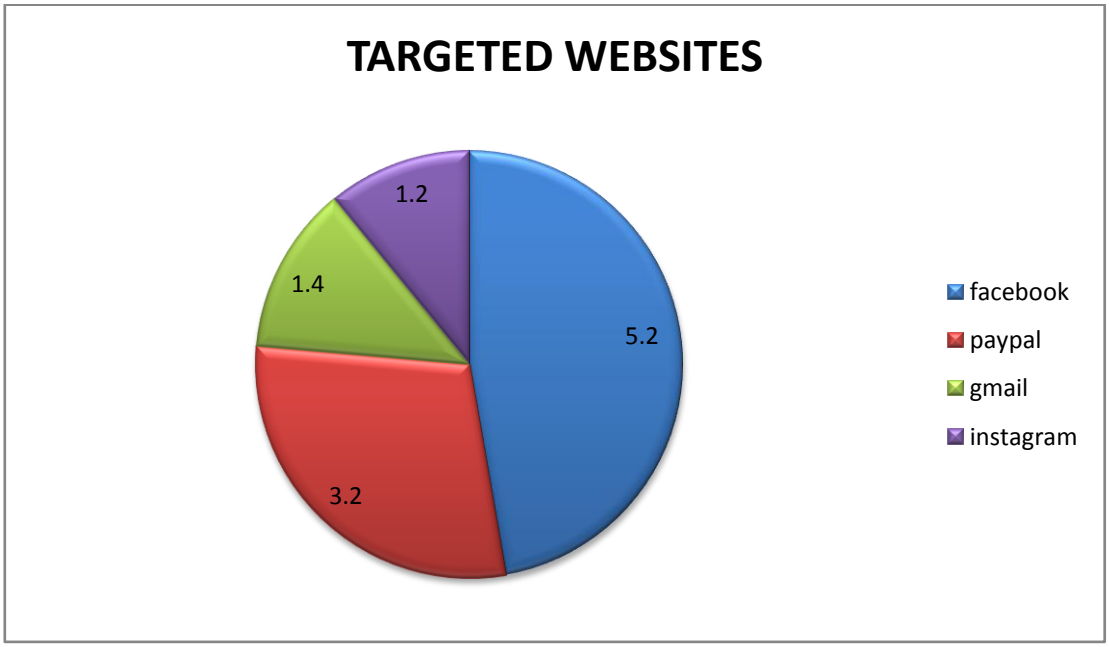
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Graph below shows the top websites affected through phishing:



IV. PREVENTIVE MEASURES

Phishing attacks have become common malicious practices to gain the personal information of the users. Awareness among the people is the only way to prevent such cases. Cyber crime Investigation cells are at many places but here the issue is our privacy. A small attention can save your personal information and reduce number of fraud cases.

Some common ways to prevent Phishing scams :

1. Guard against scam.
2. Communicate personal information on secure websites.
3. Do not click on links, download files or open attachment in emails from unknown senders.
4. Never send your personal or financial information even if you are close with the recipient.
5. Beware of links in emails that ask for personal information. Businesses should not request personal information to be sent via email.
6. Beware of pop-ups. Never enter personal information in a pop-up screen. Do not click on links. Don't copy web addresses into your browser from pop-ups.
7. Protect your computer with a firewall, spam filters, anti-virus & anti-spyware software.
8. Check your online accounts & blank statements regularly.
9. Enter a fake password when promoted.
10. Keep browser and Operating System up to date.
11. Always use updated antivirus & firewall software.
12. Check URL. Verify HTTPS with green secure sign on address bar. Use Firefox to differentiate between sub-domain and domain.
13. Utilize back up system copies to revert to an uncorrupted system if attack is suspected.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

V. CONCLUSION AND FUTURE SCOPE

Criminals find an easy way to commit crime in this world of Internet. Many Anti-Phishing techniques have been developed today to reduce the cases. These Anti-Phishing techniques provide security at various levels. But still there is a need of attention and awareness among the users also. Lack of awareness is the main cause to open such fake links. Using preventive measures is the only way to reduce such malicious activities. A small attention can save our data and privacy. The preventive measures as mentioned above must be kept in mind while working on the Internet. Government is taking many steps to investigate such crimes but to reduce them we must put our hands together. These cases could be reduced through awareness because criminals try such type of practices where there is knowledge but lack of awareness.

REFERENCES

1. V. Suganya, A Review on Phishing Attacks and Various Anti Phishing Techniques, IJCA(0975-8887), Vol. 139 No 1, April 2016
2. Jyoti Chitkara, Ritu Dahiya, Neha Garg, Monika Rani, Phishing & Anti-Phishing Techniques: case study, IJARCSSE, ISSN - 2277.128X, Vol 3 Issue 5, May 2013
3. U. Naresh, U. Vidya Sagar, C. V. Madhusudan Reddy, Intelligent Phishing website Detection & Prevention System by using link Guard Algorithm, IOSR Journal of Computer Engineering, vol. 14, issue 3