International Journal of Recent Trends in Engineering & Research
ISSN : 2455-1457 Impact Factor : 3.344

PHISHING ATTACKS: A NEED REVIEW

Mr. Shailesh P. Thakare[1], Mr. Shrikant N. Sarda[2], Mr. Nitin M. Shivratriwar[3]
[1, 2, 3] *Department of Information Technology, PRMIT & R, Badnera-Amravati*

Abstract—Phishing is the act of using electronic media fraudulently to try to get the recipient to reveal personal data. In this artists send messages which look like original urging the recipient, to take some action to avoid a negative consequence or to receive a reward. Today almost everyone uses an electronic media to send and receive a messages it is very easy for phishers to track target users and get their personal information by using some tricks. There are so many types of such phishing attacks and tricks. We tried to cover some information about phishing and its types.
Keywords—*phishing, reasons of phishing, phisher, types of phishing*

I. INTRODUCTION

Phishing is an automatic form of social engineering where criminals also called phishers use the Internet services to get the sensitive information of businesses or individual persons, without knowing them. Phishers mimic electronic communications from a trustworthy or public organization in an automated fashion. Phishing emails or communications always ask victims to click a link that will guide the victim to a forged website where personal information is requested. For general consumers' email attack, the purpose of phishing is to get personal identity, credit card number or authentication information such as user name and password. Email phishers are always in search of high profile targets to steal authentic information such as intellectual properties, trade secrets, even national security related information. Phishing is a dangerous to online-businesses. The damage caused by phishing is unrecoverable. Ladder of trust that organizations build with their customers may be ended. Customers decreases their level of trust on the reliability of online-businesses, companies loss their customers foundation, reputation, and credibility, which turn into financial loss, resources and time loss. [1, 2]

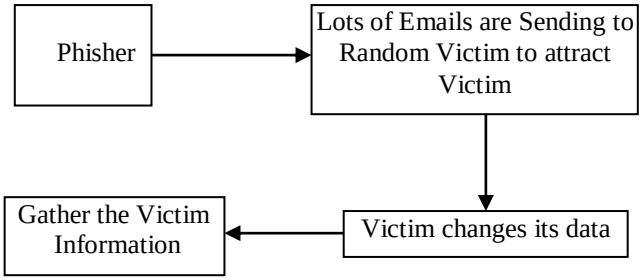
Most methods of phishing use some form of technical deception designed to make a link in an e-mail appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by phishers. Example: www.gmail.com – original link, www.gmai1.com – Fake link. Here are a few phrases that a phishing page may contain verify your account, businesses should not ask you to send passwords, login names, social security numbers, or other personal information through e-mail.

II. GENERAL PHISHING PROCESS

Phisher uses replica of original website as a trap that is send to the user. When user hooked up in the trap by filling and submitting his information phisher saves the data for his own use.

Generally, phishing attacks are carried out as follows:

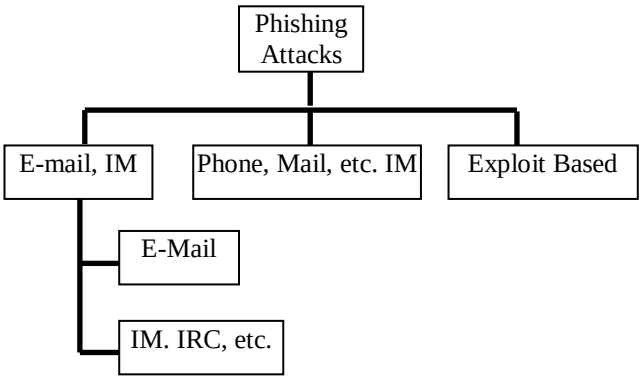
- Creation of fake web site which mimics the original Web site.
- Phisher then send link of the fake web site with large amount of spoofed e-mails to target users in the name of legitimate companies and organizations, trying to convince the victims to visit their web sites.
- Victims visit the fake web site by clicking on the link and input their useful information.
- Phishers then collect the personal information and perform fraud such as transferring money from the victims' account.



There are thousands of fake phishing websites established online every day, luring a number of customers [3].

III. TYPES OF PHISHING ATTACKS

Phishing can be done in various ways like, email to include VOIP, SMS, instant messaging, social networking sites, phone call and even online games. Below are some major categories of phishing [3, 4].



1. **Deceptive Phishing:** In this type messages like, need to verify your account information, due to system failure needs user to re-enter their information details, undesirable account changes, new or promotional free services requiring quick action, and many other are broadcast to a wide group of users with the hope that the some of them will respond by clicking a link to or signing onto a bogus site from where their information can be gathered.

2. **Clone phishing:** In this phisher creates an exact replica of email. This can be done by gathering information such as data and recipient addresses from a legitimate email which was send previously, and then phisher sends the same email with his links. He also employs address spoofing so that the email appears to be from the original sender. The email can claim to be a re-send of the original or an updated version as a trapping strategy.

3. **Spear phishing:** in spear phishing specific group is get targeted. Spear phishers target selected group of users with some common attribute.

4. **Phone phishing:** it refers to calls/messages that claim to be from a bank, insurance company, asking users to dial a phone number regarding problems with their accounts.

5. **Malware-Based Phishing:** it involves running malicious software on target machine. Malware can be planted using an email attachment, downloadable file from a web site, or by exploiting known security vulnerabilities.

6. **Keyloggers and Screenloggers:** These are types of malware which trace the keyboard input and pass to its tracker via Internet. They can merge themselves with users' browsers as utility

programs called as helper objects which run automatically when the browser is opened as well as into system files as device drivers or screen monitors.

7. **Web Trojans:** Pop up in hidden mode when users are getting log in. They collect the user's credentials locally and transmit them to the phisher.

8. **Hosts File Poisoning:** When a user enters a URL in address bar of browser to visit a website it must first be translated into an IP address before it's transmitted over the Internet. The majority users' PCs running a Microsoft Windows operating system first look up these "host names" in their "hosts" file before undertaking a Domain Name System (DNS) lookup. By "poisoning" the hosts file, hackers have a bogus address transmitted, taking the user unwittingly to a fake "look alike" website where their information can be stolen.

9. **Content-Injection Phishing:** In this phisher replace chunk of the content of a legitimate site with fabricated content designed to misguide or misdirect the user so that user can reveal their confidential information to the phisher.

10. **Session Hijacking:** In this type user activities are monitored until they sign in to a target account or transaction and establish their bonafide credentials. At that point the malicious software takes over and can undertake unauthorized actions, such as transferring funds, without the user's knowledge.

11. **System Reconfiguration Attacks:** In this phisher customizes user's computer so that he can use those customization for malicious activities.

12. **Data Theft:** Most of user's computers often have sensitive information stored somewhere on secured servers. Computers are used to access such information from servers and can be more easily compromised. Data theft is a widely used approach to business espionage. By stealing confidential communications, design documents, legal opinions, and employee related records, etc., thieves profit from selling to those who may want to embarrass or cause economic damage or to competitors.

13. **DNS-Based Phishing ("Pharming"):** Hosts file modification or Domain Name System (DNS)-based phishing is also called pharming. In this hackers tamper with an organizations host's files or domain name system so that requests for URLs or name service return a bogus address and subsequent communications are flow towards fake site. In this users are unaware about that the website where they are reveling their personal information is controlled by hackers and is probably not even in the same country as the legitimate website.

14. **Man-in-the-Middle Phishing:** this type of attack is complicated to detect than other types of phishing. In this type of hacker sit in between the user and the legitimate website or system. They record the information being entered but continue to pass it on so that users' transactions are not affected. Later they can sell or use the information or credentials collected when the user is not active on the system.

15. **Search Engine Phishing:** In this phishers create websites with attractive offers and have them indexed legitimately with popular search engines. Users search the sites in the normal course of searching for products or services and are get trapped into giving up their information..

IV. REASONS OF PHISHING

Use of phishing tricks to cheat the user is very had been widely used at least half a decade ago but it still remains as one of the popular method to scam internet users. Just recently, thousands of Tumbler bloggers were affected by a phishing attack which caused their credentials such as username, passwords, and email addresses to be stolen. Many of us might still be wondering why there are so many victims out there even though we had been taught from time to time to stay aware of a phishing scam. There are five reasons here why phishing is still a popular trick and below are the reasons [5].

- **Availability of personal data on social networks**

Popularity of social networks is one of the strongest reason by which it is easier to get information of targeted user. Phisher may collect collect any information or ask users his personal information by using some tricks.

- **Trend of data compromises**

There has been an ongoing trend of data compromises in which email and personally identifiable data have been stolen. To name just a few here, the Epsilon data breach saw hackers gaining illicit access into the company's system and presumably making away with email addresses and contact details of these clients. Beyond five financial organizations that were affected, drug giant GlaxoSmithKline PLC have also issued a warning to customers that their email addresses, names, and the "product website" on which they have registered with the company – may have been stolen.

It is important to remember that not all businesses opt to come clean on data breaches. Moreover, the average hackers endeavor to erase their tracks after gaining what they came for. The bottom line: A wealth of stolen information is floating around out there available for exploitation.

- **It tricks the victim with fear**

One of the most common methods is to trick the victim by sending them an email and tell them that their internet banking account is being compromised and need to click on a link to resolve the issue. Once the user followed the link, the user will be redirected to some forged website that looks similar to the banking website which requires the user to input his/her username and password. Once that form is sent, all the data will be transmitted to the attacker controlled server. Users who have a large amount of cash in their banking account will be scared to see this mail and some of them will follow the mail to avoid their account being compromised.

- **It tricks the victim with special interest**

Some phishers use the tricks like you won lottery, selected for some promotional events or viewing adult material to create a temptation for the victim to click on a link that redirects to the phishing site.

- **Effectiveness of spam filters against traditional spam**

Spammers have tried practically every trick in the book over the years, including the use of image spam, creative misspelling of words, and even resorted to the use of email attachments. Modern spam filters have the benefit of borrowing from all the lessons learnt since the invention of electronic mail, and employs a plethora of advanced technologies such as cloud-computing to eliminate them. Indeed, one may almost be tempted to consider the problem of spam as one that has already been overcome on some days. As you can imagine, spammers are forced to adopt sophisticated spear phishing techniques in order to reach their victims.

The damage cause by phishing ranges from the users who become victim to a phishing site, some of these examples are:

- Loss of e-mail accounts
- Substantial Financial Loss
- Users cannot access accounts that they own

Phishers can use the information they gain to create accounts in their victim's name. They can then also ruin a person's credit or even prevent the user from accessing their account is estimated that, between May 2004 and May 2005, approximately 1.2 million computer users in the United States suffered losses caused by phishing totaling approximately $929 million.

V. WHAT NEED TO DO

Phishers are getting successful due to users negligence, not because of technological lacunas; its users responsibility to be aware while browsing, they must be aware about what information should share over the Internet, and to whom they are sharing the information. Phishers uses many sophisticated techniques for their purposes which are more difficult to detect, even for experienced computer users. As recently as 2007, the adoption of anti-phishing strategies by businesses needing to protect personal and financial information was less. Now days there are various techniques to fight with phishing, including legislation and technology created specifically to protect against phishing. These techniques include steps that can be taken by individuals, as well as by organizations. People can take steps to avoid phishing attempts by slightly modifying their browsing habits.

Education: Education is a vital component of the phishing battle—as well as other online scams. The Federal Trade Commission suggests some things to remember:

- Don't reply to e-mails asking to confirm account information. Call or logon to the company's web site to
  Confirm that the e-mail is legitimate.
- Don't e-mail personal information. When submitting information via a web site, make sure the security lock is displayed in the browser.
- Review credit card and bank account statements for suspicious activity
- Report suspicious activity.

Social Responses: One strategy for combating phishing is to train people to recognize phishing attempts, and to deal with them. Education can be effective, especially where training provides direct feedback. One newer phishing tactic, which uses phishing emails targeted at a specific company, known as spear phishing, has been harnessed to train individuals at various locations.

Technical Responses: Anti-Phishing measures have been implemented as features embedded in browsers, as extensions or toolbars for browsers, and as part of website login procedures. The following are some of the main approaches to the problem.

a. Helping to identify legitimate sites
b. Browsers alerting users to fraudulent websites
c. Augmenting password logins
d. Eliminating Phishing mail
e. Monitoring and takedown

Legal Responses: In the United States, Senator Patrick Leahy introduced the Anti-Phishing Act of 2005.Companies has also joined the effort to crack down on Phishing.

Using anti-phishing software: Anti-phishing software consists of computer programs that attempt to identify phishing content contained in websites and e-mail. It is often integrated with web browsers and email clients as a toolbar that displays the real domain name for the website the viewer is visiting, in an attempt to prevent fraudulent websites from masquerading as other legitimate web sites. Anti-phishing functionality may also be included as a built-in capability of some web browsers.
Some of the Client-based anti-phishing programs are:-

- avast
- Avira Premium Security Suite

- EarthLink Scam Blocker (discontinued)
- eBay Toolbar
- Some of the Cloud-based anti-phishing services are:-
- google Safe Browsing API
- Web root Real-time Anti-Phishing API
- isitphishing.org (http://www.isitphishing.org) - URL analysis service /api

Technology: Unfortunately, phishing usually involves social engineering tricks, and, thus, even the best defenses that a company might have in place to combat outside threats are sometimes useless against these types of attacks. Although education is likely the best defense against phishing scams, there are technologies that make phishing harder to accomplish. When implemented with a defense-in-depth approach, software and hardware can be installed to slow the phishers down.

VI. CONCLUSION

In this paper we have tried to explain what is phishing, phishing is very dangerous and causes many critical problems if we cant aware and fight against it. There are many technological solutions are available as antiphishing tools but they have their own limitations since phishers uses new tactics day by day. Yet avoiding or stopping the phishing completely is impossible. Awareness about phishing, carefulness while browsing or communicating with others are the only solutions to protect individuals as well as organizations from the phishing attacks.

REFERENCES

i. Qingxiong Ma" The process and characteristics of phishing attacks: A small international trading company case study", University of Central Missouri, Journal of Technology Research, http://www.aabri.com, pp 1-16.

ii. Bryan Parno Cynthia Kuo Adrian Perrig, "Phoolproof Phishing Prevention", December 3, 2005 CMU-CyLab-05-003, Carnegie Mellon University.

iii. Gaurav, Madhuresh Mishra, Anurag Jain / International Journal of Engineering Research and
iv. Applications (IJERA) ISSN: 2248-9622 www.ijera.com, Vol. 2, Issue 2,Mar-Apr 2012, pp.350-355

v. Md Rashid Hussain, Garima Srivastava, "A REVIEW PAPER ON PHISHING – A GROWING SCAM", International Journal of Advance Research In Science And Engineering http://www.ijarse.com,IJARSE, Vol. No.3, Issue No.5, May 2014 ISSN-2319-8354(E) ,www.ijarse.com

Gaurav Kumar Chaudhary "Development Review on Phishing: A Computer Security Threat "International Journal of Advance Research in Computer Science and Management Studies Volume 2, Issue 8, August 2014 pg. 55-64,www.ijarcsms.com