

# Phishing Attack

<sup>1</sup>MR. MOHIT KUMAR

<sup>2</sup>MR.SATENDER YADAV

<sup>3</sup>MR.SHOBHIT KUMAR

<sup>1</sup>CCSIT TMU, Moradabad

<sup>2</sup>CCSIT TMU, Moradabad

<sup>3</sup>ASSISTANT PROFESSOR ,CCSIT TMU, Moradabad

<sup>1</sup>[lavchauhanlav888@gmail.com](mailto:lavchauhanlav888@gmail.com)

<sup>2</sup>[satenderyadavyadav8@gmail.com](mailto:satenderyadavyadav8@gmail.com)

<sup>3</sup>[shobhit.computers@tmu.ac.in](mailto:shobhit.computers@tmu.ac.in)

**Abstract**— The Internet has a remarkable platform for common people Communication .persons with criminal mind have found a way of stealing Personal Information without actually meeting then with the least Risk Of being caught. It is called phishing. poses a threat to the e- commerce industry. Not only does it shatter the confidence of electronic services example is “we need you to confirm your account Customers towards e-commerce, but also causes Providers tremendous we must shut your account approach down phishing .This paper gives About awareness about phishing attack and anti- phishing tools .

**Keywords**— phishing, phishing step, phishing types ,anti-phishing tools.

## I. INTRODUCTION

Phishing is an act of attempting a victim for fraudulently acquires sensitive Information by impersonating a trustworthy third party which could of phishing Attack Is to trick receivers into divulging sensitive information as bank such account Numbers, password and credit card details .for instance phishing may misrepresenting Himself as banking corporation or popular on Both academia and industrial practitioners have proposed various anti-phishing Measures in order to safeguard the interests of customers, and online security survey Policies. Some commercial ant-spam and from anti-phishing products stop blacklisted” Sites that they claim are known sites, The usability evaluation a indispen sable for the future .now a day five typically Anti-phishing Toolbars are in use as built in phishing toolbars are in use as built-in phishing prevention in the Internet Explore7.0 netcraft anti-phishing toolbar and spoof Guard, In addition, internet Explorer plug-in, anti-phishing IE plug. Account to the heuristic

Usability evaluation, a number of usability issue may found.

## 2. STEPS IN PHISHING

A persons who engaged in mal ware activities is called a phisher. Phishing attacks today typically employ generalized ‘iures”, intimidated users and creating fear –a common example is “we need you to confirm your account details or we must shut your account down “,an approach which is believed To become more and more common is context a were attack: this is a more complex approach as it not only use threat or enticement, but makes the victim think of the message as expected, therefore legitimate.

The method used by phishers is usually to make fraudulent website by mimicking the HTML code containing the same images, text and sections. some phishing websites register a similar domain name to the legitimate website of company or a bank. The most common method used phishers is by forms, for example, the internet banking login page a form for password verification many phishing attempts use domain spoofing or homographic attacks (Gabilovich & Gontmakher) as a step towards persuading victim to give out personal information. Including user names and password, and other personal information.

A phisher could target many kinds of confidential information, including user names and password,

credit card numbers, bank account numbers, and other personal information. In a study by Gartner(Gartner Inc,2004),about 19% of all those surveyed reported having clicked on a link in a phishing email, and 3% a admitted to giving up financial or personal information.

A common phishing attack is (for a phisher) to obtain a victim’s authentication information corresponding to one website (that is corrupted by the attacker) and then use this at another site. This is meaningful attack given that verbatim or with only slight modifications. phishing attack lifecycle can be decomposed in:

- .planning,
- .attack,
- .collection,
- .fraud and.
- .Post-Attack Actions.

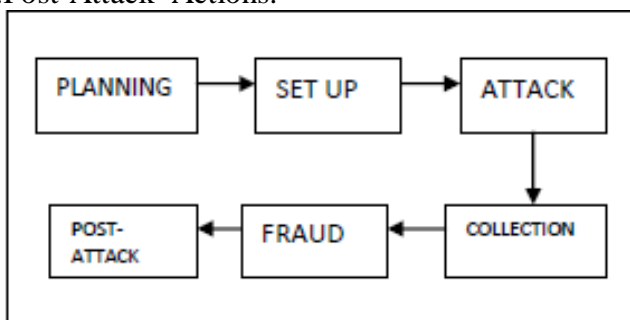


Figure.2.1 steps in phishing

The phishing plans the attack, created the attack code /message and sends to the target user. A malicious message arrives at the target site. The ignorant target reads the message and takes some action which makes him or her vulnerable to an information compromise. The server to the phishing. The phishing engages in fraud Using confidential information to impersonate the user.

There is no single way that can prevent all phishing. But Different method applied at different stage of phishing attack can abort a phishing attempt a

phishing attempt and properly applied technology can significantly reduce the risk of identity theft.

### 3. TYPES OF PHISHING ATTACKS

Phishing send legitimate looking emails from government agencies and other financial institution with A motive to obtain personal information or unknowingly install a malware on their computer. The categories of phishing shown .

There are different types of phishing attacks prevalent at Present .Analyzing is categorized into 3 different kinds

- 1 Deceptive phishing
2. Crime ware based phishing
3. Other types as DNS based phishing ( content injection phishing)

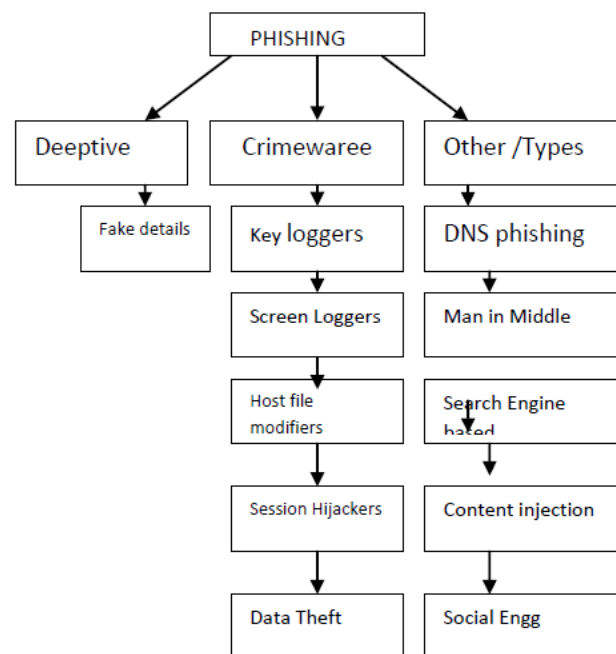


Figure.3.1 Types of phishing

3.1.Deceptive phishing- involves the sending of email message using make believe logos of reputable financial institutions and other organizations, which the user are prompted to click .

Users may be fooled by the domain name in these types of attacks.

Eg. [www.paypi.com](http://www.paypi.com) use a lowercase “i” which looks similar to the latter i for the latter “i” and [www.paypal.com](http://www.paypal.com) substitutes the no 1 for the latter i.

### 3.2. Malware based phishing

Is a widely prevalent collection of phishing techniques which include key loggers and screen loggers hosts file poisoning web Trojan, system reconfiguration attack and spear phishing, session hijacking data theft malware based techniques tend to install and run malicious software on the users machine.

### 3.3. Other types

#### (a) DNS based phishing

relies on hosts file modification. Using this type of phishing change the hosts file such a way that request for URLs the website where they are entering confidential information to the phishing.

(b) man- in- middle phishing the phishing position himself between the user and a genuine website and captures the information and sells.

#### (c) Fake website

APWG member PandaLabs tracks the number of malware variants detected, which has been growing each

quarter, During the fourth quarter of 2014 this figure broke a new record, with 23,500,000 malware samples detected, an average of 255,000 new threats each day. Never in the history of computer security has the amount of new malware created been so high. In fact, the vast majority are just variants of existing malware modified by their creators to evade signature based detection systems, while the functionality is the same .still the escalating numbers illustrate the adaptability of the code and the creativity of the malware authors. The following figure shows the increase of fake website during the year.

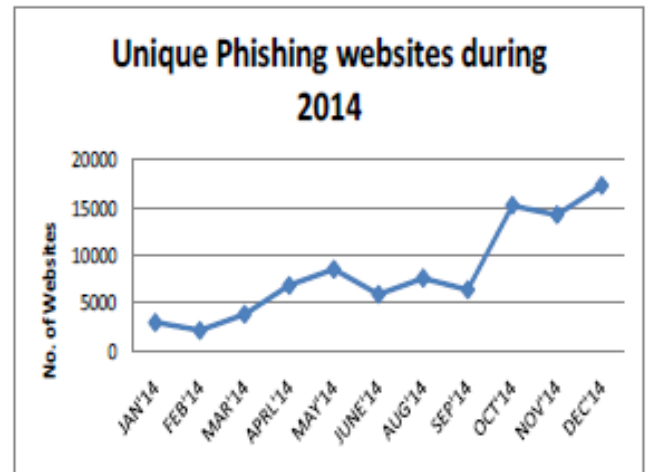


Figure.3.2 Increase of fake website during the year2014

#### (d) Phishing email

It will typically direct the user to visit a website where they are asked to update personal information, such as a password, that the legitimate organization already has

Phishing e-mail will contain some of these common elements:

- 1.The “form field” appears to be from the legitimate company mentioned in the e-mail. It is important to note, however, that it is very simple to change the “from” information for any e-mail client.
2. The e-mail will usually contain logos or images that have been taken from the web site of the company mentioned in the scam e-mail.
- 3.The email will contain a link or hyperlink to a website with a similar URL name as the “real” sender. Note that the hyperlink does not point to the legitimate Citibank website URL.

#### (a) Filter evasion

Phishing have used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing e-mails. More fraudsters are adopting new approaches in an effort to make phishing sites undetectable by common

security measures such as firewalls and content filtering web proxies.

#### (b) Phone phishing

Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone numbers were dialed, prompts told users to enter their account numbers and PIN. Phishing sometimes uses fake caller-id data to give the appearance that calls come from a trusted organization.

### 4. ANALYSIS ABOUT PROBLEMS

#### 4.1 Security loop holes

3 main areas

- a. Non uniformity of internet standard,
- b. Security loopholes in mail transferring Mechanism and
- c. Security loopholes in users system.

#### 4.2 General Phishing solutions

(a). Primarily the solutions are

1. technological remedies
2. policy changes
3. awareness and training programs

(b). Technological

1. Stripping URL that contains IP address
2. Blocking internet address that originates outside the perimeter
3. Monitoring bounced email message

#### 4.3 Potential policy changes

(a). Registering any obvious and available deceptive domain names

(b). Establishing standards of the styles and distribution of mass email.

(c). Using personalized messages

#### 4.4 Awareness and training programs

(a). Making use of regular communication to explain the phishing problem

(b). Establishing a simple mechanism reporting phishing attacks

(c). Posting alerts on security website

### 5. ANTI-PHISHING TOOLS

#### 5.1 mail-secure

Mail secure anti-phishing combines several layers and technology to detect and block phishing attempts. The main technologies used are:

(a). Anti-phishing database-mail-secure maintains a database which is updated on a daily basis. This database features millions of known phishing URLs. If a URL appears in a mail, it is blocked.

(b). SURBL- RBL which is designed to block in the body of the message. In this case, message. Instead, SURBL is used to block the source of the spam based on its message content.

Even if a spammer uses new domains, they may point to the old, blocked IPs and will therefore be blocked, right from the first spam message received.

(c). Commtouch RPD- Commtouch's recurrent pattern detection [RPD] is based on the fundamental characteristic of phishing, spam and email-borne malware-its mass distribution over the Internet. Sniffers located worldwide, look out for real traffic in over 60 million operational mailboxes. They then extract patterns to detect recurring patterns and examine the number of sources to determine if they are Trojan-based outbreaks. Commtouch RPD™ differentiates between bulk mail (which can be a mailing list), and confirmed spam.

Commtouch RPD™ advantages

- Generates patterns from more than 300 million daily messages, from over 15 locations worldwide.
- Real-time – blocks spam from the first minute of the outbreak.
- Near-zero false positives – as the pattern of legitimate mail sent from one to another will probably appear only once.
- Content-agnostic – effective against Phishing, fraud and innocent-looking spam.

- Language independent.
- Detects spam of any file type.
- Adaptive technology – As spam is economically motivated, spammers constantly change tactics to achieve mass distribution.

#### **(d).Heuristic Fraud detection sets of rules -**

Mail-Secure uses Heuristic rules in order to detect possible new Phishing attempts. Mail-SeCure has over 2,500 sets of rules to detect characteristics of Phishing. The heuristic engine uses a score-based system to identify Phishing.

**Zombie detection** - Most Phishers use zombie computers to distribute their mail. Zombie computer are computers that were involuntarily hacked (whether by Trojan horses or by direct hacking) and used for mail distribution.

Mail-SeCure has a unique Zombie Detection System – ZDS. It identifies zombies and automatically blocks them at the session level (similar to RBL). PineApp has a central ZDS, RBL-like server, which dynamically blocks identified IPs. Since a zombie computer owner can change his IP, ZDS automatically adds or removes IP addresses from blacklists.

**(e). IP Reputation** - a powerful addto block Zombies at the SMTP session level. The IP Reputation mechanism is based on sniffers located at various points of the world, monitoring traffic of hundreds of millions of email messages daily. IP Reputation center dynamically classifies IPs, according to a profile built from parameters such as: volume, percentage of spam & viruses and elevations. When an SMTP session is established, Mail-SeCure queries the IP Reputation system (or uses local cache) and performs various actions according to the IP classification, such as: permanently reject the mail, respond with a temporary error to be able to re-evaluate the IP on the retry time, activate grey-listing, activate Rate limit, etc.

**(f) Rate limit** - provides an advanced layer against layer usedby limiting the amount of messages or

SMTP sessions allowed from a certain IP on a pre-defined time. Rate limit uses a complex algorithm using a sliding-window method. Limitations can be defined for timeframes of: minutes, hours and days. IP Reputation. Saves bandwidth and lowers the load on your Mail-Secure system.

#### **5.2 Security Tool Bar - 5Netcraft**

An Internet services company based in Bath, England's product is Netcraft. It provides web server and web hosting market-share analysis, including web server and operating system detection., The service is able to monitor uptimes uptime performance monitoring is a commonly used factor in determining the reliability of a web hosting provider depending on the queried server's operating system. Netcraft also provides security testing, and publishes news releases about the state of various networks that make up the Internet.

The company is also known for its free anti-phishing toolbar for the Firefox and Internet Explorer browsers. Starting with version 9.5, the built-in anti-phishing filter in the Opera browser uses the same data as Netcraft's toolbar, eliminating the need for a separately installed toolbar. A study commissioned by Microsoft concluded that Netcraft's toolbar was among the most effective tools to combat phishing on the Internet, although this has since been superseded by Microsoft's own Internet Explorer 7 with Microsoft Phishing Filter, possibly as a result of licensing Netcraft's data [8].

#### **5.3 ESET SECURITY**

**(a).ESET Smart Security** incorporates anti-spam and a bidirectional firewall along with traditional anti-malware features of ESET NOD32 Antivirus. The acronym NOD stands for *Nemocnica na Okraji Disku* ("Hospital at the end of the disk"),[1] a pun related to the Czechoslovak medical drama series *Nemocnice*

na kraji města (*Hospital at the End of the City*).[2] The first version of NOD32 - called NOD-ICE - was a DOS-based program. It was created in 1987 by Miroslav Trnka and Peter Paško at the time when computer viruses started to become increasingly prevalent on PCs running DOS [9].

**(b).ESET System Inspector** is a diagnostic tool which allows in-depth analysis of various aspects of the operating system, including running processes, registry content, startup items and network connections. Anti-Stealth Technology is used to discover hidden objects (rootkits) in the Master Boot Record, boot sector, registry entries, drivers, services and processes. System Inspector Logs are standard XML files and can be submitted to IT experts for further analysis. Two logs can be compared to find a **ESET** set of items not common to both logs. A log file can be saved as a service script for removing malicious objects from a computer.

**(c).System Rescue Live** is a Linux-based bootable Live CD/USB image that can be used to boot and clean heavily-infected computers independent of the installed operating system. The program is offered free of charge, and can download updates if a network connection is present.

#### 5.4 Browser Integrated Tools

A browser-integrated tool usually relies on a blacklist, which contains the URLs of malicious sites, to determine whether a URL corresponds to a phishing page or not. In Microsoft Internet Explorer 7, for example, the address bar turns red when a malicious page is loaded. The effectiveness of a blacklist is strongly influenced by its coverage, credibility, and update frequency. At present, the most well-known blacklists are those maintained by Google and Microsoft, which are used by the most popular browsers, Mozilla Firefox and Microsoft Internet Explorer, respectively.

#### 5.5 Using Antiphish And Dom Antiphish Techniques

AntiPhish is a browser plug-in that keeps track of sensitive information. Whenever a user

attempts to enter sensitive information on one site, and this information has previously been associated with a different, trusted site, a warning is generated. This is effective when a user inadvertently enters bank login information on a phishing site. However, AntiPhish suffers from the problem that legitimate reuse of credentials is also flagged as suspicious.

To address this usability problem, DOM AntiPhish was proposed. For that approach, the authors compared the Document Object Models (DOMs) of the pages under analysis to determine whether the two pages are similar. When information is reused on a page that is similar to the original page (that is associated with the sensitive data), a phishing attempt is suspected. When the information is entered on a site that is completely different, the system assumes legitimate data reuse. Although DOM AntiPhish is able to identify phishing pages effectively, its major limitation is that the DOM tree is not necessarily a reliable feature to establish similarity between pages. In some cases, it is possible for the attacker to use different DOM elements to create a similar look-and-feel and appearance of a page. Furthermore, a phishing site that only consists of images cannot be detected. A new technique to detect phishes has been implemented in the project, which removes the above said disadvantages.

## Conclusion

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious

Phishing is the attempt to acquire sensitive information reasons, by masquerading as a trustworthy entity in an electronic communication. Now days it has become very serious. There are many techniques to solve these problems. But people may don't aware of the seriousness of phishing. Periodical updating of anti-phishing tools or softwares in their own

systems may help to secure their confidential information and credentials. This study may give the awareness about the phishing problems and solutions.

## References

- [1] Anti-Phishing Working Group, Phishing Activity Trends Report (May 2014). [[www.antiphishing.org/reports/apw](http://www.antiphishing.org/reports/apw)]
- [2] Anti-Phishing Working Group. Phishing Activity Trends Report (November, 2014).
- [3] AVIRA antivirus report. [[www.avira.com/en/threats/section](http://www.avira.com/en/threats/section)].
- [4] Camp LJ, Goodman S, House CH, Jack WB, Ramer R and Stella M. Chapter 6: Offshoring: Risks and Exposures [[www.acm.org/globalizationreport/](http://www.acm.org/globalizationreport/) ... ].
- [5] CERT-In Annual Report (2014). [[cert-in.org.in/knowledgebase/ann ...](http://cert-in.org.in/knowledgebase/ann...)]
- [6] Emigh, A (2014). Online identity theft: Phishing technology, chokepoints and countermeasures. ITTC Report on Online Identity Theft Technology and Countermeasures; <http://www.anti-phishing.org/Phishing-dhs-report.pdf>.
- [7] Gabrilovich E and Gontmakher A. (2014). "The Homograph Attack," Communications of the ACM, 45(2):128.
- [8] Gartner Inc. (2014). Gartner study finds significant increase in e-mail phishing attacks. [[www.gartner.com/5about/press re](http://www.gartner.com/5about/pressre)].
- [9] ESET NOD32 - Wikipedia, the free encyclopedia
- [10] [[https://en.wikipedia.org/wiki/ESET\\_NOD32](https://en.wikipedia.org/wiki/ESET_NOD32)]