# PREDICTION OF PHISHING - An Online and Offline Technique of Spamming

Nishan.A.H[1], Mari Selvi.K[2], Ms. S. Agnes Joshy[3]
[1,2] UG Scholar, Department of Information Technology, Francis Xavier Engineering College, Tirunelveli.
3 Faculty, Department of Information Technology, Francis Xavier Engineering College, Tirunelveli.

## ABSTRACT

In computing, phishing is a criminal activity that uses social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using email or an instant message, although phone contact has been used as well. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, and technical measures. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of the legitimate entity's URL over the address bar, or by closing the original address bar and opening a new one containing the legitimate URL. Phishing generally requires the fake website but, not all phishing attacks require a fake website the term phishing is a variant of fishing, probably influenced by phreaking, and alludes to the use of increasingly sophisticated lures to "fish" for users' financial information and passwords. There are several different techniques to combat phishing, including legislation and technology created specifically to protect against phishing.

## INTRODUCTION

In the field of computers security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as user names, passwords and credit card details, by masquerading as a trustworthy entity in an electronic attempting to acquire sensitive information such as username, password and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing is a fraudulent e-mail that attempts to get you to divulge personal data that can then be used for illegitimate purposes.


There are many variations on this scheme. It is possible to phish for other information in additions to user names and passwords such as credit card numbers, bank account numbers, social security numbers and mother's maiden names. Phishing presents direct risk through the use of stolen credentials and indirect risk to institutions that conduct business on line through erosion of customer confidence. The damage

caused by phishing ranges from denial of access to e-mail to substantial financial loss.

This report also concerned with anti-phishing techniques. There are several different techniques to combat phishing, including legislation and technology. Created specially to protect against phishing. No single technology will completely stop phishing. However a combination of good organization and practice, proper application of current technologies and improvement in security technology has the potential to drastically reduce the prevalence of phishing and the losses suffered from it. Anti phishing software and computer programs are designed to prevent the occurrence of phishing and trespassing on confidential information. Anti-phishing software is designed to track websites and monitor activity, any suspicious reported and even reviewed as a report after a period of time

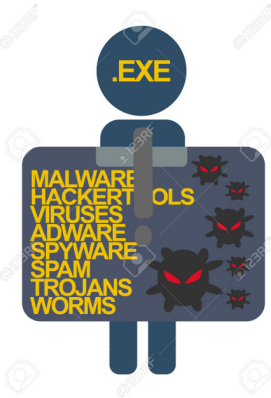
This also includes detecting phishing attacks, how to prevent and avoid being scanned, how to react when your suspect or or reveal a phishing attack and what you can do to help stop phishers.

**PHISHING TECHNIQUES**

Phishers use a wide variety of techniques, with one common thread

**LINK MANIPULATION**

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.




An old method of spoofing used links containing the '@' symbol,originally intended as a way to include a username and password. For example, *http://www.google.com@members.tripod.com/ m*ight deceive a casual observer into believing that it will open a page on *www.google.com* ,whereas it actually directs the browser to a page of members.tripod.com, using a username of *www.google.com :* the page opens normally, regardless of the username supplied.

**WEBSITE FORGERY**

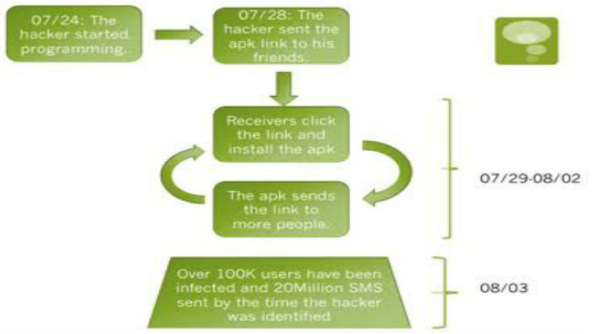
Once a victim visits the phishing website the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original address bar and opening a new one with the legitimate URL.

**PHONE PHISHING**

Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phishers) was dialed, prompts told user to enter their account numbers and PIN. Vishing (voice Phishing) users' use fake caller-ID data to give the appearance that calls come from a trusted organization.

## DAMAGES CAUSED BY PHISHING

The damage caused by phishing ranges from denial of access to e-mail to substantial financial loss. This style of identity theft if becoming more popular, because of the readiness with which unsuspecting people often divulge personal information to phishers, including credit card numbers, social security numbers, and mothers' maiden names. There also fears that identify thieves can add such information to the knowledge they gain simply by accessing public records. Once this information is acquired, the phishers may use a person's details to create fake accounts in a victim's name. They can then ruin the victim's credit, or even the victims' access of their own accounts.




## EXAMPLES OF PHISHING

Phishing e-mails messages take a form. They might appear to come from your bank or financial institution, a company you regularly do business with, such as Microsoft, or from your social networking sites.

The main thing phishing e-mail messages have in common is that they ask for your personal data, or direct you to websites or phones numbers to call where they ask you to provide personal data. The following is an example of what a phishing scam in an e-mail message might look like. Example of a phishing e-mail message, which includes a deceptive web address that links to a scam web site

To make these phishing e-mail messages look even more legitimate, the scam artists may place a link in them that appear to go to the legitimate website (1),but actually takes you to a phony scam site(2) or possibility a pop-up window that looks exactly like the official sites .

Phishing links that you are urged to click in e-mail messages, on websites, or even in instant messages may contain all or part of a real companies name and are usually masked, meaning that the link you see does not take you to that address but somewhere different, usually an illegitimate websites. The mouse pointer resting on the link reveals the real web address. The string of cryptic numbers looks nothing like companies web address, which is the suspicious sign.

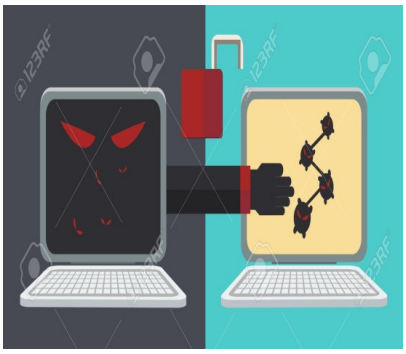
## REASONS OF PHISHING

Some of the reasons people fall victims to the phishing scams are,

## TRUST OF AUTHORITY

When a phishing e-mail arrives marked as "High priority" that threatened to close our bank account unless the update our data immediately, it engages the same authority response mechanism that we have obey for millennia. In our modern culture, the old marker of authority-physical strength, aggressiveness, ruthlessness-have largely given way to sign of economic power. "He is richer than I am, so he must be a better man". If you equate market capitalization with GDP then the bank of America is the 28$^{th}$ most powerful country in the world. If you receive a personal e-mail

purported to come from BOA questioning the validity of our account data, you will have a strong compaltion to respond, and respond quickly.



**TEXTUAL AND GRAPHIC REPRESENTATION LACKS TRADITIONAL CLUES OF VALIDITY**

Most people feel that can tell an honest man by looking him in the eye. You can spot a "professional" panhandler before he gets to the fourth world in his spiel. Without clues from the verbal and physical realms, our ability to determine the validity of business transaction is diminished. this is a cornerstone of the direct mail advertising business. if a piece of mail resembles some type of official correspondences, you are much more likely to open it.car dealers send sales flyers in manila envelopes stamped" official business" that look like the envelops tax refund checks are mailed in. bank send credit card offers in large cardboard envelops that are almost indistinguishable from FedEx over my package. Political advertisements are adorned with all manner of patriotic symbols to help us link the candidate with our nationalistic feelings.

**E-MAIL AND WEB PAGES CAN LOOK REAL**

The use of symbol laden with familiarity and repute lend legitimacy ( or the illusion of legitimacy)

To information-whether accurate or fraudulent –that is placed on the imitating page. Reception is possible because the symbol that represents a trusted company or no more 'Real' that the symbols that are reproduced for a fictitious company. Certain elements of dynamic web content can be difficult to copy

Directly or often easy enough to fake, especially when 100% accuracy is not required. E-mail messages are usually easier to replicate that web page since their elements are predominantly text or statics HTML and associated images. Hyper links are easily subverted since the visible tag does not have to match the URL that you click with actually re-direct your browser to. The link can look like http://bankofamerica.com/login but the URL could actually link to http://bankofcrime.com/got_your_login

**CONCLUSION**

No single technology will completely stop phishing. However, a combination of good organization and practice, proper application of current technologies, and improvements in security technology has the potential to drastically reduce the prevalence of phishing and the losses suffered from it. In particular:

High-Value targets should follow best practices and keep in touch with continuing evolution of them.

Phishing attacks can be detected rapidly through a combination of customer

reportage, bounce monitoring, image use monitoring, honeypots and other techniques.

E-mails authentication technologies such as sender-ID and cryptographic singing, when widely deployed, have the potential to prevent phishing emails from reaching users.

Analysis of imagery is a promising area of future research to identify phishing emails.

Personally identifiable information should be included in all email communications. Systems allowing the user to enter or select customized text and/or imagery are particularly promising.

Browser security upgrades, such as distinctive display of potentially deceptive content and providing a warning when a potentially unsafe link is selected, could substantially reduce the efficacy of phishing attacks.

Information sharing between the components involved in a phishing attack – spam filters, email clients and browsers- could improve identification of phishing messages and sites, and restrict risky behavior with suspicious content.

Anti-phishing toolbars are promising tools for identifying phishing sites and heightening security when a potential phishing site is detected.

Detection of outgoing confidential information, inching password hashing, is a promising area of future work, winsome technical challenges.

An OS-level trusted path for secure data entry and transmission has the potential to dramatically reduce leakage of confidential data to unauthorized parties.

Two-factor authentication is highly effective against phishing, and is recommended in a situation in which a small number of users are involved with a high value target. Device identifier based two-factor authentication offers the potential for coast savings.

Cross-site scripting is a major vulnerability. All user content should be filtered using a let-in filter. Browser security enhancements could decrease the likelihood of cross-site script attacks.

**REFERENCE**


- www.wikipedia.com
- www.w3schools.com
- https://www.slideshare.net/AryanRagu/phishing-attacks-ppt
- https://www.scribd.com/doc/12966916/Phishing-ppt