Phishing Attacks and Counter Measures

Sophia Kingsley Okore[1], Benisemeni Zakka[2]

[1]Msc student, Department of Information Technology, SRM University Chennai, India.
[2]Lecturer, Computer Science Department. Federal Polythenic, Bauchi, Nigeria.

ABSTRACT *Phishing is a term used to describe various scams that use fraudulent e-mail messages, sent by criminals, to trick people into exposing personal information. The criminals use this information identity to rob bank accounts, or take over computers. Counterfeit web sites, using "hijacked" company brands and logos are created to lure individuals into revealing information that are confidential. These digital thugs are "phishing" for any data they can obtain to prey on people and further their criminal activities.*

E-mail has become an invaluable communication tool, both for business and personal use. Among the many security issues that affect computer users, there is a rapidly growing threat known as "phishing". Criminals use phishing attacks to lure the unsuspecting into visiting a fraudulent web site, calling a fraudulent phone number, or downloading malicious software, expressly to steal sensitive information such as credit card numbers, account credentials, social security numbers, PINS, or passwords.

Keywords*: phishing, legitimate, White lists, Black lists.*

1. INTRODUCTION

A. *OVERVIEW OF PHISHING*

Gone are the days when criminals carry guns and tools to break into people homes to steal money and other valuables from them, as a result in the advancement of technology, they have also advanced in their methods of operations. All they need do is to sit in the comfort of their homes to perpetuate this evil act digitally by obtaining personal information through disguising oneself as a legitimate online entity. More specifically phishing is the process of creating a fraudulent email or website that appears to originate from a legitimate source. Phishers, who are authors of phishing websites, create a fraudulent or fake website in hopes that visitors will divulge sensitive information such as account numbers, usernames, passwords, pins, social security numbers, etc.

B. *The Phishing Life Cycle*

Typically, there are three main phases to the phishing cycle, first, the phisher creates a phishing website that may resemble some branded websites and then goes phishing by sending out numerous emails to unsuspecting users. When the user "bites" on the phish, the link in the email redirects the user to the phishing site which appears similar or identical to the legitimate target site. The phish is successful when the user enters confidential information on the phishing page, or by embedding virus (phishing software in form of adverts and enticing programs that when the user double clicks on it,the viruses are downloaded to their system and gets sensitive information such as bank account numbers, passwords and so on.

Afterwards the phisher tries to exploit the confidential information by transferring money, opening accounts, or making purchase using the captured information. Or acts as a middleman and sells the information to other criminals.

C. *The Phish*

The phishing life cycle begins with a mass email that attempts to convince the reader to visit the included website link. This phase is anomalous to fishing, instead of using a fishing lure and line to catch a fish, a phisher sends out many emails in hopes that a few readers will "bite" at the email lure by visiting the included link.

Typically, the email looks legitimate and will include a famous company logo and a return address of the legitimate company in order to make the phishing site as authentic as possible for victims to bite. The content is usually for the user to update his or her information without which services will be stopped with a sense of urgency in it.

D. *The Bite*

The bite occurs when the victim clicks on the link in the email and is directed to the phishing website, which looks identical or similar to the legitimate site its attempting to impersonate. Mostly, the legitimate site is copied and hosted someplace on the phishing page to make it look authentic, such contents may include the company logos, styles, keywords and security notices.

Once the user is assured that the page is legitimate and visit the site, the phisher can request confidential information. It is a critical step for the phisher to first build the trust so that the user thinks that the page is legitimate.

E. *The Catch*

Once a user has visited the phishing page and is convinced that the page is familiar and legitimate, the phisher requests confidential information from the user. Often there is a user login and password box that requests a username and a password from

the user. Confidential information such as account numbers, pins, date of birth, etc. once the user divulges this information, it is typically stored in a database on the phishing server, emailed to a phisher's email address. After the form has been submitted, the user will definitely receive an error or be directed back to the legitimate site and will appear to the user that nothing has happened.

F. The Damage

Phishers harvest confidential information and then either try to exploit it by transferring funds, making purchases, etc. or they sell the information to a third party criminal.

H. Prosecution

Typically phishing sites are active for only a short period of time before being discovered and shutdown. Most sites are active for as short as a few hours to as long as a few days. Usually the site will be reported and confirmed phishing and then the Internet Service Provider will delete the site.

However, it is often difficult to remove the site and prosecute the phisher if the site is hosted in a foreign country because of differing laws and jurisdiction. Often financial institutions will refund the lost money from customers because it is easier and less costly than trying to find and prosecute the criminals.

II. REVIEW OF RELATED WORK

The purpose of the paper is to identify the fundamental design principles that inform decisions for the development of usable and secure anti-phishing applications. It is designed to assist user interface designers and developers who are not trained in the "field of usability and security" (Garfinkel, 2005, p. 37) also known as HCI-Sec, to create secure and usable anti-phishing applications.

This article addresses the various ways in which phishing occur, how to recognize it and counter measure to its attacks. Web and application developers tend to concentrate more on the software start-date to completion-date without paying much attention to the security of the software, during development and after completion such as educating the clients and users for which it is intended for on online security.

The paper indentifies learning methods and techniques that are important to overcoming of phishers on the web.

It also provides developers of anti-phishing applications with a set of theories and fundamental design principles to consider prior to system design and the selection of technology solutions. According to Jakobsson (2005), the development of successful security solutions is dependent on a clear understanding of current and future threats.

A. The Evolution Of Phishing Attacks

Kasperskey Lab carried out statistics on 50 million users that anonymously agreed to contribute their data and detected threats to the Kasperskey Security Network Cloud. They used Computers running on Windows that were conducted by Kasperskey experts. The duration of the research was from 1st March 2011 -30th April 2013. The following findings were the facts they came out with.

- That Phishing was originated and launched from the United States, United Kingdom, Germany, Russia, India, Canada, France, Australia and others.
- In 2012 – 2013, 37.3 million people were attacked by phishers amounting up to 87% of the world's population.
- The two top ways in which phishing are spread are
  1. Browser 87.91%
  2. Mail 12.09%

Ten Countries Mostly Affected by Phishing:

United States	12.29%
United Kingdom	3.36%
Germany	6.22%
Russia	18.7%
India	9.92%
France	3.2%
Italy	2.4%
China	2.70%
Vietnam	3.35%
Ukraine	2.25%
Others	35.95%

B. Impersonation Phishing Attacks and Phishing Email.

Impersonation is the most common type of phishing approach and is implemented using legitimate –looking content (Emigh, 2005).Phishers take advantage of the relationships and trust that these companies have built with home users (Dhamija & Tygar, 2005a). In order to deceive their victims, phishers create a presence that is so convincing that users fail to differenciate and act upon legitimate security indicators.(Dhamija, Tygar, & Hearst, 2006; Wu, Miller, & Garfinkel, 2006).

Impersonation phishing attacks are commonly carried out through a bulk email that has a sense of urgency in it. (Berghel et al., 2007;Chou et al.,

2004; Emigh, 2005; Jackobsson, 2005; Moore & Clayton, 2007) Usually, a single, large-scale spam phishing attack includes 100,000 emails (James, 2005). A mass mailing of 100,000 emails may achieve a 10% receive rate and yield a phishing success rate of 1% (James, 2005). Spam email is a primary phishing technique because it is inexpensive to carry out and difficult to trace back to the attacker (Herzberg & Gbara, 2004).

Almost all phishing emails utilize HTML and other web designs softwares technology, enabling phishers to create enticing, legitimate or authentic looking emails and websites through the use of graphical user interface (GUI) ,URL, links and obfuscation techniques (Chou et al., 2004). Phishing emails typically make use of trusted brands and logos that are copied from legitimate web sites. Since attackers cannot get customers lists from specific companies, they spoof companies that are popular such as amazon.com or ebay and so on. With clever phishing scams, attackers personalize emails so that they appear credible to their victims. Personalized elements, such as the user's name, or digits from an account number and the use of legitimate brands and logos, make phishing emails and web sites appear genuine. Attackers lure users to spoofed web sites using redirected links contained in the emails. Examples of phishing emails calls to action include the followings: (Emigh, 2005):

- Notification about problems with an account (Chou et al., 2004).
- Ironically, offers for enrollment in anti-fraud programs.
- Opportunities to cancel orders that were never placed.
- Notification that a fictitious change will be made to an account, unless action is taken to stop it.
- Limited–time offers for free services at financial institutions.

C. The Phishing Web Site.

Almost all phishing emails utilize HTML and other web designs softwares technology, enabling phishers to create enticing, legitimate or authentic looking emails and websites through the use of graphical user interface (GUI) ,URL, links and obfuscation techniques (Chou et al., 2004). Phishing emails typically make use of trusted brands and logos that are copied from legitimate web sites.

User information pages and submission task flow typically mirror that of legitimate web site (Berghel et al., 2007). Visible differences between a phishing web site and a legitimate site might include text anomalies, the amount of information requested from the users(Dhamija & Tygar, 2005b). Once the phishing web sites have been developed, it can be reuse for multiple attacks. (James, 2005).

The phishing web site domain name and URL are carefully designed so that they appear legitimate to users. The personal information most often collected by phishers include login name and password, credit card information, bank account numbers, social security numbers, driver's license or any standard identification means.
Once victims enter their personal information, online thieves steal their identity and use it to withdraw money from financial accounts, purchase goods any perform any other activities which are detrimental to the victim.
Usually, phishing web sites are online just enough for attackers to phish personal information from enough users to make their effort worthwhile.

III. COUNTER MEASURES

Anti-phishing filters already exist and integrated into web browsers

→ (MS internet Explorer 7.0, Mozilla Firefox 3.0)
→ External tools (Spoof Guard)

- These approaches are only reactive and cannot act proactive due to static input.
- Most tools use blacklist:

  →High ratio of false negatives (> 50%)

- Some use heuristics:
  →High ratio of false positive (>40%)
  →Combination of whitelist, blacklist and heuristic behavioral analysis guarantees reactives as well as proactive approach and low ratio of false positives and false negatives.

- Whitelist stores distinct identifiers from legitimate websites grouped by business types(banks, insurances etc)
- Blacklist stores distinct identifiers from known phishing sites.
- Heuristic store algorithms which detect suspicious set-up or suspicious behavior of the websites, detects anomalies that strongly indicate phishing behavior.

A. DETECTION PROCESS

General Procedure (PW=Phishing website):

1. Extract URLs from potential phishing e-mails

(in real-time since URL should still be resolvable).

2. Look for hit in whitelist

→ if Y, cancel (no PW)

3. Look for hit in black list
→ if Y, classify as PW

4. Else: Use heuristics to return probability of target being a PW (unlikely, very likely): P(PW)

IV. PHISHING & ANTI-PHISHING TECHNIQUES

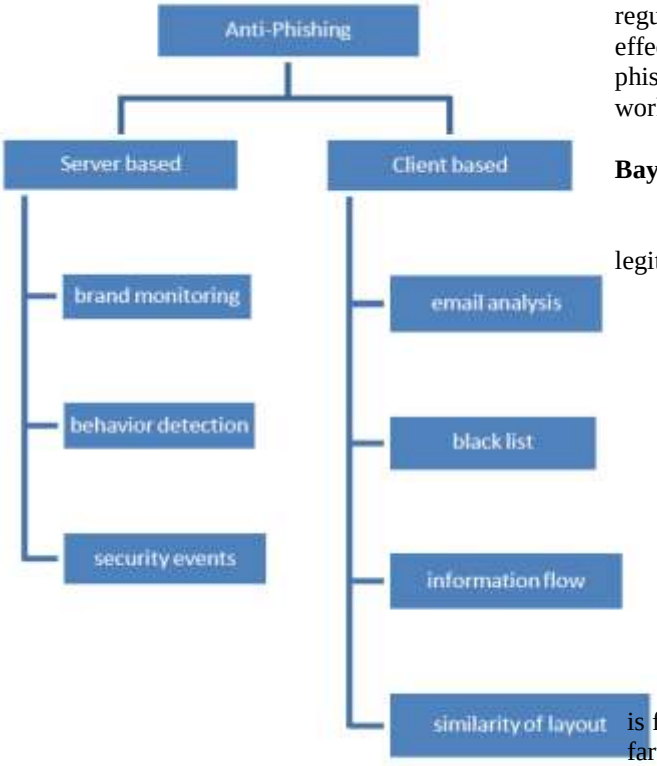

Figure 1.0*server/clients techniques*

A. Server Based

These techniques are implemented by the service providers (ISP, etc) and are of the following types:

***Brand Monitoring*:** cloning online websites to identify "clones" which are considered phishing pages. Suspected websites are added to centralized "black list".

Behavior Detection: for each customer, a profile is identified (after a training period) which is used to detect anomalies in the behavior of users.

Security Event Monitoring: Security event analysis and correlation using registered events provided by several sources (OS, application, network device) to identify anomalous activity or for post mortem analysis following an attack or a fraud.

B. Client Based

These techniques are implemented on user's end point through browser plug-ins or email clients and are of the following types:
Email Based on Analysis: email based approach typically use filters and content analysis. If trained regularly, Bayesian filters are actually quite effective in intercepting both spamming and phishing e-mails. Bayesian algorithm explains the working of Bayesian filter:

Bayesian Algorithm:

1. Split email in tokens
→Need number of messages for spam and legitimate
→Need frequency of each word for each type.

2. Calculate Probabilities
P (legitimate) = word frequency / number of legitimate messages.
P (spam) = word frequency / number of spam messages.
3. Calculate likelihood of being spam (spamicity) using a special form of Bayes' rule where likelihood = a/(a+b), where a is the probability of a legitimate word and b is the probability of spam word.

4. Choose tokens whose combine probability is farthest from 0.5 either way. This is because the farther it is from 0.5 (neutral), with more certainty we can say it belongs to either strategy.

→Do this for n numbers for n instance

→Combine their probability to get a figure for the message using Bayes' rule. In basic terms, Bayes' rule determines the probability of an event occurring based on the probabilities of two or more independent evidentiary events. For three

evidentiary events a, b, c the probability is equal to abc abc+ (1-a)*(1-b)*(1-c).

→If the end result is closer to 1.0, then the message is classified as spam, and if it is closer to 0.0, the message is classified as legitimate.

V. CONCLUSIONS

This paper identifies and describes the strategies used in phishing and its countermeasures. Important usability issues with web browsers and current tools in the fight against phishing are examined. Design principles intended to improve the transparency and visibility of anti- phishing are outlined. To be successful, phishing attacks must reach the appropriate target to be successful, (potential victims) appear legitimate, and allow the attacker to disappear undetected.

Phishing is commonly conducted from multiple countries and is expected to continue its expansion throughout the world and is likely that smaller attacks that leverage partial information about fewer victims and results in higher success rates will become an increasing threat and in the best case scenario, when users expect spoofs to be present and are motivated to discover them, many users cannot distinguish a legitimate website from a spoofed one.

Phishing technology has advanced, instead of directly asking for confidential information in scam emails or on web sites, cybercriminals are using hidden malicious software downloaded to users' desktops or any electronic device to monitor their online activities and records bank codes or any confidential information, which means users do not need to reveal confidential information themselves, only a click on a link directs them to a malware-infected web page.

Social networks also serve as a potential tool for cybercriminals. By leveraging the social connections in a network like Facebook or Twitter, phishers could send messages to a site's users that seem to be sent by a friend, and suggest visiting a page infected with bank code stealing software and other phishers software.

AKNOWLEDGEMENT

Our sincere gratitude goes to our husbands and children who encouraged and sacrifice the time required to complete this paper, also a big thank you to Mrs kachana Kabendiran and B. Rebecca Jeya Vadhanam both of Computer Science Department, SRM University India.for their encouragement and guidance. To my colleague Mfon-abasi Idio, thank you for the encouragement.

REFERENCES

[1] http://www.forbes.com/2007/12/27/phishing-hacking-virus-tech-security-cx_ag_1228phish.html
[2] Anti-Phishing Working Group. *Phishing Activity Trends Report November 2005* (2005).
[3] Anti-Phishing Working Group Phishing Archive. http://anti-hishing.org/phishing_archive.htm
[4] *Why Phishing Works:* Rachna Dhamija, Conference on Human Factors in Computing Systems, April 2006
[5] *Phishing: An Analysis of a Growing Problem*, Anthony Elledge. SANS Institute InfoSec Reading Room January 2007
[6] *The Evolution of Phishing Attacks*: Kasperskey Lab 2011-2013
[7] A framework for detection and measurement of phishing attacks, Cho et al. 2004, Sujata Garera et al.
[8] Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why Phishing Works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Canada*, pp. 581-590. Retrieved October 29, 2007, from ACM Digital Library.
[9] Berghel, H., Carpinter, J., & Jo, J.-Y. (2007). Phish Phactors: Offensive and Defensive Strategies. *Advances in Computers, 70*, 223-268. Retrieved November 3, 2007, from Web of Science database
[10] Camenisch, J., Shelat, A., Sommer, D., & Zimmerman, R. (2006). Securing User Inputs for the Web. *Proceedings of the Second ACM Workshop on Digital Identity Management, USA*, pp. 33-44. Retrieved October 28, 2007, from ACM Digital Library.
[11] Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do Security Toolbars Actually Prevent Phishing Attacks? *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Canada*, pp. 601-610. Retrieved October 28, 2007, from ACM Digital Library.
[12] Milletary, J. (2005). *Technical Trends in Phishing Attacks.* Retrieved December 1, 2007, from http://www.us-cert.gov/reading_room/phishing_trends0511.pdf
[13] Anti-Phishing Working Group. (2007). *What is Phishing and Pharming?* Retrieved December 1, 2007, from http://www.antiphishing.org/DOJ_Special_Report_On_Phishing_Mar04.pdf
[14] *Web Identity Security: Advanced Phishing Attacks And Counter Measures*, Anthony Yingjie Fu City University Of Hong Kong September 2006
[15] Enhancing Home Computer User Information Security: Factors to Consider in the Design of Anti-phishing Applications, Melinda Geist ,Intel Corporation Febuary 2008
[16] *International Journal of Advanced Research in Computer Science and Software Engineering* Jyoti et al.*3(5), May - 2013, pp. 458-465*
[17] Jakobsson, M. (2007). *The Human Factor in Phishing*. Retrieved November 21, 2007, from Indiana University, School of Informatics Web site: http://www.informatics.indiana.edu/markus/papers/aci.pdf
[18] *Techniques on Phishing and Counter measures* Muhammad Khalil and Marcus Wolffl Fall 2008