Phishing Attack Prevention: How to Identify and Detect Phishing Attacks

Proposal #5 – Methods

by

**Suraj Pratap Samirlal Poddar**

Harrisburg University of Science and Technology

Spring 2021

# Overview

Phishing has been one of the major concerns which has become a common vector and has been used for many years. The risks and the potential impact involved are known to many users who are on the Internet. Despite of the awareness people still tend to fall for scams and other phishing attacks pulled by the phishers. We dive deeper into various types of phishing attacks and scams pulled in the past by providing insights to the modern phishing scams and how they make these campaigns effective. The research shows recent phishing campaigns to be highly effective and highly distributed out in the wild

# Objective

The objective is to do a qualitative research to gather a wide range of information to get in depth knowledge. The information is not meant to focus and test a hypothesis, it is more so to review various documents to gather information. This research study is to spread awareness on different phishing techniques and implement/perform an experiment to see if an educational support tool can be leveraged to best identify phishing.

The objective of doing a Quantitative research will be to find the relations ship between the users and the attacks and if there are any dependent variables. The information here will be gathered through a survey or an experimental analysis. The end results will be used to test the strength of evidence

Both methods are being used to strengthen the weakness of each method. The goal is to gather information on phishing and identify the relationship between target group , based on which quantitative approach will be used to perform an experiment

Table of Contents

[Overview 2](#_Toc69392086)

[Objective 2](#_Toc69392087)

[Methods 4](#_Toc69392088)

[Participants for Experiment 4](#_Toc69392089)

[Educational Tool 5](#_Toc69392090)

[Survey 6](#_Toc69392091)

[Anatomy of Phishing Solutions 8](#_Toc69392092)

[Anti-Phishing Solutions 9](#_Toc69392093)

[References 9](#_Toc69392094)

# Methods

A qualitative research study approach was used to understand various components involved and get a better understanding on the attacks and finally develop a phishing education tool which can help get users up to speed and spread awareness. An initial test is carried out to see if there are any improvements with the experimental approach on Users who have received education vs the Users who have not received the educational tool

# Participants for Experiment

Users will be randomly picked and will be divided into multiple blocks based on their profession. There will be two groups one named control group and the other experimental group. (Abawajy, 2013) The experimental group will receive the education on different types of phishing and how to identify them and the other group will not receive any type of information related to phishing. The process of the experiment will be to have the participants take the course as explained in the flow chart below (Jakobsson, 2007)

Diagram

Description automatically generated

Structure of Experiment

As described above both the groups are going to get similar structure of Experiment, Experimental group is going to get education related to Phishing however on the other hand the control group is going to get some alternative education, but not related to phishing (Basit, n.d.)

# Educational Tool

The tool is developed in a simple form of a web application, this is to provide users with easy navigation through the tool and to make it look real. The tool will have various modules based on the types of phishing techniques. The users will be asked to complete the modules and answer few questions at the very end to test their skills. The Users will have complete control to opt in or out of the experimental group. As soon as the user’s login the users will be presented with an information detailing about the experiment and the reason behind the research.

Before taking the course, both the groups will be asked to fill out a survey which will be based on phishing. Post this survey the Educational Group is going to continue with their educational tool online whereas the control group will be directed to alternative content which is not based on Phishing. Post completion of their course both the groups will be receiving a new survey which will be different than the first survey. The data collected will then be analyzed for further study (Jampen, 2020)

# Survey

Each user is going to receive two separate surveys and will be evaluating 20 different emails with attachments on the Education Tool from the Web portal, 12 emails will be legitimate email and the rest 8 will be phishing emails. The users will have the option to mark it Legitimate or Phish and based on the right answer each user is going to obtain points as they move along. Each email will be different and will have different characteristics. The users can be selected from HU University which will solely depend on user’s choice. They can certainly decline to be a part of this study or to provide any contribution to the research (Neupane A, 2015)

|  |  |
| --- | --- |
| Questions | Purpose |
|  |  |
| Introduction, Greet Users and provide them a brief introduction on your study. The users are free to answer the Questions as they like. | To build trust and gather information, scammers or phishers use to target individuals |
| After each email module, the user will be presented with the following question |  |
| Has the education provided you the necessary information to identify phishing before taking this course | To Take users feedback on training program and to understand if the education was of any value |
| What is the reason behind clicking on the phishing email? | to know whether it was out of curiosity, was not paying attention or just did not care and wanted to click |
| Have you clicked on any Phishing emails before home or at work? | To understand if the user has a knowledge on phishing emails - yes, no, not sure |
| Do you feel Technology makes you feel less safe? |  |
| You can come across a phishing email which has malicious content or fake email by? | By Typing in the incorrect URL, by not paying attention, by simply opening up the link or by going to a link the email is asking you to do |
| Do you use some sort of a antivirus at home or any phishing filter on your laptop? | Is the user taking the right measures to protect against emerging security threats |
| As per you, how much information can a hacker get by sniffing or logging data | Users’ knowledge on phishing |

# Anatomy of Phishing Solutions

Graphical user interface, application

Description automatically generated with medium confidence

A phishing attack takes 3 stage approach Bait ,Phishing and the catch lure a victim into a scam. A phishing attack can be described in the following stages

Diagram

Description automatically generated

Users receive a phishing email

Attacker lures the victim into attack as a result user falls for the attack

Attacker brings up forged website asking for users’ credentials or sensitive information

As soon as the Attacker has user information

The Attacker impersonates the user and finally gets users financial account compromised

# Anti-Phishing Solutions

Phishing can be further avoided by following few guidelines, Installing Anti Phishing Techniques, using an addon or plugin on any browser which can protect users from spoofed email sources. Deploying Anti Phishing tools bars which can alert users by generating a passive warning against the attack. (Gürel, Detection of phishing attacks, 2018) Using Spam filters to categorize emails on basis of data set filters. Installing and staying up to date with Anti-Virus installed on the machine and by paying attention to the detail of an email

# Proposed Plan

The above Research study will be conducted over a period of 4 months. Once the required information has been collected the results will be posted in accordance to experiment and analysis. The proposed paper will discuss issues and problems related to phishing while we take a deeper dive in the analysis as mentioned above. The above data will be backed up with practical analysis and an effective education tool to spread awareness

# References

(2013), A. A. (April 2013, Volume 68–No.3, pp. 7-11 ). *Preventing Phishing Attacks using One Time Password and User Machine Identification.* International Journal of Computer Applications.

A. Alswailem, B. A. (2019). Detecting Phishing Websites Using Machine Learning. *2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia*, pp. 1-6, doi: 10.1109.

A. N. Shaikh, A. M. (2016). A literature review on phishing crime, prevention review and investigation of gaps. *10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA), Chengdu*.

Abawajy, R. I. (2013). A multi-tier phishing detection and filtering approach. *Journal of Network and Computer Applications, vol. 36, no. 1*, pp. 324–335, 2013.

*APWG*. (n.d.). Retrieved from APWG: https://www.antiphishing.org

*APWG*. (2003). Retrieved from APWG: https://www.antiphishing.org

Bakhshi, T. P. (2008). *A Practical Assessment of Social Engineering Vulnerabilities”, Proceedings of the 2nd International Conference on Human Aspects of Information Security and Assurance.*

Basit, A. Z. (n.d.). *A comprehensive survey of AI-enabled phishing attacks detection techniques*. Retrieved from Telecommun Syst 76, 139–154 (2021). : https://doi.org/10.1007/s11235-020-00733-2

Carella A, K. M. (2017). *Impact of security awareness training on phishing click-through rates. In: 2017 IEEE international conference on Big Data (Big Data).*

Chhikara, J. (2013). Phishing & Anti-Phishing Techniques. *Case Study International Journal of Advanced Research in Computer Science and Software Engineering*.

Easttorn, C. &. (2011). *Computer Crime, Investigation, and the Law. Boston, MA: Course Technology.*

El Aassal, A. B. (2020). An in-depth benchmarking and evaluation of phishing detection research for security needs. *IEEE Access, 8, 22170–22192*.

Gürel, M. B. (2013). Detection of phishing attacks. *2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, 2018, pp. 1-5, doi: 10.1109/ISDFS.2018.8355389 Chhikara, Jyoti. (2013). Phishing & Anti-Phishing Techniques*.

Gürel, M. B. (2018). Detection of phishing attacks. *6th International Symposium on Digital Forensic and Security (ISDFS), Antalya*, pp. 1-5, doi: 10.1109/ISDFS.2018.8355389.

Gupta, A. K. (2016). Comparative analysis of features-based machine learning approaches for phishing detection. *10th INDIA-COM, New Delhi, India*.

J, S. (2017). *Persistent training. In: Advanced persistent training, Apress, Berkele.*

Jakobsson, M. &. (2007). *Phishing and Countermeasures:Understanding the Increasing Problem of Electronic Identiry Theft.* Hoboken, New Jersey.

Jampen, D. G. (2020). *A comparative literature review. Hum. Cent. Comput. Inf. Sci. 10, 33* . Retrieved from https://doi.org/10.1186/s13673-020-00237-7

Khonji, M. &. (2013). Phishing Detection: A Literature Survey. *IEEE Communications Surveys &amp Tutorials*, PP. 1-31. 10.1109/SURV.2013.032213.00009.

Kumaraguru P, R. Y. (2007). *Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. In: Proceedings of the anti-phishing working groups 2nd annual eCrime researchers.* Pittsburgh, PA.

M. Adil, R. K. (2020). Preventive Techniques of Phishing Attacks in Networks. *3rd International Conference on Advancements in Computational Sciences (ICACS), Lahore, Pakistan, 2020*, pp. 1-8, doi: 10.1109/ICACS47775.2020.9055943.

Moore, T. &. (2007). *Examining the Impact of Website Take-down on Phishing. Proceedings of the Anti-Phishing Working Group 2nd Annual e-Crime Researchers Summit.* Pittsburgh.

Neupane A, R. M. (2015). *A multi-modal neuro-physiological study of phishing detection and malware warnings. In: Proceedings of the 22nd ACM SIGSAC conference on computer and communications security—CCS ’15. ACM Press,.* Denver, Colrado.

Orunsolu AA, S. A. (2017). *An empirical evaluation of security tips in phishing prevention: a case study of Nigerian banks. Int J Electron Inf Eng.*

Purkait, S. (2012). *Phishing counter measures and their effectiveness – literature review*. Retrieved from Information Management & Computer Security, Vol. 20 No. 5 pp. 382-420.: https://doi.org/10.1108/09685221211286548

Vahid Shahivari, M. M. (2020). *Phishing Detection Using Machine Learning Techniques.*

Vayansky, I. &. (2018). Phishing – challenges and solutions. *Computer Fraud & Security* , 15-20. 10.1016/S1361-3723(18)30007-1.

White, M. &. (2008). *Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Efforts. Criminal Justice Policy Review.*