Phishing Attack Prevention: How to Identify and Detect Phishing Attacks

Proposal #1 – Intro & Doc Setup

by

**Suraj Pratap Samirlal Poddar**

Harrisburg University of Science and Technology

Spring 2021

Table of Contents

[Introduction 3](#_Toc63963785)

[Research Questions 6](#_Toc63963786)

[Significance and Justification 6](#_Toc63963787)

[Background 7](#_Toc63963788)

[Justification 8](#_Toc63963789)

[References 9](#_Toc63963790)

# Introduction

Internet has changed the way we live, it has dominated many fields by increasing the comfort level for users/humans, however on contrary it has also brought few disadvantages with it, one of the most important things that comes to everybody’s mind is security, when surfing on the Internet. Everyone online takes utmost caution to protect their business by patching their server and by fixing the vulnerabilities to safeguard their business through Internet. Phishing is one of the online forms of identity theft that can be used to steal private information of an individual. Phishing scams has been receiving the utmost attention as this clearly have been on the rise, there is no single remedy that can protect a user from phishing scams

In the current generation Phishing is a form of cybercrime where a hacker/attacker for that fact pretends to be the real person or an entity by elevating them as the official owner through any communication medium, the famous of all and easy to drag attraction is through e-mails. This form of attack can do various types of captures that includes luring victim to give away their login credentials or their personal account information which alludes to identity theft and loss of funds from the victim. It is one of the con games used to collect Personal information from a random user. The following research is going to provide us information on how we can not only identify these phishing attacks but also how to avoid it at the same time. There is anti-phishing software’s and browser addons which helps a user in identifying these types of threats and alerting us from falling for these types of attacks. This paper will provide information about types of phishing attacks and steps that can be taken to shield user’s confidential information

The word ‘Phishing’ was introduced in 90s, in the earlier day’s hackers used to use ‘ph’ in replacement to letter ‘f’ and the hackers in that generation were also known as *Phreaks*. Phreaking is the term used for study, exploring, experimenting of telecom system. Since phreaks and hackers were closely linked, ‘ph’ was linked to phishing instead of fishing and since this attack lures a victim to give away their personal information just as the analogy with ‘angling’ where the attacker sets email lures by positioning the hooks to ‘fish’ for sensitive information which can include their identity information or banking passwords or any type of financial data from the ‘sea’ of users on the Internet

One of the main goals of phishing is to conduct a fraudulent transaction by using a fake email by luring the user to click on the URL and redirect them to an illegitimate website which looks exactly the same as their banking website and steal their username and password that way or to entice a user to give away their social security number or any private information such as name, address , phone of an user which can be used to either apply for a loan or for a credit-card on behalf of the user

There are various types of phishing scams and these tend to continue as the techniques has been successful enough for cyber criminals in making hefty profits. Phishing has been around since the origination of Internet and they are not going away any time soon. There is always a chance for you to fall for these traps and therefore it becomes imperative to adapt basic guidelines in keeping yourself safe. Always keep up with the information on Phishing, think twice before clicking on any URLs, Install an Antiphishing toolbar, Verify the certificate and the site security of the website, check your Online A/c’s and passwords regularly, rotate the passwords frequently, enable Multi Factor Authentication, never give away your private/personal information

While many methods have been developed to tackle phishing attacks none of them are efficient enough to mitigate new phishing attacks that are constantly being developed and cannot filter all the malicious email content. This paper describes about the methodology and approach along the various phases and the differences between a normal approach to a website versus a phishing attack redirect. While Phishing websites are designed to looks like the original page there is always a slight difference which one needs to understand. The Sony hack which was pulled in 2015 is a great example of a successful phishing campaign and illustrates the damage that can do to an organization, the damage done to Sony was at a bigger scale in millions of USD

Therefore, the key is to take a proactive approach by educating your users which is the most important part in anti-phishing strategy. To Design an effective anti-phishing strategy includes various factors, and is intended to improve person’s knowledge on phishing, this can be in the form of videos or simlets or printed materials. Phish tank is a website which has database of all the phishing websites, it updates its records by monitoring the entire Internet and I mainly created for user’s awareness. By submitting the URL, you can verify whether the url is a potential phishing site. Deep packet inspection is one of the Network Techniques which is used to dig into a packet level, many countries use this mechanism to surveillance on the Internet and to monitor any malicious activity over the Internet

# Research Questions

Question 1: How do you classify & identify Phishing Attacks

In the following Research question, we will classify the types of phishing attacks such as Email Phishing, Smishing & Vishing, Spear Phishing, Angler Phishing, Deceptive phishing, fight Phishing, pharming etc. by explaining their techniques and the methods used to exploit or lure a victim

Question 2: What steps can you take to avoid phishing scams

In this, we are going to discover how phishing scams are being developed all the time and in order to stay on the top of this, the first step towards is to educate and spread awareness which can be carried out through security awareness training. By providing awareness we can have our users take the responsibility to think before clicking on any random links.

Question 3: Anti phishing techniques and best practices

This question will help in determining what software’s/network devices can be installed on the perimeter and inside the organization to protect from these attacks like installing Firewall, enabling IDS/IPS, by keeping the browser updated, by keeping the virus signatures updated on the Antivirus client, by checking Sites Security and its certificate, by using reverse proxies etc.

# Significance and Justification

## Background

In the past few years, the amount of unique phishing emails has exponentially increased, Phishers can steal sensitive data from users to access an individual’s financial information and initiate a illegitimate wire transfer or withdraw money without the users consent, this has put the organization and the individuals both at risk. Due to these consequences, most of the companies have now started to educate their employees about different types of phishing through security awareness and various training program and have implemented a way to inform their IT department of any phishing email s they receive. The training provided by the organization can be limited for a short time and therefore the long-term benefit of Phishing attack prevention remains a question. Fascinated by this challenge, this study/research targets to determine the stretch one can experience by using various techniques to keep the user engaged in preventing Phishing attacks

Chart, pie chart

Description automatically generated

Chart, bar chart

Description automatically generated

## Justification

The main objective of this paper is to propose a study/research to assess the concept model of how to encourage individuals to participate which will help a user in long run to identify and prevent phishing attacks at the same time by improving phishing reporting. The research will take a mixed approach and will include various measures or methodologies developed to tackle Phishing scams. Furthermore, a research is going to be performed on various phishing software platforms and browser addons to gauge the tools capabilities and use them in the real-world shielding user’s sensitive data. The outcome of this research will have potential to be published in a security research journal and can potentially be a funding initiative by NIST as this is an important area of research for Cyber security

# References

M. Baykara and Z. Z. Gürel, "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: Case Study. International Journal of Advanced Research in Computer Science and Software Engineering. 3

Anti-Phishing Working Group, <https://www.antiphishing.org>

[APWG] The Anti-phishing Working Group, “Proposed Solutions to Address the Threat of E-mail Spoofing Scams,” December 2003

Jampen, D., Gür, G., Sutter, T. *et al.* Don’t click: towards an effective anti-phishing training. A comparative literature review. *Hum. Cent. Comput. Inf. Sci.* **10,** 33 (2020). https://doi.org/10.1186/s13673-020-00237-7