Phishing Attack Prevention: How to Identify and Detect Phishing Attacks

Proposal #3 – Abstract and Cleanup

by

**Suraj Pratap Samirlal Poddar**

Harrisburg University of Science and Technology

Spring 2021

# Abstract

Internet has become the means to live a life which has been deeply integrated and embedded in our day-to-day life. It can be anything ranging from an online app which you visit or any social networking sites, financial sites, booking a Doctor’s appointment, ordering food, navigating to a destination, advertisements, movies and many more which makes humans life easier by accessing them in a short amount of time and mostly on the fly. Because of extensive use of Internet in daily life the technology has started to become vulnerable and therefore intense threats have been discovered following the technology. It has given birth to a new way for hackers to lure a victim into giving away their personal identity or to steal information digitally. Phishing is a form of cybercrime where a hacker/attacker for that matter 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 most popular is through e-mails, where an attacker spoofs an email or through instant messaging. The attack mainly focusses on people with no knowledge on Internet Security or to those who don’t take care heir security or privacy seriously. It can be a Bank Account or any social engineering account such as Facebook, Yahoo, Instagram, Gmail or any Online account. This paper will provide information about types of phishing attacks and steps that can be taken to shield user’s confidential information

Table of Contents

[Abstract 2](#_Toc65776032)

[Introduction 4](#_Toc65776033)

[Research Questions 6](#_Toc65776034)

[Significance and Justification 7](#_Toc65776035)

[Background 7](#_Toc65776036)

[Justification 9](#_Toc65776037)

[Literature Review 9](#_Toc65776038)

[Problems and Challenges 10](#_Toc65776039)

[Prevent Phishing 10](#_Toc65776040)

[Detect Phishing 11](#_Toc65776041)

[Providing Stake holder training 11](#_Toc65776042)

[Different Types of Phishing Attacks 12](#_Toc65776043)

[Malware Phishing 12](#_Toc65776044)

[Pharming 12](#_Toc65776045)

[Vishing 12](#_Toc65776046)

[Deceptive Phishing 12](#_Toc65776047)

[Spear Phishing 13](#_Toc65776048)

[Content Injection Phishing 13](#_Toc65776049)

[Host File Poisoning 13](#_Toc65776050)

[Learning to Detect Phishing Emails 13](#_Toc65776051)

[Hybrid Learning based Phishing Detection 15](#_Toc65776052)

[CRI approach to address phishing 15](#_Toc65776053)

[Taxonomy of phishing Attack 15](#_Toc65776054)

[Anti-phishing Technique Modus Operandi 16](#_Toc65776055)

[Lifecycle of Phishing Attack 16](#_Toc65776056)

[Visual Similarity Based Phishing Detection and Filtering Approach 16](#_Toc65776057)

[Taxonomy of Phishing Detection and Filtering Based on Visual Similarity 17](#_Toc65776058)

[Visual Similarity Assessment 17](#_Toc65776059)

[References 18](#_Toc65776060)

# 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 (A. Alswailem, 2019)

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 (Gürel, Detection of phishing attacks, 2018)

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 Anti-phishing 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 (M. Adil, 2020)

# 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 (Chhikara, 2013)

# 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 (APWG, 2003)

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

# Literature Review

Over the years, given the fast adoption of latest technological advancements, security exploitation/attacks have significantly on a rise topping the human vulnerability. Phishing has become one of the threats to cyber world creating a massive damage of worth billion dollars every year. Phishing can be performed in different methods involving web, email, messages etc. Over time there has many articles describing the techniques and new attacks based on phishing however, they have failed to outline all the risk factors involved and provide and efficient/effective solution to mitigate this form of a threat. In this section we will be comparing different data from various sources to perform a literature review. Emails has been always one of the main online application which is used extensively by lots of users, business, Govt and different organization for communicating with one another and sharing data and therefore phishing emails has always shown us a serious threat to digital commerce as they are used to scam both individual and financial institutions (A. N. Shaikh, 2016)

# Problems and Challenges

Hacker/phishers have become advanced and more talented/skilled at recreating/forging sites to appear identical including recreating logos and graphical presentation. No doubt Phishing is evolving to tackle the defenses and bypass the detection. In these circumstances I think a sequential approach is needed which will help mitigate these kind of attacks

1. Prevent Phishing
2. Detect Phishing
3. Provide Stake holder training

Diagram

Description automatically generated

Figure 1 Step by Step process

### Prevent Phishing

Phishing can be prevented by taking extra precautions and blocking it before it reaches the users, this includes blocking or blacklisting the phishing site by filtering emails. The first procedure is to identify the URL either manually or by ML, although this can help catch few sites, it cannot catch them all

### Detect Phishing

This method is deemed to be one of the effective methods as this can identify the link to phishing sites through the spam filters which are majorly used by the email servers. Phishing filters are constructed by Machine Learning techniques. Most of the browsers already have an extension installed on their browser which has a passive or an active indicator warning the users and alerting them at the same time

### Providing Stake holder training

By providing training to all the users can help avoiding the users clicking random sites and falling into Phishing scams. Most of the organizations create internal training program to combat against advanced phishing attacks which is often referred as anti-phishing techniques/methods. One of the famous anti-phishing game is Anti-Phishing Phil which is a micro game that helps a user identify suspicious URLs and spread awareness also provide a detail view of the consequences (Jampen, 2020)

# Different Types of Phishing Attacks

### Malware Phishing

A Malware which runs on the user’s machine, these are populated either via wicked softwared or by sending malicious files to the user via email as an attachment which upon downloaded can record the keystrokes

### Pharming

Pharming is a technique which is used to install a malicious code on users machine to manipulate and direct them to a fraudulent website without the users knowledge

### Vishing

Vishing is a technique which happens through a voice communication system in this case by making phone calls or by leaving a voicemail to the user acting to be a real company to lure a user to give away their personal identifiable data such as their back A/c Details, SSN, or Credit card details

### Deceptive Phishing

Deceptive Phishing is known as a very common type of phishing scam. In this technique a scammer can fake invoices or any attachments in deceiving users into opening an email or a text which is related to user’s day to day activity. For example, users W2 form or users tax statement. Malicious actors/scammers can send you a text/email with a company name which users trust and respond to

### Spear Phishing

Spear Phishing is a technique where email is sent to a well-researched target which claiming to be a trusted user, the entire intent is to lure the user to give away their personal information or infect devices with malware.

### Content Injection Phishing

Content injection phishing is a type of phishing where a illicit actor creates the contents of a legitimate sites with fake content and makes it look like a trusted site by luring the victim to give away their personal/confidential information to a hacker

### Host File Poisoning

Host File Poisoning converts a FQDN/URL into an IP address before it is routed over the Internet

# Learning to Detect Phishing Emails

Even though there are few advantages to filter a phishing attack delivered in the form of an email , there are not that many methods tailored to concentrate on phishing emails as opposed to spams in general. The closely related option is to create policies on the smtp server based on the classification of what we call it as a good email vs a phishing email. As the attacks improve, we expect there will be new features that will be added which will help in identifying and combining the information form internal as well as external resources. This approach is used to detect phishing websites, or the content sent via email to lure a user. While most of the email gets filtered it is very hard to accurately differentiate, although 90% of the phishing emails are blocked there is still a 10% chance where the user can always fall into the trap

The prosaic approaches for phishing detections have always been at a lowest accuracy, machine learning provides us a better outcome for phishing detection, however, are time consuming and not a match at scale. There are various methods that can help us in Phishing detection (Khonji, 2013)

Machine Learning Based Phishing Detection

Diagram

Description automatically generated

Figure 2 Machine Learning

To tame ML and make it effective in detecting phishing attacks is to collect data at hand and they must have features related to legit websites and phishing websites. Figure 2 Machine Learning shows the working model of ML for phishing attack detection. A stream of data is provided as input to train ML model to help predict the phishing attacks and legit traffic (Gupta, 2016)

Author in El Asssal et al. introduced a conventional structure which is named after phish Bench, which enables us to not only analyze but also assess the current detection techniques by understanding the framework and performance measurements. The tests show us that the classification dropped when the portion dropped among the authentic and phishing decreasing from 1 to 10

### Hybrid Learning based Phishing Detection

The technique compares real and phishing with counter strategies like tokenization, word/text parsing and by stopping word evacuation, this type of approach has been found to be accurate against existing techniques (Abawajy, 2013)

### CRI approach to address phishing

This type of approach focuses on a solution resulting in a holistic anti phishing review. All the approaches primarily focus on how to prevent the attack without actually thinking about the crime and the respective problem associated with it, the following literature shows that providing solution without knowing/exploring the actual issue is not the right way to tackle the threat. As a reason to which a CRI approach was implemented to explore the crime factor, review mitigation techniques and investigate the missing pieces. The major goal is to provide a future researcher with the information at the same time strengthen the literature review. Crime has increased with the expansion of IT, IoT and any form of digital devices that can talk over the Internet where cyber criminals have got their hands on to exploit in the real world (Purkait, 2012)

### Taxonomy of phishing Attack

Attackers use different techniques for phishing. In social way they try to attract by sending emails to provide bank information, credit card and convenience them to respond. They might also include links to open which can directly hack your system and attackers can also remote to victim’s computer to collect all the data.

### Anti-phishing Technique Modus Operandi

After receiving phishing emails anti-phishing techniques are also implemented either by redirecting them to SPAM folder or by showing a warning when user tries to open the link (Vayansky, 2018)

### Lifecycle of Phishing Attack

* Attackers try to create a fake copy of organization and sends URL to all Internet users using email id & social networking sites.
* In case of fake emails there are different solutions to block them based on structure features of mails so that fake email ids are not blocked.
* If fake email id works and user tries to open link, there will be some browser techniques based on client end.
* If it by passes through all the blockages, then attacker can steal all the data from user.

### Visual Similarity Based Phishing Detection and Filtering Approach

A user will not understand phishing attack as it will look similar to legitimate sites by seeing high standard URL’s layout, Images, fonts. Fake and original sites look exactly same except the URL’s are not same, but user may not check URL’s before clicking the link. If attacker doesn’t match with the original website, then there are chances of users using it are very less. (Basit, n.d.)

An attacker can fool user by following

1. Visual Appearance: Phishing website will exactly look like original website as attackers will copy the HTML source code to look same.
2. Address Bar: They can also cover the address bar by using any image so that users will not understand.
3. Embedded Objects: Use of different images, text to hide the content from phishing detection techniques.
4. Favicon: Every website will have a unique favicon image and attacker will try to copy same image if not user can easily identify fake website.

Based on different surveys 90% of users couldn’t identify fake websites by seeing the visual appearance and content. Even experienced users cannot understand and most of them doesn’t even look at the address bar because of this most of the users are trapped by attackers. (El Aassal, 2020)

### Taxonomy of Phishing Detection and Filtering Based on Visual Similarity

Different approaches have been proposed to detect phishing attack based on user’s education and software. An educated user should always check address URL before clicking any link and software-based approach like black-list will have all phishing URL’s but fails as it’s difficult to update new websites that are created every day.

### Visual Similarity Assessment

Based on approach there are two modules in which first module will detect the suspicious URL’s and other module will detect the layout, content. In Block level each block is compared with original website and then it shows matching blocks. Layout level is dividing the total number of matching blocks to all blocks in original site. Overall style is calculated by style feature and similarity if threshold is more than legitimate website then it is considered as phishing webpage

# References

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

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

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

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*.

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.

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.

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

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