BOOK CHAPTER | Web of Deceit

A Review of Phishing Attacks - Types, Prevention Measures and Detection Features

[1,] Ogundokun, Roseline O.. [2] Gbolagade, Morufay, D. & [3]Oladipo, Idowu D.
[1]Department of Computer Science, Landmark University Omu Aran, Nigeria
[2]Department of Computer Science, Al-Hikmah University, Ilorin, Nigeria
[3]Department of Computer Science, University of Ilorin, Ilorin, Nigeria
Corresponding Email: *ogundokun.roseline@lmu.edu.ng

Abstract

Phishing attacks (PAs), which have been in existence for decades and remain an enormous topic nowadays, pose a serious risk to the cyber world. PAs are on the rise, and attackers are adopting a range of novel and ingenious ways to carry them out. Therefore, a detailed investigation of past and modern phishing strategies is necessary. This document provides an overview of the methods utilized in phishing assaults. This article begins with a survey of the literature, followed by a detailed discussion of the six most prevalent phishing attempts, and countermeasures that can be employed to prevent them. In this review, the characteristics in PAs detection were also explored. The goals of this article are to promote consciousness of phishing strategies, educate persons concerning these attacks, and advocate the usage of phishing avoidance approaches, including fostering professional dialogue on the subject.

Keywords: Phishing attacks, phishing types, Phishing Prevention, Phishing detection features

Introduction

Phishing is a social engineering approach that pursues to encourage the target of an attack to let out individual information, for instance, an email address, username, password, or fiscal information by engaging innumerable techniques. The invader then attains this knowledge to the prey's harm (Stavroulakis, P., & Stamp, 2010). Phishing resulted from the word "fishing," which is spelled with what is known as Haxor or L33T Speak. The concept behind this terminology is that an attacker uses "bait" to entice the victim before "fishing" for the individual details invader wants to steal. The first-time attackers employed this tactic was in 1995 when they used phishing to induce victims to hand over their AOL account information (Jakobsson et. al, 2006). The term "phishing" first appeared in the media in 1997 (Rekouche, 2011).

BOOK Chapter | Web of Deceit - June 2022 - Creative Research Publishers - Open Access – Distributed Free

Citation: Ogundokun, Roseline O.. Gbolagade, Morufay, D. & Oladipo, Idowu D. (2022).
A Review on Phishing Attacks: Types, Prevention Measures and Detection Features.
SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series
Book Chapter on Web of Deceit - African Multistakeholders' Perspective on
Online Safety and Associated Correlates Using Multi-Throng Theoretical, Review, Empirical
and Design Approaches. Pp 219 -224. www.isteams.net/bookchapter2022.
DOI https://doi.org/ 10.22624/AIMS/BK2022-P37

As a result, phishing has advanced and progressed. Hackers have developed innovative tactics and utilized new media, and it is currently one of the most common attack routes. According to Symantec, email-built phishing extent has dropped to 1 in 3207 emails in 2018, down from 1 in 2995 emails in 2017 and lastly 1 in 392 emails in 2013 (Rader et. al. 2015; Symantec, 2019). During the last four years, the proportionate incidence of this general kind of phishing assault has steadily decreased; nevertheless, this might be attributed in part to a higher sum of emails being sent relatively than a decrease in PA.

The concept behind this terminology is that an attacker uses "bait" to entice the victim before "fishing" for the individual details invader wants to steal. The first-time attackers employed this tactic was in 1995 when they used phishing to induce victims to hand over their AOL account information (Jakobsson et. al, 2006). The term "phishing" first appeared in the media in 1997 (Rekouche, 2011). As a result, phishing has advanced and progressed. Hackers have developed innovative tactics and utilized new media, and it is currently one of the most common attack routes. According to Symantec, email-built phishing extent has dropped to 1 in 3207 emails in 2018, down from 1 in 2995 emails in 2017 and lastly 1 in 392 emails in 2013 (Rader et. al. 2015; Symantec, 2019). During the last four years, the proportionate incidence of this general kind of phishing assault has steadily decreased; nevertheless, this might be attributed in part to a higher sum of emails being sent relatively than a decrease in PA.

Despite this outward drop in PA, the Anti-Phishing Working Group (APWG) revealed that phishing extents increased to their maximum levels since 2016 in the third quarter of 2019 (Symantec, 2015; APWG, 2019). Figure 1 shows the inclinations in exclusive phishing sites from 2013 to 2019. Furthermore, phishing assaults are still popular; for instance, spear phishing is the utmost frequent contagion vector for malware spreading, with 71 percent of groups using it in 2018 and 65 percent using it in 2019 (APWG, 2019). Furthermore, between 2017 and 2018, the sum of phishing Uniform Resource Locators (URLs) climbed by 20% (Symantec, 2019), with two-thirds of these phishing sites nowadays employing a Secure Sockets Layer (SSL). This was the uppermost ratio since 2015, prompting the innovative and alarming deduction that HTTP is on no account a reliable indicator of a website's security (Symantec, 2015).

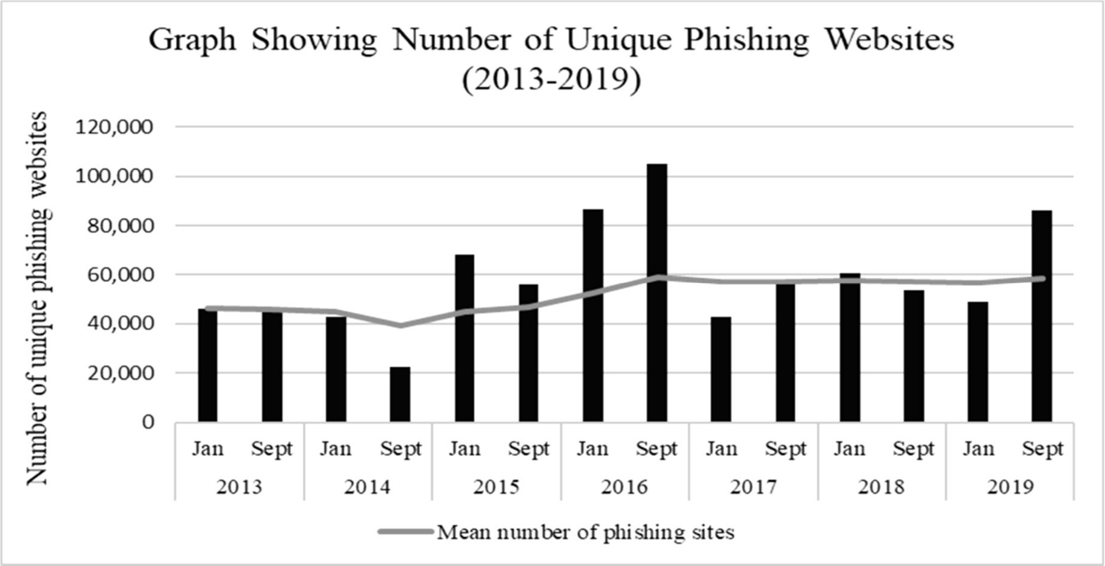

Figure 1. Number of exclusive phishing internet sites between 2013-2019
Source: APWG, 2019

SaaS (Software as a Service) and webmail have been the top aimers of phishers in recent years, accounting for 33% of attacks across a wide range of businesses (APWG, 2019). In 2018, 27 percent of phishing assaults were directed at webmail services, according to IBM. In addition, phishing emails were discovered to be the source of the breach in 29% of the X-Force-evaluated attacks against businesses (Symantec, 2018). In terms of the fiscal elements of phishing, Symantec discovered that "convention phishing page facilities" are offered for 3-12USD (Symantec, 2019) in the underground economy, showing that the overhead for building up a bespoke phishing assault is low. Gift cards have also been discovered to be one of the utmost typical mediums for a fraudster to pay out their winnings (Symantec, 2015). According to the FBI, phishing prey losses in 2018 were USD 48,241,748, with 26,379 persons impacted (IBM, 2019).

The FBI acknowledged over 100 grievances in 2018, with the utmost typically aimed domains being medical, education, and air travel, resulting in a total net loss of nearly 100, 000, 000USD. This fraud involves sending phishing emails to workers to get their login credentials. These were hence employed to get entrée to the payroll system, following which the phishers established controls to prevent workers from receiving alerts about account changes. The phisher was subsequently capable of altering account holders' unswerving deduction records, allowing them to siphon payments into their account, which in this case was paid in advance card (Symantec, 2018).

Phishing Attacks (PAs)

PAs are on the increase, creating a key danger to businesses worldwide. If corporations are to safeguard their company information, they must be capable of identifying a few of the utmost typical phishing frauds. It's similarly critical that individuals comprehend some of the preventive strategies that can be used against PAs (Jupin, et. al. 2019).

To that end, we'll go through six of the most prevalent forms of phishing attacks, as well as some preventive strategies:

Table 1: (Phishing Attacks and Prevention Measures)

Phishing attacks	Prevention measures
Deceptive phishing: This type of attack is the utmost common one. Attackers acquire an individual's private information or login details by impersonating a real establishment. They use the means of threatening and sounding the necessity of urgency in the emails to make recipients do what they want.	The accomplishment of a misleading phish is driven by how closely an attack email resembles authentic mail from a fictitious corporation. Therefore, handlers should carefully analyze every URL to perceive whether they forward to a strange or doubtful site. They should likewise be aware of common greetings, grammatical flaws, and spelling issues.
Spear Phishing: To trick the receiver into thinking they have a relationship with the sender, fraudsters customize attack emails using the target's name, position, firm, work phone number, and other information. Given the quantity of information required to build a convincing attack effort, it's no wonder that spear-phishing is widespread on social media sites like LinkedIn, where attackers may combine data from many sources to create a targeted attack email.	Organizations should perform continuing staff safety consciousness training that, amongst other things, restrain people from disclosing delicate private or corporate information on social media to defend against this kind of attack. In addition, organizations should invest in technologies that scan inbound emails for recognized harmful links or add-ons. This solution should be able to perceive symbols of known malware including zero-day threats.

Table 1 Contd: (Phishing Attacks and Prevention Measures)

Phishing attacks	Prevention measures
Whaling: Fraudsters might opt to carry out CEO fraud if their attack is effective. CEO fraud is the second step of a business email compromise (BEC) scam, in which attackers exploit a CEO's or other high-ranking executive's hacked email account to approve fraudulent wire transfers to a financial institution of their choice. Alternatively, they can use the same email account to perform W-2 phishing, in which they seek W-2 information from all workers to submit false tax returns on their behalf or post the information on the dark web.	Whaling assaults are successful because employers usually neglect to engage in security awareness training with their employees. Businesses should ensure that all employees, especially executives, get regular security awareness training to counteract worries about CEO fraud and W-2 phishing. Multi-factor authentication (MFA) channels should also be injected into financial authorization procedures so that no one can authorize payments alone through email.
Vishing: Instead, of sending an email, this type of phishing effort opts for a phone call. According to Comparitech, an attacker can conduct a vishing campaign by setting up a Voice over Internet Protocol (VoIP) server to simulate a variety of organizations to steal sensitive data and/or cash. The FBI discovered that in 2020, malicious actors employed such approaches to ramp up their vishing attempts and target remote employees.	Users should avoid taking calls from unfamiliar phone numbers, never give out personal information over the phone, and use a caller ID app to protect themselves from vishing attempts.
Smishing: Vishing isn't the only type of phishing that fraudsters may do on a phone. Smishing is another activity they might partake in. This method involves sending users fake text messages to induce them to click on a harmful link or disclose personal information.	Users may assist protect against smishing attacks by investigating strange phone numbers and, if they have any questions, phoning the firm listed in suspicious SMS messages.
Pharming: Some con artists are abandoning the tactic of "baiting" their victims as customers become more aware of common phishing scams. Instead, they've resorted to pharming. This phishing strategy takes advantage of the domain name system (DNS), a naming system used by the Internet to transform alphabetical website names, such as "www.microsoft.com," to numerical IP addresses so that it can identify and route people to computer services and devices.	Organizations should urge employees to submit login credentials exclusively on HTTPS-protected sites to evade pharming attacks. Anti-virus software should be mounted on the entire company devices, and bug databases should be modernized regularly. Finally, they must maintain safety updates given by a trustworthy Internet Service Provider (ISP).

Features in PA Detection

In the literature and commercial solutions, there have been several proposals for PA detection. To detect a phishing attempt, there are four indicators to look for. Figure 2 shows the features. The URL-based feature is a feature that works with URLs. A PA uses a URL to lead a visitor to a page that the attacker has replicated from the official site. A malicious URL may be distinguished by the URL and the replicated page. The entire length of the URL, the count digit in the URL, the right spelling of the URL, and if or not the URL contains a real brand name may all be used to identify the malicious URL (ICC, 2018; FBI, 2018). The domain-based functionality works by recognizing the URL's domain name, which determines whether the URL is a PA or not.

The third element, page-based work, is based on the information from the pages, and the information will be used to calculate the reputation ranking services. The pages' dependability will be determined by their reputation. The Global PageRank, Country PageRank, and Alexa position index are usually used to establish the reputation rating (ICC, 2018; FBI, 2018). Typically, ranking services will include information on user behaviors on the site, such as the projected number of daily, weekly, or monthly visits to a page, the average visit to the page, web traffic, domain category, and comparable websites to the page. Meanwhile, the domain scanning method is used to power the content-based functionality. The page title, meta tags, hidden content, body text, and photos on the page are the most often components analyzed. The scanning process determines if the page requires a login procedure, the page's category, and the user of the page (ICC, 2018; FBI, 2018).

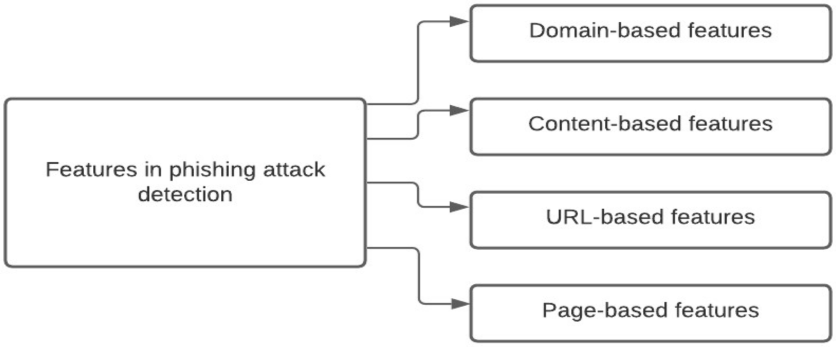

Figure 2. Phishing Attacks Detection Features (ICC, 2018; FBI, 2018).
Source: Jupin et al., 2019

All of the features mentioned are commonly utilized to identify phishing attempts. Due to the limits of these capabilities, the aforementioned features may not be successful in detecting PA in some circumstances. Consider a scenario in which the content-based functionality is used to provide a quick technique for detecting phishing on a large number of sites. Scanning a large number of documents will take time. As a result, the characteristic that will be chosen is determined by the detecting mechanism's goal and should be carefully chosen.

Conclusion

This article demonstrates that phishing is a present and important global issue. Phishing is still one of the most common malware infection vectors (APWG, 2019) the most common form of breach penetration, and the most common technique of social engineering assaults (Bisson, 2021). There's also the concerning trend that towards the end of 2019, the number of phishing sites discovered had reached its highest level since 2016. (as shown in Figure 1). The range of phishing vectors will continue to develop as technology progresses, and spiteful individuals will unquestionably discover new means to attain these innovative vectors in further advance, pioneering PAs (for instance, the current advancement of QRishing or the use of sound crouching on voice supporters like Amazon's Alexa).

This chapter examined the many kinds of PAs, spanning from the ancient to the modern. Each form of assault, as well as the strategies used to carry out the attacks and the precautions taken to avoid them, are described and discussed. Therefore, it is intended that by presenting an extensive knowledge founded of prevailing phishing prevention approaches, this article will assist to raise awareness amongst researchers and handlers, including promoting the development of preventive methods.

References

1. Stavroulakis, P., & Stamp, M. (Eds.). (2010). Handbook of information and communication security. Springer Science & Business Media.
2. Jakobsson, M., & Myers, S. (Eds.). (2006). Phishing and countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons.
3. Rekouche, K. (2011). Early phishing. arXiv preprint arXiv:1106.4692.
4. Rader, M., & Rahman, S. (2015). Exploring historical and emerging phishing techniques and mitigating the associated security risks. arXiv preprint arXiv:1512.00082.
5. Symantec. ISTR Internet Security Threat Report 2019. Symantec 2019, 24, 61. Available online: https://docs.broadcom.com/doc/istr-15-april-volume-20-en (accessed on 15 December 2019)
6. Symantec. ISTR Internet Security Threat Report 2015. Symantec 2015, 20. Available online: https://docs.broadcom.com/doc/istr-24-2019-en (accessed on 15 December 2019).
7. Anti-Phishing Working Group. Phishing Activity Trends Report: 3rd Quarter2019. 2019. Available online: https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf (accessed on 15 December 2019).
8. APWG. Phishing Activity Trends Reports. Available online: https://apwg.org/trendsreports/ (accessed on 27 December 2019).
9. Symantec. ISTR Internet Security Threat Report Volume 23. 2018. Available online: https://www.phishingbox.com/assets/files/images/Symantec-Internet-Security-Threat-Report-2018.pdf (accessed on 15 December 2019).
10. IBM. IBM X-Force Threat Intelligence Index 2019. 2019. Available online: https://www.securindex.com/downloads/8b9f94c46a70c60b229b04609c07acff.pdf (accessed on 15 December 2019).
11. ICC (IC3)/Federal Bureau of Investigation (FBI). Internet Crime Report 2018. 2018. Available online: https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219 (accessed on 20 December 2019).
12. Jupin, J. A., Sutikno, T., Ismail, M. A., Mohamad, M. S., Kasim, S., & Stiawan, D. (2019). Review of the machine learning methods in the classification of a phishing attack. Bulletin of Electrical Engineering and Informatics, 8(4), 1545-1555.
13. Bisson D., 2021. The state of Security. Retrieved on 5th January 2022 from 6 Common Phishing Attacks and How to Protect Against Them (tripwire.com)
14. Kumar, A., Chatterjee, J. M., & Díaz, V. G. (2020). A novel hybrid approach of SVM combined with NLP and probabilistic neural network for email phishing. International Journal of Electrical and Computer Engineering, 10(1), 486.