IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024

Design Efficient Method for Protecting User from Phishing Spam

Hiralal Ranu Katke
Institute of Distance and Open Learning, Mumbai, Maharashtra, India

Abstract: *Phishing is a common method hackers use to attack computer systems. Successful phishing attacks pose a serious threat to the security of electronic records and personal information. This algorithm is used for finding the phishing emails sent by the phisher to grasp the information of the end user. Link Guard Algorithm is totally based on the characteristics of the phishing hyperlinks. Each and every user is implemented with this algorithm. After that the user can recognizes the phishing emails and avoid responding to such mails. This paper presents an overview about phishing attacks and various techniques to protect the information.*

Keywords: Cyber Security, phishing , scam, Phishing attacks

I. INTRODUCTION

Phishing is a type of scam. It involves
scammers sending communication (usually email but may also be a phone call or SMS) disguised as being from a trusted sender in order to steal confidential information or to make it unavailable.
In the VPS, phishing attacks often involve an employee receiving a scam email containing a hyperlink or an attachment. Where the
employee clicks on the link or opens the attachment, they are typically taken to a website where malicious software is installed on their device or they are asked to provide confidential information (such as a username and password). The scammer will then often try to gain access to the employee's device and accounts.
Phishing is a type of online attack in which an attacker — using both technological and psychological tactics — sends one or more individuals an unsolicited email, social media post, or instant message designed to trick the recipient into revealing sensitive information or downloading malware.
Types of Phishing
Phishing can take on many different forms in order for cybercriminals to execute their schemes. Here are several variations of a phishing attack that is used to steal data:
Angler Phishing: This cyberattack comes by way of social media. It may involve fake URLs, instant messages or profiles used to obtain sensitive data. Social profiles are also inspected by attackers for any personal information that can be used for social engineering.
Clone Phishing: Clone phishing involves the exact duplication of an email to make it appear as legitimate as possible.
Domain Spoofing: In this category of phishing, the attacker forges a company domain, which makes the email appear to be from that company. Threat actors commonly do this with large and notable business identities to dupe users into actively volunteering their information.
Email Phishing: Phishing emails are often the first to come to mind when people hear the term phishing. Attackers send an illegitimate email asking for personal information or login credentials.
Search Engine Phishing: Rather than sending correspondence to you to gain information, search engine fishing involves creating a website that mimics a legitimate site. Site visitors are asked to download products that are infected with malware or provide personal information in forms that go to the attacker.
Smishing: Combine SMS with phishing, and you have the technique called smishing. With smishing, attackers send fraudulent text messages in an attempt to gather information like credit card numbers or passwords.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024

Spear Phishing: Spear phishing is particularly targeted as attackers take time to gather details that they can use to present themselves as trusted entities. They then construct personalized phishing emails, including details that make it seem as though the email is coming from a friendly source.

Whaling: A whaling attack targets the big fish, or executive-level
employees. An attack of this sort often involves more sophisticated social engineering tactics and intelligence gathering to better sell the fake.

Vishing: Combine VoIP with phishing and you get vishing. This type of phishing involves calls from a fraudulent person attempting to obtain sensitive information.

How to Recognize Phishing

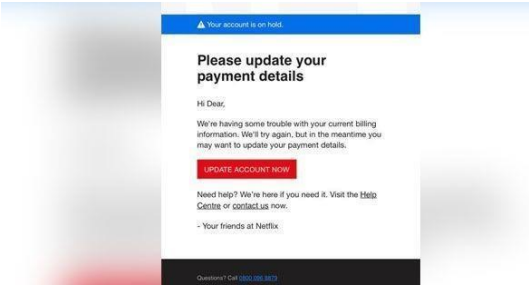
Scammers use email or text messages to try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could get access to your email, bank, or other accounts. Or they could sell your information to other scammers.

Scammers launch thousands of phishing attacks like every day — and they're often successful.

Scammers often update their tactics to keep up with the latest news or trends, but here are some common tactics used in phishing emails or text messages:

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. You might get an unexpected email or text message that looks like it's from a company you know or trust, like a bank or a credit card or utility company. Or maybe it's from an online payment website or app. The message could be from a scammer, who might say they've noticed some suspicious activity or log-in attempts — they haven't claim there's a problem with your account or your payment information — there isn't say you need to confirm some personal or financial information — you don't include an invoice you don't recognize — it's fake want you to click on a link to make a payment — but the link has malware say you're eligible to register for a government refund — it's a scam offer a coupon for free stuff — it's not real

Example of Phishing Email



Imagine you saw this in your inbox. At first
glance, this email looks real, but it's not. Scammers who send emails like this one are hoping you won't notice it's a fake.

Here are signs that this email is a scam, even though it looks like it comes from a company you know — and even uses the company's logo in the header:

The email has a generic greeting.

The email says your account is on hold because of a billing problem.

The email invites you to click on a link to update your payment details.

While real companies might communicate with you by email, legitimate companies won't email or text with a link to update your payment information. Phishing emails can often have real consequences for people who give scammers their information, including identity theft. And they might harm the reputation of the companies they're spoofing.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024

How to Protect Yourself from Phishing Attacks

Your email spam filters might keep many phishing emails out of your inbox. But scammers are always trying to outsmart spam filters, so extra layers of protection can help. Here are four ways to protect yourself from phishing attacks.

Four Steps to Protect Yourself from Phishing

Protect your computer by using security software. Set the software to update automatically so it will deal with any new security threats.

Protect your cell phone by setting software to update automatically. These updates could give you critical protection against security threats.

Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi- factor authentication. The extra credentials you need to log in to your account fall into three categories:

something you know — like a passcode, a PIN, or the answer to a security question.

something you have — like a one-time verification passcode you get by text, email, or from an authenticator app; or a security key

something you are — like a scan of your fingerprint, your retina, or your face

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

Protect your data by backing it up. Back up the data on your computer to an external hard drive or in the cloud. Back up the data on your phone, too.

Phishing website detection approaches

To identify and prevent phishing attacks, various anti-phishing methods are available. As illustrated in it is classified into five groups in this work.

II. METHODOLOGY

The systematic literature review is a research process that follows a set of rules. The paper follows the methodology introduced by Singh & Kaur (Singh and Kaur, 2018), Singh et al. (Singh and Beniwal, 2021), Kitchenham et al. (Kitchenham et al., 2010), and Brereton et al. (Brereton et al., 2007). The review methodology includes constructing research questions, identifying the list of electronic databases to be explored, data collection, data analysis, discussion on findings, and a comparison study of final selected research articles once all exclusion criteria have been applied. This systematic literature review aims to find the best approach, data set, and algorithm researchers employ for phishing website detection.

Methodology of the review

As discussed in the above para study will start by designing research questions and then explore the databases used for detection and analysis by comparing the findings of other literature as a part of the review methodology. The procedure includes searching primary and secondary databases, implementing inclusion–exclusion criteria, analyzing results, and discussions are all part of the process, only electronic databases are explored for the literature survey, which includes the most reputable journals, conference proceedings, and research thesis. During the initial search, 537 papers were found, and only 80 research items were selected after applying the inclusion– exclusion criteria

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024

How Can You Stop Phishing Attacks?

Because they are so hard for users and for security technologies to detect, phishing attacks. are often very successful. So how can you stop them?

Email Filtering

Your first line of defence against phishing is a Secure Email Gateway.

Email gateways are used to filter out harmful and malicious emails, and quarantine them automatically away from user inboxes. A good email gateway will block 99.99% of spam emails, and will remove any email that contains any malicious links or attachments. This means they are crucial in stopping users from receiving fraudulent phishing emails.

Email gateways such as Proofpoint also expose when accounts have been compromised, and so can prevent business email compromise attempts within your organization, and stop your accounts being used to send out spam or phishing emails to companies that you work with.

Having an email gateway in place is important for organizations of any size. There are a number of different vendors providing cost- effective, easy-to-use and highly secure email gateways that will help you to stop phishing attacks.

Phishing Protection Inside the Email Inbox

One of the challenges surrounding phishing is that once a phishing email is within an inbox, or an account has been compromised and is sending out internal phishing emails, it can be very difficult for admins to reach into user inboxes and remove the threat. Cloud-based email security solutions that integrate with email networks via API provide a comprehensive solution to this problem, with advanced phishing protection capabilities.

Cloud email security solutions protect users from threats within the email inbox. Typically, they use algorithms powered by machine learning and artificial intelligence (AI) which are fed typical attributes of phishing emails. They then apply these attributes to the emails your users send and receive, along with analysis from anti-virus engines, to detect suspicious emails. The best cloud email security services will then display warning banners on these emails, alerting users they may be harmful, or according to admin policies, they will remove the emails from your network entirely.

Having cloud email security in place is especially important for organizations who deal with high value or sensitive data and need strong protection in place from all forms of phishing attacks.

These platforms work alongside the secure email gateway. Using them together, you have a multilayered security approach that allow you to stop most phishing attacks before they can enter your email network, and have the tools to remove any sophisticated attacks that can bypass the spam filter.

Website Filtering

Web filtering is one of the most important ways to prevent your users from accessing phishing websites. There are a few different ways that web filtering works, such as a web proxy or filtering using DNS. Without going too deep into the technical specifics, these filters sort web pages into different categories and use anti-virus systems to scan pages for threats.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024

Organizations can then block certain categories and enable polices that will block users from accessing any phishing pages. This is crucial to stopping users going onto fake phishing websites that look legitimate and downloading malware, or inputting their account or financial details.

Sophisticated web filtering solutions will also use machine learning algorithms to scan webpages for signs that they are phishing, even if they do not contain anything outright malicious.

The Danger of Advanced Phishing Techniques

Common phishing techniques will lure victims to enter their credentials or to click a malicious link. But there are many more advanced techniques employed by attackers that make phishing difficult to detect. We'll give a couple of examples.

Phishing Sites Using Legitimate Domains: Website builder tools like Weebly or Wix are providing attackers with free, quick and simple templates to build sites for attacks. Since these websites are delivered vialegitimate links, e.g. a site hosted on Wix platform, they are hard to spot and require a combination of abilitiesfrom advanced threat detection tools, such as the ability to add new logic that will recognize new malicious URLs on the go, ability to adjust image recognition capabilities to recognize new phishing site URLs and more.

Phishing Attacks using legitimate filehosting services: Services such as WeTransfer and JUMBO mail can be easily and freely used by attackers to deliver malicious files. These websitesobviously pass as legitimate sites, so Advanced Threat Detection solutions will need to actually scan and intercept each file before it is delivered or downloaded by the user,and files can be quite large so scanning speed can be an issue.

Example 1: Using a legitimate file hostingservice for sending a malicious file

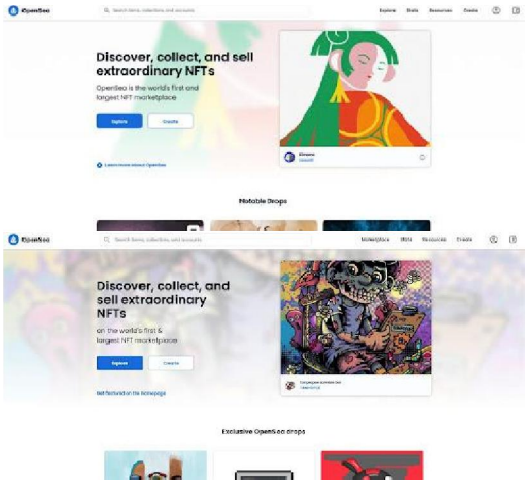
How to Prevent Phishing with Next- Generation Anti-Phishing Technology

The task of protecting employees and organizations from phishing attacks is not an easy one, however there are key techniques that advanced threat detection security solutions must provide in order to sufficiently protect against these attacks from ever successfully entering end-user inboxes.

Identifying Brand Impersonation with ImageRecognition

In brand impersonation phishing attacks, attackers impersonate targeted popular brands using the brand logo, brand signature, brand colour pallet and language, and more. An excellent example can be seen in this recent Open Sea phishing attack where you cannot see the difference between the malicious and actual site:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024



Example 2: Brand impersonation difficult to catch with the human eye

Image recognition is a key technology used to be able to validate if any URL is actually the legitimate site it is claiming to be. Similarities that are difficult to identify using human eyesight are easily caught using algorithms that know the original brand and analyze the potentially malicious content (e.g. an email, or a URL) against it – not leaving it up to chance, if the user is able to spot the attempt or not.

Identifying Malicious URLs with Lexical Analysis

Lexical analysis is another technique, helpful in determining if a URL is malicious or not. In Lexical analysis, the structure of the URL is analysed to detect:

If it contains suspicious words

How many parameters are passed inside the URL

What type of encoding is used to encode the parameters

If the URL contains email address or suspicious domain names, and more

Analyzing Reputation Vectors of Sender and Recipient Parameters

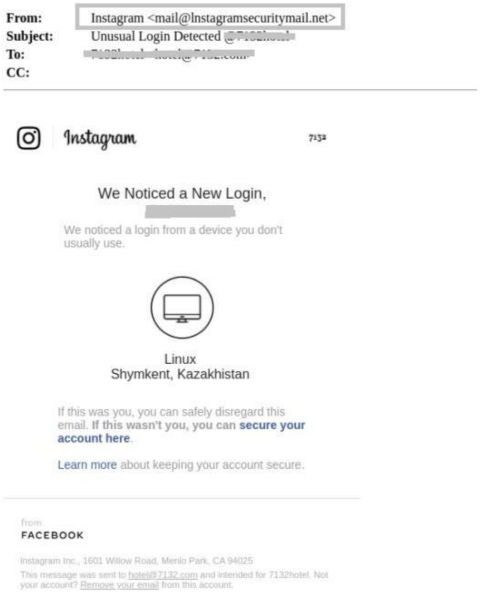
A Reputation vector is the collection of parameters maintained on both the sender and recipient, derived from the data and metadata collected on them. Information collected could be related to the legitimacy of the IP or the domain that the email is being sent from and more. The reputation vector will ultimately result in a score that will assist in making the decision if any type of content is malicious or not.

Identifying Smartly Spoofed Domains with Advanced Algorithms

Attackers will use similar domain names that are visually very close to popular brands that they are spoofing. A standard approach to address spoofed domains is to use a database of known domains, for example: Coca Cola and Microsoft, and then counting the number of differences. While this technique can work in some cases, it can be challenging to identify more sophisticated obfuscations.

Novel algorithms, available in advanced email security solutions, significantly lower the success rate of such evasion attempts. A good example is usage of biological algorithms that have been found to significantly help identify such spoofing attempts.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024



Example 3: Spoofing the Instagram domain

Dynamically Scanning URLs via Sandboxing

In addition to using the techniques mentioned above, and checking potential threats against threat intelligence sources, it is critical to dynamically scan all URLs, including the ones buried several levels deep inside the original content that was sent. Scanning all URLs dynamically, also referred to as "Sandboxing", will make sure new and unseen attacks, or new senders that look legitimate but actually are not, are identified. Next generation sandbox technologies will perform this scan in a speedy and accurate manner, getting rid of "traditional" sandboxing technologies' delays.

III. CONCLUSION

Phishing is a form of scam in which an attacker poses as a legitimate entity or person via email or other forms of communication.

Phishing emails are frequently used by attackers to distribute malicious links or attachments that can perform a variety of functions.

Though it may not truly warrant being called a hack in its own right, phishing is a favoured tool of malicious hackers because of the low cost and high potential. As a social engineering attack, phishing is difficult to defend against, but the risks can be mitigated through a well-designed information security program. Varonis Edge and Varonis Data Alert are both well-suited to detect and mitigate phishing threats throughout their entire lifecycle.

REFERENCES

[1]. Why Phish Should Not Be Treated as Spam by Norman M. Sadeh and Ph.D. http://www.drdobbs.com/security/why-phish- should-notbe-treated-as-spam/240001777, published May 18, 2012

[2]. Anti Phishing Working Group. Origins of the word "phishing". http://www.antiphishing/org/word_phish.html. Accessed: March 10, 2012

[3]. Computerworld Quick Study: Phishing by Russell Kay, http://www.computerworld.com/s/article/89096/Phishing Accessed: 27 March 2013

[4]. Verma, R., Shashidhar, N., & Hossain, N. (2012, September). Detecting phishing emails, the natural language way. In European Symposium on Research in Computer Security (pp. 824-841). Springer, Berlin, Heidelberg.

[5]. Varshney, G., Misra, M., & Atrey, P. K. (2016). A survey and classification of web phishing detection schemes. Security and Communication Networks, 9(18), 6266- 6284.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024

[6]. Bergholz, A., De Beer, J., Glahn, S., Moens, M. F., Paak, G., & Strobel, S. (2010). New filtering approaches for phishing email. Journal of computer security, 18(1), 7- 35.

[7]. Andrews, L. W., and Gutkin, T. B. (1991) The effects of human versus computer authorship on consumers' perceptions of psychological reports, Computers in Human Behaviour, 7, 4, 311-317.

[8]. APWG (2010) "Phishing activity trends report," A.-P.W. Group (ed.).

[9]. Bart, Y., Shankar, V., Sultan, F., and Urban, G. L. (2005) Are the drivers and role of online trust the same for all web sites and consumers? A large-scale empirical study, Journal of Marketing, 69, 4, 133-152.

[10]. Beldad, A., de Jong, M., and Steehouder, M. (2010) How shall i trust the faceless and the intangible? A literature review on the antecedents of online trust, Computers in Human Behaviour, 26, 5, 857-869.