A Study on Phishing Attack during the Covid-19 Lockdown

Sona Parani
431 Sadhuwaswani Nagar, Near Lucky Electronics, Indore, M.P

Mohit Raikwar
102, Ajay Bagh Colony, Near Daily College, Indore, M.P

ABSTRACT
Phishing is a mendacious attempt for gathering the sensitive information like debit MasterCard , net banking other secure details, user names and passwords. A standard approach in phishing is through the transmission of messages and email communication with an embedded hyperlink. The detection and mitigation of phishing attacks are a big challenge because of the complexity of current phishing attacks. Existing techniques are often too much time consuming to be applied in the real world in terms of detection and mitigation approach. Phishing is becoming more malicious during covid-19 lockdown and its detection and awareness is extremely important. Objective of this paper is to develop more security and protection requires by both users and enterprises towards the safe services. We discuss types of phishing, phishing impact during the covid-19 lockdown and methods to teach and train users against phishing.

General Terms
Phishing, unreadable hyperlink , Two-factor authentication (2fa), Fake Email and Messages, vigilance and preparedness.

Keywords
Covid-19 lockdown, phishing, two-factor authentication (2fa), security

1. INTRODUCTION
The term 'Phishing' initially introduce in the year 1990. The hackers commonly use 'ph' to replace 'f' to produce new term in the hacker's community, since they generally hack by mobile phones. Phishing is a new word produced from 'fishing', it refers to the act that the attacker allure users to divert a faked Web site by sending them faked messages e-mails, and stealthily get victim's secure private information like as user id and user name, password, and banking information etc. Messages and emails of phishing contain link to the infected website. Phishing email directs the user to the `malicious website where they are asked to enter the personal information, so that the website will hack the information whatever the user enters. Phisher's use the information to steal money or to launch other attacks. A malicious email and messages from a social networking sites or banking site asking us to proceed a messages and verify our account information.

2. TYPES OF PHISHING ATTACKS
According to Cisco, Cisco is the worldwide leader in it and networking[11]. It has described the most widely types of phishing attack are.

2.1 Deceptive Phishing
Deceptive phishing is the most applying type of phishing. In this case, an attacker attempts to obtain confidential information from the target victims. Phisher's utilize the data to take cash or to make different attacks. A fake email and messages from a internet bank asking you to click a link and verify your account details is an example of deceptive phishing.

These phishing emails generally threaten by creating urgency to scare the users into doing the attackers bidding such as paytm scammers sends an email attack that asks the user to click on the link provided for rectifying a mistake in their account. As this link takes to a fake paytm login page and thereby collect credentials like user's login etc., which will be either used by the attackers or sell this data to other attackers.

2.2 Whaling
When attackers go after a "big fish" like a ceo, it's referred to as whaling. These attackers regularly spend sizable time profiling the goal to locate the opportune moment and potential of stealing login credentials. Whaling is of precise subject due to the fact high-level executives are capable to get admission to a splendid deal of organization information

This type of phishing generally happens on company targeted board members. It is very easy to apply on them as they use only company email id. As they are the usage of private e-mail address, that will have protection and safety aspects giving through company.

2.3 Spear Phishing
Spear phishing objectives particular humans as an alternative of a extensive crew of people. Attackers regularly lookup their victims on social media and different sites. That way, they can customize their communications and show up extra authentic. Spear phishing is frequently the first step used to penetrate a company's defenses and lift out a focused attack.

Phishers generally collect the information of individuals through social media sites such as twitter, instagram, linkedin, facebook and use of fake addresses for sending emails and messages that similarly happens to be the email that was received from anyone of our team member or co-workers. For example, phisher may target the selected person in finance dept. By requesting bank transfer of large amount within a short time and acts like a victim's manager.t

2.4 Pharming
Similar to phishing, pharming sends customers to a fraudulent internet site that seems to be legitimate. However, in this case, victims do now not even have to click on a malicious hyperlink to be taken to the fake site. Attackers can infect both the user's pc or the website's dns server and redirect the consumer to a faux web page even if the right hyperlink is typed in.

3. LITERATURE REVIEW
In Economic Time, Surbhi Agarwal stated that the government of india has issued an advisory to citizens warning them against a large scale phishing group which

pretend to the Indian government and promises free Covid -19 checup and other service.

With this types of activity , attacker steal secire personal and financial information of peoples. The malicious actors are claiming to have 2 million individual email addresses and the attack a series of malicious operations are expected to start on June 21st.

The email id expected to be used is ncov2019@gov.in with the subject: Free Covid-19 testing for all residents of india , inciting them to provide personal and financial information. [12]

Barracuda Networks, IT Security company ,USA, Barracuda researchers detected 467,825 spear phishing email attacks, and 9,116 of those detections were related to COVID-19 between March 1 and March 23.

Researchers of Barracuda stated they have considered three most important sorts of phishing assaults the usage of coronavirus COVID-19 issues scamming, company impersonation, and commercial enterprise e mail compromise.. [13]

There are several research in which we have studied the few existing methods and technique that are comparison methods, which compare the similarity of the links to the anchor text of that links. Findings: With this algorithm we found a way to mitigate email phishing. Applications/ Improvements: In this technique writer accelerated accuracy of the discovering phishing emails by using checking the http hyperlinks which are the email equipment to redirect person to the phishing website. Discuss about a new server side anti phishing email addon algorithm, by using the properties associated with the hyper-links, which present in emails. The methods we used here are comparison methods, which compare the similarity of the links to the anchor text of that links. [1]. Another technique which Detecting Phishing Web Pages based on DOM-Tree Structure and Graph Matching Algorithm, In this paper an strategy which calculates similarity of two net pages based totally on genetic algorithm and utilized it to detecting phishing net pages the use of DOM-Tree structure. (Third party detection) [2]. Browser-side Countermeasures for Deceptive Phishing Attack, Phishers use the downloaded webpage from the real Web site to make the phishing webpage appears exactly the same as the real one does. Intuitively, phishing webpage detection is similar to duplicated or plagiarized document detection in some extent. Digital watermarking is one of the most widely used measures to protect digital information from copyright infringements. In the next, we will focus on a new technology called webpage watermark to fight against deceptive attack.[3]. In the research of "A Framework for Phishing Detection in Mobile Devices", this paper propose a novel framework for phishing detection in Android mobile devices which, on the one hand exploits well-known techniques already implemented by popular web browsers plug-in, such as public blacklist search, and, on the other hand, implements a machine learning detection engine which ensure zero-hour protection from new phishing campaigns.[4].Some researchers implemented LinkGuard in Windows XP which are generally for fixed operating system[6]. Many Review on Phishing Attacks and Various Anti Phishing Techniques introduce with researchers[8] in which many techniques have some advantages and disadvantages that are show in the Table 1.[14]

Table 1. Advantages and disadvantages of existing techniques

Techniques	Advantages	Disadvantages
Blacklist	Simple	Cannot detect new phishing attacks.
White list	Simple	Positive rate is less.
Content based	Highest accuracy	Depends on standard databases.
Network based	Easy to block ip addresses	Time consuming and costly.

4. PROBLEM STATEMENT

During the covid-19 lockdown, widely used platform such as ecommerce, e-education have largely affected. As we know about the main important factor in phishing attack are web hyperlink , as link takes to a fake web page. This two platform Ecommerce and E-education system are largely deal with hyperlink due to this attacker get more opportunity to hacked the target user easily. Main problem between us that many user's doesn't not understand the concept of valid hyperlink and they focus on layout and content of web pages instead of valid hyperlink.

As many researcher have mentioned the concept of self awareness and develop IT skills when we talk about the phishing attack. We always read that before taking any action on emails or messages, we have to focus on web hyperlink or the source that it is valid or not, but at the same time in current scenario many popular platform such as Ecommerce, Payment and Online Education platform are make the user more friendly and more comfort to trust on unreadable invalid hyperlink .Because, this types of trustable platform which are currently working to generate shorten hyperlink or unreadable hyperlink as seen in figure 1 to 4. In ecommerce as upi payment platform and e-education online learning platform like google meet , zoom and google form and many other platform still generating the unreadable hyperlink which makes user more friendly to trust with this type of hyperlink without any fear. This is the most harmful current issue due to this still many people are getting hacked by phishing attack by granting and proceed the fake hyperlink.

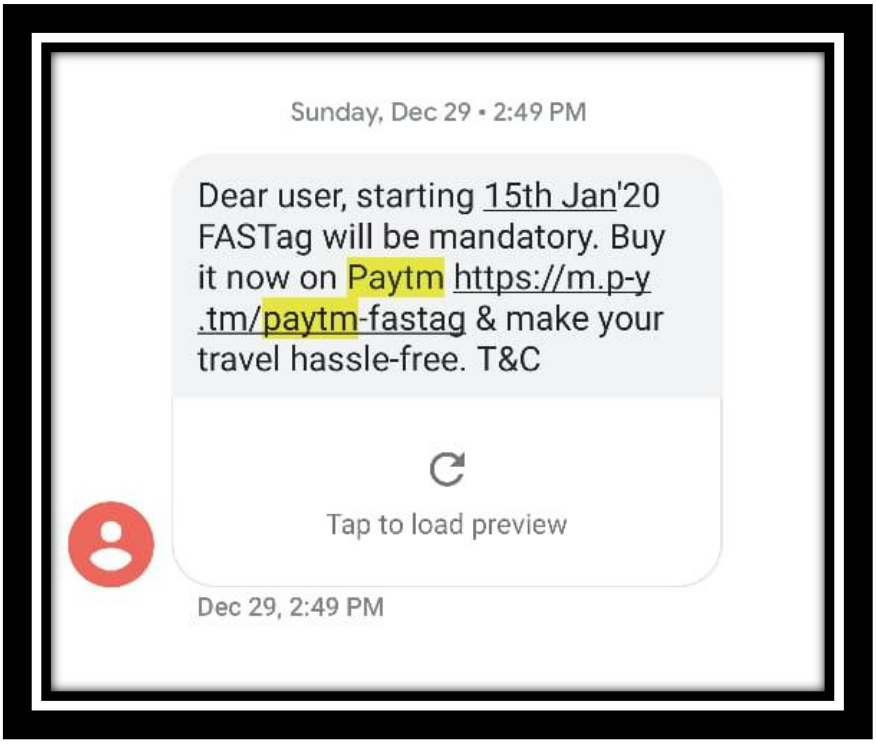

Fig 1: Valid HYPERLINK of Paytm

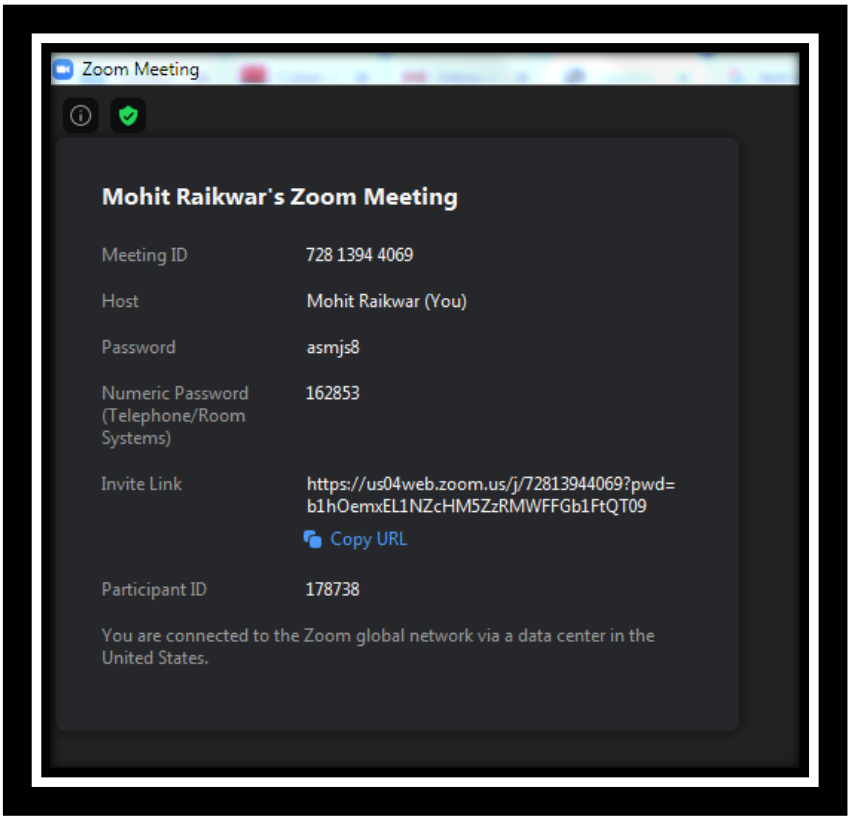

Fig 1: Valid HYPERLINK of Zoom- a web-based video conferencing software

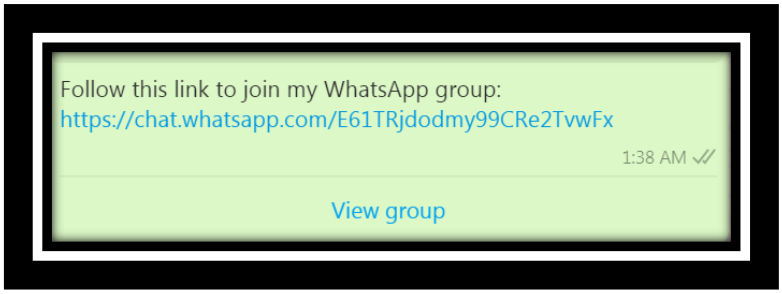

Fig 1: Valid Hyperlink of watsapp application for invitation to join watsapp group.

5. PROPOSED SOLUTION

Phishing attack protection requires by both users and enterprises.

For users, greater vigilance and preparedness is key. A spoofed message frequently includes refined errors that expose its real identity. These can include spelling mistakes or changes to domain names, By seen unpredictable emails/messages, users should also stop and think about why they're even receiving such an email or messages. User must not be granted the indistinct HYPERLINK.

For enterprises, a variety of steps can be taken to mitigate each phishing and spear phishing attacks:

The most effective method is Two-factor authentication (2fa) for countering phishing attacks, as it adds an extra verification layer when logging in to sensitive applications. Two-factor authentication depends on users having two things: something they know, such as a password and user name, and something they have, such as their smart phones. Even when peoples are compromised, Two-factor authentication (2fa) prohibit the use of their compromised credentials, since these alone are insufficient to gain entry.

In addition to the usage of 2fa, corporations ought to put in force strict password administration policies. For example, personnel have to be required to often exchange their passwords and to no longer be allowed to reuse a password for more than one applications.

Enterprises have to take the decision to promote themselves using only with unique domain and identical HYPERLINK. So that user can easily identify the valid and invalid web HYPERLINK for the particular domain. If such the scenario will be follow by several enterprises, user will be habitual to remember the valid HYPERLINK and never granted the fake HYPERLINK.

6. CONCLUSION

A phishing attack is a very common social engineering approach to targeting an organization and end users. It has become of the most harmful attacks nowadays. There have been numerous studies on detecting and mitigating phishing attacks and still no effective solution has found. As due to the trend of unreadable variable and shorten hyperlink, which are mainly used by most popular platform such as e-learning platform, online upi payment platform, google form invitations and more. So the suggestion arise by studied overall all with past researches and literature survey that enterprises should reduces or stop to introduce themselves using variable hyperlink as we mentioned in the figure 1 to 4. In this paper, we have proposed that educational campaigns will help diminish the threat of phishing attacks by enforcing secure practices, such as not clicking on external email/messaged links. Both users and enterprises have to develop the phishing attack protection like two-factor authentication. Enterprises promote themselves by it's genuine domain hyperlink and stop to make an unreadable hyperlink.

7. REFERENCES

[1] Addon, J. Dileep Kumar1*, V. Srikanth2 and L. Tejeswini. Email Phishing Attack Mitigation using Server Side Email. Indian Journal of Science and Technology.

[2] Le Dang Nguyen,Dac-Nhuong Le, Le Trong Vinh from Haiphong University. Detecting Phishing Web Pages based on DOM-Tree Structure and Graph Matching Algorithm.

[3] International Conference on Information Assurance and Security. Huajun Huang, Shaohong Zhong, Junshan Tan, College of Computer Science, Central South University of Forestry & Technology, Changsha,China.

[4] G. Bottazzi, E. Casalicchio, D. Cingolani, F. Marturana, M. Piu Dep. of Computer Science.University of Rome "Tor Vergata" - Italy. MP-Shield: A Framework for Phishing Detection in Mobile Devices.

[5] Mahmoud Khonji, Youssef Iraqi, Senior Member, IEEE, and Andrew Jones. Phishing Detection: A Literature Survey.

[6] Juan Chen,Institute of Communications Engineering, Nanjing 210007, P.R. China.Chuanxiong Guo. Institute of Communications Engineering. Nanjing 210007, P.R. China, Online Detection and Prevention of Phishing Attacks (Invited Paper).

[7] Pratik Patil1, Prof. P.R. Devale2 M Tech Student, Information Technology, BVUCOE, Pune, India1 Professor, Information Technology, BVUCOE, Pune, India 2. A Literature Survey of Phishing Attack Technique.

[8] V. Suganya Assistant Professor Department of Computer Science and Engineering Avinashilingam Institute for Home Science and Higher Education for Women.A Review on Phishing Attacks and Various Anti Phishing Techniques. International Journal of Computer Applications.

[9] Phishing: An Analysis of a Growing Problem. Anthony Elledge GIAC Security Essentials Certification (GSEC) Practical Version 1.4b, Option 1.

[10] Global Phishing Survey 2H2012: Trends and Domain Name Use. Greg Aaron, Illumintel Inc. Rod Rasmussen, Internet Identity. APWG.

[11] Cisco: cisco is the worldwide leader in it and networking, https://www.cisco.com/c/en_in/products/security/email-

security/what-is-phishing.html.

[12] The Economic Times, https://economictimes.indiatimes.com/tech/ites/indian-govt-warns-against-major-upcoming-phishing-attack-which-promises-free-covid-19-testing/articleshow/76469119.cms?from=mdr

[13] Barracuda Networks & IT security Comapny, US. https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing.

[14] A Survey on Phishing And It's Detection Techniques Based on Support Vector Method (SVM) and Software Defined Networking(SDN).