International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 01 | Jan 2021 www.irjet.net p-ISSN: 2395-0072

Phishing Attack During Covid-19 Pandemic

Menon Sanoop Govindankutty

Student, M.Sc IT, Keraleeya Samajam (Regd.) Dombivli's Model College, Maharashtra, India

---

Abstract – *Phishing is a type of attack by use of electronic communications to deceive and take advantage of users. Phishing attacks attempt to gain users confidential and sensitive information such as usernames, passwords, credit card information, and more. Phishing attack is done through mails, text messages and telephone calls. After the hackers collects the information through attacks use this information to commit crimes and identity theft. Hackers will always try to exploit a crisis, and the covid-19 outbreak is no different. During the pandemic, almost the world started to run over internet like corporate, education, business and hackers used this pandemic to exploit the greatest cyber security vulnerability of all human emotion. It is a smart tactics. Hackers know that the majority of the breaches are the result of human mistakes and with so any people working from home, away from regular contact with IT security and generally on edge with stress, now is the perfect time for hackers to test the limit of individual alert. As per the Google threat analysis 18 million covid-19 themed phishing emails where blocked by mid of April. This paper provides an explanation on phishing attack and create awareness and countermeasures against this attack.*

Key Words: Phishing, Cyber Security, IT, Covid-19, Pandemic.

1. INTRODUCTION

Cyber Security is the practice or body of technology which is used to secure the network, device, program from different types of attacks. Cyber Security is one of the key concerns in this new world as the technology is developing day by day and faster. In each and every department they are dependent on IT infrastructure and so to make them secured is important. Data is most valuable think in this new era for industries as well as individual and they are very much vulnerable to many attacks while in transit and storage. To secure the data from unauthorized person and from attack industries and individuals spend lot on cyber security experts and ethical hackers.

There are mainly 2 types of attacks Passive attack and Active attack. Passive attack is a method where a attacker just observe the messages but they do not make any changes in data. Active attack is a attack where the attacker tries to modify the content of the data.

The attackers try various methods to find loophole in the system as a gateway to get into the victim system and access try to gain unauthorized access to confidential data.

Phishing is a method involves sending fraudulent emails, text or telephonic call to get the victims confidential data like bank account details, bank cards details, personal information and their credentials. The mails, text and calls seem to be come from a creditable source. Mails, text and calls may be like your bank card is blocked share the OTP to continue the service, or you won a lottery please register to claim the price. Making a copy of ecommerce website and making the victim to believe the site is legitimate and victim fill his/her credentials and make payments, for example flipkart.com is the real domain name of the Flipkart ecommerce website but the attacker copy the code and just make a small change like replacing "k" with "c" many of them will not notice and become a victim.

Every Crisis is a platform or best time to use find the vulnerability of human error by attackers. To expose their vulnerability is easy as they are already affected with the crisis. So Covid-19 was a big platform for the hackers to explore the human error. During Covid-19 individuals as well as industries was heavily dependent on the IT infrastructure as the lockdown was imposed all over the world. In India Kerala sees the highest phishing mails in this covid-19 during February to April mid 2020.

The phishing links was made in name of WHO, Centers of Disease Control and prevention etc. People where in panic so they accessed this links to know the information regarding covid. Just by clicking the link malware would automatically downloaded into system in some cases. Even the most educated people where also became the victim because the attackers used the panic and created the urgency.

2. HOW PHISHING ATTACK WORKS.

Hacker's motive of phishing attack is to gain the confidential data from the victim. They create a look like of a legitimate website and send it through social media, mails and texts. Attackers create exactly the copy of legitimate website so the common users will not be able to find out the difference. Then victim will do the steps that thinking the website is exactly what he/she needs but they are not aware that the data they are giving is going to the attacker server.

The first step is they plan to attack, they make a script understand the scenario what's happening to the world and make a plan according to it. If the attacker want to attack random people from a big population they study about the situation going on, for example COVID-19 whole world was under panic situation so the attackers creates a websites, mails, text and call making the subject covid-19 like WHO, Disease Control websites etc. As this covid pandemic hits the

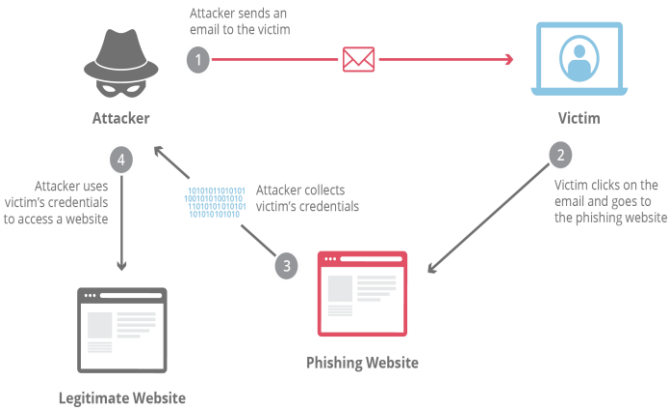
schools where also shut like any other industries, so they started the online platform to teach students. But many of the family were not having the necessary technologies to provide to the children. Hackers sensed the need of urgency in mobile phones, tabs and laptop, due to lockdown offline shops were shutdown all over the world so here there is only one way which is online ecommerce. Hackers created the dummy frontend of the legitimate ecommerce site and spread in social media with several discounts and many of them trusted the advertisement and clicked the link and ordered the mobile phones, tabs and payment is done through online gateway. Victim lost their money and given their credential. If the Attacker wants to attack certain individual they start to observe his mental health, likes, dislikes, on which type of topic he is active in social media, personal details etc. So according to the details attacker collect he plan the attacks.

Compose Mail is the second step of phishing attack. By collecting the information in planning phase, they create the script how should the mails and text looks like genuine.

Then after composing the mail they attack, they send the mails, texts or call and the victim will not be able to differentiate the legitimate website or hacker website. The victim gives the information asked in links and calls.

Then the attacker collects the information which they get from the phishing link and mails. They segregate the data from other datas and select needed data.

Then the last step is fraud, they use the data for which they have aimed for example to steal the money form the victim.



[1]Fig -1: Phishing Attack Mechanism

IFig -1 shows the phishing attack mechanism.

i) Here the attacker sends an email to the victim.

ii) Victim click on the given link.

iii) The page redirect to the phishing website.

iv)Victim insert all the credentials.

v) Attacker collects the credentials from victim

vi) Finally attacker use the credential from victim for fraud works.

3. TYPES OF PHISHING ATTACK

There are different type of Phishing attack but the motive of every attack is one. The mechanism used for to gather the data is different.

- **Deceptive Phishing**

[2]Deceptive phishing is the most common type of phishing scam. These scams occur when a recognized source emails you in order to compromise information. Typically, these emails request that you.

- Verify account information
- Re-enter information, such as logins or passwords
- Request that you change your password
- Make a payment

Once this information is input, hackers can access your accounts and then utilize the sensitive information in order to steal payment card information, sell your personal information or otherwise utilize your sensitive information for gain.

- **Spear Phishing**

[3] Spear –phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons. This is achieved by acquiring personal details on the victim such as their friends, hometown, employer, locations they frequent, and what they have recently bought online. The attacker then disguise themselves as a trustworthy friend or entity to acquire sensitive information, typically through email or other online messaging.

- **Whaling**

[4] A Whaling attack is a method used by cyber criminals to masquerade as a senior player at an organization and directly target senior or other important individuals at an organization, with the aim of stealing money or sensitive information on gaining access to their computer systems for criminal purposes. Also Known as CEO fraud, whaling is similar to phishing in that it uses methods such as email and website spoofing to trick a target into performing specific actions, such as revealing sensitive data or transferring money.

[5] Cyber criminals have been using a phishing kit featuring fake office 365 password alerts as a lure to target the credential of chief executives, business owners and other

high level corporate leaders. In a blog post, researchers from Trend Micro reported that they uncovered 70 email addresses that they have been targeted with the so-called "Office 365 V4 phishing kit" since May 2020, 40 of which belongs to "CEOs, directors, owners and founders, among other enterprises employee[s]."

4. PHISHING SCAMS DURING COVID-19

Hackers always try to exploit the crisis, and covid outbreak is producing a perfect storm for cyber criminals. They create urgency among the people during this pandemic even the most educated one fall in to the trap as tension and stress is high. Some of the coronavirus phishing attacks are:-

1) Help desk impersonation

[6] At a time when technical support teams are helping employees transition to remote workstations, cyber criminals are impersonating IT help desks to take advantage of their increased visibility and communication.

Employees working remotely for the first time are likely in contact with IT and security teams more than ever before. Employees anticipation communication from your help desk may be more susceptible to clicking a malicious link in this type of attack.

2) Safety measures turned into malicious

During this covid everyone was depended on WHO orders and precaution steps. And the hackers tried to trick the victims as sending mails which look like a mail from WHO in which they provide a link which is given to download the precautions regarding the safety measures. If the victim clicks the link, they are redirected to the spoofed WHO website to gain the victims credential.

3) Internal organization alert

This attack is done inside an organization. They send mail as President or CEO of organization to their employee's regarding the pandemic and along with an attachment regarding the precaution steps should be taken by the employees. The objective is to infect an employee's machine.

4) New Cases in your area

Here the attacker tries to make fear against the people. In this pandemic situation when someone receive a mail regarding new cases in your area majority of the people will be curious to open the link. To make them safe and to aware about their area they click the link and they are asked to login with their mail id. By this the attacker can get their email credential.

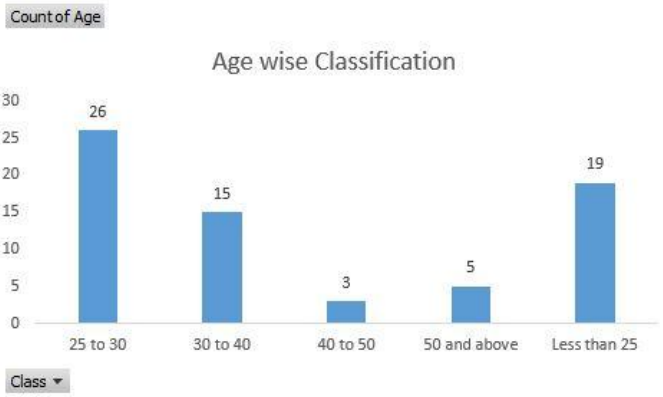
5) The Donation scam

[6]Like the tried-and-true donation scams used after natural disasters, the phishing attack solicits donations to fight the spread of the coronavirus. The attack imitates a CDC emergency outreach email and asks victim to deposit money into a Bitcoin account.

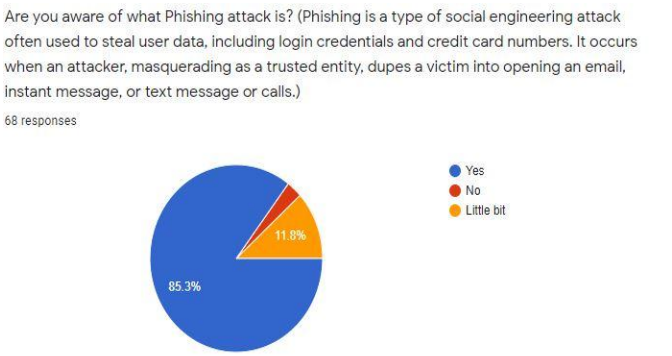
Like the above mentioned examples there are more and more phishing scams occurred during this pandemic whole over world. [7]The number of coronavirus COVID-19 related email attacks has increased by 667 per cent since the end of February, according to a new report.

5. SURVEY REGARDING PHISHING ATTACK

This survey is conducted by me on few people about regarding some general information about phishing attack and what know about it.

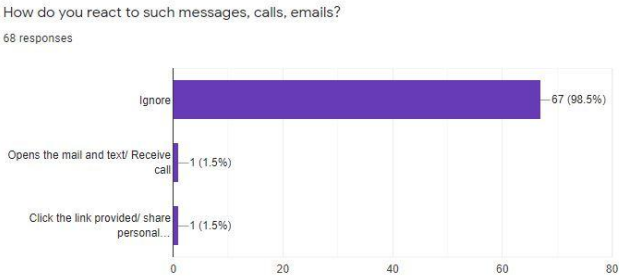


25-30 is the age group filled my questioner most 26 people, other age groups are 30-40, 40-50, 50 and above, less than 50. So total of 68 responses I got from this survey

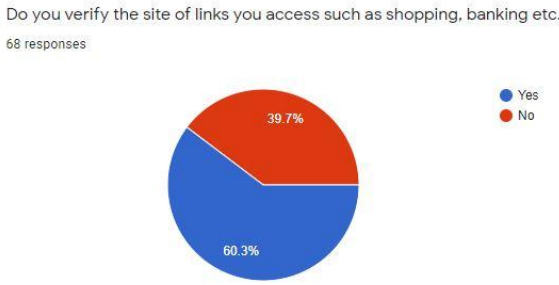


In 68 responses 85.3% are aware about what phishing attack is and 11.0% are aware little bit.

This question was intended to know about how many of them get such spam messages, mails and calls. In which 17.6% says they get the email, calls and messages on regular basis. And 79.4% gets them occasionally. By this response I understood that the attackers are trying regularly to attack.

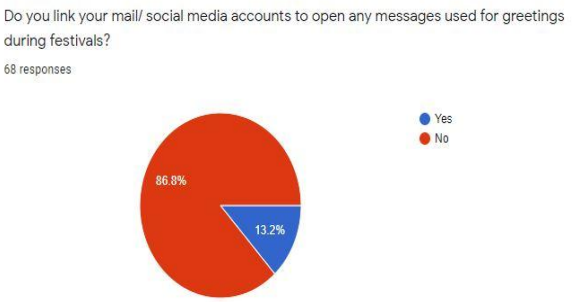


Next I want to know, what is their reaction against such emails and calls is. From the response of 68 people 98.5% ignores such emails and text but still in 68 1.5% is responding. Every attacker don't expect that they will get 100/100 victim, they always try to convert 1 of 10 attacks.

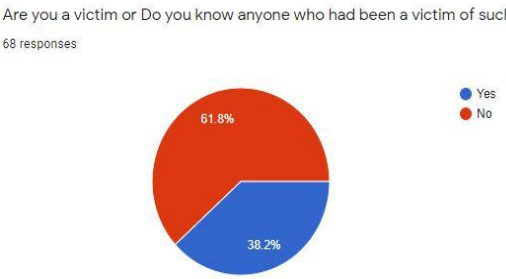


From above graph it shows that 60.3% verify the site of links they access but 39.7% does not. Attackers create a dummy page of legitimate website and share the link.

When victim clicks the links he believe that the site in front of him is legitimate. Without verifying the site the insert the details asked in website. Such cases are happened in many places. For example Flipkart is one of the famous ecommerce website, attackers create a dummy page of flipkart the only change is that in URL the spelling of domain name will be changed like they put "c" instead of "k". Many of them have does not verified the URL and became victim of such attack.



Many of us receive messages during festival season, in which there will be a link and we have to login our facebook or google account to use it. This is also a type of attack when victim insert the credential the attackers gets all the credential. The response I got is 13.2% still link their email/social media account to such links while 86.8% does not.



From above graph 38.2% are a victim or know any one who is victim from 68 responses and 61.8% are not.

6. ANTI-PHISHING

Counter Measures for phishing include training, knowing legal concepts, implementing security control measures and building awareness through better security practices.

- Secured Login

The first and foremost important security step is every one should use https than http as http will not give guarantee that the login credential is encrypted. Two-way authentication should me used. A code will be sent to you on your phone when u insert your username and password and you have to use that code to login

- Implementing organizations policies and procedures

Every organization should follow some policies and procedures under IT department. They should update there policies and procedures regularly. Employee should always keep backup of data so the IT department can restore and can change passwords monthly.

- Reporting

Always report suspicious activity noticed in email accounts is a must for employees. Everyone should be always alert for suspicious emails, links, attachment to maintain security

- Software update

Always update your software by updating and installing firewalls in order to prevent email spam

7. CONCLUSIONS

As according to my survey majority of them are aware about phishing attack. But as this pandemic every industries started to dependent on IT infrastructure. Now every age group from school students to aged people are now using technology and internet. So the vulnerability is high. We should give the knowledge to every one as now every one is using internet. Teach the aged people and students who attend online lecture to not open the unwanted messages and links. The theme and method of phishing attack changes, so the only way to away from such attack is get updated, alert on such spams.

8. REFERENCES

[1] What is phishing attack?, Cloudflare.com

[2] Types of phishing attack, https://a-lign.com/types-of-phishing.

[3] DigitalGuardian.com, https://digitalguardian.com/blog/what-is-spear-defining-and-differentiating-spear-phishing-and-phishing.

[4] Kaspersky.com, https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack, October13, 2017.

[5] Scmagazine.com, https://www.scmagazine.com/home/security-news/phishing-scheme-shows-ceos-may-be-most-valuable-asset-and-greatest-vulnerability, Badley Barth, Jan26, 2021.

[6] Resources.infosecinstitute.com, https://resources.infosecinstitute.com/topic/top-7-coronavirus-phishing-scams-making-the-rounds, Tyler Schultz, March 24, 2020.

[7] Cisco.economictimes.indiatimes.com/news,covid-19-related-phishing-attacks-up-by-667-report, March 27, 2020

AUTHOR

Name: Menon Sanoop Govindankutty

B.Sc.(Computer Science)

Pursuing M.Sc. (Information Technology)