Page 1019 - 1025

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 3 | Issue 3

2020

Cyber Phishing: A Trap of Disguise during the COVID-19

SAKSHAM KUMAR[1] AND HARSH VARDHAN SINGH[2]

ABSTRACT

Does security defines technology or technology defines security? The internet has grown at a rapid scale in the 21st century especially in India which has been accompanied with threats of cyber crimes. Cyber crimes in these days come with many forms under which one form is cyber phishing. According to many reports, Cyber phishing in India has surged amidst the country's unprecedented coronavirus lockdown. In one of the reports published by Reuters, cyber phishing during the lockdown has soared in the country by 87 % in between March and April only.

There has been an inundation of fake apps, links, domain names and websites in order to steal personal information and data including bank account details especially when the companies across the globe and even the Indian Government are encouraging towards 'work from home' via the online medium. In this paper we will discuss about the cyber fishing how it's surging amidst the coronavirus and we will also try to figure out the answer of the question asked above.

Keywords: *Cyber Fishing, Cyber Crime, Technology, Internet, Lockdown.*

I. INTRODUCTION

The Internet is one of the fastest-growing areas of technical infrastructure development.[1] It is omnipresent in almost all the spheres of the life. With each passing minute the network and users of internet is increasing at a rapid growth. Along with the growth of internet, many kinds of cyber crimes have emerged in the 21st century. Cyber security is one of the biggest challenges for the world today. Majority of big crimes today like Cyber Phishing, counterfeiting, terrorism, piracy, privacy etc. are somewhere connected to the cyberspace in one way or the other. The Cyberspace of India is also becoming vulnerable to cyber crimes and the crimes have taken up a fast growth especially during the time of Coronavirus.

Cyber Phishing is a process to gather personal information from other devices using deceptive links websites and emails. Phishing attacks an individual by seeking them to

[1]Author is a student at New Law College, Bharati Vidyapeeth University, Pune, India.
[2] Author is a student at New Law College, Bharati Vidyapeeth University, Pune, India.

provide their personal and sensitive information such as name, date of birth, password of the accounts, login credentials, card numbers, etc of an individual and the attackers ultimately end up performing the crime of identity theft by the aid of impersonation of someone who is trustworthy such as anyone from the bank of that person or police etc.

Phishing attacks leads to an infection of malware into the computers of the victim by the virtue of mails this malware is transmitted by the way of email and which is disguised as either in the form of an attachment document or even a link. In an era, where virtual word has made the life of an individual simpler and almost everything is carried out online it had resulted in the rapid increase in the instances of phishing, where one's safety is put at stake.

II. Concept and Development of Cyber Phishing

According to Oxford Dictionary which has recently added the meaning of cyber fishing to its latest publication that *"he fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online".*

The schemas of Cyber Phishing during different periods are as follows:

i. The first case has been witnessed when a user receives misleading email which seems to be sent from a genuine authorized source, such as a business partner, containing an explicit request to verify the account information with a web service, without which user's account will be suspended.

ii. In another situation, it has been witnessed that users are encouraged to visit malicious websites whether through advertisements or sometimes the user visit the website by himself. When a user visits the fake website, malicious software gets automatically downloaded to his computer. Typically, the malware records the credentials used by the users to access to target services such as banking, sending them to the command and control servers managed by the attackers.

iii. Sometimes the user also receive links in form of messages from pretentious charitable institutions for donations for e.g., it has recently seen in Delhi when a fake facebook page claiming to be page of Dalai Lama asked Buddhists to donate in order to extend the help to the needy people during lockdown.

iv. One of the landmark cases has been seen in India (Jamtara Case) form of Vishing (Voice Phishing) which uses fake caller ID data to trick the user about the real origin of the call, when the users receive a phone call which claims to be from legitimate organizations such as banks or private organizations which asks the user to dial a certain number in because of problems with his bank accounts or sometimes offering services. When the user dials the certain number he/she is requested to enter his account number or other personal account credentials. The attacker hence, by this method of Vishing steals the money from the user's bank account.

From the above mentioned points, one can draw an inference that phishing is not merely restricted to the email-phishing but it also includes within its ambit various others forms of phishing i.e. from Whaling to Vishing and from Angler phishing to spear phishing which marks some of the major phishing threats to the people at large

III. Cyber Phishing during the time of Corona virus

According to a report by Barracuda Sentinel, the number of Phishing related activities have been spiked up by 667% during the time of COVID-19.[2] A variety of phishing campaigns are taking advantage of the delicate focus on COVID-19 to distribute malware, steal credentials, and scam users out of money. As per the report, in only 22 days, i.e. between March 1 and March 23, researchers have detected 467,825 spear phishing email attacks, and 9,116 of those detections were related to COVID-19, which is about 2 per cent of attacks. Although, the percentage of attacks is still low, but it growing at a very fast pace during the time of Coronavirus Disease in all over the world, which is quite alarming for the cyber security authorities in order to maintain peace and keep the people safe from tech attacks.

The Cyber Phishing Campaigns usually send attractive invitations to the people. A month before, there was a trend when people were receiving mails stated as "Click this link and get a free subscription of Netflix". All they had to do is click the link and fill out their personal information and forward the message to other people. That mail turned out to be a scam capable of stealing their information. During the COVID 19 times, it has been reportedly seen that phishing emails and links claiming to be from UN, WHO, ICMR, or from corporate are potential to steal the information of the people.

According to the Director of Quick Heal Security Labs, the emails are generally lucrative so people follow them and for theft of information, the *modus operandi* is simple. Either a malware is dropped on to the device via links and attachments in the mails or ransom ware is circulated as part of a mobile app. The malware can enter in the user's device's security system and can steal up the persons entire private credentials even his or hers bank account details.

During the time of COVID-19, another trend has been witnessed, in quest to extend the help to the poor people affected from lockdown, the users click on a link which says that one could offer help of donations simply by clicking the following link. Recently, on May 24th, 2020, a similar incident has been reported with the cyber cell, Delhi Police when a South Delhi based Real Estate Consultant donated money to the poor via a link and later did not receive any notification and got to know that the website was a scam and could be a potential phishing campaign.

Another trend for Cyber Phishing has been come up in the light when a report published by India's cyber security agency CERT-In stating that phishing attacks in the name of *Aarogya Setu* the Indian COVID-19 tracking mobile application have witnessed a "high rise" as online phishers are taking advantage of the increased inquisitiveness of internet users during the COVID-19 pandemic.

Along with phishing emails, some other new cyber cons are overtaking the pandemic. In a case to Delhi Police Crime Branch, a fake facebook page of Dalai Lama was created by another cyber phishers sent fake messages to Buddhists asking them to donate money in the light of the Coronavirus.

IV. Legal Aspects

The laws for cyber crime protect citizens from dispensing sensitive information to a stranger online. The IT Act was introduced in 2000 which extent to whole of India in order to implement proper cyber laws in the country. It was further amended in 2008 covering various kinds of cyber crimes in India along with the punishments for them.

Sec 66, IT Act: This section penalizes identity theft. It says a person who performs identity theft will be subjected to an imprisonment which may extend to a period of three years and even fine which may extend to Rs. 1 lakh.

Moreover, Section 66 D talks about cheating through personation by the use of computer devices and resources.

Legal aspects can be assessed with the help of the following landmark illustrations and case laws:

(A) National Association of Software and Service Companies v. Ajay Sood & Others[3]

In this case Cyber Phishing was declared as an illegal act by the Delhi High Court, the high court also explained the concept of phishing and wherein a person pretending to be a legitimate person extracts and misuses the personal data of an individual for his own *Mala fide* intentions.

(B) The infamous RBI phishing scam

There was an email which in the an email was circulated impersonating of RBI which rendered a promised to its recipient a Rs. 10 lakh as prize money, and for that a link was provided which looked similar to that of RBI, seeking various personal information of the users such as the numbers of their savings account, passwords, etc. Later RBI posted a notification on its official website regarding this fraud.[4]

(C) ICC World Cup, 2011

The attackers made a similar looking website like that the organizers of the World Cup and tempted the victims by showcasing ample offers. For this purpose, the credit card details along with other personal details of the victim was asked by the attackers which would have resulted in the access of the Internet banking of the victim and ultimately would have caused losses to him.[5]

(D) Vishing Con Artists of Jamtara

Located in the Santhal Pargana region, Jamtara, which was demarcated as a district in April 2001, has been an epicenter to India's vishing activities. The town has many teenagers and youths who consider their profession as vishing con artists. As per the records, between April 2015 and March 2017, police teams from 12 different States have visited the station 23 times and arrested around 38 accused. More than 80 cases have been registered against 330 residents of the area *suo motu* by the Jamtara district police between July 2014 and July 2017. At Karmatar police station alone, the number of arrests in relation to vishing in 2017 has crossed 100[6].

V. Measures to curb Cyber Phishing

During these times, especially when the cyber phishing is on rise the below and numerated steps which could be instrumental for safeguarding the prospective victims of cyber crime:

1. Awareness is the biggest factor to curb the phishing attacks as the more people are aware regarding these predators, the more secure they will be from phishing. Training the people at large with an aid of carrying out various awareness campaigns, advertising, hoardings, etc

2. Safety at individual level also reduces the risk of falling prey to cyber phishing. Filtrating the emails and links and verifying them before clicking and accessing them as it can bring on board the risk of cyber phishing. Checking the source of emails and if one finds any suspicious or fabricated mail, then one should directly contact the service provider who is being impersonated through these mail. One should enter their sensitive personal data only on trusted websites.
3. Avoiding the use of public networks as they increase the risk of cyber phishing and even while using such websites one should check appropriately the security of these websites and one must avoid clicking the various pop ups that come across the websites.
4. One should keep the browser up to date and even the personal computers should be made secure and the bank accounts must be reviewed periodically.
5. The usage of latest and appropriate antivirus softwares and refraining from feeding the data on any suspicious online platforms can help in providing safety from becoming victim to cyber phishing.

VI. CONCLUSION

Advancement of technology is a boon to the making but at the same time it has gradually increased the risk associated with it more proactive. On the other hand, Covid-19 has proved out to be like a double-edged sword, which has not only brought along its way disparity to the people at large but also has made lives of people miserable by drastic increase in cyber crimes and one such crime is cyber phishing. The lockdown imposed all over India has proved out to be a golden opportunity to the potential attackers to manipulate and make the use of such a situation for fulfilling the best of their mala fide intentions. When most of the people around the globe have mostly their data online it is at that time when the real threat of cyber fishing comes into picture and the need of the hour is adequate and efficient security measures to ensure the risk is reduced to minimal. Security in the bigger pictures, possess a potential to transcend the technology and however, for ensuring a better pace and harmonious growth of technology without causing any unfavorable impacts on the society at large, it is must that both technology and security go hand in hand.

*****

VII. References

[1] Shilpa Yadav et al., CYBER CRIME AND SECURITY, 4, *IJSER, 855, 856 (2013)*

2 *COVID-19-related phishing attacks up by 667%: Report*, THE ECONOMIC TIMES, (March 27, 2020, 08:38 IST),https://ciso.economictimes.indiatimes.com/news/covid-19-related-phishing-attacks-up-by-667-report/74839322

[3] National Association of Software and Service Companies v. Ajay Sood & Others, 119 (2005) DLT 596

[4] *How RBI spreads awareness about fictitious offers, reporting frauds,* THE ECONOMIC TIMES (Aug 30, 2018, 12.13 PM IST), https://www.google.co.in/amp/s/m.economictimes.com/wealth/personal-finance-news/how-rbi-spreads-awareness-about-fictitious-offers-reporting-frauds/amp_articleshow/65604505.cms

5 David Bisson, *Phishing Scams Target World Cup Fans — Here's What to Do,* SECURITYINTELLIGENCE, (June 22, 2018, 9:15 AM), https://securityintelligence.com/news/phishing-scams-target-world-cup-fans-heres-what-to-do/

6 Shiv Sahay Singh, *The cyber con 'artists' of Jharkhand's Jamtara district*, THE HINDU, (OCTOBER 26, 2017 20:07 IST), https://www.thehindu.com/news/national/other-states/the-cyber-con-artists-of-jamtara/article19476173.ece

*****