VOLUME 24 ISSN 2456-9704

PHISHING ATTEMPTS IN CYBER CRIME

By Urvasi Bhoopal
From Amity Law School, Noida

ABSTRACT

With the advent of technology, the human workings and habits around the world are seeking tremendous transformation and positive growth. The adaptation of technological advancement has really created the definition of human efficiency to become profit centres around the world. But much like most other evils associated with all great inventions, even technology has its own downsides. The world is woefully connected these days using the common means such as the means of internet. The internet-based connectivity comes bearing its own risks. In this project I would be taking up the research work and due diligence work that is required to understand the most common practice of a new form of problem as well as crime i.e. the cyber based crimes.

Internet with its inception in times around 1995 has seen a tremendous growth in one and all sectors. From using the connective net in the military operations to advancing it for the commercial use has been nothing short of a rapid induction of charged pace. Some important facts about the growth can be that in 2000 there were about 400 million internet users world wide that included the personal, corporate and military uses. This number is accountable for most of the capacities around the world when the computers were bulky and phone connection was out of question. Now currently there are over 4.75 billion internet users in all capacities.

As there is an increase in the attractiveness in the fields due to the avid usage of the private networks there has been an increase in the fraudulent activities regarding the usage of connected networks and private networks. Consequently, the online crimes have been given the name of cybercrimes and there are various different methods and analogies related to how the art of cybercrimes have increased and similarly what has been done to counter the same in short, medium and long run.

In this project the main focus would be upon the establishment of understanding of cybercrimes and the use of phishing attempts in cybercrimes. This is a broad topic so it would be fair to divide and discuss about the advent of cybercrimes in general the move on to the specific fields in cyber-crimes i.e. the phishing attempts in the industry and private networks. Followed to this some landmark cases and judgements regarding the cybercrimes and phishing in general and would be examined.

1. INTRODUCTION

Before starting the exploration of the cybercrimes but firstly it would be important to look at some important statistics about the usage of internet as a whole.

(a) Internet Usage Patterns

Fig-1 illustrates the growth in the number of users from the year 2005-2019 which is a tentative but mostly audited dataset. The numbers about the statistics behind the internet usage explains that in 2000 there were about 400 million internet users worldwide that included the personal, corporate and military uses. This number is accountable for most of the capacities around

the world when the computers were bulky and phone connection was out of question.

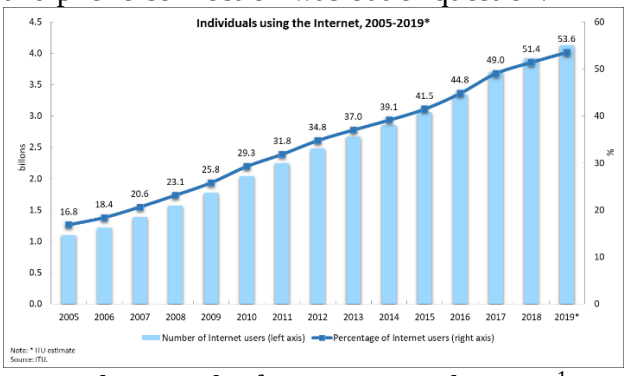

Fig-1 The growth of internet over the years[1]

Looking at the numbers and figures it can be concluded that the increase in the usage of internet has gained traction around the year the 2006- 2012 which covered the usage of the internet by heavy masses.

(b) Cyber crimes

A cybercrime can be termed as a fraudulent and immoral behaviour of a which can be termed a crime. In this crime a computer is the object of crime or a tool which is predominantly required as well as is used as a specified tool or vehicle of offense to commit an online crime. A cybercrime is committed by a cybercriminal and this criminal can or may use a device to access other persons' user information, personal private and official credentials, government infographics, or may even disable a device without having the authority to do so. In certain cases, the crime is to sell and buy or exploit the given user information online.

Online or Cyber based crimes can be further subdivided in two of the major categories:

Crime targeting networks and device	Crime with intention to criminal activity
Virus	Phishing Email
Malwares	Cyber stalking
DoS Attacks	Theft of Identity

The category of Cyber-crime would include the cybercrime falling into three broad categories which are individual, government and property of both personal and private capacities.

1) Property: This is like criminal and illegal possession of a persons' bank and credit card details. The cybercriminal steals victims' details and gain access to funds, do the further and illegal transactions online or run phishing scams to divulge the greater part of the user's information. Usages of a malicious software and viruses is common in this segment.
2) Institutional or Govt.: This is the less common one, and is the gravest of the all offense. An attack on the govt is mostly called CT i.e. cyber terrorism. Govt cyber-crime consist of gaining access to govt sites, military sites or spreading the hateful propagandas. The offenders are normally known as terrorists or nemesis of the governments of other nations.
3) Personal and private (Individual): In this from of cyber-crime involve one or more than one individual spreading malicious or illegality based online info online. The concurrent situation can consist of cyber

[1] https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

based stalking, child or general pornography and human and child trafficking.

(c) Types of Cyber-crimes[6]:

Identity Theft – The cyber offense generally happens when a cybercriminal gets access of a person's private info and theft of funds, gets the confidential info, and various other frauds. Criminals searches the person's passwords by hacking, social engineering, and by sending phishing emails.

Cyberstalking- The cyber offense generally happens when a cybercriminal subjects a victim to a huge number of messages & mails. Mostly most of the stalkers exploits the social media to intimidate victim & impart fear.

PUPs - These are called Potentially Unwanted Programs and these are in a sense less intimidating than most of the other online crimes and are a form of malware. They work by uninstalling a lot of unnecessary software in your system.

Banned or Illegal Content - The cyber offense generally happens when a cybercriminal shares or distributes not appropriate forms of e-content which is considered to be highly disturbing and offending. Disturbing contents precludes, pornography between adults, images or moving images of violence & images with criminal intent. The content consists of materials containing terrorism & child porno and exploitation. The content is on the net & on the dark web.

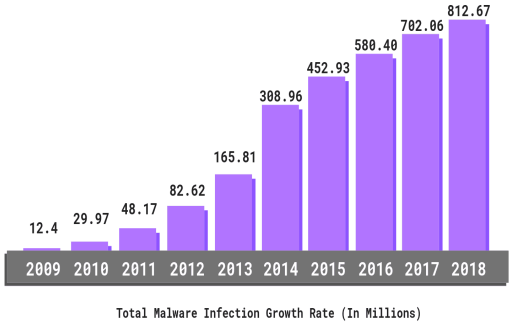

Fig-2 Growth of malware injections across all networks in the world[2]

Online Scams- The cyber offense generally happens when a cybercriminal pushes adverts or spam mails including rewards & unrealistic propositions which can be termed "too good to be true".

DDoS Attacks – DDoS attacks are mostly used to create a web-based service temporarily unavailable & push the network into downtime by blasting the website by traffic using various resources. Larger network of affected machines also called as Botnets are formed by pushing various malwares on user's machines. The cybercriminal then gain access to the system when the networks are down.

Botnets - Botnets are formed when networks of the compromised machines are controlled with external usage remotely by hackers. The remotely located hacker sends spammed and/or attacking or corrupting malware to other machines by these botnets. Botnets are also used as malware attacks & for performing malice and illegal tasks.

Social Engineering - The cyber offense generally happens when a cybercriminal makes contact with victim usually via phones

[2] https://www.av-test.org/en/statistics/malware/

or mail. Attacker wants to gain victim's confidence & poses as a consumer servicing agent and hence you give your necessary info. Typically, passwords, company's name, & bank info is divulged. Cyber-criminal finds about the info they can get about you using the social media or general-purpose internet. Once they gain that information then they can sell this info on the internet or even can scam or dupe the victim further. The growing use of the internet is also a propellent in helping the social engineering scammers to dupe the targets.

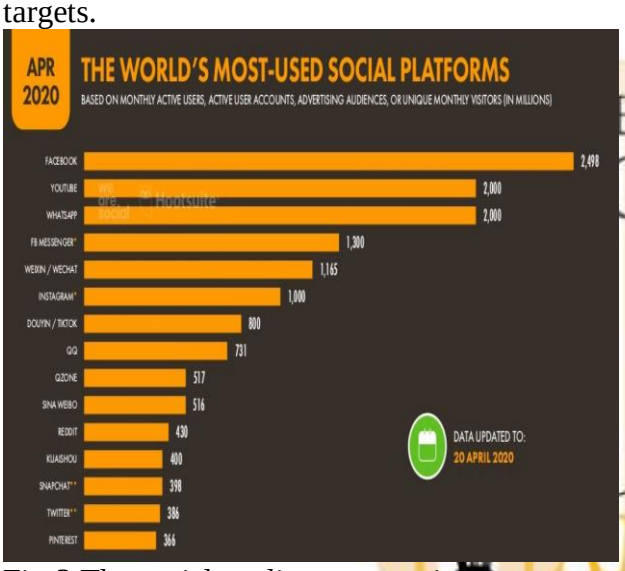

Fig-3 The social media usage statistics

Phishing- The cyber offense generally happens when a cybercriminal pushes malicious mails and attachments or User request links to individuals to get control of their accounts or machines. Online cyber offenders are getting more and more focused & most of the mails aren't flagged as spam-mails. The individuals are scammed in mails asserting the need to change pass-word or update billing info, and in the process providing the cybercriminal access.

Dark Web operations- In this from of cyber-crime involve one or more than one individual spreading malicious or illegality based online info online. The concurrent situation can consist of cyber based stalking, child or general pornography and human and child trafficking.

(d) Behavioural aspect behind cybercrimes

The reason behind the rapid growth of the cybercrimes over the years has been the behaviour of the users that has presented itself as a risky measure. This would mean that the behaviour of the users and the stats behind it has actually been one of the behavioural reasons for the growth of online scamming and cyberattacks. Cyber-criminal finds about the info they can get about you using the social media or general-purpose internet. Once they gain that information then they can sell this info on the internet or even can scam or dupe the victim further. The nature of the same explains that people sitting in the SMEs or small to medium scale enterprises are extremely vulnerable too. This increases the cost to increase the security to the system and the human interaction to the same makes it even more complex to control. The outcome is simple that people, organisations and governments across the world have to suffer huge monetary and otherwise losses in these fields and to combat the same extremely costly systems are to be put in the place. These are some causes behind the surge of online cybercrimes. Some key overviews are:

1) There are about 4.57 billion plus users of the internet around the world.
2) On an average this number accounts to about 60% of the global population.
3) Annual CAGR or compound annual growth rate is about 7% per annum.

4) On an average the adults spend about 7 hours online on the internet.

(e) Legal Aspect of Phishing:

The legal view was initially not defined in the legal framework which could prevent or even challenge the legality of phishing as fraud till the year 2005. The act of phishing is relatively new and neither the companies nor the legal framework is robust enough to tackle such problems. In the year 2003 the Anti-Phishing Working Group was formed in the city of San Francisco. This was the first major attempt at the global level that recognised the act of phishing and gave a proper definition to it. This organisation was formed, by Tumbleweed communications, financial institutions and e-commerce providers, with an intent to give visibility on the act of phishing to the global lawmakers to cite. The definition according to the organisation for the legal purview is "the act of phishing is a fraud and an act of online identity theft which employs the use of social engineering and technical prowess to dupe and steal the personal identity and financial accounts credentials of consumers.

In the year 2009 Indian Computer Emergency Response Team (CERT-In), Department of Information Technology which reports to the Ministry of Communications & Information Technology of the government of India, reported that CERT-in handled about 374 phishing incidents and still there was no robust way of attacking and coercing the criminals behind it.

There have been multiple phishing attempts in the past over the banks such as ICICI bank, HDFC bank, SBI bank etc. since the years 2000. All the usually had same modus operandi where the customers were sent mails which reflected that the mail was from the original source i.e. their bank, the recipients received the mails which contained some percentage of data that looked legit and there were sent under false pretences. The intent in all the cases were to acquire the bank account details and information like CVV, or passcodes.

The act primarily attracts penal provisions under the IT act of 2000 under sections like Section 66, Section 66A, Section 66C and section 66D with provisions to penalise the culprit in the form of penalties and possible prison term. This however must be noted that it still remains a bailable offense under Section 77B of the Information Technology Act 2000[3].

2. LITEREATURE REVIEW

Taking the Bait: A Systems Analysis of Phishing Attacks authored by Lacey, David & Salmon, Paul & Glancy, Patrick. (2015).[4] Review – The author starts by explaining the true form and activity behaviour of phishing as a tactic to gain the target or victims computer access. It is explained that this cyber offense generally happens when a cybercriminal pushes malicious mails and attachments or User request links to individuals to get control of their accounts or machines. Online cyber offenders are getting more and more focused & most of the mails

[3] https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf

[4] Nurse, Jason. (2018). Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. 10.1093/oxfordhb/9780198812746.013.35

aren't flagged as spam-mails. The individuals are scammed in mails asserting the need to change pass-word or update billing info, and in the process providing the cybercriminal access.[3]

Further he describes the true mechanism behind the concept of phishing. The author here develops a framework that authorizes many or a single victim attack with a sole intention of fraudulent or monetary assault on the victim.

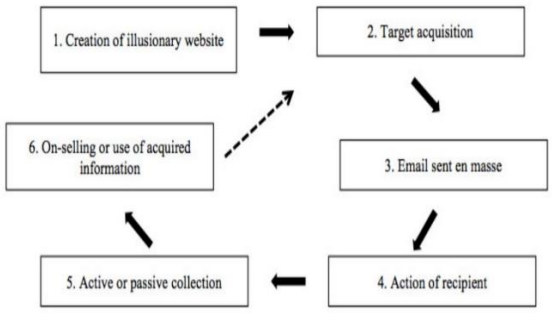

Fig-5 Typical framework of phishing attack

The framework of the phishing attack is described in the above picture. It usually starts with the creation of illusionary website that is usually required as a bait to the victim. These websites are generally acquired by snooping through the cookies of the users. Then this results in target acquisition and consequently now moves to the further step. The next step in the process would generally be a sending of a generic email to the victim as a bait. When the victim receives it, the action decides the passage of the further phishing attack. Depending on a few variable tactics this would generally result in a full-blown attack on the victim.

The user database of the attacker or the cybercriminal would decide whether the attack is of active nature or passive in nature. The further steps can be varied by attacker to attacker on the intensity of the attack and the type of attack. In certain areas the information of the user would be sold on the dark web, in the other scenarios if possible then the information relating to the financial transactions of the victim will be gathered. This is a privileged information and hence this would lead to the generation of substantial amount of money if the cards are played right. The author further explains that the attack would not generally stop at this point. What would happen further would be decided by the nature of the attack. In some powerful cases as seen in Indian or Chinese attack[2] the attacker would further resort to social engineering to further lead it to a scam. The scam bait would be elaborate in nature, He explains that in the year 2016 the amount of a call-based software glitch scam was about 220 million dollars in USA alone. This scam was elaborate and the attacker used social engineering to a good use to solicit large number of sums from the victims.

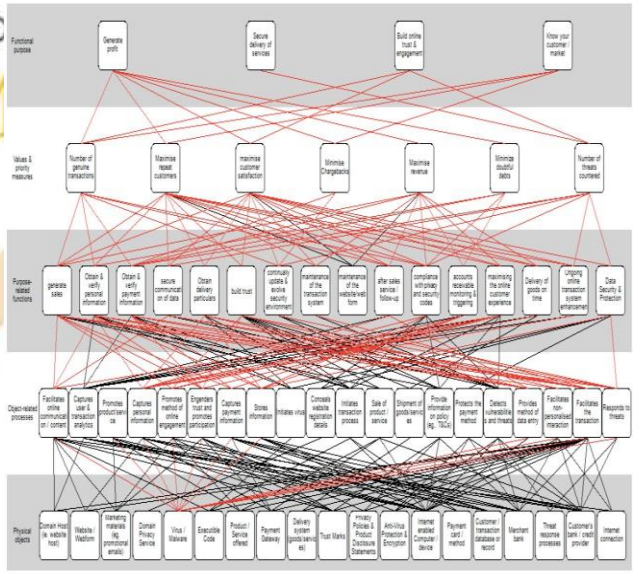

Fig-6 WDA for phishing attacks on Transactions processing systems[7]

The researchers are very distinct in its procedural method of WDA[2] or Work Domain Analysis to get understandings of structures of phishing attack & online monetary platforms as targeted in a socio-technical systemic nature. Examining the functional aspects of WDA within context, the work provides distinct perspective of phishing & interlinkage & dependencies in many levels of abstractions starting in 'baiting' all the way to achievement of overall objectives by cyber-criminals. Findings provide chances to improve preventions & detections methods & improves sole resilience to them attack, also to make way for future efforts.

Legal Court Cases in India which gave shape to the legal framework against Phishing as a cybercrime.

NASSCOM vs. Ajay Sood & Others[5] –
This is the landmark case and its judgment in the specific case of National Association of Software and Service Companies vs. Ajay Sood & Others. The judgement was delivered in the month of March of the year 2005. Delhi High Court after due diligence and by citing this landmark case declared 'phishing' an illegal act and to do phishing as crime for which the culprit may be liable to pay damages.

The court after due diligence stated that the act of phishing of the internet is a fraud, the court further explains that in this process the person acts to be a legitimate association of the victim, like the victim's bank or the insurance company etc. to get the victim to divulge personal data such as access codes, passwords, etc. The collection of the personal so collected by misrepresentation of identity is used for the scamming party's gain.

The court stated, through an example, phishing scams are generally used by scammers by misrepresenting or by giving false representation of the legitimate identity to dupe the victim out of cash.

Delhi High Court stated that, there is no particular legislation in India penal code to penalize phishing. The Delhi HC upheld phishing as an illegal act the plaintiff, in the given case, was the National Association of Software and Service Companies (NASSCOM), which is one of India's premier software organisation. The defendants were in association with the placement company which was involved in the business of professional recruitment. For obtaining the private and personal data, which they used for their business, the defendants used to send emails to third parties, falsely representing them as NASSCOM.

The Delhi high court recognised that the use of the name of the plaintiff's domain was wrong as the plaintiff had exclusive rights to use their email as well as domain names. The deceptive and false representation by the company as NASSCOM was fraud and illegal.

Two hard disks were recovered on the court's order for searching the defendant's premise, these were used to send fraudulent e-mails to various parties. These were sealed by the local commissioner. The emails were then presented as evidence in court.

The defendants finally admitted to the illegality of their acts & the parties settled the

[5] 119 (2005) DLT 596, 2005 (30) PTC 437 Del

matter through compromise. The terms of compromise were that the defendant would agree to pay Rs1.6 million as damages to plaintiff for violation of trademark rights. This case is termed as a milestone in bringing the act of "phishing" in front of the eyes of law, the court stated about the legality of the misrepresentation as being the legitimate party that knows the victim to be an act of fraud and termed as illegal. This would attract the guilty to pay damages and a possible jail term.

(A) RBI Phishing Scam[6]: Being one of its kind and extremely daring in nature, the scammers attacked the Reserve Bank of India. The phishing mail was disguised smartly like it was from the Reserve Bank of India, the email announced the recipient has won Rs.10 Lakhs. This amount was to be redeemed within 48 hours. The link seemed to be from the official website of Reserve bank of India which had the same logo and identical looking website address. The recipient was asked to reply with information such as his password, CVV number and bank account number. Reserve Bank of India responded by posting a warning regarding this fraudulent venture by the fraudsters.

(B) Google Phishing Attempt[7]: The users of the Google's Gmail service received a fake legal notice from a spoofed Gmail team which wanted the users of the actual Gmail service to service their account's names, passwords, occupations, and residing country with a warning that the users who who might fail to do so within 7 days would lose account permanently. The Google India head denied any such legal notice and pronounced it to be a 'spoof' or 'password phishing'.

3. OBJECTIVES

The objective of the project which is to understand the phishing attempts in cyber crime can be manifold but the key aspects are given blow:

(a) To understand what are cyber crime and what are phishing attacks in cybercrime.
(b) To understand and assess the losses and damages pertaining to phishing attacks in cybercrimes.
(c) To understand the legal frameworks for the phishing attacks in India and rest of the world.
(d) To understand what can be done to safeguard against phishing attacks.

4. RESEARCH METHODOLOGY

In this project I will conduct in-depth qualitative exploratory research using the secondary data. I have reviewed various research papers and presented the findings. The secondary data will be in the form of research papers, online articles and textbooks. Through the deep analysis we will find out the increasing dependencies of phishing attempts in the cybercrimes and will understand the workings behind it. For the data collection the online databases such as EBSCO, ERIC, Research gate, Google Scholar and SAGE were used. Further the collected data was used for the assessment by using the appropriate frameworks and analysis tools as taught in the class.

[6] https://www.timesnownews.com/business-economy/economy/article/beware-of-this-fake-rbi-lottery-email-in-circulation/304488

[7] https://indianexpress.com/article/india/google-nearly-500-users-in-india-warned-of-govt-backed-phishing-attacks-in-3-months-6140270/

5. ANALYSIS

The analysis of the content would be set in a deep learning tone with the facts being presented would explain the nature and framework of the phishing attack industry and would explain with the use of statistics that what are the overall value of damages that are sought by the world due to these sort of cyberattacks. The cyberattacks in some countries have been termed as cyber terrorists and which kills the SMEs which are small to medium scale enterprises. Some key findings with the analysis are:

- ❖ Methods by which the phishing attacks are marked:

1) Spam Email [3] – Here, a fake email from a look alike correspondent or from a true institution is sent to the victim.
2) Hostile profiling- It is a more specialized version of the above method where a targeted mail or attack is sent to the victim by using the victims tracking history and usage practices or by social engineering.
3) Install a Trojan [3] – This is done by sending a package sometimes with the useful packages and consequently killing the victim's computer.
4) 'Spear phishing' – It is an attack on a wider organisation with target to gain access to one computer so that access could be gained further to organisations all computers.

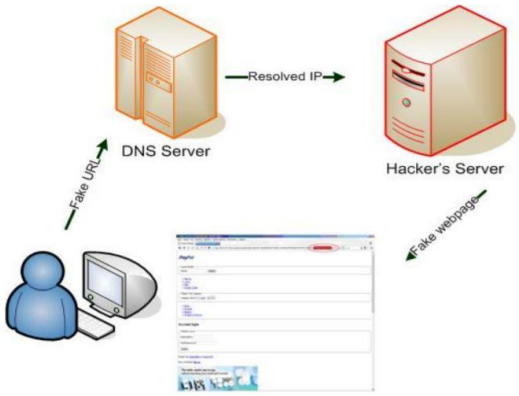

Fig-7 Process of phishing attempt

There were some famous cases which gave the act of 'Phishing attempts' the spotlight and most of them explained that the act of phishing is a fraud which employs social engineering to a very large extent. This have all the characteristics of a typical fraud except that it is employed through a virtual website. The court through its proceedings and judgements emphasizes the use of secure IP networks [2]. The legal system emphasizes the use of very secure networks so that it makes the process of phishing or mimicking a digital signature very difficult.

- ❖ **Legal framework for Phishing based cybercrimes**:

Indian Legal framework-

Phishing attempts and the jurisdictions to their legality is listed in the provisions of the Information technology act of 2000 under various articles.

1) Section 66 – The or the ID of the victim will be considered compromised until the phisher makes changes through deletion, modification or alteration of data electronically stored on the machine.
2) Section 66A - A disguised mail which contains fake weblink of an organization with intent to deceive the recipient about origins

of the mail is punishable under the provisions of section 66 IT act 2000.

3) Section 66C: In the mail if the phisher disguise him/her as genuine banker & use uniquely identified features of the organization like trademark, Logo etc attracts punishment under the provisions of section 66 IT act 2000.
4) **Corrective Action**[8] under section 66c of the IT act the person with proven malicious attack and intent can be prosecuted for phishing attack and if proven guilty then the provision for correction and the person is punishable by imprisonment up to 3 years and liable to pay a fine or Rs. One lac.

In the United States of America framework for the Anti-phishing Act of 2005[9] – Amendment to the Federal criminal code to criminalize Internet scams involving phishing attempts and attacks and fraudulently obtaining personal information. Hence under 18 U.S.C. Section 1028, phishing attacks are punishable by fine or imprisonment for up to five years, or both, if proven the intent was to provide harm to the party or the victim.

6. CONCLUSIONS

The research on this topic gives extreme insights about the behaviour of the internet users around the world and vulnerabilities that are associated to them. The assessment explains that not only people on individual levels are affected, people in multinational conglomerates are affected too. The nature of the same explains that people sitting in the SMEs[2] or small to medium scale enterprises are extremely vulnerable too. This increases the cost to increase the security to the system and the human interaction to the same makes it even more complex to control. The outcome is simple that people, organisations and governments across the world have to suffer huge monetary and otherwise losses in these fields and to combat the same extremely costly systems are to be put in the place. This reduces the scalability and flexibility of the companies.

The methods of these attacks are getting sophisticated day by day and general method would go by attacking in manner such as phishing attack being started with the creation of illusionary website that is usually required as a bait to the victim. These websites are generally acquired by snooping through the cookies of the users. Then this results in target acquisition and consequently through further steps this would lead to a full-blown identity theft. Certain measures are being taken up in the world to combat and make these attacks punishable by law. Certain specified rules that target the phishing attempts are varied in nature throughout the world but attacks the core premise of the attack by segmenting it by the glasses of identity theft, unidentified and unlawful forced access to someone's machine or scamming under false pretences to gain access or dupe financially.

The Indian legal response in the favour of corrective and coercive action in response to phishing attempts is strong and effective. The measures seem to be appropriately balanced and now i.e. in 2020 have enough previous cases to cite and deal with more peculiar cases of phishing. The fraud or cybercrime that is phishing is punishable under the IT act

[8] https://indiankanoon.org/doc/326206

[9] https://www.congress.gov/bill/109th-congress/senate-bill/472

of 2000 under sections like Section 66, Section 66A, Section 66C and section 66D with provisions to penalise the culprit in the form of penalties and possible prison term. This however must be noted that it still remains a bailable offense under Section 77B of the Information Technology Act 2000.

Possible changes/corrections that can be made in the current legal framework:

1) **IP based crimes** – As the technology is advancing the crimes have become more sophisticated in nature. The use of IP bouncing is quite prevalent. The fraudster bounces the IP addresses using multiple servers across the globe, since this is so common in the usage the bouncing of IP addresses itself should be made punishable. Hence by correcting this more and more phishing scammers can come under the radar.
2) **Non-Obstante clause**[10] – The IT act of 2000 makes the punishing and corrective provisions under the Chapter 11, the section 81 of the of the IT act 2000 has a non obstante clause. This non-obstante clause gives an overriding effect on It act and IPC and the phishing scams are made bailable under section 77B of the IT act. When this is made bailable the culprit who is actually technologically smart may try to destroy evidences against him by getting an online connection. Since the world is much more connected than it was when the act came in to effect, the bailable nature can potentially lead the culprit to get away by using active internet connection.

Certain measures that can help safeguard and prevent phishing attacks are:
For a company:

- Creating such corporate policies that for the use of Emails' content which is so unique and hence the legitimate mails can't be confused with phishing.[5]
- By Providing a correct way & a much stronger authentication process at the sites for the end customer, so that he/she can separate the legitimate email from the phishing mails. [5]
- By creating stronger email facilities which can check and flag the phishing and spam mails correctly. [2]
- By Monitoring the net for potential harmful sites & implementing better quality anti-virus solutions to block known phishing mails at the gateway. [5]

For a consumer:

- Automatic blocking of emails by the use of spam detectors and phishing mail blockers.
- Automatically detection & deletion of malicious software by having any specialized third party specific trusted anti-virus solution. [5]
- Finally, by educating the end customers about the potential phishing traps and general cyber health review for everyone should be implemented. This is perhaps one of the most powerful things to do because all the stakeholders are made aware about the practical problems.

7. REFERENCES

❖ Nurse, Jason. (2018). Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. 10.1093/oxfordhb/9780198812746.013.35.[1][3]

[10] https://www.itlaw.in/section-77b-offences-with-three-years-imprisonment-to-be-cognizable/

- Vayansky, Ike & Kumar, Sathish. (2018). Phishing – challenges and solutions. Computer Fraud & Security. 2018. 15-20. 10.1016/S1361-3723(18)30007-1. [5]

- Lacey, David & Salmon, Paul & Glancy, Patrick. (2015). Taking the Bait: A Systems Analysis of Phishing Attacks. Procedia Manufacturing. 3. 1109-1116. 10.1016/j.promfg.2015.07.185.[2]

- Harriman, D. D.: Password Fishing on Public Terminals. Computer Fraud and Security Bulletin, Elsevier Science Publishers, New York, Jan.1990, pp. 12–14.[6]

- Anti-Phishing Working Group, Origins of the Word Phishing, Retrieved April 1 2015. URL: http://docs.apwg.org/word_phish.html. [7]

*****