VOLUME 3 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

VICTIMIZATION OF THE INDIANS THROUGH THE LENS OF PHISHING: A CASE STUDY BASED IN KOLKATA

- Soumya Roop Mukherjee & Sagar Dutta[1]

I. ABSTRACT

In the information age, the flow of information has been very fluid. One of the main vantage points of the information age has been the relative fluidity in the area of communication. However, it has also led to a rise in the misuse of information as well. One of the most prevalent misuses of information has been in the form of cybercrime. Cybercrime in very simple terms can be defined as a crime involving computers and networking. One of the most prominent forms of cybercrime has been the use of phishing to take advantage of the technology-illiterate section of society. Phishing as a crime is generally used in the process of grabbing/snatching personal data. The research paper will look into some of the most prominent phishing activities based in Kolkata. Thepaper will analyze the existing Indian laws like how the specific provisions of The Information Technology Act of 2000 deals with the crimes related to phishing and find out the scope of required amendments in the existing laws. Through the research, the paper will try to delve into the lack of awareness and the everyday victimization of the citizens due to phishing. The research looks to establish the intricate correlation between the cyber laws and the victimization of the citizens within the society.

[1]Pursuing Masters in Mass Communication from St. Xavier's University & Pursuing B.Com LL.B (Hons.) from St. Xavier's University

KEYWORDs: "Phishing", "Victimization", "Information Technology Act,2000", "Focused Interviews", "Cyber Law", "Cybercrime"

II. HISTORY OF PHISHING

In the early to mid-1990s, paying for "dial-up" access to the Internet was the only option. A thirty-day free trial to access the Internet using an AOL floppy disc was available for people who didn't want to pay for Internet access. Some people discovered a technique to alter their screen names so that it appeared as though they were AOL administrators rather than deal with life without the Internet when the trial period ended. They would "phish" for log-in information using these fictitious screen names in order to keep receiving free Internet access[2]. Scammers modified these techniques when Internet usage became more widespread and used them to send emails to ISP customers pretending to be administrators in order to obtain user login information. After spoofing someone, the hacker had access to that person's account on the Internet and also had the ability to transmit spam from that person's email address. The stakes may not have altered, but the phishers' methods certainly have. The international economy is now at risk from phishing schemes rather than unrestricted Internet access. When a well-crafted phishing email may be just as successful at giving the hacker access to sensitive information, why spend the time and effort to get past a firewall?[3]

The growth of social media has been a significant development. As was previously said, there was little to no information on businesses and the people who worked for them on the Internet just ten years ago. Nearly everyone in every company has a LinkedIn, Facebook, or Twitter account these days; some people even have all three[4]. Even while they are important business tools, these social media platforms provide a veritable gold mine of personal data that fraudsters can and do use to tailor emails to particular recipients—a technique known as spear phishing. Consider the amount of data a criminal may discover about a business simply by using LinkedIn.

[2] *"THE WEAPONIZATION OF SOCIAL MEDIA: SPEAR PHISHING AND CYBERATTACKS ON DEMOCRACY"* - Michael Bossetta, Published by: Journal of International Affairs Editorial Board ,pp: 97-98
[3] ibid,P:99-100
[4] ibid,P: 101-102

The hacker can then use Facebook and Twitter to dive further into the personal lives of targets after using it as a starting point.[5]

An email with a relevant subject from a source that seems trustworthy or familiar puts the recipient at rest. The recipient will feel more authentic and at ease as a result of the personalized features, increasing the likelihood that they will interact with the links or files.

Criminals looking to gain access to sensitive data kept on the networks of big businesses and organizations have chosen spear phishing because of the risks involved and the low resources needed to carry out an assault. Three recent high-profile breaches that are thought to have started with an employee falling for spear phishing include Target, Home Depot, and Anthem.[6]

Although it would make sense that technological defenses would advance, the recent experience of phishing suggests that it is doubtful that technology will ever completely shield employees from spear phishing emails reaching their inboxes. Crowdsourcing phishing detection makes sense as a result since it enables the first line of defense to report assaults as soon as they occur. A noteworthy example is the fruit vendor who, in 2010, helped stop a terrorist attack in Times Square. In this case, a seller alerted authorities after observing that an automobile had been parked on a roadway in Times Square for a number of hours, an unusual occurrence in such a crowded place. It was discovered that the automobile had explosives[7]. The seller was the best individual to spot suspicious conduct despite the fact that a busy place like Times Square has expensive monitoring technology and a significant police presence. Users on a network frequently report odd emails, which is crucial information in preventing data breaches because users are frequently the first to receive assaults.

[5] Ibid,pp: 100-101

[6] "*Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*"-Jennifer Lynch ,Source: Berkeley Technology Law Journal , 2005, Vol. 20, No. 1, Annual Review of Law and Technology (2005), Published by: University of California, Berkeley, School of Law ,pp:260-261

[7] "*Phishing Evolves: Analyzing the Enduring Cybercrime"*- Adam Kavon Ghazi-Tehrani & Henry N. Pontell, published by: Routledge Taylor and Francis Group, pp: 316-317

III. ANALYZING THE CASE STUDIES-

Criminals utilize the Internet to engage in phishing, an automated kind of social engineering. Fraudulently get sensitive data from organizations and people, frequently by using misleading methods. Scanning reliable websites. High reward potential (for instance, via bank access). The simplicity of sending fake emails impersonating legitimate recipients (such as bank and credit card details). Lawful authority and the challenges law enforcement faces while chasing criminals responsible have caused an increase in phishing assaults recently. Typically, a phishing attack starts with an email sent to the victim that claims to be from a trusted organization, but actually from the scammer. The message's text com-regularly informs the user that a problem has to be fixed with their help right away. The victim is then directed to a spoofed website, which is a phony website created to look. The victim is prompted by a website to enter account details (such as username and pas-word) and may also ask for other sensitive information, like the victim's Social Security number, ATM PINs, bank account numbers, etc. This information is transmitted to the user's accounts and can then be accessed by the phisher using it. In order to understand cybercrime, ideas include social learning theory and self-Control theory and subcultural ideas are still considered to be offenders (Stalin's& Donner, 2018), targeted explaining techniques. to examine the reasons phishing exists, continues, and potential solutions. Situation-focused theory is more suited as a response to it. Routine activity is a situational theory of criminal potential developed by Cohen and Felson in 1979.enables the analysis of the effectiveness of both technology-focused (target hardening) and human-focused (competent guards) anti-phishing measures. This enables suggested policies testing interventions designed to lower victimization risk. Email is used in the vast majority (96%) of phishing efforts. In the past, these emails were sent to many people ineffectively and with little effort with the hope that even a small one would. Even with a 0.5% response rate, there would be hundreds of victims. extensive use of "spam" filters has rendered this brute-force approach increasingly useless and phishers are now using increasingly sophisticated methods. These consist of: Smishing, Vishing, Spear phishing, Whaling, and Business E-Mail Compromise BEC happens when a hacker sends an email to a worker at a lower level, often someone who poses as an employee of the

accounting or finance department but is actually the CEO of the business or a different executive, manager, or supervisor. These emails frequently seek to convince their target to transfer money to a fictitious account while taking advantage of the common inclination for workers to not challenge their superiors at work. SMS stands for "short messaging service," the industry standard, while "smishing" is short for "SMS phishing." uses of text messaging in the globe Smishing attacks use text messages from phones using SMS as the attack vector rather than emails, in part to get around SPAM filters and to enlist more prospective victims. Voice phishing, sometimes known as "vishing," is a type of phone scam that achieve the same results for identical purposes. As earlier "basic" bulk phishing has fallen out of favor, spear phishing has gained prominence; Unlike regular phishing emails, which are untargeted, a spear phishing attack make use of spam-like strategies in large-scale email campaigns, spear Phishing emails use numerous social engineering techniques to target specific persons within an organisation. Technical strategies to customize and personalize the emails for the recipients. For instance, they might employ subject lines that address subjects the recipients might find interesting and mislead them into reading the message and accessing any attached files. Whaling is a type of Instead, BEC might be seen as the "reverse" of spear phishing. Instead of sending messages to lower-level employees within a firm, the cybercriminal targets CEOs andCFOs. One of the first investigations into why people fall for scams was carried out by Dhamija et al. in 2006.They found that the majority of participants on phishing sites were duped by 90% of the most skilled sites, and for these end users, browser indications were unclear. Victims were unaware that websites might be easily replicated, leading to inaccurate evaluations of these websites' substance and design professional presentation. Downs et al. (2006) carried out a parallel investigation looking at phishing emails that reproduced the findings of the Dhamija et al. (2006) investigation, which found that Participants chose their reactions to stimuli using simple, frequently inaccurate heuristics. For instance, some participants believed that because the company already have their knowledge More recent studies investigate the connections among social networks, internet forums, and phishing and cybercriminal networks. For instance, according to research by Leaflet et al. (2016), social bonds are crucial to the emergence of certain diseases. The expansion of most networks that criminals who have access to forums can utilise. Thereis research on phishing outside the discipline of criminology, which concentrate on

education. to criminally exploit swiftly and easily and instruction. Arachchilage and Love conducted two tests to gauge the effectiveness of security consciousness These investigations revealed that after playing a game based on security best practices, participants' phishing avoidance behavior significantly improved.

Some more studies on phishing and Routine Activity theory, In the part about the applicability of Routine Activity Theory for digital studies on phishing that make use of RAT are scarce (Hutchings & Hayes, 2009;(2014) and (2015) Leukfeldt. (Leukfeldt, 2015) and Leukfeldt (2014) concentrate on appropriate aims and risk factors, in that order. According to Leukfeldt (2014), a person's history and financial victimization by phishing is not influenced by features, and having current antivirus. The role of software as a technological guardian is insignificant, and no single, an organized group has a higher risk of becoming a victim. The research reveals that Despite the potential benefit of target hardening, there are few chances for preventative initiatives.

directed at specific target audiences or risky online behaviors, situational crime prevention is difficult. Leukfeldt also contrasts the risk factors for victimization for two different types of phishing: high-tech phishing (using, for example, malicious software) and low-tech phishing (using, for example, emails and calls on the phone). The results indicate that groups must be the focus of situational crime prevention. In addition to the users themselves. Criminals are mostly drawn to well-known online locations, and it is the responsibility of the operators of these virtual spaces to safeguard their users from both high-tech and low-tech phishing victims consequently, there is now a definite gap in our understanding of the utility. This study aims to investigate the contribution of RAT to phishing prevention and control. There are currently no commonly used, technologically advanced, or human-centered methods to avoid being a phishing victim.

Many businesses often conduct phishing simulation campaigns that target their own employees in order to evaluate the success of their instruction. Those who fail the mock attempt receive further instruction and anecdotes. Proof of the temporary suspension of email access for repeat offenders. A few hackers jokingly suggested that target testing could be made better by including a shameful statement: "If Jerry were in accounting, this issue would resolve itself very quickly. “Each time he clicked on a false link, receivable was added to a list of public "Hall of Shame" users. It's interesting to note that studies on other white-collar offenses like embezzlement, highlights how offenders can be changed by public shame

The 2000 Love Bug- On May 4, 2000, a shift in strategy led to the Love Bug's global demise. Mailboxes all across the world were flooded with the message "ILOVEYOU," which first appeared in the Philippines. Simply verify the attached LOVELETTER from me, it mentioned in the message body. When those who couldn't help it opened what they thought was a harmless.txt file, they unintentionally released a worm that caused harm to the local computer. In addition to overwriting picture files, the worm transmitted copies of itself to each contact listed in the user's Outlook address book.

With a cleverly crafted virus that preyed on human psychology and technical flaws, malware could rack up vast numbers of victims, as demonstrated by the malware known as "LoveBug," which also demonstrated how to make spam send itself. About 45 million Windows PCs were estimated to have been affected overall.

The Symantec company discovered the "SowBug" cyber spying group. Investigators from the company discovered that the hackers, who appeared to be operating since 2015, conducts covert cyber-attacks on foreign policy institutions. Argentina, Brazil, Ecuador, Peru, and Uruguay have government bodies and diplomatic targets. Malaysia. The group infiltrates its targets using a malware called "Felismus."A sophisticated Remote Access Trojan (RAT) built in modules that allows attackers to gain access to the attacked system and communicate with remote servers, execute shell commands and download files.

According to Saudi security officials, the Kingdom has been under ongoing cyber spying attacks since February against five Middle Eastern countries, including Israel, and several countries outside the region. The National Center for Cyber Security in Saudi Arabia announced that the Kingdom had been attacked by a cyber-attack.

"MuddyWater" is a hacker collective.[8]

A report published by FireEye revealed the existence of the APT33 Iranian hacker group, which has the capability of carrying out devastating cyberattacks. Company analysts revealed in the report that the group has the ability to Since 2013, they have been carrying out spying operations, believing that their actions are being supported by the Iranian government. The group attacked a variety of targets, including command and control centers in the United States, Saudi Arabia, and

[8] *"Cyber Report 24 September-November 2017"*- International Institute for Counter-Terrorism (ICT), pp:22-23

South Korea. The group is very interested in aviation, both military and commercial, as well as the energy sector and petrochemical plants (September 25, 2017). Its technique of the operation is called "spear phishing," and it involves sending emails to company employees. Itcontain content tailored to the recipient, enticing the recipient to open it. The email contains malicious code, which opens a "backdoor" for hacker access[9].

Naturally, hacking into critical infrastructure computing systems is more difficult, but the following incidents demonstrate its viability-

1. DETENTION FACILITY — DAMAGE TO INFORMATION INTEGRITY-

A 27-year-old man from Michigan named Konrad Voits was accused of hacking into the government computer system of the Washtenaw County Jail in order to release his friend before the expected time by changing the information in his prisoner file and updating the release date to an earlier date than the one imposed on him by the court. He confessed to the actions attributed to him, which he performed a year ago while using malware, phishing and social engineering. By breaking into the system, he had access to the passwords, e-mail addresses and personal information of over 1,600 employees, as well as search warrants and personal files of prisoners, but he was caught when guards noticed changes and alerted the FBI.[10]

2.*CRITICAL INFRASTRUCTURE – DAMAGE TO INFORMATION CONFIDENTIALITY*

Hackers targeted critical infrastructure such as power, energy, nuclear, and aviation facilities. The campaigns were designed for spying, but it appears that the attackers have offensive knowledge/experience to cause significant damage, for example-

The hacker group, "Dragonfly", hacked into American and European electrical facilities

[9] Ibid,p: 24

[10] *"Cyber Report 24 September-November 2017"*- International Institute for Counter-Terrorism (ICT), pp:25

(September 7, 2017). The group is of eastern European origin and is responsible for cyber spying campaigns against the critical infrastructure of energy companies in various countries in recent years. In 2014, it was reported that the Dragonfly group had the capability to carry out destructive cyber activities against the operators of oil pipelines, electric companies and other industrial control systems (ICS). Symantec researchers are now warning against Dragonfly 2.0, which they say can disrupt or take over such systems should it decide to do so.[11]

The US Department of Homeland Security and the FBI warned (October 22, 2017) that hackers have been carrying out sophisticated cyber-attacks against nuclear, electrical, aviation and water facilities, critical infrastructure and government agencies in the US since May. It seems that in several cases, the hackers managed to breach the attacked systems and gather intelligence, but it was not possible to estimate the damage that was caused. The attack is carried out through targeted phishing of employees at the attacked companies. The hackers have been identified as the "Berserk Bear" group associated with the Russian government and have known experience in attacking organizations in the energy, transportation and financial sectors.[12]

3. RANGE OF ATTACKS AGAINST TRANSPORTATION AND AVIATION SYSTEMS

Black hat hackers targeted a public transportation system and white hat hackers breached a Boeing passenger plane system; a private transportation company (Uber). As a result, a pattern of attacks on these sectors is emerging-

Sacramento's transit department system suffered a ransom attack during which the hacker's deleted information while threatening to inflict greater damage if they were not paid $8,000 in virtual bitcoin currency. According to Deputy General Manager, MarkLonergan, the attack encrypted portions of computer programs on the agency's servers that affect internal operations, including the ability to use the computers to dispatch workers and assign buses to routes. After the incident, the agency removed its home page from the network and shut down its credit card processing systems as part of the recovery process.[13]

[11] Ibid, p:25
[12] Ibid,p: 27
[13] *"Cyber Report 24 September-November 2017"*- International Institute for Counter-Terrorism (ICT),PP: 29-30

Uber was hacked and 57 million customer records were stolen by hackers. These lists included information about customer names, email addresses, telephone numbers and drivers license numbers. Instead of informing the customers, Uber paid the hackers $100,000 in exchange for deleting the information collected and as hush money. The CEO of the company noted that at the end of 2016, the company was informed that two non-employees had unauthorized access to user data stored on the third-party cloud-based servers that it uses. He noted, however, that the incident did not disrupt the company's systems or organizational infrastructure. The Attorney General of New York opened an investigation and Uber was even sued for negligence by a customer who seeks to file a class action against the company.[14]

"White hat" hackers breached the system of a Boeing passenger plane as part of an experiment by the US Department of Homeland Security using radio communication (November 16, 2017). Although it is an old airplane, it is still used by airlines around the world. Hacking into airplanes requires great expertise and is considered one of the major dangers of flflying.[30] The choice to hack into the plane adds to the trend of incidents involving transportation and aviation,

which was evident during the period under review, and is consistent with remarks made by the Deputy Secretary of the US Department of Homeland Security, who warned that terrorist organizations are looking to bring down aircraft and continue to plan showcase attacks similar to the attack on the Twin Towers.[15]a Merchant Navy officer from Indore received an email on refund of his Customs duty worth a hefty sum, for which he was asked to pay Rs 62 lakh as processing fee. He paid up and didn't get the refund. Investigations led MP Police to a Nigerian based in Delhi, who used his contacts in Indore and Gwalior to pursue unemployed/poor people to open bank accounts. These accounts were used to 'park' the cyber fraud money. At least 15 such accounts were tracked in MP.[16] In Bihar, a NALCO officer was duped of `40 lakh. A former DRDO scientist was conned Rs 5 lakh in a similar case. These networks are well spread and Bihar Police have made cyber-crime arrests from UP, Delhi and Bengaluru. Faking social media accounts is rampant and among victims are former state minister Vinod Jha, a DIG of

[14] Ibid,pp: 31-32
[15]Ibid, p: 33
[16]https://www.newindianexpress.com/thesundaystandard/2021/aug/01/cyber-crimes-rise-in-several-states-during-lockdown-2338361.html

Patna and an IAS officer. In Bengal, four cases were lodged by film and serial actors, alleging their photographs were morphed and circulated with objectionable content on social media.[17]

The Federal Office for Information Security (BSI), which is in charge of IT security in Germany, issued a warning in early April 2020 about an "increasing number of coronavirus-related cyber-attacks on businesses and citizens." In the same month, the Ministry of Economic Affairs of the State of North Rhine-Westphalia stopped paying out emergency aid to self-employed recipients and businesses after the state criminal office issued a warning against fake websites on which criminals attempt to collect data via the required application forms, then use this data to file fraudulent emergency aid claims.[18]

The Consumer Center North Rhine-Westphalia raised awareness of a professional phishing campaign in mid-March. Cyber criminals masquerade as banks and deliberately appeal to people's emotions, telling them that communication must be maintained during bank branch closures in order to entice them into entering sensitive customer data into an authentic-looking website.[19]

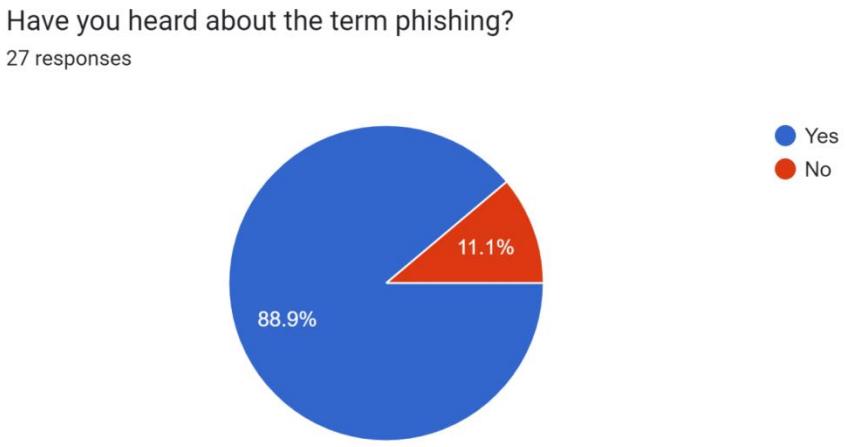
IT security experts are currently warning of an increase in cyber-attacks on healthcare organizations and institutions. 12 Criminals who launch cyber-attacks on hospitals are primarily interested in obtaining demographic and financial information in order to profit from digital identity data. Hospital IT systems may be intentionally or unintentionally compromised during this process. On March 13, the university clinic of Brno, Chechnya's second largest hospital, became the target of an unspecified cyber-attack. Security experts are currently warning of an increase in cyber-attacks in Chechnya's second largest hospital which became the target of an unspecified cyber-attack from an unknown source. The hospital, which is also in charge of performing Corona tests, had to shut down parts of its IT system and postpone planned operations. However, the clinic was able to ensure basic operations. There was no adverse effect on its work.

[17] ibid

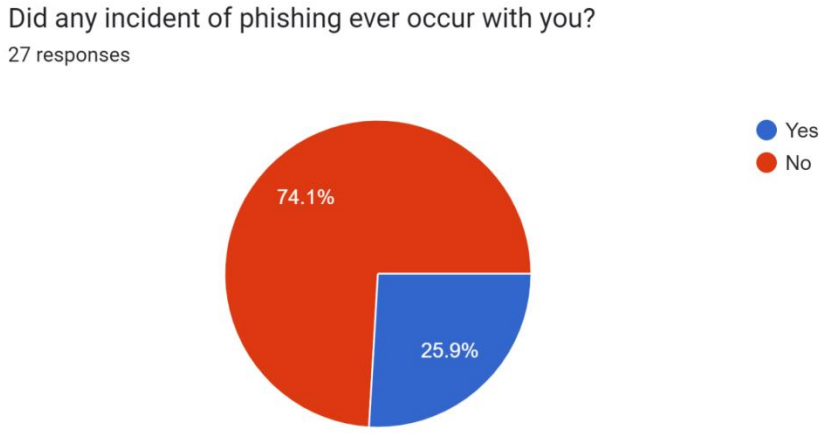
[18] *"The impact of COVID-19 on cyber crime and state-sponsored cyber activities"*- Author(s): Johannes Wiggen, Konrad Adenauer Stiftung (2020), pp: 1-3

[19] ibid,pp:3-4

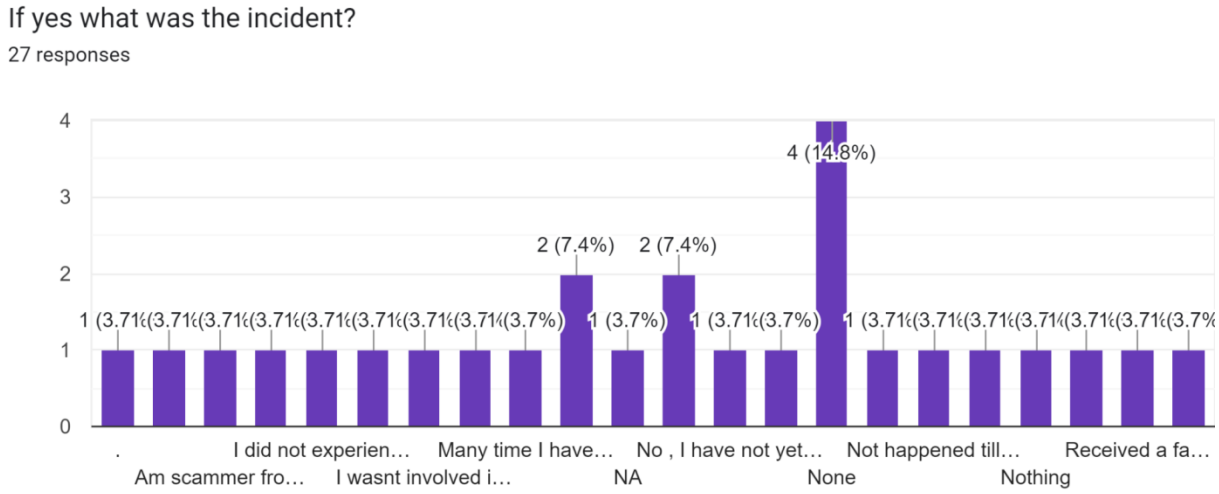
After the primary survey the researchers have collected the data: -



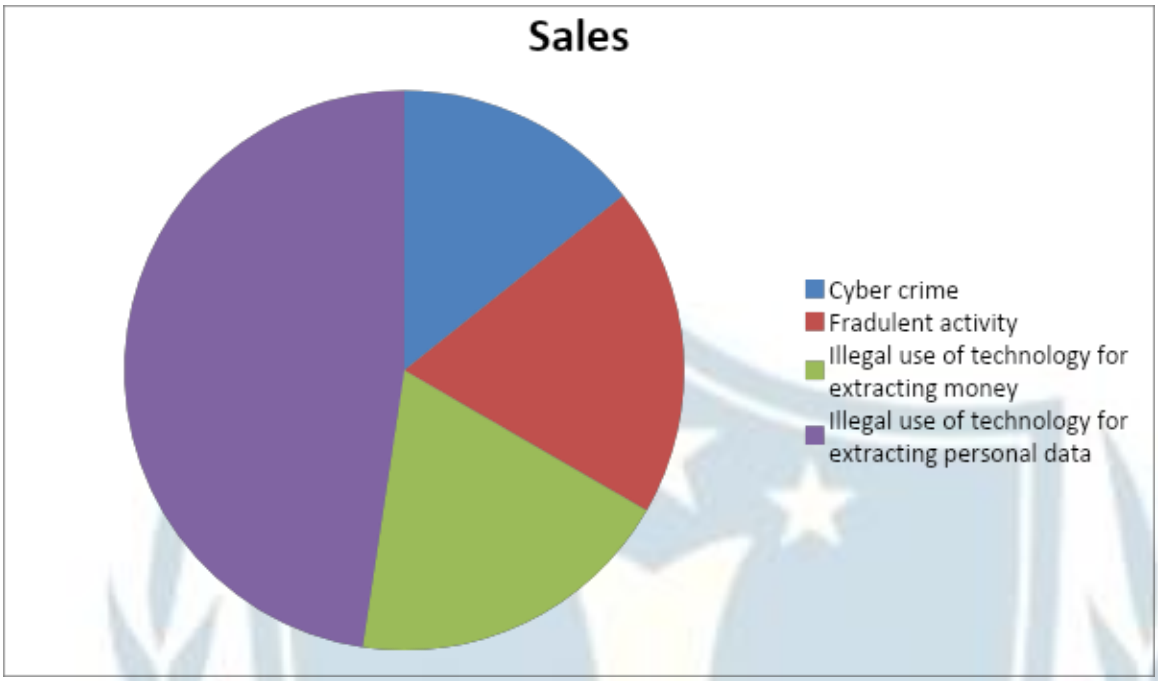
Pie Chart-1



Pie chart-2

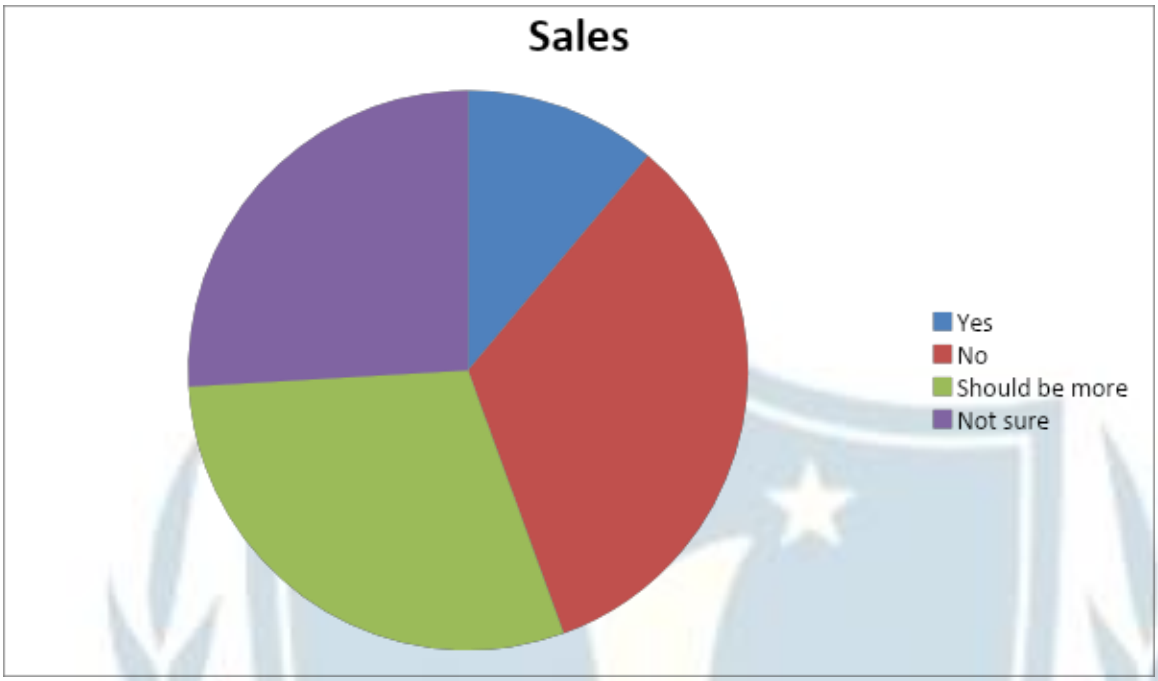


General opinion of the public on the term phishing-



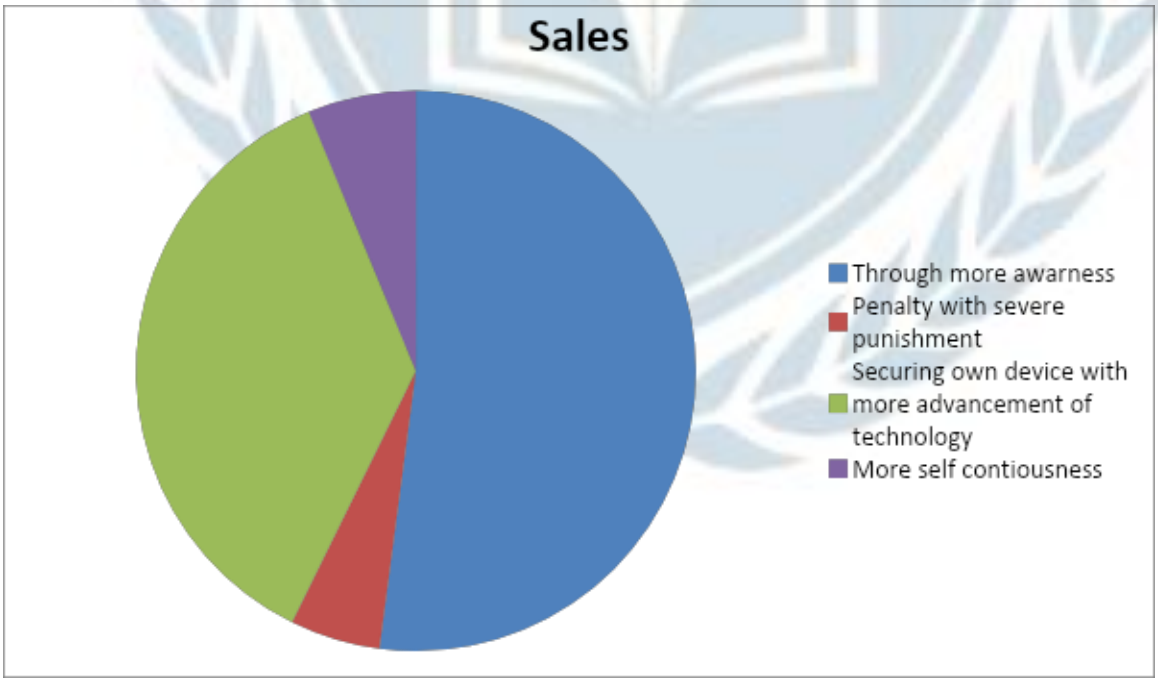
Pie chart-3

General opinion of the public on whether awareness of cyber-attacks like phishing is there or not-



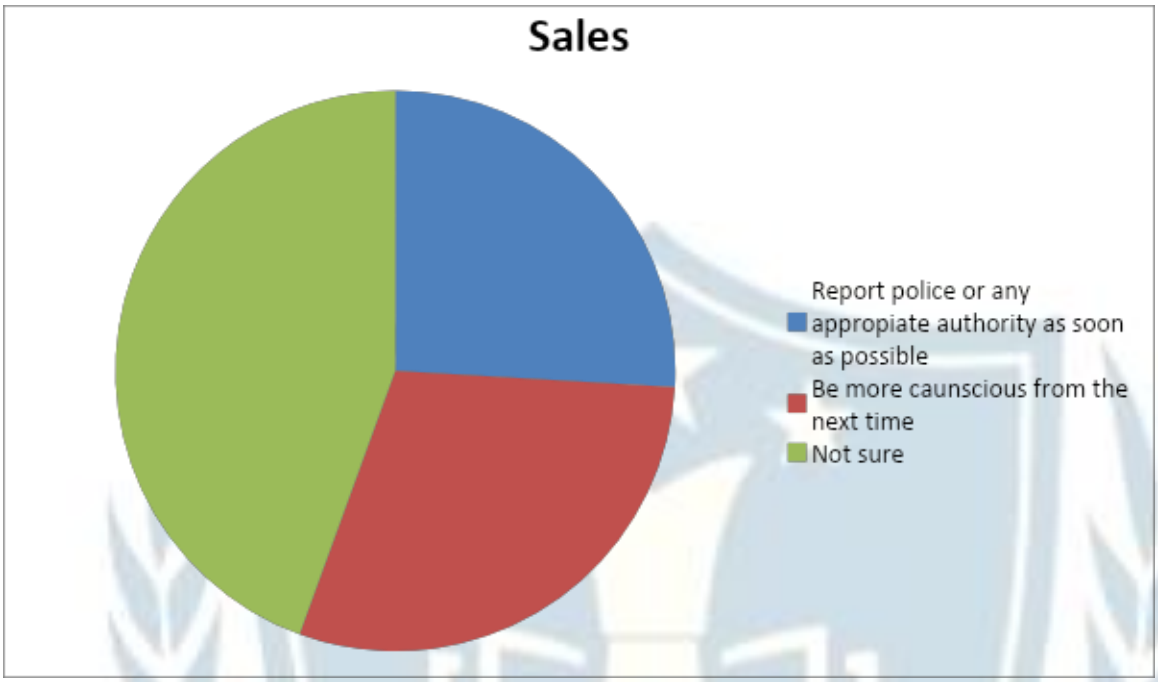
Pie chart-4

Suggestions of public to avoid phishing-



Pie chart 5

Suggestion to the people who has been victim of cyber-attack like phishing-



Pie chart- 6

After analyzing the primary data survey, the research shows that -

- About 90% (88.9%) people who refer to pie chart-1 have heard about the term phishing.
- About 74% of people said that they have never faced anything like phishing and 26% of people have facedthis. (Refer to pie chart-2)
- 90% of the respondents refer to phishing as a cybercrime and the rest also refer to phishing as a different form of cybercrime. (Refer to pie chart -3)
- The response of the respondents regarding awareness about cybercrimes like phishing was mixed, maybe because half of them have not faced it and the rest are not fully informed about the dangers of cybercrimes. (Refer to pie chart-4)
- The 90% of the respondent's suggestions to avoid phishing was through awareness programmers and the rest are of the opinion of penalty or security of own device or more advancement of technology, etc. (Refer to pie chart 5)

- The 40% of respondents who have been a victim of cyber-attacks like phishing suggests to report the police but in the pie chart it can be seen that maximum number about 70% are not sure about what steps should be taken. It is because the lack of awareness in India about cybercrimes and its disasters confuses people and also the authority about the guidelines or the protocols to be followed. (Refer to pie chart-6)

Responses to cyber threats were reflected on a number of fronts: (1) The trend of promoting joint activities, including joint and synchronized operations, continued.
between law enforcement agencies, as well as the signing of intelligence-sharing agreements between law enforcement and technology companies (2) In the political-legal context
The United States and Europe are promoting cyber-specific legislative initiatives. Furthermore, the US is filing indictments against foreign hackers for a variety of cyberattacks against US firms. (3) During the review period, cyber departments were established in intelligence systems, the Securities Exchange, and the courts. The variety demonstrates the importance of functional cyber departments to specialize in a particular field.[20]

Cooperation is a fundamental principle for dealing effectively with cyber threats and terrorist operatives. The trend reflected during the period provided a response to the UN Task Force recommendations from 2011, which emphasized the need for cross-sectoral cooperation, with an emphasis on the participation of technology companies alongside legislative changes.

Covid 19 has opened new ways of cybercrimes. The COVID-19 pandemic highlights digital security risks and the need for adequate action to protect IT systems in critical infrastructures by increasing the use of digital applications and the use of poorly protected private IT devices when working from home. Cybercrime is currently benefiting from a general sense of insecurity and people's desire for information.[21] States are increasingly utilizing cyber espionage to obtain information on corona virus countermeasures, potential vaccines, and treatment options. Cyber risks can only be reduced to an acceptable level by implementing a set of actions: for example, in terms of cybercrime, programmers for education, prevention, and digital literacy must be

[20] *Cyber Report 24 September-November 2017"*- International Institute for Counter-Terrorism (ICT),PP: 32-35
[21] *"The impact of COVID-19 on cyber crime and state-sponsored cyber activities"*- Johannes Wiggen,pp:1-2

strengthened, and law enforcement agencies' resources to prevent and investigate cybercrime must be increased through targeted recruitment of young staff; state-sponsored cyber activities should be addressed by imposing political and economic sanctions or bringing legal charges. [22] To combat the spread of the coronavirus, governments around the world-imposed curfews and restrictions on physical social contact in March 2020. Employers permitted this whenever possible. Their employees to work from home, where private IT devices are increasingly being used for official business. This larger IT surface is frequently less well protected than IT devices used at smaller organisations. work. Under time constraints, new programmers, such as those for conference calls and video conferences, are being introduced, often without adequate security checks. There are also more and more reports of cyber-attacks on health-care organizations, on whose proper operation governments and societies rely more than ever. Major regional trends in Asia and South Pacific region include COVID-19 related fraud and phishing campaigns as well as the illegal online sale of fake medical supplies, drugs and personal protective equipment.[23]Cybercriminals are exploiting security vulnerabilities of teleconference tools. Circulation of fake news and misinformation related to COVID-19 has been reported by most ASP member countries that participated in the survey. The lack of cybersecurity awareness and 'hygiene' was named among the main challenges in this region. According to Kaspersky's telemetry, when the world went into lockdown in March 2020, the total number of brute force attacks against remote desktop protocol (RDP) jumped from 93.1 million worldwide in February 2020 to 277.4 million 2020 in March—a 197% increase. In India, the number increased from 1.3 million in February 2020 to 3.3 million in March 2020. Monthly attacks never fell below 300 million from April 2020 onward, reaching a new high of 409 million in November 2020. India had the highest number of attacks in July 2020, with 4.5 million.[24] Consider the recent data breach at the payment company Mobi Kwik. The data breach incident was reported to have affected 3.5 million users, exposing know-your-customer documents such as addresses, phone numbers, Aadhaar cards, PAN cards, and so on. Until now, the company has maintained that no such data breach occurred. Only after the regulator Reserve Bank of India (RBI) directed Mobi

[22] ibid,p:3
[23]Cybercrime covid 19 Impact , published by: Interpol 2020
[24]https://www.business-standard.com/article/technology/india-becomes-favourite-destination-for-cyber-criminals-amid-covid-19-121040501218_1.html

Kwik to immediately conduct a forensic audit by a CERT-IN accredited auditor and submit the report did the company begin working with the necessary authorities.[25]Rajshekhar Rajaharia, cybersecurity researcher who first tweeted about the MobiKwik issue, and many such breaches in India said: "Most companies, small or big, accept that they have been breached, especially when evidence of a data breach comes forward. In my experience, this makes their customers trust them even more. In the case of MobiKwik, it is surprising why they are not admitting to having been breached. They have threatened legal action against cybersecurity researchers andthe fact that the leaked data has now been taken off the dark net is possibly giving them a false sense of security."[26] In the event of a data breach, users in India are in a bind because India lacks specific legislation dealing with user data breach cases or penal actions relating to the same. Since 2019, the Lok Sabha has been debating the Personal Data Protection Bill, which is intended to address such data breaches. One reason for the high number of data breaches is that India, with its thriving startups and powerhouses, is a very appealing market for cybercriminals. Aside from the massive amount of personal, financial, and user behavioral data that Indian companies hold today, they also have a brand to worry about. According to a recent Infosys-Interbrand study, the potential brand value risk of a data breach to the world's 100 most valuable brands could be as high as $223 billion.[27] According to a study by IBM Security, the average total cost of a data breach in India touched Rs 14 crore in 2020 (an increase of 9.4 per cent from last year) as the average time to contain a data breach increased from 77 to 83 days. The cost comes to Rs 5,522 for a single lost or stolen record, an increase of 10 per cent from 2019.[28]With data gradually transcending into the open domain with numerous firms permitting employees to work from their homes amid the pandemic, sensitive information has become susceptible to security vulnerabilities. The rise of digital payments has also increased complex cyber crimes.[29] According to General Rawat, the Information Technology Act of 2000, which addresses cybersecurity and cybercrime, is not equipped to address new-age changes in business operations and criminal tactics in cyberspace. Several states have seen an increase in cybercrime during the

[25] ibid
[26] ibid
[27] ibid
[28] ibid
[29]https://www.thehindu.com/news/national/cybercrime-went-up-by-500-per-cent-during-pandemic-chief-of-defence-staff/article37457504.ece

Covid-19 lockdowns. Numbers were higher in 2020 than in 2019, and the trend is expected to continue this year. Official figures show that registered cases nearly tripled in Punjab and nearly doubled in Chhattisgarh. Bihar saw a 20% increase. According to unofficial estimates, cyber crime increased by 70% in Madhya Pradesh during this time period. West Bengal, Chhattisgarh, and Assam face similar challenges.[30] The nature of these crimes follows a pattern. They are broadly classified into four categories. 1. Creating fictitious agencies and duping customers under the guise of supplying food, medicine, oxygen, and other necessities. 2. luring people into online transactions and then robbing them after obtaining their account information/hacking accounts 3. Creating fake social media accounts of powerful figures such as IAS and IPS officers and deceiving the public with their names. 4. Filming and distributing pornographic material online/blackmailing women by threatening to publish intimate images.[31] "Activities are carried out on electronic platforms. A section of people, who have become jobless because of the pandemic, entered the cyber world to find prey. People are using digital platforms without limit and exploring all possibilities. Other than financial frauds, cases targeting women are also taking place,'' said Amitesh Mukhopadhyay, professor of sociology in Kolkata's Jadavpur University.[32]

IV. NATURE OF CRIME-

1.Floating non-existent agencies & duping customers on the pretext of supplying food, medicine, oxygen & other essentials.

2.Luring people into online transactions & robbing them after getting hold of account details

/hacking accounts.

3.Creating fake social media accounts of influential figures like IAS/IPS officers, deceiving the public using their names.

4.Filming & circulating pornographic material online/blackmailing by threatening to share images of intimate moments.

[30]https://www.newindianexpress.com/thesundaystandard/2021/aug/01/cyber-crimes-rise-in-several-states-during-lockdown-2338361.html
[31]ibid
[32] ibid

In the time of chaos in the pandemic, as the world is suffering through a major health crisis many other dark elements with atrociousness and treacherousness have risen since the lockdown has started. As people were in their respective homes and following the rules of the government, the medium to get used to the lifestyle was internet browsing and social media surfing which turns out to be dangerous due to data transferring or acquiring personal information of anyone by hacking, frauds or unknown internet viruses. It has been discovered that such viruses or frauds are a medium to get access to personal information of the user. The internet is also a necessity for many corporateand government office employees who are working from home in the lockdown. Cases of a data breach through unsecured apps for official meetings in the lockdown has been a major concern. Zoom app has been detected as a part of a medium for cybercrime. It was observed that hackers were able to get access to meeting ids and passwords and during online lectures and other official meetings, inappropriate content used to come out of nowhere. In India, internet security is not taken seriously which has resulted in the rise of cyber[33] crime in the pandemic. The Cambridge Analytica scandal which shook the world for internet security and a big alert for social media security.

V. CONCLUSION

The history of phishing demonstrates that while delivery methods have changed over the past two decades to avoid being picked up by spam filters and other technology, the techniques used by phishers have largely remained the same. It would stand to reason that users would have discovered how to avoid providing login information, clicking links, or even opening attachments. However, hackers can still use this method to their advantage. From the research it can be understood that maximum people are aware about phishing but not so much on a large scale. Most of them take it as some stray and casualty incidents and do not pay much heed to it. As a result, the danger of cybercrimes larks behind the technologically advanced world. This

[33] https://blog.ipleaders.in/rise-cybercrimes-covid-19-lockdown/

phishing showed its worst form during the covid-19 pandemic lockdown where people were subjected to stay at home and work.

VI. BIBLIOGRAPHY

1. *"Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*"- Lynch Jennifer, Source: Berkeley Technology Law Journal , 2005, Vol. 20, No. 1, Annual Review of Law and Technology (2005), University of California, Berkeley, School of Law pp: 270-300
2. https://www.newindianexpress.com/thesundaystandard/2021/aug/01/cyber-crimes-rise-in-several-states-during-lockdown-2338361.html,, Published on: 1st August 2021 by Mondal Pranab, Singh Anurag and Bajwa Harpreet
3. https://www.thehindu.com/news/national/cybercrime-went-up-by-500-per-cent-during-pandemic-chief-of-defence-staff/article37457504.ece, Published on: 12th November 2021
4. https://blog.ipleaders.in/rise-cybercrimes-covid-19-lockdow, Published on: 24th January 2021
5. https://www.business-standard.com/article/technology/india-becomes-favourite-destination-for-cyber-criminals-amid-covid-19-121040501218_1.htm, Published on: 6th April 2021 by Shinde Shiwani and Allhawadi Neha
6. CYBERCRIME: COVID-19 IMPACT, Published on: August 2020, Interpol 2020
7. *"The impact of covid-19 on cybercrime and state sponsored cyber activities"*, by Wiggen Johannes and Stiftung Konrad Adenauer, pp:Cyber Report 24 September-November 2017, pp: 1-4
8. *"International Institute for Counter-Terrorism (ICT) (2018) ,Cyber Report 24 September-November 2017*, pp: 23-27

9. "*Phishing and Cybercrime Risks in a University Student Community*" , by-Roderic G. Broadhurst, Katie Skinner and Sifniotis and Matamoros-Macias ,published by: International Journal of Cybersecurity Intelligence & Cybercrime, volume -2, issue-1,
10. "*THE WEAPONIZATION OF SOCIAL MEDIA: SPEAR PHISHING AND CYBERATTACKS ON DEMOCRACY*", Bossetta Michael, Journal of International Affairs, Vol. 71, No. 1.5, Special Issue: CONTENTIOUS NARRATIVES: DIGITAL TECHNOLOGY AND THE ATTACK ON LIBERAL DEMOCRATIC