BRIDGING CYBERCRIME AND LAW IN INDIA: THE CASE OF PHISHING ATTACK TYPES THROUGH THE PRISM OF THE IT ACT

Aalan Joe Edwin J J, Practising Advocate, District Court, Tamil Nadu

ABSTRACT

The constant increase in cyber threats seriously threatens both personal privacy and international security. Phishing constitutes a form of cybercrime that targets individuals through various means, including emails, phone calls, text messages, and the exploitation of personally identifiable information, banking details, credit card information, and passwords. Primarily, phishing represents a type of online identity theft. Perpetrators, known as phishers, employ social engineering techniques to unlawfully acquire the personal data and account information of their victims. This study thoroughly analyzes the threat of phishing attacks, including their types and countermeasures, how to spot them, how to stop them, where to make a complaint, and how to prevent them. This review aims to give scholars, cybersecurity experts, and legislators a useful resource that will help them understand and deal with the difficulties of phishing attack threats. This study offers a comprehensive summary of hacking attacks. This study paper also studies phishing attacks in India and the sort of regulation we follow through case law analysis.

Keywords: Phishing attacks, cybersecurity, detection techniques, case studies, IT Act

Introduction:

Cybersecurity has always been a big concern. There has never been a time when cybersecurity researchers have overtaken cybercriminals because cybercriminals have to find only a small loophole to sabotage the entire cybersecurity infrastructure. This can be gauged from the fact that in the year 2020, hackers placed their payload into the Orion product of the SolarWinds company and they stole the information without being detected for a long time, until about a year later, when the cybersecurity Company FireEye reported it, around 30000 customers of the SolarWinds were infected[1]. Of these, more than 18000 are government and private users in this current situation and technological developments, the Indian digitalization platform is expanding quickly, bringing it closer to becoming the biggest player in the IT sector. Currently, everyone between the ages of 5 to 90 uses the Internet, and children are in a different situation concerning smartphone accessibility. Today, each child insists on obtaining a smartphone, which also involves internet usage. Similarly, regardless of who knows how to access and use the Internet, everyone is busy using the Internet[2]. People often give access to many things they do not know they are giving access to. Google has stated that 50% of mobile ad clicks are accidental and that 72% of those lead to malicious sites[3]. These sites are also very popular for internet fraud.

Google reports that the number of phishing and hacking websites has grown by 350% since the coronavirus pandemic began[4] (Google Publishing) - Cybercriminals exploit the digital illiteracy of victims to elicit or extract sensitive information easily. “In 2024, the BSNL data was breached by hackers, and they leaked 278GB of sensitive information. In February 2025, the Grub Hub food delivery company's data was hacked. Grub Hub declared a data breach that affected the personal information of a large number of customers, merchants, and drivers after attackers infiltrated its systems via a service provider account”[5].

Not only do cybercriminals use websites for phishing, but they also employ email and telephone to engage in phishing. Cybercriminals use social engineering to obtain information from victims by pretending to be legitimate individuals of authority. Each year, Google blocks

[1] https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know
[2] PHISHING_IN_INDIA_-_ANALYTICAL_STUDY.pdf
[3] Sixty percent of mobile banner clicks are accidental - Digital Content Next
[4] https://www.forbes.com/sites/jessedamiani/2020/03/26/google-data-reveals-350-surge-in-phishing-websites-during-coronaviruspandemic/?sh=45f4cbac19d5
[5] February 2025: Major Cyber Attacks, Ransomware Attacks & Data Breaches

thousands of phishing websites and hacking activities, yet the number of phishing websites continues to grow. Web browsers have numerous implicit algorithms that can identify phishing websites and warn the user, but there are still numerous websites that engage in phishing activities at a very large scale.

As a result, it provides a forum for discussions about cyber security[6] issues. Indeed, if we follow the United Nations ITU Global Cybersecurity Agenda rankings[7], India has risen from its prior position of 47 to 10th place in the Cyber Security Ranking of Countries[8]. However, India still has a way to go before it can provide businesses and assets across all industries with comprehensive protection from cyberattacks.

Meaning of Phishing:

Phishing is a type of cybersecurity attack that attempts to obtain sensitive data such as Usernames and passwords. It attacks the consumer through mail, text, or direct messages. The attacker sends an attachment to the user, which the user opens because the user thinks the email, text, or message came from a trusted source. It is a type of Social Engineering Attack.

For example, the end-user may find some messages like the lottery winner, then the user clicks on the attachment the malicious code activates that can access sensitive information details or "if the user clicks on the link that was sent in the attachment, they may be redirected to a different website that will ask for the login credentials of the bank"[9].

Phishing can be carried out using a variety of vectors and media; three popular channels for phishing are the Internet, short messaging services, and voice calls.[10]

[6] What is Cyber Security? | Definition, Types, and User Protection (kaspersky.co.in)
[7] Global Cybersecurity Agenda (GCA) (itu.int)
[8] Top countries GCI cyber security ranking 2020 | Statista
[9] https://hacksheets.in/phishing-notes
[10] https://www.sciencedirect.com/science/article/abs/pii/S0957417418302070

The example is given below.

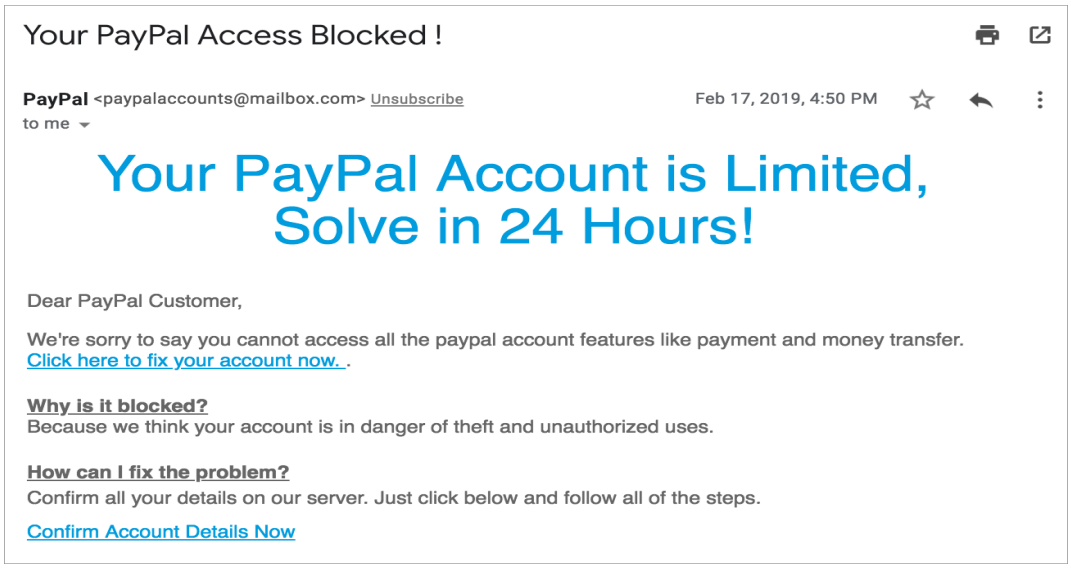

Image Source:[11]

How Does Phishing Work:

Phishing is usually initiated with a fraudulent email, link, URL, pop-up, or communication created to entice a victim. The message is designed to appear as if it is coming from a trusted source. If a victim is fooled, they will be prompted to enter their confidential information or aspects of information, sometimes on a fraudulent website. In some phases, malware is also downloaded onto the target's computer. In other situations, the cybercriminal only needs a victim's credit card or personal information for monetary gain. Sometimes, phishing is done to gain employee login information or other credentials to perpetrate an advanced attack against a given organization or target. Cybercrime attacks, like an advanced persistent threat (APT) or ransomware, typically begin with a phishing piece. A phishing attack is usually a part of a larger campaign, focusing on capturing as many victims as possible within a target space, or a large sample of individuals. As a phishing type of attack goes from the sender to the successful retrieval of a credential must consist of four independent phases that are executed.

Phase 1: A hacker with malicious intent sends either an email, a URL, or a message to the target posing as a reputable source. Oftentimes, it includes a call to action, making the target

[11] https://www.khanacademy.org/computing/ap-computer-science-principles/x2d2f703b37b450a3:online-data-security/x2d2f703b37b450a3:cyber-attacks/a/phishing-attacks

believe they need to follow a third-party link to perform a security inspection or to simply update a feature.

Phase 2: The target, or customer, follows the malicious link to a fake page that looks as much like a website as possible since they think the email came from the sender, which might be a bank or a business.

Phase 3: On the fraudulent site, the user is prompted to enter some sensitive information specific to the website, such as account credentials. Once the information is submitted, all the sensitive information will be sent to the hacker who created a malicious email and a fraudulent web page.

Phase 4: Upon receiving the account credentials, the hacker may use them to his advantage and is free to log in or sell the obtained information to the highest bidder on the dark web.

Types of Phishing:

- **Deceptive Phishing** - In a deceptive phishing scheme, carriers broadcast one phishing email to a mass audience of individuals, sometimes thousands, without putting in that much legwork. They're hoping for a small percentage of users to click the malicious link and provide their private data on the fake site.

- **Pharming** - In a pharming attack, hackers are purchasing domain names, and try to copy the domain names of popular websites like www.google.com or www.facebook.com in hopes of a target accidentally typing in such a URL with any possible haste. When a target arrives at the site, they will be presented with a webpage that looks identical to the original site and is asked to input their login credentials without checking the URL first.

- **Whaling** - In this approach, phishing attempts that are carefully planned and set up to ensure a security breach frequently target influential individuals, such as CEOs and administrative managers. The hacker conducts a great deal of study before determining the best time and method for these attacks.

- **Spear Phishing -** Spear phishing targets any specific organization for unauthorized access, or the target is anyone willing to access any individual who is in the organization. These attacks are not coming from a random or an unknown hacker, and these attacks are not

initiated trying to scam individuals into paying money; these attacks come from someone searching for money or some other piece of data that is important to them.

- **Clone Phishing -** In this approach, cybercriminals copy email messages that come from a trusted source. The hacker alters the message by including a link that causes the user to access a malicious or fake website. This message is then sent to many users, while the originator can observe who clicks on the attachment sent via email. This spreads through the contact list of the user who opened the attachment.

- **Cat Phishing -** This is a type of social engineering attack that manipulates emotions and exploits them for money and information. They target them on dating sites. This is an example of an engineering threat.

- **Voice Phishing -** Typically, attacks involve the user being directed to a fake website, while some attacks do not involve visiting a fake website. This type of phishing is sometimes called "vishing." In this form of attack, the criminal uses modern caller ID spoofing so the victim believes the call is from a trusted source. They also use IVR to make it harder for law enforcement to trace, block, or monitor. This kind of phishing attack is used to steal credit card numbers or other confidential personal information from the user. It damages more than other types.

- **SMS Phishing -** To obtain account information from the user is the aim of this attack. Similar to other phishing attempts, this SMS phishing scam is used by cybercriminals to obtain private data or credit cards. Cybercriminals use text messages to lure victims to try and turn them into account suspenders, so the text claims to be from a trusted organization and tries to get you to redirect the user to their fake website. The fake website looks like it is the real original website.

Who Is Targeted for Phishing:

Anyone can be targeted by a phishing attack, but sometimes phishing is done to very specific and particular people. Threat actors occasionally send out generic emails to a large number of recipients in the hopes that someone will fall for the ruse because of a shared characteristic. An example: the attackers say something is wrong with your Facebook or Amazon account, and you need to click this link right away to log in and fix it. The link would likely lead to a spoofed

webpage where you might give away your login credentials.

Threat attackers use more targeted phishing attacks if they are after something specific, like access to a certain company's network data information from a politician or political candidate or details about a political party. This is called spear phishing. In this case, they may research information to make their attack sound familiar, credible, believable, and reliable, so the consumer is more likely to click a link or provide information. An example would be researching the name and communication style of a target company's CEO, then emailing or texting specific employees at that company pretending to be the CEO, asking for something.

High-profile people like;

- Big company CEOs
- Executives of the company
- Shareholder of the company
- Celebrities
- Well-known wealthy individual
- Businessman
- Politician
- Political party
- Personal security of the government ambassadors
- Chief of the army
- Employees of the top company

How to Detect a Phishing Attack:

Detecting or finding a phishing attempt is not always easy, but if we follow some steps, a little discipline, and some common sense will go a long way. Look for something unfair or unusual.

Ask yourself if the message passes the "smell test." Trust your intuition, but do not let yourself get rushed up with fear.

Here I am going to mention a few more signs of a phishing attempt:

- The offer in the email seems too good to be true. That mail might say you have won the lottery, an expensive prize, or some other over-the-top item.

- Sometimes you recognize the attacker, but it is someone you don't talk to. Even if the sender's name is known to you, be suspicious if it's someone you don't normally communicate with, especially if the email's content has nothing to do with your normal job responsibilities. On the other hand, if you're cc'd in an email to folks, you don't even know, or perhaps a group of colleagues from unrelated business units.

- Occasionally, you may receive a warning telling you to "act now" before your account is cancelled, such as "beware if the email contains charged or alarmist language to create a sense of urgency." Remember, responsible organizations or companies will not ask for personal details over the Internet.

- The content of the messages includes unexpected or unusual attachments. Those attachments may contain malware, ransomware, or another online threat.

- Some messages contain links that look a little off. Even if your spider-sense is not tingling about any of the above, don't take any embedded hyperlinks at face value. But out of curiosity, we click the link to see the actual URL. "Be especially on the lookout for subtle misspellings in an otherwise familiar-looking website, because it indicates fraud". It is always better to type a URL yourself rather than clicking on the embedded link.

Way To Protect Against Phishing Attacks:

As mentioned earlier, phishing is an equal opportunity threat, capable of blowing in desktops, laptops, tablets, and smartphones. Most of the time, Internet browsers have ways to check if showing links is safe or not, but the first line of defense against phishing is your judgment. Train ourselves to recognize the signs of phishing and try to practice safe computing to check our email, read Facebook posts, or play our favourite online game.

Here are a few steps and ways to practice to keep the phishing attacks;

- Do not open emails from an operator you are not familiar with.
- Do not ever click on a link inside an e-mail unless you know exactly where it is going.
- "To form a layer of protection, if you get an e-mail from a source, you are unsure of, navigate to the provided link manually by entering the legitimate website address into your browser".[12]
- Look out for the digital certificate of a website.
- If the website or webpage asks to provide sensitive information like passwords or other details, check out the URL of the page and whether it starts with "HTTPS" instead of just "HTTP." The "S" stands for "secure. There is no guarantee that a site is legitimate, but most legitimate sites use HTTPS because it is more secure. Even trustworthy HTTP websites can be compromised by hackers.
- If you suspect or doubt that an e-mail is not legitimate, then take a name or some text from the message and put it into a search engine to look or find if any known phishing attacks exist using the same methods.
- Moreover, the link to check whether the link is legitimate or not.

How to Prevent a Phishing Attack:

- **Email Authenticity**: If the email asks for private information, we must always cross-check the link. Whether it comes from a bank or a shopping website means checking the sender's address is the first step in protecting ourselves from attack.
- **HTTPS Webpages**: Users or consumers should be using websites that have an HTTPS certification. It is not only less likely to be phishing web pages, but running network attacks on such secured websites is more challenging than usual.
- **Avoid Pop-Ups:** Internet users must avoid following random pop-ups like advertising

[12] https://www.malwarebytes.com/phishing

games or attracting monetary rewards for clicking on them. Designed to dupe innocent users, these types of pop-ups are primarily used to inject malware into a target system or laptop or tablet to steal important credentials.

- **Password Rotation:** To keep our browsing data as secure as possible, we need to change our passwords every few months. The target of a phishing attempt, for instance, is likely to have already changed the compromised password even if the website manages to obtain certain credentials**.**

- **Anti-Phishing Extensions:** To identify email vulnerabilities that could result in a phishing attack, we need to utilize free anti-phishing extensions like Cloud Phish and Netcraft scan. Filtering the majority of phishing emails is simple and requires no manual labour when using such add-ons.

- Do not open a suspicious email attachment or any suspicious or doubtful links.

- Don't give any sensitive information like personal data or banking data via message or email.

- Always use an antivirus to make sure the system is not affected.

The Role of Emerging Technologies – Sword of Double Edge:

New technologies - especially artificial intelligence (AI) - are increasingly important to India's cyber threat landscape, acting as both an accelerant to more sophisticated attacks and a possible enhancement to defenses. Cybercriminals are quickly introducing AI to hack or otherwise increase their phishing capabilities. For instance, generative AI can be used to generate elevated, convincing phishing emails that are much more difficult to flag as fraudulent. Deepfake technology enables attackers to call the target of a vishing (voice phishing) attack and pretend to be a person of authority who could induce employees to release sensitive information or move money. AI has even been embedded into malware to create adaptive and evasive threats that would evade preventive security controls. There is also increasing apprehension around AI systems themselves being subverted by techniques like data poisoning that exploit malicious data to compromise AI models. Looking to the horizon, quantum computing threatens to potentially be an existential crisis for, based on its power, the encryption

we use today. It could potentially lead us to consider the longevity of our sensitive data if we determine that encryption in its current form would not endure.

AI isn't just something that bad people can use to cause trouble; it can also help keep us safe online. For example, AI can watch out for dangers by checking how people use the internet and spotting anything unusual that might mean an attack is happening. It can help fix problems quickly by isolating affected computers and blocking bad websites. AI can also learn from past attacks to guess what kinds of attacks might happen next, allowing companies to take steps to protect themselves ahead of time. In the finance world, businesses are using AI to find and stop fraud more effectively. Overall, AI can be used both to attack and defend, creating a situation where both sides are constantly getting better. Companies need to be aware of the dangers that AI can bring, but they also need to know how to use it to protect themselves. Additionally, as technology like quantum computing develops, organizations must think ahead and work on new ways to keep digital information safe.

Recent Trends in Phishing Attacks:

Cybercriminals are now using a new evasion technique called "Precision-Validated Phishing", which only displays phishing login pages for accounts the attackers have checked against a list. Unlike mass phishing attempts that target dozens of people at once, this technique ensures only verified high-value targets receive phishing emails thanks to real-time email validation.

"According to Cofense, the threat actors use two main techniques to achieve real-time email validation.

In the first, third-party email verification services that are incorporated into the phishing kit and use API calls to verify the victim's address in real time are abused.

The second method is to deploy custom JavaScript in the phishing page, which pings the attacker's server with the email address victims' type on the phishing page to confirm whether it's on the pre-harvested list."[13]

[13] https://www.bleepingcomputer.com/news/security/phishing-kits-now-vet-victims-in-real-time-before-stealing-credentials/

Legal Provisions Regarding Information Technology Act,2000:

The phishing attack and a fraudulent attack are online attacks to disguise and use false and fraudulent websites of banks and other financial institutions, and URL Links to deceive people into disclosing valuable personal information and data, which is then used to later steal money out of an account. This is likely to attract and engage many penal provisions of the **Information Technology Act, 2000,** amended in 2008, adding some new provisions for the act of phishing. The following Sections of the **Information Technology Act, of 2000,** apply to Phishing Activity:

"Section 66: The account of the victim is compromised by the phisher, which is not possible unless & until the fraudster fraudulently effects some changes by way of deletion or alteration of information/data electronically in the account of the victim residing in the bank server. Thus, this act is squarely covered and punishable u/s 66 IT Act.

Section 66A: The disguised email containing the fake link of the bank or organization is used to deceive or to mislead the recipient about the origin of such email, and thus, it attracts the provisions of Section 66A IT Act, 2000.

Section 66C: In the phishing email, the fraudster disguises himself as the real banker and uses the unique identifying feature of the bank or organization, say Logo, trademark, etc., and thus, clearly attracts the provision of Section 66C IT Act, 2000.

Section 66D: The fraudsters using the phishing email containing the link to the fake website of the bank or organizations impersonate the Bank or financial institutions to cheat innocent persons, thus the offense under Section 66D too is also attracted.[14]

The Information Technology (Reasonable Security Practices and Procedures and Personal Data or Information) Rules, 2011 (SPDI rules) regulate how to handle personal data. The SDPI rules require a body to corporate and retain only as much data as is necessary for their collection. "They must also uphold appropriate security policies and procedures and only provide personal information to a recipient who shares or exceeds their security requirements.

[14] https://ciet.ncert.gov.in/storage/app/public/files/17/Presentation%20PDF/PHISHING.pptx.pdf

Separately, the **Reserve Bank of India (RBI)** has issued a directive on the Storage of Payment System Data, according to which payment data may only be stored in India. While the purpose of the directive is to ensure that the RBI can access all payment data for monitoring payments, it will likely make it easier for authorities to identify and punish payment system operators that do not employ adequate security measures."[15]. The RBI has also notified a Cyber Security Framework in Banks, which:

(i) provides the baseline requirements for cybersecurity that all banks must follow,

(ii) mandates the establishment of a security operations center by each bank,

(iii) "Provides for the reporting of cybersecurity incidents to the RBI"[16].

The RBI also oversees other organizations, like payment gateways and aggregators, which must follow basic technology-related guidelines, such as data security guidelines, and make sure their merchants follow the Payment Card Industry Data Security Guidelines.

Case Laws Related to Phishing:

- **Shreya Singhal v. UOI[17]**

In this case, the Supreme Court of India ruled that Section 66A of the Information Technology Act, 2000 is unconstitutional, owing to its vagueness. The Petitioners claimed that Section 66A's purpose to protect people from annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, or ill will fell outside the limits of restrictions that can be lawful under Article 19(2) of the Indian Constitution. The Court said that the prohibition on provocations through a computer resource or communication device to annoy, inconvenience, or insult fell outside reasonable permissible exceptions to freedom of expression. The Court held that Section 66 A's inconsistency, especially in failing to define concepts such as discomfort or annoyance, constituted a grave risk sanctioning a significant degree of protected and innocuous speech, and held a scope too vast as to be lawful, and too vague to satisfy due

[15] https://www.lexology.com/library/detail.aspx?g=a6e35288-c18d-433f-83c1-4525d348d6cf/
[16] https://www.lexology.com/library/detail.aspx?g=a6e35288-c18d-433f-83c1-4525d348d6cf/
[17] AIR 2015 SC 1523; Writ Petition (criminal)No. 167 OF 2012

process.

- **Poona Auto Ancillaries Pvt Ltd v. Punjab National Bank (2013) [18]**

One of the principal arguments raised in the Poona Auto Ancillaries case is the carelessness exhibited by the police in its dealings with cyber-crimes, such as phishing, which led to a loss of more than Rs. 45 lakhs in this instance. The Bombay High Court subsequently directed the Maharashtra police department to conduct specific training seminars for all officers involved in cyber-crime units. Reports from the media stated that many police in some of the states in India are turning to private cyber-forensics expertise to help them deal with cyber-crimes, which is a good step taken by law enforcement agencies. However, at the same time, it was mentioned that it can be problematic for the police to rely on a private company for sensitive information, and that should motivate law enforcement agencies to develop their in-house teams of cyber security professionals.

- **NASSCOM v. Ajay Sood & Others (2005)[19]**

The Delhi High Court described phishing, to bring the first case in this area in India, as "A form of internet fraud in which a person poses as a legitimate organization, such as a bank or an insurance company, to obtain personal data from the customer, such as account access codes, passwords, and other personal identifying information." The personal information that is obtained by impersonating the legitimate party is only used for the benefit of the party obtaining the personal information, and will be used to commit further wrongs.

The Delhi High Court defined phishing as an illegal act that was a "misrepresentation made in the course of trade," even though India lacks a particular law that makes it illegal., and therefore leads to a confusion concerning the source and origin of the email, and causes huge damage not only to the consumer, but also to the legitimate party whose name, identity or password is exploited." Ultimately, the court said the act of phishing was a type of impersonation that damaged the Plaintiff's reputation.

[18] SCC 394

[19]https://www.bing.com/ck/a?!&&p=6083aa44c0d04c9cf5cf277df569a5392a4f1297d1f70db43fc24c06936494aeJmltdHM9MTc0NDI0MzIwMA&ptn=3&ver=2&hsh=4&fclid=2c730493-5581-68a9-0505-162f542c6990&psq=%e2%80%a2%09Nasscom+v.+Ajay+Sood+%26+Others&u=a1aHR0cHM6Ly9sYXdmdWxsZWdhbC5pbi9uYXNzY29tLXZzLWFqYXktc29vZC1vcnMtZGVsaGktaGMtMjAwNS1jYXNlLWFuYWx5c2lzLw&ntb=1

This case accomplishes two important objectives – first, it manages to place "phishing" in the context of Indian law, even if it is not explicitly legislated; and second, it ends the understanding that there is a lack of "damages culture" in India for infringement of intellectual property rights. This decision validates IP owners' confidence in the willingness and ability of the Indian court system to protect intangible property rights, as well as sending a clarion call to IP owners that they can conduct business in India without relinquishing their intellectual property rights.

Conclusion:

"Phishing is a huge issue all over the globe in the context of the existing state of e-commerce, and this will continue to be a problem for as long as new web users lack knowledge as well as awareness. Phishers and Hackers often make use of people's weaknesses in combination with the technical advancements they possess"[20].An individual's susceptibility toward phishing may be influenced by a variety of factors such as age, gender, internet dependence, user anxiety, and many other factors. At the same time, the motivations of phishing have expanded, and it now involves obtaining personal information, financial fraud, cyberattacks, hacktivism, reputational damage, cyber warfare, and governmental cyberattacks. Phishing scams are becoming increasingly sophisticated, utilizing old and new methods. Phishing scams that take place through different social media platforms have also become more common in recent years. As a result, to efficiently and effectively address "Phishing," it is essential to consider both preventive and corrective measures. Combating the threat posed by phishing and hacking will require involvement from law enforcement, the government, and the private sector. To combat phishing attacks, there must be anti-phishing technologies developed that can protect the average user from becoming a victim of phishing and hacking.

One fundamental reason for the failure of cyber laws in India is the non-coverage of many types of developing cybercrimes or hacks. India currently has only one piece of legislation on cyber law, which has very few provisions due to its scope of applicability being significantly narrow. The current legislation, as it stands, is almost pandering to a cyber-criminal. Even though the conviction rate of a law is a crucial measure of its coverage, given the simple fact that there are so many legislative acts, we have not solved the ineffectiveness of the

[20] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf and Imtiaz Khan, Phishing Attacks: A Recent Comprehensive Study and a New Anatomy, Frontiers, (Mar. 19, 2021), https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full

implementation of the law. However, an impressive conviction rate will show the effective use of cyber laws in India. A low conviction rate is half the ineffective usage of the current cyber laws in India.

As we move forward, the changing threat landscape calls for ongoing research, development, and adjustment. Keeping up with those threats will require ongoing vigilance, innovation, and resilience. But, through proactive security, continual education, and ongoing evolution of detection and prevention technologies, we can aim to stay one step ahead of the attackers. While the challenges of the future may be daunting, we can achieve a more secure digital environment with collaborative efforts.

References:

I. https://www.bluevoyant.com/knowledge-center/8-phishing-types-and-how-to-prevent-them

II. https://btcirt.bt/common-phishing-attacks-in-bhutan-and-how-to-protect-yourself

III. https://www.jdsupra.com/post/fileServer.aspx%3FfName%3Db1decbc1-9271-4395-ab56-ca9c86dc9ef9.pdf

IV. https://blogs.siliconindia.com/neerajaarora/phishing-scams-in-india-and-legal-provisions-bid-vkXYC7Gm32628069.html

V. https://ciet.ncert.gov.in/storage/app/public/files/17/Presentation%20PDF/PHISHING.pptx.pdf

VI. https://www.lawyersclubindia.com/articles/phishing-scams-in-india-and-legal-provisions-3606.asp

VII. https://www.lexology.com/library/detail.aspx?g=a6e35288-c18d-433f-83c1-4525d348d6cf

VIII. https://www.infosecinstitute.com/resources/phishing/a-brief-history-of-spear-phishing/

IX. Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges.

X. https://www.frontiersin.org/journals/computerscience/articles/10.3389/fcomp.2021.563060/full

XI. A survey of phishing attacks: Their types, vectors, and technical approaches by Kang Leng Chiew, Kelvin Sheng Chek Yong, Choon Lin Tan

XII. Phishing kits now vet victims in real-time before stealing credentials. By Bill Toulas