IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

"Mitigating Cyber Threats: Legal Remedies For Victims Of Phishing Attacks As A Social Engineering In India And Worldwide"-A Comparative Study

Submitted by: 1.) LEENA.S.B (Author)

5th year - BBA, LL.B. (Hons.) from SASTRA Deemed University

2.) PREETHI.S.M (Co-Author)

5th year - BBA, LL.B. (Hons.) from SASTRA Deemed University

1. ABSTRACT :

The proliferation of phishing attacks and email scams has emerged as a critical concern in the digital landscape, posing significant threats to individuals and businesses alike. In an era dominated by digital communication, phishing attacks and email scams have become pervasive threats, causing substantial financial and emotional distress to individuals and businesses in India. People's inability to recognise social engineering assaults is the reason why the number of them is growing daily. Thus, there is a pressing need for resources to aid in the understanding of social engineering methods and crimes. This research paper delves into the landscape of phishing attacks and email scams, specifically examining the legal avenues available to victims in the context of India and various countries' jurisdictions. Through a comprehensive and comparitive analysis of relevant legislation, case law, and regulatory frameworks, this paper aims to elucidate the legal remedies accessible to victims in India. It explores the roles of various stakeholders including law enforcement agencies, regulatory bodies, and financial institutions in mitigating the impact of such cybercrimes. Furthermore, this study provides practical insights and recommendations to enhance the efficacy of legal recourse for victims, fostering a safer digital environment in India. The findings of this research are instrumental in augmenting the existing legal framework and strengthening the mechanisms to combat cyber threats effectively.

Keywords: Phishing attacks, legal remedies, awareness, comparative study.

2. INTRODUCTION :

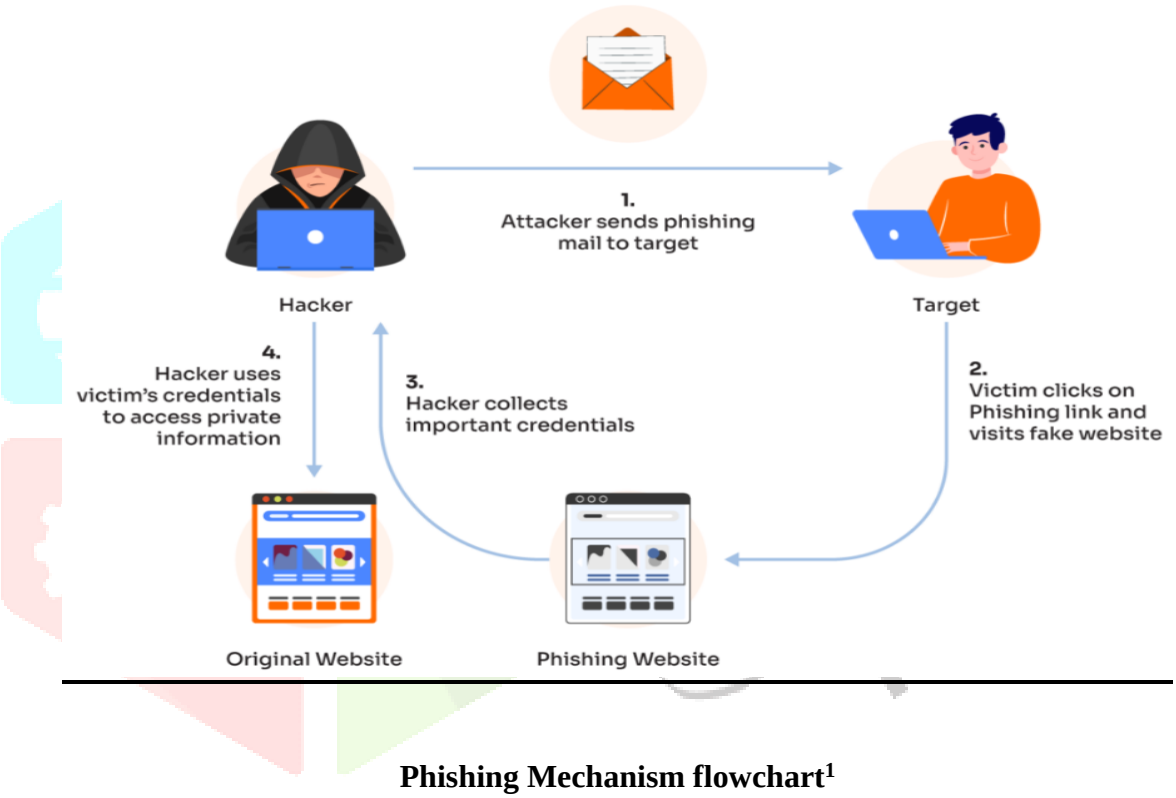
The Internet provides a phenomenal medium for communication among regular people. Today's networks are seeing a sharp rise in social engineering assaults, which threaten cybersecurity. To promote the aims of cybercriminals, they seek to influence people and organizations to reveal sensitive and valuable information. Although a network has strong firewalls, encryption techniques, intrusion detection systems, or anti-virus software, social engineering poses a threat to network security. Compared to computers or other technology, humans are more inclined to trust other humans. They are the weakest link in the security chain as a result. Malicious acts carried out through interpersonal interactions psychologically coerce a person into disclosing private information or violating security protocols. Criminal minds have discovered a means to steal personal data with the least chance of detection and without really meeting the victim. It is called Phishing. Phishing websites, emails, advertisements, scareware, antivirus software, PayPal websites, prizes, and freebies are all involved. An example of an attack may include receiving a call or email from a fictitious lottery department claiming to be the winner of a large quantity of money and asking for personal information, or it could involve clicking on a link that is attached to the emails. Phishing is a danger to the e-commerce sector. Customers' trust in e-commerce is not only damaged, but electronic service providers suffer severe financial losses as a result. For this reason, understanding phishing is crucial. This paper describes an analysis of Phishing Attacks in India and some methods to prevent phishing.

3. HOW PHISHING WORKS?

A phishing attack is a malicious scheme employed by cybercriminals to deceive individuals into divulging confidential informations.Phishing is described as a deceptive effort, typically conducted via email, with the intention of fraudulently obtaining your personal information. Phishing constitutes a cybercrime tactic designed for online identity theft, with the primary objective of pilfering sensitive data such as online banking passwords and credit card information from unsuspecting users. This malicious strategy involves the creation of deceptive websites that mimic legitimate ones, aiming to extract confidential information from the target and subsequently deliver it to the perpetrator. Victims are often unable to discern between genuine and fraudulent websites, making them susceptible to falling to the phisher's ploy. The phishing process can be outlined in five distinct stages:

- planning
- composing the deceptive email
- executing the attack
- collecting the obtained data, and
- ultimately perpetrating fraud.

The initial step involves the attacker strategizing the assault, determining both the authentic website to be replicated and the intended victim from whom information is to be obtained. Subsequently, the attacker crafts an email designed to appear authentic, enticing the victim into providing their personal data. Once the email is sent to the target, the victim's susceptibility to distinguishing between genuine and phishing correspondence leads them to open the email. The email then directs them to the deceptive website, where they unknowingly input their login credentials. The phishing site subsequently forwards these credentials to the attacker, as depicted in the fourth step. In the final phase, armed with the victim's data obtained from the phishing website, the attacker gains unauthorized access to the target's accounts, enabling them to engage in cybercrimes such as bank /ATM card fraud or theft.



Phishing Mechanism flowchart[1]

3.1 TYPES OF PHISHING :

Deceptive phishing

Deceptive phishing stands as the most prevalent form of phishing attack. In this method, cybercriminals replicate a legitimate website and dispatch an email to the target, meticulously designed to appear authentic. Within the email, there is a malicious URL or link, guiding the individual to engage in a particular activity. Once the instructions are followed, the fraudulent website covertly captures all login credentials and other sensitive data, subsequently delivering it into the hands of the attacker.

[1] Kumar, B. (2023, September 15). *What is Phishing Attack in Cyber Security - Complete Guide*. Simplilearn.com, https://www.simplilearn.com/tutorials/cryptography-tutorial/what-is-phishing-attack

Spear Phishing

Spear phishing closely resembles deceptive phishing, with a crucial distinction lying in the specific target selection. Unlike deceptive phishing, spear phishing is highly targeted, focusing on a single individual. The perpetrator personalized their strategy to appeal specifically to the targeted individual, aiming to allure them into disclosing sensitive information. The culprits customize the email by including specifics about the recipient, like their name, company affiliation, position, and additional details. Spear phishing often leverages social media platforms, notably LinkedIn, as a readily accessible database of professional details regarding the individual or the entity being the targets. This allows the attacker to shape a message that exudes enhanced credibility and reliability making it more persuasive to the intended recipient.

Whaling

Whaling attacks are a specialized type of attack which particularly attacks high-ranking individuals, such as Directors of the company, CEOs or other executives. The attacker invests significant time in profiling the victim before launching the attack. Like other phishing techniques, the attacker sends an email to the target, aiming to deceive them into divulging sensitive information. Whaling attacks are particularly perilous because executives often possess access to an organization's most sensitive and confidential data. This makes them prime targets for cybercriminals seeking to gain unauthorized access to critical information.

Pharming

Pharming is a distinct variant of phishing that sets it apart from other techniques. Unlike other methods, pharming does not require specific individual targeting. Instead, it has the potential to victimize a large number of people without the need for individualized focus.

These are the two basic methods of executing a pharming attack:

- The first approach involves sending a code to the target via email. This code alters the local host files on the system. Consequently, URLs are converted into numerical strings, a format utilized by the system to access websites. This manipulation results in redirecting the target to a malicious site, even if they enter the accurate URL, as the code transforms URLs into numerical strings, a format the system employs to reach websites.
- The second method employs a technique known as DNS Poisoning. As a result, the target is redirected to malicious websites without their awareness. They may believe they are accessing legitimate sites, but due to DNS Poisoning, they end up on a malicious website.

Link Manipulation

Link Manipulation is a type of phishing attack where the attacker sends a link to a counterfeit or malicious website. Upon clicking the link, the user is directed to the phisher's website instead of the legitimate site indicated in the link. To safeguard against falling victim to link manipulation, users can hover their mouse over the link to preview the actual web address.

Voice Phishing

Voice phishing, often referred to as "vishing," is a kind of criminal attack conducted through phone communication. This technique relies on social engineering tactics and exploits telephone systems to illicitly access an individual's personal and financial information for fraudulent purposes, particularly in the realm of financial transactions and activities.

Smishing

Smishing involves exploiting SMS or text messages as a type ofPhishing attack, wherein the messages might contain links to websites, email addresses, or phone numbers. Clicking on these links can trigger actions like opening a web browser or email client, or initiating a phone call.

Man-In-The-Middle Phishing

The Man-In-The-Middle Phishing, or MITM, represents a phishing technique where attackers interpose themselves between two parties, typically the user and the genuine website. The purpose is to block dispatches from both parties and excerpt information. In this scenario, the messages intended for the legitimate recipients are redirected to the assaulter. The attacker records this information for later misuse. The assaulter records this information for after abuse. Different ways, including DNS spoofing, URL obfuscation, Address Resolution Protocol(ARP) poisoning, and Trojan keyloggers are employed to deflect the stoner to a vicious server in an MITM attack.

Search Engine Phishing

In this method of phishing, the attacker designs malicious websites featuring enticing offers and employs Search Engine Optimization (SEO) strategies to ensure their legitimate indexing. Consequently, these websites show up for those looking for goods or services-a tactic known as
black hat SEO.

4. BACKGROUND OF THE STUDY/SIGNIFICANCE OF THE AREA :

Cyber threats are increasing globally due to the widespread use and growth of the internet and the development of digital technology. Phishing attacks have become the most persistent and sneaky types of cybercrime among the other dangers. With its rapidly growing digital economy, India has emerged as a top target for phishing scams. The nation has seen a concerning increase in phishing events over the last ten years across a variety of industries. Phishing is a serious danger to the e-commerce sector. Customers' trust in e-commerce is not only damaged, but electronic service providers suffer severe financial losses as a result. For this reason, understanding phishing is crucial. This paper provides awareness of phishing scams and the victims' legal options. People are also informed through various advertisements, but there is not much difference. And this is because of digital literacy.

Cybercriminals are enticing individuals to readily extract secretive and sensitive details from the users by preying on people's lack of digital literacy. Phishing attacks are carried out via email and phone calls in addition to websites. Cybercriminals pose as an official authority to get information from individuals. Google bans hundreds of phishing websites annually, but the number is rising.

Past Implications:

In the past, India has grappled with a surge in phishing attacks, resulting in substantial financial losses and compromised data security. Notable incidents have included large-scale data breaches, fraudulent financial transactions, and breaches of sensitive government information. The impact of these attacks has reverberated through the economy, affecting both public and private sectors. When we talk about scams and fraud, India no longer sits back.

In the past two decades, there have been major online scams like the Freedom 251 mobile scam of 2016, OLX scams, online discount scams, etc. The largest negative aspects of scams such as online item sales are usually associated with online transfers. These days, the primary venues for online scams are intermediate, or broken types, websites, and applications like OLX or Faster. These showcase a few real estate items at incredibly low rates, as well as moveable items like LCD or LED TV cameras. The irony of these ads is that, although the seller's location is indicated as being in the local area, it is not. The sellers are located far away. The vendors describe themselves as busy professionals who work 1,000 miles away when contacted. They will request a payment transfer into their account in advance if we get in touch with them to purchase some goods. A few succumb to their allure, driven by their avarice to purchase goods at reduced prices. And it is the entire workings of the selling deception. Other kinds of scams are carried out in India.

During COVID-19, Scammers took full advantage of the epidemic to perpetrate a sharp rise in fraud. Many people became victims of the numerous false schemes that con artists created under the guise of the Indian or State governments. Furthermore, individuals on social media continue to forward things without hesitation, adding fuel to the flames. Whenever we receive a message on WhatsApp about a phony scheme, we frequently notice that it says ―Forwarded many times. This allows us to determine the approximate number of persons who must have forwarded the message to us.

Present Implications:

As of the present date, the digital realm in India remains under the persistent menace of phishing attacks.The existing legal framework in India, including the IT Act, of 2000, and subsequent amendments, forms the cornerstone of the country's response to cybercrimes, including phishing. However, the practical application and enforcement of these laws remain a subject of scrutiny.

Future Implications:

Different countries have varying legal systems, approaches to cybercrime, and levels of technological infrastructure. These differences can lead to disparities in how victims are protected and perpetrators are prosecuted. Given the rapid pace of technological advancement and the increasing sophistication of cyber threats, understanding and strengthening legal remedies for phishing attacks is of paramount importance for India's cybersecurity landscape.

5. RESEARCH PROBLEM:

The increasing prevalence of email scams and phishing attacks poses a significant threat to persons and institutions, raising critical concerns about the legal remedies available to victims in the aftermath of such cybercrimes. This study aims to comprehensively analyze the existing legal framework in India and in other countries furthermore, this paper tries to make a comparative analysis and finally conclude whether Indian laws are effective in dealing with phishing attacks or not.

6. RESEARCH METHODOLOGY:

The researcher would be using a doctrinal methodology which includes a depth analysis of an existing object. The research will gather essential data through the utilization of both primary and secondary sources.

7. RESEARCH QUESTION:

1. What causes led to the development of phishing, and how would Indian and other countries' laws address phishing?
2. "Are the existing legal remedies for victims of phishing and email scams effective in India compared to other countries, and to what extent do they mitigate the impact of cybercrimes?
3. Does India need to implement new legal frameworks or enhance existing ones to provide more robust protection?"

8. REVIEW AND LITERATURE:

This study exclusively draws upon secondary data, utilizing the listed papers and articles for the evaluation of the current research. The reviewed literature will play a indispensable role in elucidating the present research study, aiding in comprehension, and facilitating the identification of the underlying issue.

1. Solution: Email authentication

Utility: Gmail, Hotmail, Yahoo

Approach: Authenticate by password hashing with domain name

Limitation: Most users do not use email authentication.[2]

2. Solution: User Education-based Approach

Utility: Assess the effectiveness of training materials, online tests, embedded training approaches, etc.,

Approach: Use of short training materials will enable users to read immediate training after a person becomes a phishing victim.

[2] Adida, B., Hohenberger, S., & Rivest, R.L. (2005). Fighting Phishing Attacks: A Lightweight Trust Architecture for Detecting Spoofed Emails.

Limitation: Participants were more educated than the average Internet users.[3]

3. Highlighted the steps and efforts in the fight against phishing. A crew conforming of some members made these works and conducted different mindfulness sessions and works for internet druggies to encourage the use of anti-phishing ways and make them mindful of using everything on the internet. They concluded that to combat phishing attacks, mindfulness sessions should be ongoing. [4]

4. In this research paper, the author analyzes the various kinds of phishing methods such as email phishing, social media phishing, link manipulation, social engineering, spear phishing, whaling, smishing, IDN spoofing, search engine phishing, vishing and the most recent one cryptocurrency phishing as well as how phishing attacks operate and why it's the most popular type of cybercrime.[5].

5. Musuva *et al.* conducted experiments to detect whether users are vulnerable to social engineering attacks, especially phishing attacks. The experiment was conducted at a university in Kenya. Musuva *et al.* sent random phishing emails to users at the university. As many as 31.12% of users are vulnerable to phishing.[6]

6.The paper delves into an in-depth exploration of phishing attacks, encompassing a comprehensive examination of their history and the underlying motivations driving attackers. Achieving precise detection of phishing attacks has long been a pivotal area of concern. Recent advancements in detection techniques have ushered in a range of novel approaches, specifically tailored to enhance accuracy in identifying phishing attempts. Given the diverse methods employed in executing such attacks, it becomes evident that a singular solution is insufficient in effectively combating this pervasive issue.[7]

---

[3] Kumaraguru, P. (2008, October). Lessons From a Real World Evaluation of Anti-Phishing Training. *2008 eCrime Researchers Summit*. 10.1109/ECRIME.2008.4696970

[4] Moul, K. A. (2019, October). *Avoid Phishing Traps*. ResearchGate. https://www.researchgate.net/publication/336857093_Avoid_Phishing_Traps

[5] Richter, F. (2022, May 18). *The Most Common Types Of Cybercrime*. statista. https://www.statista.com/chart/24593/most-common-types-of-cyber-crime/#:~:text=According%20to%20a%20recent%20FBI,common%20type%20of%20cyber%20crime

[6] Musuva, P., Chepken, C., & Getao, K. (2019). A Naturalistic Methodology for Assessing Susceptibility to Social Engineering Through Phishing. *The African Journal of Information Systems*, *11*(3). : https://digitalcommons.kennesaw.edu/ajis/vol11/iss3/2

[7] Gupta, B.B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2016, March 17). *Fighting against phishing attacks: state of the art and future challenges*. ResearchGate. https://www.researchgate.net/publication/298908229_Fighting_against_phishing_attacks_state_of_the_art_and_future_challenges

9. CURRENT ISSUES AND CHALLENGES :

Numerous ways to prevent phishing assaults have been provided in the literature review; nevertheless, we discovered that no one method can be considered "bulletproof" against phishing. Phishing is increasingly being used as a means of committing online crimes. The moment researchers discover a way to identify and stop phishing attempts, phishers immediately adapt their attack plan by taking advantage of flaws in the available defense. Thus, we might conclude that there is a dynamic race between researchers and phishers. To the best of our knowledge, there isn't a comprehensive literature review that addresses social engineering assault prevention; this research fills the gap.

Multiple security strategies have been suggested to guard the IoT terrain, yet there's a notable absence of approaches specifically designed for relating spam and phishing emails within this environment. Despite the current use of encryption in numerous approaches, the vulnerability lies in the fact that IoT devices warrant protection from constant anti-spam oranti-virus software. Accordingly, addressing IoT attacks at their source point becomes grueling . This decentralized nature of attacks on IoT devices contributes to the success of vicious emails insinuating inboxes.

10. STATISTICAL DATA:

WORLDWIDE:

Recently, scammers have capitalized on the COVID-19 pandemic to deceive their targets. Exploiting people's anxieties about contracting the virus, attackers have circulated numerous scam messages with a Coronavirus theme. These messages prey on individuals' fears and the urgency to seek information related to COVID-19, including scams related to Personal Protective Equipment (PPE) like facemasks. The World Health Organization (WHO) has acknowledged the creation of an Infodemic due to COVID-19, providing a favorable environment for phishing activities. Moreover, cybercriminals have solicited individualities to open attachments by falsely claiming they contain information about original entities with COVID- 19.

- According to a report by Zscaler ThreatLabz, "*phishing attacks increased by 47.2% in 2022 compared to the previous year. The report also highlights that education was the most targeted industry in 2022, with attacks increasing by 576%, while the retail and wholesale sector dropped by 67% from 2021*".[8]
- Another report by CNBC states that *"there was a 61% increase in the rate of phishing attacks in the six months ending October 2022 compared to the previous year. The report also notes that phishing attacks are getting more sophisticated and are spreading beyond emails to text messages and other forms of personal communication".*[9]

[8] Zscaler ThreatLabz. (2023, April 18). *2023 Phishing Report shows 47.2% more attacks*. Zscaler from https://www.zscaler.com/blogs/security-research/2023-phishing-report-reveals-47-2-surge-phishing-attacks-last-year

[9] CNBC. (2023, January 7). Phishing attacks are increasing and getting more sophisticated. Here's how to avoid them. *CNBC*. https://www.cnbc.com/2023/01/07/phishing-attacks-are-increasing-and-getting-more-sophisticated.html

- Cybersecurity firm Kaspersky's report states that "*in the year 2021-2022, Cryptocurrency phishing was 3,596,437 in the year 2021 and increased by 5,040,520 in 2022".*[10]

INDIA:

- According to reports released by Subsex in 2019, *"India beat the USA and became the country with the Highest Cyberattacks in 2019. This has alarmingly increased after the outbreak of the COVID-19 pandemic in 2020".*[11]
- According to a survey by Local Circles, *"42% of Indians surveyed said they or someone in their family has been a victim of financial fraud in the last three years. In the instances of bank account fraud, fraudulent activities by transient eCommerce operators, and credit and debit card frauds rank high among the frauds encountered during this period. Out of the households that fell victim to financial fraud in the past three years, a mere 17% successfully recovered their funds, leaving a substantial 74% without any resolution".*
- A report from Bhagwad Kharad, minister of state for finance in Rajya Sabha states that *"over 9 Lakh incidents of Phishing and vishing attacks have been reported in the last two years and customers have collectively lost nearly Rs.1500 crore due to such incidents between Apr 2020- Mar 2022".*[12]
- According to the FTC (Federal Trade Commission) 2022 report, "*there was an increase in messaging scams between 2021-2022. India increased by 9 %".*
- Norton Life Lock's global research team report states that "*Over 1.5 crore Phishing attacks via social media cases were encountered between April 2022- July 2022".*[13]
- Harshil Doshi, Country Manager (India and SAARC) at - Securonix 2023 Threat Report observed that *"phishing emails, SSH honeypot activity, and RAT tools increased by 62 % in the period 2022-2023".*[14]

[10] Kaspersky. (2023, March 29). *Cryptocurrency phishing grows by 40 percent in one year*. Kaspersky. https://www.kaspersky.com/about/press-releases/2023_cryptocurrency-phishing-grows-by-40-percent-in-one-year

[11] Mihindukulasuriya, R. (2020, March 3). *India was the most cyber-attacked country in the world for three months in 2019*. ThePrint. https://theprint.in/tech/india-was-the-most-cyber-attacked-country-in-the-world-for-three-months-in-2019/374622/

[12] Chadha, S. (2022, August 5). *Over 9 lakh incidents of phishing, OTP compromise reported in last two years; 42% Indians have experienced financial fraud - Times of India*. The Times of India. https://timesofindia.indiatimes.com/business/india-business/over-9-lakh-incidents-of-phishing-otp-compromise-reported-in-last-two-years-42-indians-have-experienced-financial-fraud/articleshow/93361388.cms

[13] Norton Life Lock's Global Research Team. (2022, July 27). *India saw over 1.5 crore social media phishing attacks in Q2*. ET CISO. https://ciso.economictimes.indiatimes.com/news/india-saw-over-1-5-crore-social-media-phishing-attacks-in-q2/93153430

[14] *Reports show 62% jump in phishing attacks last year*. (2023, August 16). The Hindu Business Line.https://www.thehindubusinessline.com/info-tech/reports-show-62-jump-in-phishing-attacks-last-year/article67201918.ece

11. Phishing is still successful:

In general, as hackers create increasingly complex ways to get past barriers, cyberattacks are generally getting riskier. This reflects the continued success and risk of phishing. Criminals may rent new phishing attack types, including "EvilProxy," on a subscription basis. The ability of EvilProxy to evade multi-factor authentication increases the likelihood of data breaches even in the presence of strong security measures.

11.1 **These are the major factors that cause an increase in Phishing in India:**

- Lack of Awareness among the Public:

  Worldwide, particularly in India, there has been a lack of knowledge regarding phishing attacks among the common public. People (users of the internet) are unaware that their personal information is actively being targeted by attackers and they are not undertaking proper precautions when they conduct online activities.

- Lack of Awareness regarding Policies:

  The fraudsters constantly count on the victim's incognizance of Bank/ fiscal institution programs and procedures for reaching guests, particularly for issues relating to account conservation and fraud inquest. Individuals unaware of the protocols of an online sale are prone to falling victim to the social engineering aspects of a phishing scheme, regardless of its technical complexity.

- Technical Sophistication:

  Criminals are employing sophisticated technology, previously effective in activities like denial of service , spam, and electronic surveillance, for fraudulent purposes. Indeed as guests are getting apprehensive of phishing, Attackers are developing ways to fight this mindfulness. These methods involve using URL obfuscation to enhance the legitimacy of emails and websites used for phishing. Additionally, cyber attackers exploit vulnerabilities in web browsers, enabling the downloading and execution of malicious code from a hostile website.

- Rapidly Evolving Technology:

  Technology evolves quickly, and cyber criminals adapt their tactics. Legislation might struggle to cope with the pace of technological advancements, making it challenging to cover all possible attack vectors.

12. Legal framework:

12.1. USA:

The Federal Trade Commission (FTC) in the United States (Jan 2004) is the nation's consumer protection agency and takes reports about scammers who cheat people out of money and businesses that don't make good on their promises. The Bureau of Consumer Protection at the FTC prevents unfair, deceptive, and fraudulent business practices by gathering consumer reports, initiating investigations, and taking legal action against individuals and companies that breach the law. The FTC also releases an annual report with information about the number and type of reports they receive. Subsequently , the ''Anti-Phishing Act'' was introduced in the US Congress in March 2005.

The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 regulates the frauds or any attacks committed on the federal computer system or any banks, interstate having access to sensitive information relating to foreign commerce and international trade.

Cybersecurity Information Sharing Act (CISA) -The act was introduced in 2015 to enable the sharing of cybersecurity concerns between different federal agencies. Its main aim was to build a strong cyber infrastructure by allowing prompt sharing of cybersecurity difficulties, glitches, and any other concerns between different agencies of the government.

California Anti-Phishing Act 2005 (Business & Professions Code 22948):

This law prohibits "phishing," the act of posing as a legitimate company or government agency in an email, Web page, or other Internet communication to trick a recipient into revealing his or her personal information.

California became the first state in the USA to pass an anti-phishing law:

Business and Professions Code Division 8, Chapter 33 provides the Anti-Phishing Act of 2005, which is contained in Sections 18400 to 22949.51.

Section 22948.1 outlines definitions for key terms including "electronic mail message," "identifying information," "Internet," and "web page."

Section 22948.2 prohibits any individual from, through a web page, electronic mail message, or any other means via the Internet, enticing another person to provide identifying information by falsely presenting themselves as a business without proper authorization or approval.

Section 22948.3 grants specific individuals the authority to take legal action against those who violate the aforementioned section. Such actions may seek to recover either actual damages or $500,000, whichever is greater. Furthermore, the Attorney General or a district attorney retains the right to initiate legal proceedings against individuals in violation of this section, seeking both an injunction against further violations and a civil penalty of up to $2,500 per violation.[15]

[15] *California Anti-Phishing Act – California Globe*. California Globe. https://californiaglobe.com/articles/california-anti-phishing-act/

12.2.INDIA: In India, there are laws such as the Information Technology Act, of 2000, and the Indian Penal Code, of 1860, which provide remedies for phishing attacks. Victims of phishing scams can bring a fraud action against a defendant who intentionally deceives them. The provisions that have been incorporated and regulate the crime of phishing under the
IT Act 2000 are :

- Section 43 – extracting or accessing data without consent
  Section 43 stipulates that if an individual accesses another person's computer system or network to download, access, disrupt, deny,or corrupt the data contained therein, without the consent of the owner – then that person may be held liable under this provision.
- Section 66 of the Act outlines penalties for phishing, prescribing punishment for perpetrators who unlawfully access a victim's account. The penalties may involve imprisonment for up to three years, a fine exceeding five lakh rupees, or a combination of both, depending on the gravity of the offense.
- Under Section 66C, the use of unique identification features such as passwords or electronic signatures is prohibited. Phishers engage in fraudulent activities by posing as legitimate account owners and executing deceptive actions.
- Section 66D addresses impersonation-related offenses, encompassing cheating through the use of communication devices or computer resources. Fraudsters engage in deceptive practices by impersonating banks and other entities, utilizing URLS that redirect customers to counterfeit versions of official websites. creating a false association with the genuine organization.

Additionally, the Indian Penal Code,1860 contains the following provisions under which an individual can be held liable for the crime of phishing:

- Theft under Section 378 and 379
- Criminal breach of trust under Section 405 and 406
- Cheating under Section 415 to 419
- Mischief under Section 425 and 426, and
- Forgery under Sections 463 – 465, and Sections 467-477.

Digital Data Protection Act,2023

In response to the escalating threat of data breaches, the Digital Data Protection Act of 2023 has been introduced in India. The primary objective of this act is to regulate the processing of digital personal data, ensuring individuals' rights to protect their data while acknowledging the lawful necessity of data processing. The Act becomes crucial in light of recent incidents, such as the hacking of personal data on the CoWIN portal, leading to the public exposure of vaccinated users' information on platforms like

Instagram. The introduction of the Digital Data Protection Act aims to prevent such consequences by establishing a framework for safeguarding digital personal data.

BOARD:

CERT (Computer Emergency Response Team) 2008 under section 70B was established. The Function of this board is to take action in case of cyber attacks. It operates under the Ministry of Electronics and Information Technology (MeitY) and serves as the nodal agency for coordinating cybersecurity efforts across various sectors. CERT-In plays a crucial role in addressing various cyber threats, including phishing attacks, in India. It provides advisory, early warning, and incident response services to government departments, critical infrastructure sectors, and other organizations.

Nasscom vs. Ajay Sood (2005)

In a landmark judgment in the case of the National Association of Software and Service Companies vs Ajay Sood & Others, delivered in March, '05, the Delhi High Court declared `phishing' on the internet to be an illegal act, entailing an injunction and recovery of damages.

The legal framework does not provide a specific meaning for the term phishing. However, in this case, phishing was initially characterized as "*a kind of internet fraud where an individual pretends to be a legitimate entity, like a bank or insurance company, with the intention of soliciting personal information from a customer, including access codes, passwords, and other confidential data.*"

12.3.CANADA:

In Canada, the Canadian Anti-Fraud Centre (CAFC) serves as the primary organization responsible for gathering information and insights on identity theft and fraud. The CAFC offers assistance and tools to individuals who have fallen victim to fraud and collaborates with law enforcement entities to scrutinize and bring legal action against those engaged in fraudulent activities.

Canada's anti-spam law (CASL)

CASL, a federal law instituted in 2014, aims to safeguard individuals and businesses from the exploitation of digital communication channels like emails and SMS. Its primary purpose is to reinforce ethical practices in email marketing, combat spam, and regulate all forms of Commercial Electronic Messages (CEMs). CASL addresses various issues, including appropriation, phishing and the passing of malicious software such as viruses and trojans (malware).

The impact of this legislation has been notably positive. In 2014, when CASL came into effect. Canada was home to seven of the world's top 100 spamming organizations. However, by 2019 and up to the present date, there are no Canadian organizations listed among the top spammers globally.

12.4.AUSTRALIA: Australia has the Australian Cyber Security Centre (ACSC), which provides advice and assistance to persons and institutions to help them guard themselves from cyber threats, including phishing attacks.In addition, the ACSC collaborates with law enforcement organizations to look into and prosecute cybercrime.

Phishing emails would be illegal under the *Spam Act 2003* (Cth), which came into effect on 10 April 2004. Under this Act, it is illegal to send, or cause to be sent, 'unsolicited commercial electronic messages' that have an Australian link.While the Act prohibits unrequested messages, and it does provide a pathway for businesses to send commercial electronic messages legitimately. The Act mandates that all commercial electronic messages must contain specific, explicit and precise information about the sender.

The *Criminal Code Act 1995* (Cth) has various offenses that criminalize phishing u/s 134.2, 135.1(1), 135.1(5), 478.1, 477.3, 480.4

13. MEASURES AND RECOMMENDATIONS:

Multi-Factor Authentication (MFA):

MFA enhances security by demanding multiple authentication methods (e.g., password, fingerprint, OTP) to validate a user's identity. Authentication and authorization are pivotal defenses against phishing, ensuring the legitimacy of a person. This thwarts phishers from infiltrating protected resources and executing their attacks. Authentication comes in three forms: single-factor, requiring only a username and password; two-factor, necessitating additional information like an OTP sent to the user's email or phone; and multi-factor, utilizing a combination of knowledge, biometrics, and possession. Authorization methods, such as API authorization, enable system access for previously generated APIs.

Human Education:

Education of individuals is a highly effective preventive measure against phishing attacks. The proposed methodology emphasizes awareness and human training as the initial line of defense in combating phishing, acknowledging that while it may not guarantee absolute protection, it remains a crucial component. Educating end-users diminishes their vulnerability to phishing attacks and serves as a valuable supplement to other technical solutions. The current training for phishing detection is insufficient to counter the sophistication of contemporary attacks.

Moreover, certain security experts argue that user education lacks effectiveness because security is not the primary concern for users, and they lack motivation to self-educate on phishing.

Furthermore, the majority of phishing training programs primarily concentrate on instructing individuals on recognizing and steering clear of phishing emails and websites, often neglecting other equally threatening types of phishing, such as voice phishing and malware or adware phishing. Effective user training should encompass three key aspects: firstly, conducting awareness training through seminars or online courses, targeting both

organizational employees and individuals. Secondly, implementing mock phishing attacks to assess users' vulnerability and thirdly, enable them to evaluate their own understanding of phishing.

Continuous Monitoring and Threat Intelligence:

Employing tools and services that provide real-time threat intelligence to stay informed about the modern phishing tactics and trends.

Security Awareness Training:

Ongoing education and training for employees and individuals on recognizing phishing attempts and best practices for online security.

Global Co-operation:

Given the global scope of cybersecurity risks, it could be challenging for one country to combat them on its own. Information systems also transcend national borders and are heavily networked. Therefore, nations must work together to create and implement shared resilience initiatives.

Reporting:

Many times cases of cyber crime are never reported. This may be because there is lack of implementation authority and lack of awareness about the laws about cybercrime. This has to do with creating, enforcing, and raising public awareness of pertinent legislation. It should be mandatory to notify each instance of cyberattack to the cyber cells in order to provide investigators with an accurate understanding of the scope and occurrence of these crimes. In the end, this would open their path to greater comprehension.

End-user perspective:

Cyberattacks have an immediate impact on information technology end users. Therefore, in these kinds of situations, the end user's perspective is crucial. As a result, any legal requirement should be implemented with their viewpoint in mind. It is necessary to provide a technique to ascertain the end user's perspective.

14. SCOPE AND LIMITATION:

This research tells how existing legal remedies address the Obstacles encountered by those who have fallen prey to phishers' attacks and email scams under social engineering, considering the dynamic nature of cyber threats and jurisdictional complexities. In this research paper, I have tried to focus on social engineering, especially phishing attacks, its types, the Indian legal framework and comparative analysis with other countries. This article may touch on any other laws, rules, or regulations of the other countries but will not deal with them deeply. It will contain some cases from India but there is no period limit for the cases.

15. CONCLUSION:

Cybercriminals will continue to evolve their strategies in tandem with technology. Proactive measures, including enhanced legislation, robust cybersecurity infrastructure, and widespread awareness campaigns, are imperative in mitigating the future outcome of phishing attacks in India. People are also informed through various advertisements, but there is not much difference. And this is because of digital literacy. According to a comparative

analysis of other countries' laws and Indian laws against phishing attacks, India's IT Act of 2000 provides specific provisions against cybercrime, including phishing. The act punishes fraudulent or dishonest use of electronic signatures, passwords, or any other unique identification feature, and using a computer resource for cheating, with imprisonment and a fine. Phishing may also be prosecuted under the Indian Penal Code (IPC) as forgery, cheating by personation, and cheating and dishonestly inducing the delivery of property . The Indian legal framework is sufficient to address these cyber threats but the main reason why still phishing attacks are successful is due to lack of awareness among the public about the policies and rules. While educating individuals remains a highly effective defense against phishing, completely eliminating the threat proves challenging given the sophisticated nature of these attacks and the involvement of social engineering elements. Although ongoing awareness training against phishing attacks and email scams is crucial for preventing phishing attacks and minimizing their impact, it is equally imperative to develop effective anti-phishing techniques that proactively shield users from exposure to such attacks. Therefore, it should be the permanent goal of authorities and legislators to guarantee that laws controlling technology include all relevant aspects and concerns linked to cybercrime and continue to expand healthily and continuously in order to maintain ongoing oversight over associated crimes. This research aims to increase understanding of the issues contributing to phishing and to provide solutions for mitigating phishing attacks, which stand as significant threats to digital information security.

REFERENCES:

1. Kumar, B. (2023, September 15). *What is Phishing Attack in Cyber Security - Complete Guide*.Simplilearn.com.https://www.simplilearn.com/tutorials/cryptography-tutorial/what-is-phishing-attack
2. Yadav, D. A. (2021, August). PHISHING IN INDIA – ANALYTICAL STUDY. *International Advanced Research Journal in Science, Engineering and Technology*, *8*(8). 10.17148/IARJSET.2021.88110
3. Adida, B., Hohenberger, S., & Rivest, R.L. (2005). Fighting Phishing Attacks: A Lightweight Trust Architecture for Detecting Spoofed Emails.
4. Kumaraguru, P. (2008, October). Lessons From a Real World Evaluation of Anti-Phishing Training. *2008 eCrime Researchers Summit*. 10.1109/ECRIME.2008.4696970
5. Moul, K. A. (2019, October). *Avoid Phishing Traps*. ResearchGate. https://www.researchgate.net/publication/336857093_Avoid_Phishing_Traps https://www.researchgate.net/publication/336857093_Avoid_Phishing_Traps
6. Richter, F. (2022, May 18). *The Most Common Types Of Cybercrime*. statista. https://www.statista.com/chart/24593/most-common-types-of-cyber-crime/#:~:text=According%20to%20a%20recent%20FBI,common%20type%20of%20cyber%20crime
7. Musuva, P., Chepken, C., & Getao, K. (2019). A Naturalistic Methodology for Assessing Susceptibility to Social Engineering Through Phishing. *The African Journal of Information Systems*, *11*(3). : https://digitalcommons.kennesaw.edu/ajis/vol11/iss3/2
8. Gupta, B.B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2016, March 17). *Fighting against phishing attacks: state of the art and future challenges*. ResearchGate.

https://www.researchgate.net/publication/298908229_Fighting_against_phishing_attacks_state_of_the_art_and_future_challenges

9. Zscaler ThreatLabz. (2023, April 18). *2023 Phishing Report shows 47.2% more attacks*. Zscaler.https://www.zscaler.com/blogs/security-research/2023-phishing-report-reveals-47-2-surge-phishing-attacks-last-year
10. CNBC. (2023, January 7). Phishing attacks are increasing and getting more sophisticated. Here's how to avoid them. *CNBC*. https://www.cnbc.com/2023/01/07/phishing-attacks-are-increasing-and-getting-more-sophisticated.html
11. Kaspersky. (2023, March 29). *Cryptocurrency phishing grows by 40 percent in one year*. Kaspersky. https://www.kaspersky.com/about/press-releases/2023_cryptocurrency-phishing-grows-by-40-percent-in-one-year
12. Mihindukulasuriya, R. (2020, March 3). *India was the most cyber-attacked country in the world for three months in 2019*. ThePrint. https://theprint.in/tech/india-was-the-most-cyber-attacked-country-in-the-world-for-three-months-in-2019/374622/
13. Chadha, S. (2022, August 5). *Over 9 lakh incidents of phishing, OTP compromise reported in last two years; 42% Indians have experienced financial fraud - Times of India*. The Times of India. https://timesofindia.indiatimes.com/business/india-business/over-9-lakh-incidents-of-phishing-otp-compromise-reported-in-last-two-years-42-indians-have-experienced-financial-fraud/articleshow/93361388.cms
14. Norton Life Lock's Global Research Team. (2022, July 27). *India saw over 1.5 crore social media phishing attacks in Q2*. ET CISO. https://ciso.economictimes.indiatimes.com/news/india-saw-over-1-5-crore-social-media-phishing-attacks-in-q2/93153430
15. *Reports show 62% jump in phishing attacks last year*. (2023, August 16). The Hindu BusinessLine. https://www.thehindubusinessline.com/info-tech/reports-show-62-jump-in-phishing-attacks-last-year/article67201918.ece
16. Micheli, C. (2022, July 12). *California Anti-Phishing Act – California Globe*. California Globe. https://californiaglobe.com/articles/california-anti-phishing-act/
17. Venkatesha, S., Reddy, K. R., & Chandavarkar, B. R. (2021, Feb). Social Engineering Attacks During the COVID-19 Pandemic. *National Library of Medicine*. 10.1007/s42979-020-00443-1
18. Gupta, D. R., & Agarwal, D. S.P. (2017). A COMPARATIVE STUDY OF CYBER THREATS IN EMERGING ECONOMIES. *An International Journal of Management & IT, 8*. https://globusjournal.com/wp-content/uploads/2018/07/826Ruchika.pdf
19. Gwalani, Y. (2021). Cyber Laws: Comparative Study of Indian and Foreign laws. *CENTRE FOR ACADEMIC LEGAL RESEARCH | JOURNAL OF APPLICABLE LAW & JURISPRUDENC, 1*(1). https://calr.in/wp-content/uploads/2021/04/Cyber-Laws-_-Comparative-Study-of-Indian-and-Foreign-laws.-1.edited.pdf