PHISHING SCAM IN DIGITAL AGE: MECHANISM, IMPACT, PREVENTIVE TECHNIQUES AND REGULATORY FRAMEWORK

Sneha Rastogi, Chandigarh University, Mohali, Punjab

Jayasree Chowdhury, Chandigarh University, Mohali, Punjab

Rupali Saini, Chandigarh University, Mohali, Punjab

ABSTRACT

A phishing attack is one of the popular way to commit fraud and violate people security, it has its own specific characteristics. The attacks have an impact on economy and involve user behaviour that make the attack successful. Most of such attacks are spreading through users' weaknesses and lack of awareness about this concept which makes users weakest element in security chain [1] Many solution framework and program has been developed but fails to eliminate the attacks completely, they just minimized the impact only as there is no single solution for mitigating this completely, so one has to use number of strategies and techniques to mitigate these attacks. Mitigating strategies or techniques may include user education and training to raise awareness among users. This paper includes types of phishing attack and the techniques that are commonly used for such attacks and it provides data about the economic, psychological and financial impact of phishing attack. Furthermore, it provides information about preventive strategies and policies that can be developed and adopted with the regulatory framework established by the government. The primary goal of this paper is to comprehend various forms of phishing attacks, which encompass different methods through which a user can fall prey to these attacks. The consequences of such an attack on the user and the final step is to understand the regulatory framework that aids the victims of these attacks and the preventive measures to ensure safety in the future.

Keywords: *Phishing, economic, financial, mitigating, regulatory framework*

I. INTRODUCTION

In the ever-expanding and evolving digital world, where information is readily accessible online, phishing attacks are on the rise. A phishing attack is an attempt to obtain personal information, such as usernames, passwords, and credit card details, from individuals or businesses [1][3]. Phishing attacks can have severe consequences for their victims, including financial loss, theft of intellectual property, exposure of sensitive customer information, and a general erosion of trust in others. Recently, some of the new methods to trick the user have been adopted by the attackers. These includes filling out a survey form for banking purposes and receiving monetary rewards if the user provides their account information. Additionally, there are emails claiming to be from a hotel reward club, requesting the user to verify their credit card information [2][3]. In today's world, the meaning of phishing has evolved and expanded to include a broader range of financial offenses. In addition to the fake emails and messages that lead to malicious websites and expose the user to enter their personal information, it is observed that there is an increase in the amount of malicious programs or code[3][6]. Once installed on users' devices, these programs employ various techniques to monitor their daily communication and activities, collecting relevant information with the assistance of web sites.

To describe phishing in simple terms:

- The attacker sent an email or some other form of message to the user.
- Victim clicks on that message and is redirected to a phishing website
- Attacker collects personal information of victim
- This information is further utilized by attackers to gain access to websites and manipulate individuals.

II. PHISHING SCAMS AND TYPES

Phishing is type of a cybercrime or security threat that basically target users into divulging there personal information such as credit card number, card verification value (CVV), ATM pins, security number etc. and such attacks are done by sending spoofed emails or messages[5]to the user mostly creating a sense of urgency which motivates them to provide their information.

Various kinds of phishing includes:

a) EMAIL

This is the platform that is most frequently used. In this the attacker crafts an email depicting a bank or some trusted institution and send it to the target users and trick them into revealing their personal information [1]. These emails contains a URL which leads the user to malicious website which is presented same as the original website and any information provided on such website gives attacker the access to such information[10]. Common feature of phishing emails include the sense of urgency which may force you to take action immediately, spoofed email address which looks like the original address, generic greetings, spelling or grammar mistake.

b) SPEAR PHISHING

Spear phishing is a type of email phishing, but in email phishing, the attacker sends the same email to a large number of people, while in spear phishing, the attacker tailors the email to a specific person, organization, or business. Spear phishing is tailored to the individual user and is highly convincing, often executed after closely monitoring their online behavior and gathering information about them[12].

c) WHALING

Whaling is also a targeted attack where the attacker specifically targets high-profile individuals, such as executives, CEOs, or other important figures within an organization [6]. This attack is significantly more damaging as these prominent individuals possess access to the most sensitive and critical data [7].

d) SMS PHISHING

SMS Phishing It is also referred to as Smishing, which is a type of attack where the attacker sends a fake SMS that appears to be from a trustworthy source [13].

e) VOICE PHISHING

It is also known as Vishing, a type of attack where the attacker uses phone calls to deceive the user into divulging their personal information. Scammers often pose as bank representatives, tech support personnel, government officials, or company HR representatives, and occasionally as delivery personnel [5].

f) POP-UP PHISHING

It uses pop up ads, the ads are often about a problem related to one's computer system or something they must be interested in which entices them into clicking on such add, then user id directed to download something or something automatically starts downloading on their device which ends up being a malware [17].

g) DNS- BASED PHISHING

Domain Name System also known as Pharming, the hacker corrupts the DNS of real websites and tricks users into visiting fake websites even if they enter the correct web address and these sites are identical to the real websites [6].

III. FINANCIAL IMPACT OF DIGITAL DECEPTION

The financial impact of digital deception is significant, as scam emails and voice phishing pose a threat to online marketplaces and contribute to cybercrime. The financial impact of digital deception, especially scam emails and voice phishing, is significant and diverse. Phishing scams frequently target both individuals and organizations, resulting in direct financial losses due to unauthorized transactions on bank accounts and the theft of sensitive financial information [4][15]. Voice phishing is a deceptive technique where individuals are deceived into divulging confidential information over the phone, which can result in significant financial losses. Online marketplaces can suffer financial setbacks when scammers exploit them for fraudulent activities, resulting in chargebacks, refunds, and a loss of trust from merchants. Unscrupulous bidding and sales practices can undermine the credibility of auction sites, resulting in financial losses for both sellers and buyers. Companies encounter higher operational expenses as a result of implementing security measures such as multi-factor authentication, encryption, and fraud detection, as well as adhering to regulations for data security and consumer protection. Frequent scams and phishing attempts can erode customer trust and tarnish a brand's reputation, leading to decreased user engagement and market share, and potentially jeopardizing a company's competitive advantage. Fraudulent activities can distort market dynamics, disadvantage legitimate businesses and alter consumer behavior, leading to decreased online spending and increased skepticism towards digital transactions, legal and insurance costs can arise from legal actions such as pursuing or defending against lawsuits related to financial health and potentially increasing. The prevalence of digital deception poses a substantial risk to economic progress, potentially undermining consumer trust in online platforms. Online marketplaces and digital economies may face a temporary decline in activity as a result of higher costs, such as direct losses and operational expenses.

In recent years, the frequency and severity of phishing attacks have increased significantly, leading to substantial financial losses for both individuals and organizations globally. In 2024, the global financial losses caused by cyber-attacks were approximately $17.4 billion, which was a 45% increase compared to the previous year [8]. In India, the financial sector witnessed a significant surge in phishing attacks during the first half of 2024, with over 135,000 such incidents being reported [11]. In last 2 years India has experienced a surge in financial losses due to different cyber frauds, driven by increased digital adoption and evolving cybercriminal tactics as nowadays cybercriminals have employed artificial intelligence to craft more convincing schemes to trick and manipulate people [21].

In financial year 2023-24 there was a high value cyber fraud cases in which the amount was over Rs.1 lakh, resulted in total losses of over Rs.177.05 crore (approximately $20 million) which was almost fourfold increase from the year 2022-23. In the first nine months of financial year 2024-25 (April-December 2024), the reported losses due to these attacks was Rs.107.21 crore and the losses due to cybercrime is projected to reach around Rs.20,000 crore (approximately $2.4 billion) in year 2025[15][21].

IV. SOCIETAL IMPACT

The economic impact of phishing scams remains substantial and continues to ascend as evidenced by way of data from 2024 and early 2025. These scams inflict significant financial damage on individuals, businesses and the broader economy in India and globally.

- **DIRECT FINANCIAL LOSSES-** Individuals in India are increasingly targeted by sophisticated phishing scams that lead to direct monetary losses. Scammers employ numerous tactics, inclusive of faux UPI request, fraudulent banking websites mimicking local institutions and deceptive investment schemes [9]. While specific average loss data of India in 2024 -2025 continues to be rising, global trends suggest attack are significant. For instance, a report indicated that globally individuals lost an average of $136 per phishing incident in 2021, and this figure is likely higher now due to more sophisticated techniques. Considering the increasing digital penetration and use of online financial service in India, these losses may be substantial for victims [11].

- **REPUTATIONAL DAMAGE AND LOSS OF CUSTOMER TRUST**- Indian companies that fall victim to successful phishing attacks and data breaches risk significant reputational damage. This can lead to a loss of customer trust, impacting sales and long- term business viability. In a market driven by trust and relationship, such damage can be particularly severe [14].

- **IMPACT ON DIGITAL ECONOMY IN INDIA**- The prevalence of phishing scams can erode trust in digital transactions and online services in India, potentially hindering the growth of the country‘s burgeoning digital economy initiative like Digital India and UPI [14].

- **INCREASED CYBERSECURITY INVESTMENT** - To combat the growing threat of phishing, Indian organizations are forced to invest more in cyber security infrastructure, employee training programs focused on cyber awareness [including recognizing local scam tactics], and specialized security personnel, these investment, while necessary, represent a significant economic outlay[13].

- **OPERATIONAL DISRUPTIONS AND PRODUCTIVITY LOSS**- Managing phishing attacks and their aftermath consumes considerable amount of time and resources from other crucial business activities that leads to productivity losses.

- **IMPACT ON INVESTOR CONFIDENCE**- Large –scale data breaches resulting from phishing attacks can negatively impact investor confidence in India’s companies and the overall digital infrastructure [15].

- **EMOTIONAL AND PSYCHOLOGICAL COSTS**- Beyond monetary losses, victims of phishing scams often experience exacerbated emotional distress, including feelings of shame, anger, and vulnerability. This can also indirectly impact organizations in India [10][14].

- **FINANCIAL LOSSES-** Indian businesses, from large corporations to SMEs are prime targets for phishing attacks, particularly Business Email Compromise. These attacks result in significant financial fund transfers to scammer-controlled accounts. While specific figure for India in 2024-2025 are being compiled, global data shows that the average loss per BEC incident reached $ 150000 in 2024, given India's growing digital economy, local businesses are increasingly susceptible to such attacks[19].

- **RANSOMWARE ATTACKS-** Phishing remains a primary way for ransom ware to infiltrate India organizations. Successful ransom ware attacks can halt operations, leading to significant downtime and financial losses. Paying ransoms to regain access to data further exacerbates these costs. Globally, phishing in linked to over half of all ransom ware incident and this trend is likely reflected in India as well[13][19].

- **UPI FRAUDS**: Given the widespread adopting of UPI in India, phishing scams targeting UPI users with fake payment requests and QR codes are increasingly common [9].

- **GROWTH OF CYBERCRIME ECOSYSTEM-** Phishing fuels the cybercrime economy in India and globally, with malicious actors developing and selling sophisticated tools and service to facilitate these attacks [20].

V. PREVENTIVE TECHNIQUES

Phishing continues to be one of the most dangerous form of cyber attack. Due to its evolving nature and increasing sophistication it is crucial to adopt comprehensive preventive measures. These techniques can broadly be categorized into technical safeguards, user education and organizational policies.

- **BE SKEPTICAL OF UNSOLICITED EMAILS AND MESSAGES**

  User must check the source of email and verify and confirm the source carefully before taking any action and must keep an eye out for Phishing emails as such mail addresses are often similar to the original ones with slight changes like changing `I' to `1'.

Also the user must check for the red flags and stay cautious of emails that create a sense of urgency, have slight grammar mistakes or contains generic greeting (such as `Dear User, or `Dear Customer') [5].

Before clicking any link or URL contained in the email one should hover mouse over to have an idea where that link leads. Check whether the URL is legitimate and is related to the context of email or not. Also, instead of clicking the link directly user can manually type the link in browser [12].

- **USE MULTIFACTOR AUTHENTICATION**

Multi factor authentication provides an additional sense of security as it needs some other type of verification beyond password. User must use unique and tough passwords for each of their accounts and also regularly check their account to monitor if there's any unauthorized activity [3].

An individual or business must ensure that his operating system and all other software are up to date with newest security patches and they should frequently update or modernize their anti-virus software to help detect and prevent phishing attacks [18].

- **EMAIL FILTERING AND CALL SPAMMING MEASURES**

There are various tools that automatically filters spam email addresses and calls, like blacklisted emails, there is a list that contains phishing email addresses and they are blacklisted tools that automatically identify those web addresses must be used. Also people report certain calls or messages as spams with changing some settings in you device those calls and messages are automatically identified and are rejected [13].

- **EDUCATE YOURSELF AND PUBLIC AWARENESS**

If a person does not know about phishing attacks they can educate themselves about the concept with the help of news or discussing with people who know about it and stay up to date about the latest techniques as awareness and knowledge is best protection. People who are already aware about this can educate other people about this and keep them aware too [6][16]. Business can arrange regular awareness campaign which would empower individuals and enhance their skills and knowledge to recognize these attacks and avoid them. Also, organizations should conduct employee training programs on regular intervals to train about such attacks and the ways to prevent them. Various social media channels can also be used to spread awareness about the campaigns and to highlight common phishing techniques [14].

- **EMAIL AUTHENTICATE PROTOCOLS [SPF, DKIM, DMARC] :-**

These protocols make it more difficult for attackers to pose as trustworthy organizations by preventing email spoofing and confirming the sender's identity and prevent emails spoofing, making it harder for attackers to impersonate legitimate organization.

(1) SPF [Sender Policy Framework]:- Specifies which mail servers are authorized to send emails from a domain.

(2) DMIK [Domain keys identified mail]:- Adds a digital signature to emails, verifying the sender's authenticity [20].

(3) DMARC [Domain- based message authentication, reporting and conformance]:- Builds upon SPF AND DKIM, allowing domain owners to define how receiving emails systems should handle unauthenticated emails [e.g., reject, quarantine] and provides reporting mechanisms [20].

- **SECURE EMAIL GATEWAYS [SEGs]:-**

These solutions sit between the internet and an organization's email servers, providing advance threat protection, including anti-phishing, anti-malware, and content filtering. Also, inspect web traffic for malicious content, including phishing websites, and block access. They can also prevent users from downloading malicious files or sharing sensitive data on risky sites [17].

- **SOFTWARE DEVELOPMENT AND INTEGRATION OF AI**

Software development in phishing attacks will mainly focus on advancing the application security. For example:- A list based approached can be used 2 list can be made, one would contain the original and legitimate websites and other would contain the websites that are identified as phishing websites and they can be termed as blacklisted websites and that software can be installed in computers and will be in built in new devices which would automatically filter out websites that are blacklisted [16].

Machine learning and artificial intelligence can be integrated into email filtering system. Historical data can be used in machine learning algorithms and it will also improve their ability to detect new phishing attacks [18]. AI can be used to monitor daily activity of user on his device and t analyze his behaviour based on that, to distinguish between legitimate and malicious web addresses. AI and Machine learning can also be used to improve communication channel within organization to mitigate cyber-attacks [19].

- **ENHANCE LEGAL FRAMEWORK AND MONITOR IT IMPLICATIONS**

There are various regulatory framework that govern cybercrime and phishing attacks but these frameworks are not enforced properly. So, stricter enforcement of legal policies and frameworks with significant penalties for attackers will create a sense of fear in them to not do such things.

Continuous monitoring and improvement of email filtering techniques or any software updation is important to maintain the effectiveness. Organizations should regularly review filtering performance, analyze the data such as amount of attempted phishing attacks and should also incorporate user feedback into this and make necessary adjustments. They must stay vigilant and responsive to changes in phishing culture.

VI. REGULATORY FRAMEWORK

Phishing, a deceptive practice aimed at acquiring sensitive information such as username, passwords and credit card details by disguising as a trustworthy entity in electronic communication, is subject to various regulations and laws across the globe. These regulations aims to deter such malicious activities, protect individuals and organizations and provide legal recourse for victims.

Regulation and laws in India, several provisions within the Information Technology Act 2000, and the Indian Penal Code address phishing and related cybercrimes:-

INFORMATION TECHNOLOGY ACT 2000:-

- SECTION 43:- Deals with unauthorized access to computer system and data, which can be applicable in case where phishers gain unauthorized access to a victim's account or system. The penalty can extend to fine of up to Rs.1crore [20].

- SECTION 66:- Specifies penalties for data theft and unauthorized access, including imprisonment for up to three years or a fine of up to Rs.5 lakh or both. This section is relevant when sensitive information is stolen through phishing [20].

- SECTION 66C:- Penalizes identity theft, including the fraudulent use of electronic signatures, passwords, or any other unique identification features. The punishment includes imprisonment for up to three years and a fine of up to Rs.1 lakh. This is particularly relevant to phishing attacks that aims to steal login credentials [20].

- SECTION 66D:- Specifically addresses cheating by personation using computer resources, a common tactic in phishing where fraudsters impersonate legitimate entities. The penalty includes imprisonment for up to Rs.1 lakh [20].

RELEVANT BHARTIYA NYAYA SANHITA SECTIONS APPLICABLE TO PHISHING

- Sections 302 to 303 – These correspond to the earlier IPC Sections 378 to 379, which deal with theft. These provisions can be applied when phishing leads to unauthorized transfer of funds or digital assets, constituting theft.

- Sections 316 to 317 – These replace IPC Sections 405 to 406, concerning criminal breach of trust. These are applicable when a person entrusted with digital access or data uses that trust to carry out phishing and misappropriates the data or assets.

- Sections 318 to 321 – These correspond to IPC Sections 415 to 419, dealing with cheating and dishonestly inducing delivery of property. These sections are central to phishing schemes where individuals are deceived into giving away confidential information or money.

- Section 322 - These corresponds to Section 420 (IPC) and specifically addresses cheating and dishonestly inducing delivery of property, with the penalty including up to seven years' imprisonment and fine.

- Sections 334 to 351 - These cover forgery, fraudulent documents, and falsification of electronic records, replacing IPC Sections 463 to 477A. These provisions are applicable when fake emails, cloned websites, or fabricated documents are used in phishing attacks.

VIII. CONCLUSION

In conclusion, phishing is one of the prominent way of cyber-attack and is really complicated to detect and prevent. This paper discussed the types or the ways through which attacker can target the user and how it impacts individuals and businesses, financially and economically. This paper also discusses the preventive measures and the legal framework that govern and penalize cybercrime, proposing suggestions to enhance the mitigating techniques and regulatory framework. As discussed fishers often target human vulnerability so its important for the users to stay vigilant and aware about the new techniques these phishers adopt to target the people and its important for the businesses and government to continuously monitor and improve the techniques they have enforced to prevent these attacks.

REFERENCES:

[1] Milletary, J., & Center, C. C. (2005). Technical trends in phishing attacks. Retrieved December, 1(2007).

[2] Harihar, S. S., & Potdar, M. PHISHING IN THE DIGITAL AGE: A REVIEW OF TECHNIQUES AND TRENDS.

[3] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.

[4] Business Standard. (2024, August 6). Cyber frauds cost India Rs 177 crore in FY24: How to protect yourself. Business Standard.

[5] Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on phishing attacks. International Journal of Computer Applications, 182(33), 27-29.

[6] Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. Computers & Security, 68, 160-196.

[7] Apandi, S. H., Sallim, J., & Sidek, R. M. (2020, February). Types of anti-phishing solutions for phishing attack. In IOP Conference Series: Materials Science and Engineering (Vol. 769, No. 1, p. 012072). IOP Publishing.

[8] Livemint. (2024, April 15). Cyber fraud losses: Digital payment frauds on the rise in India.

[9] Reuters. (2024, March 19). India: Digital cash is everywhere, so are scammers.

[10] Banu, M. N., & Banu, S. M. (2013). A comprehensive study of phishing attacks. International Journal of Computer Science and Information Technologies, 4(6), 783-786.

[11] Cloudsek. (2024). India to lose Rs 20,000 crore to cybercrime in 2025.

[12] Syiemlieh, P., Khongsit, G. M., Sharma, U. M., & Sharma, B. (2015). Phishing-an analysis on the types, causes, preventive measures and case studies in the current situation. IOSR J. Comput. Eng., 9, 2278-8727.

[13] Kulkarni, Mehar & Kumar, Suryansh & Panjwani, Yashika & ., Mohana & Moharir, Minal & R, Ashok. (2024). Mitigating Email Phishing: Analytical Framework, Simulation Models, and Preventive Measures.

[14] Hera, Jafer. (2024). Phishing Defense Mechanisms: Strategies for Effective Measurement and Cyber Threat Mitigation.

[15] Economic Times. (2024, April 2). Indian entities may lose Rs 20,000 crore to cybercrimes in 2025. The Economic Times.

[16] Adil, Muhammad & Khan, Rahim & Khan, Abdul & Ghani, M & Ghani, Ul. (2020). Preventive Techniques of Phishing Attacks in Networks.

[17] Pureti, Nagaraju & Khan, Danial. (2024). Phishing Scams: How to Recognize and Avoid Becoming a Victim.

[18] Maureen, Akazue & Ahweyevu, Kingsley & Ogeh, Clement & Asuai, Clive. (2024). Development of a Real-time Phishing Detection.

[19] Alani, A. A., & Al-Azzawia, A. (2025). Phishing Attacks Detection and Prevention Techniques: An Overview. Journal of Al-Qadisiyah for Computer Science and Mathematics, 17(1), 166-178.

[20] Ali, M. M., & Mohd Zaharon, N. F. (2024). Phishing—A cyber fraud: The types, implications and governance. International Journal of Educational Reform, 33(1), 101-121.

[21] Reuters. (2024, March 11). India sees cyber fraud cases jump over four-fold in FY2024, caused 20 million losses.