INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Jan 2024
ISSN: 2582-6433

ANALYSING THE TREND OF CYBER PHISING IN INDIA

AUTHORED BY – RAHUL DANDOTIYA
Designation – Junior research fellow at Devi Ahiliya University Email – rahuldandotiya.nliu@gmail.com
Contact no- 9522222512

Analysing the Trend of Cyber Phising in India Abstract:

Cyber phishing has emerged as a major cybercrime, posing a threat to information security and privacy. Phishing is a social engineering attack that involves fraudulent communication leading to the collection of personal information or credentials. Cybercriminals take advantage ofhuman psychology and exploit digital illiteracy to gain access to confidential information as such :- passwords, credit card details and bank account information. The increasing use of the internet and digital devices has made people more vulnerable to phishing, leading to financial and reputational damages. The research aims to analyse the current trends and techniques of cyber phishing, identify the impact and study effective prevention and mitigation strategies.

Keywords: Phishing, Cybercrime, Cyber security, fraud

Introduction:

In light of the swift proliferation of the internet, the menace of cybercrime has emerged as a widespread hazard affecting both individuals and entities. Among the more covert manifestations of cybercrime is cyber phishing, characterized as a form of social engineering attack strategically designed to mislead individuals into revealing confidential information, encompassing passwords, credit card details, and other personally identifiable data.Cyber phishing has emerged as a major challenge for information security, as cybercriminals continue to develop sophisticated techniques to exploit human psychology and bypass technological security measures.

The frequency of phishing attacks has notably surged in the last ten years, as evidenced by the Internet Crime Complaint Centre (IC3) of the Federal Bureau of Investigation (FBI), which

ISSN: 2582-6433

recorded over 241,000 phishing complaints in 2020 (FBI, 2021). Projections indicate a sustained upward trajectory in this trend, given the escalating dependence of individuals on the internet and digital devices for both professional and personal purposes. The repercussions of successful phishing attacks are considerable, spanning from financial ramifications to the gravitas of identity theft and harm to one's reputation (Trend Micro, 2019).

Addressing the problem of cyber phishing requires a comprehensive understanding of its nature, scale, and impact. Research on cyber phishing has grown over the years, exploring various aspects of the phenomenon, including its techniques, targets, and outcomes. However, there is still much to learn about the dynamics of cyber phishing and how to prevent and mitigate its effects.

Phishing is a type of cyber scam that has been around for many years. Within this category of security breach, malefactors endeavor to deceive individuals into disclosing personal details, including but not limited to their name, residence, and credit card information. As time progresses, perpetrators engaging in phishing activities have enhanced the sophistication of their methods, leading to a heightened success rate in duping individuals into furnishing their sensitive information. This raised a question, how it originated, and how it has evolved over time.

Origins of Phishing

The term phishing is believed to be a play on the word "fishing", which is a recreational activity that involves using a bait to catch fish. In the late 1990s, phishers began using similar tactics in the digital world. Perpetrators employ the dissemination of emails or instant messages designed to mimic authentic communication channels, often masquerading as reputable entities like banks or credit card companies. These deceptive communications aim to coerce individuals into disclosing confidential details such as account passwords or other personal information.

The first recorded instance of phishing is believed to have taken place in the mid-1990s when a group of hackers stole America Online (AOL) accounts by sending out email messages that appeared to be from AOL's billing department. The hackers requested users to furnish their account information in response, ostensibly for the purpose of identity verification. Consequently, the hackers successfully gained entry to numerous accounts through this deceptivetactic.

Despite the efforts of AOL to crack down on this type of cybercrime, phishing attacks continued

ISSN: 2582-6433

to grow in number and sophistication.

Evolution of Phishing Tactics

During the initial years of the 2000s, phishing attacks demonstrated a discernible elevation in sophistication, as perpetrators adopted more persuasive methodologies to deceive individuals into divulging their personal information. They began creating fake websites that looked identical to legitimate sites such as online banking sites, complete with realistic logos, sign-in pages, and even customer service phone numbers. These tactics allowed phishers to gain access to more and more accounts, and the attacks became more difficult to detect

By the mid-2000s, organized crime syndicates had gotten in on the act, using phishing attacks to steal bank account information and other valuable data. These groups used advanced techniques such as spear phishing, which involved targeting specific individuals or organizations with highly personalized messages. They also used "pharming," a technique where they redirected users to fake websites even if they typed in the correct URL in their browser.In recent years, phishing tactics have continued to evolve.

Attackers use more sophisticated social engineering techniques, such as pretexting, where they pretend to be someone else in order to gain sensitive information. The use of mobile devices has also become more common, with phishing attacks now being carried out via text message (smishing) or social media messages (vishingAs technological progress persists, so does the evolution of phishing strategies. According to the 2021 Verizon Data Breach Investigations Report, phishing attacks emerged as the predominant form of cybersecurity incidents in 2020, constituting more than one-third of reported cases (Verizon, 2021). The same report highlighted credential theft, frequently stemming from phishing attacks, as the second most prevalent type of data breach, trailing only behind web application attacks.

The advent of the COVID-19 pandemic has further provided fertile ground for phishing attacks, as opportunistic scammers exploit individuals' anxieties and apprehensions regarding the virus.Phishing emails related to COVID-19 have increased dramatically, with attackers using them to trick victims into downloading malware, providing personal information or to make fraudulent payments.

In addition, phishing attacks have also become more sophisticated, with attackers using AI,

ISSN: 2582-6433

machine learning, and other advanced technologies to craft convincing messages and scams. One example is 'smishing', or phishing via SMS, which has seen an increase recently thanks to new capabilities for messaging services. Attackers are also using social engineering techniques, and tools such as deepfake have been used to make content appear more legitimate.

Determining the precise inception of phishing in India proves challenging, given its status as a global phenomenon that commenced its emergence during the late 1990s and early 2000s, coinciding with the expansion of the internet and the rise of e-commerce.However, India has become one of the major sources and targets of phishing attacks in recent years due to its growing internet user base and digital economy.

Phishing attacks in India have targeted a variety of sectors, including banking, finance, e-commerce, and social media. In 2019, India was ranked as the second most targeted country for phishing attacks globally, with around 1.6 million such attacks reported in the country(Statista, 2020).

One of the factors contributing to the rise of phishing attacks in India is the lack of cyber security awareness among the general public, especially in rural areas. Many internet users are unaware of the risks associated with online transactions and are easily fooled by phishing emails or messages.

Moreover, the availability of cheap and accessible technology has made it easier for cybercriminals to conduct phishing attacks from India. In recent years, there have been several cases where Indian hackers have been arrested for conducting phishing attacks

To combat the rising threat of phishing, the Indian government and private sector organizations have taken various initiatives to raise awareness about cyber security and promote digital literacy among the population.

Phishing attacks can be classified into several types based on the method of communication and the purpose of the attack. Here are some common types of phishing attacks:

1. Email phishing: Predominantly observed, this category involves the dissemination of counterfeit emails to individuals or entities. The assailants assume the identity of reputable

ISSN: 2582-6433

sources, such as banks, government agencies, or well-established brands, with the intent of soliciting sensitive information like login credentials or financial particulars.

2. Spear phishing: Representing a targeted variant of phishing, perpetrators direct their focus toward specific individuals or organizations. Leveraging personal information available online, they tailor their messages to appear more authentic. This may include incorporating details such as the recipient's name, job title, or other pertinent information to establish a sense of familiarity and engender trust.
3. Smishing: Employing SMS or text messages, this form of phishing endeavors to entice victims into interacting with malevolent links or divulging sensitive information. The primary objectives of smishing attacks often involve coercing victims into downloading malware onto their smartphones or providing unauthorized access to their personal data.
4. Vishing: This is another form of phishing that takes place over the phone. Attackers call their victims and impersonate representatives of banks or other legitimate organizations, convincing them to reveal their personal information or transfer funds.
5. Social media phishing: With the growing use of social media, attackers have started using platforms like Facebook and Twitter to spread fake messages or create fake profiles, attempting to lure victims into clicking on malicious links or revealing their personal information.
6. Whaling: This category constitutes a specialized form of spear phishing targeting senior executives or individuals of notable prominence. In these instances, assailants meticulously construct sophisticated email messages, designed to present an appearance of legitimacy, ultimately leading to substantial financial losses or the disclosure of confidential information.

India’s cyber fraud Capital

Jamtara, situated in the Jharkhand region of India, has garnered the unenviable recognition as the cyber fraud hub of the country. The attribution of this undesirable distinction can be attributed to a confluence of factors, encompassing educational deficits, unemployment, and poverty. These conditions have given rise to the formation of organized cybercrime groups within the locality.

The cyber frauds in Jamtara are primarily focused on phishing, vishing, and identity theft. Phishing entails the practice of enticing individuals to disclose their personal information, including sensitive details such as bank account information and passwords. This is achieved

ISSN: 2582-6433

through deceptive means, often utilizing emails or websites that outwardly appear to be legitimate. Vishing, on the other hand, is a type of attack where fraudsters impersonate bank officials and coerce victims into revealing their personal information over the phone.

The cyber fraud gangs in Jamtara are organized and have a well-defined hierarchy. They are led by individuals with technical expertise, who create fake websites and email addresses thatclosely resemble those of legitimate businesses or organizations. Other members of the gang act as recruiters, who lure vulnerable individuals from the area into joining the group. These individuals possess expertise in the field of social engineering, a skill set that revolves around themanipulation of individuals to disclose personal information or passwords.

Once a victim has been duped, the gang members transfer the money to various accounts and withdraw it in small amounts from different locations. By the time the victim realizes that they have been scammed, the gang has already disappeared.

The rise of cyber fraud in Jamtara can be attributed to several social and economic factors.

Firstly, the region is plagued by poverty and high levels of unemployment. Many young people in the area do not have job prospects, and the lure of easy money through cyber fraud is too tempting to resist.

Secondly, a significant factor fostering the escalation of cybercrime in the region is the deficiency in educational opportunities. Many people in the area have not completed their education and are not digitally literate. This makes them vulnerable to cyber fraudsters who use sophisticated tactics to trick them into revealing their personal information.

Thirdly, despite the prevalence of cybercrime in the region, law enforcement agencies and local authorities have been slow to act. This has given the cyber fraud gangs in Jamtara a free hand to operate without fear of being caught.

In response to the rising trend of cybercrime in Jamtara, the Indian government has taken several steps. The Cyber Crime Police Station in Mumbai has set up a dedicated center to tackle cybercrime in the region. Additionally, the government has launched initiatives to promotedigital

ISSN: 2582-6433

literacy and educate people about the dangers of cyber fraud.

India has taken several measures to combat cyber phishing cases in recent years. One significant measure undertaken by the Indian government involves the establishment of the Cyber Crime Coordination Centre (CCCC) within the Ministry of Home Affairs. The CCCC's mandate is to address issues pertaining to cybercrime in the nation, encompassing phenomena like phishing.

Additionally, the government has enacted the Information Technology (Amendment) Act, 2008, incorporating more stringent provisions for penalties in instances of cybercrime. This legislation grants the police the authority to investigate and prosecute offenders, prescribing imprisonment and fines as punitive measures.

Furthermore, the Reserve Bank of India (RBI) has implemented various initiatives to combat instances of cyber phishing. It has mandated that banks adhere to specific security guidelines to safeguard customer data effectively.These guidelines include implementing two-factor authentication, blocking international transactions on debit/credit cards by default, and enabling transaction alerts through SMS or email.

Moreover, the Indian Computer Emergency Response Team (CERT-In), operating under the aegis of the Ministry of Electronics and Information Technology, serves as the primary national entity for addressing and responding to cyber incidents within the country.It works to maintain a 24x7 coordination centre for emergency response and handles the task of monitoring and securing the Indian cyberspace.

The Indian government has also launched a public awareness campaign to educate people about the dangers of cyber phishing. The National Cyber Security Awareness Month is organized every year in October to create awareness and educate people about cyber risks and best practices to stay safe.

Finally, the government has also worked with social media platforms and search engines to remove phishing websites and fake copies of official websites. This has helped in reducing the number of phishing cases in the country.

ISSN: 2582-6433

Some of the key laws and regulations that are used to combat cyber phishing in India are:

1. **Information Technology Act, 2000 (IT Act) -** This act provides a comprehensive legal framework to regulate cyber activities in India. The act penalises cybercrime and prescribes punishments for offences such as hacking, phishing, identity theft, and others.

- **Section 43:**

If any person without the permission of the owner of the computer, computer system, computer network; accesses, downloads, introduces, disrupts, denies, or provides any assistance to other people can be held liable under this section.

- **Section 66:**

This section provides for punishment if the accounts of a victim are compromised by the phisher, who does any act mentioned in Section 43 of the IT act, shall be imprisoned for a term which may exceed up to three years or with a fine which may exceed up to five lakh rupees or both.

- **Section 66C:**

This provision prohibits the use of electronic signatures, passwords, and any other feature which is a unique identification of a person. Phishers disguise and portray themselves as the true owners of the accounts and perform fraudulent acts.It is related to Identity Theft by phisher.

- **Section 66D:**

The provision provides punishment for cheating by personating using communication devices or computer sources. Fraudsters use URLs that contain the link for a fake website of banks and organizations and personate themselves as the bank or the financial institution.

All the provisions of the I**T Act, 2000** which are relevant to the phishing scams are howeverMade bailable under Section 77B **of the IT Act**.

1. **Indian Penal Code, 1860 (IPC)** - The IPC is another important law that is used to prosecute cyber offenders. as per the Indian Penal Code, Phishing can also be held liable **under Cheating (Section 415), Mischief (Section 425), Forgery (Section 464), and Abetment (Section 107).**
2. **The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and**

ISSN: 2582-6433

Services) Act, 2016 - This legislation governs the utilization of Aadhaar, a distinctive identification number issued by the Indian government. It explicitly forbids the inappropriate use of Aadhaar data and establishes provisions for penalties in cases of infringements.

3. **Reserve Bank of India Guidelines** - The Reserve Bank of India (RBI) has provided directives to banking institutions outlining measures to mitigate cyber fraud, encompassingphishing attacks. These guidelines necessitate the adoption of heightened security protocols, including the enforcement of two-factor authentication for online transactions.
4. **The Personal Data Protection Bill, 2019** - The legislation strives to establish provisions for the safeguarding of personal data belonging to individuals within the jurisdiction of India. It mandates the implementation of data protection policies and provides for penalties for violations.
5. **The Anti-Phishing Working Group (APWG)** -This is an industry association dedicated to addressing the escalating issues of identity theft and fraud associated with the growing challenges of phishing and email spoofing.

Overall, the legal framework in India is designed to curb cyber phishing and other cybercrime activities. The laws and regulations provide for severe punishment for offenders and empower law enforcement agencies to take action against them.

Despite the legal framework in place, there are likely several reasons for the increasing cases of cyber phishing in India, including:

1. **Lack of Cyber security Awareness**: A lack of awareness and education regarding cyber security is one of the primary reasons for the increasing cases of cyber phishing. Many peopleare unaware of the risks associated with phishing attacks and do not take the necessary precautions to protect themselves.
2. **Limited Cyber Expertise**: There is a shortage of skilled cyber security professionals in India who can implement effective measures to prevent cyber phishing attacks.
3. **Easy Availability of Online Tools:** Many cybercriminals use readily available online tools to carry out phishing attacks or purchase phishing kits from the dark web.
4. **Increased Reliance on Digital Transactions:** As the trend toward greater digitization of financial transactions continues, an expanding number of individuals are opting for digital

ISSN: 2582-6433

means to conduct financial transactions. Consequently, there has been a rise in the incidence of phisherstargeting both individuals and businesses through online channels.

5. **Ineffective Implementation of Laws:** There may be instances where the laws are not being implemented effectively or the penalties for violating the laws are not severe enough to deter cybercriminals.
6. **Sophisticated Phishing Techniques:** Cybercriminals are constantly upgrading their phishing techniques, making it harder for individuals and organizations to detect and prevent such attacks.

Steps to be taken in case of phishing attack

- Report the incident promptly to law enforcement, securing a crime reference number to facilitate collaboration with your bank and other relevant entities. In the majority of online scams and cybercrimes, reporting should be directed to Action Fraud. This not only aids in the cessation of the scam but may also expedite the process of recovering your funds.
- Simultaneously, communicate with the financial institutions involved in the transaction without delay. If your bank account is implicated, notify your bank and provide a detailed account of the situation. If the destination bank of the transferred funds is known, contact them promptly. Swift action may enable freezing of the funds in transit, initiating a fraud investigation with both institutions.
- Exercise caution regarding potential recovery scams. Following the theft of funds, it is common for criminals to impersonate banks, law enforcement, or money recovery experts in attempts to pilfer more money. Refrain from placing trust in any communications received via phone, email, or text. Instead, independently verify the legitimacy of the communication by directly contacting the organization in question to ascertain their attempt to reach out.

Conclusion:

The answer to curb cyber crime is on the question why such crime is emerging, aswe are more inclined to cyber space to ease the life and but covid 19 speed up the inclination, everything is mow online like shopping, services, education, work as well financial transaction and banking services like from net banking to UPI transfer. When everything is shifting online the criminals are changed their modus operandi to online, the physical crime is risky as well leaves footprints and the frequency of committing the crime is low, but online crime it's very high. To curb this

ISSN: 2582-6433

there is always preventive measures present in the legal framework but the way crimininals are evolving and creates a gap between the existing laws and the measures to curb cybercrime (Phishing).there are three main reasons for became a victim are fear, greed and curiosit, counter measure is cyber literacy in India that is the solution to make the people aware about the basic banking awareness, although the banking institution and the government always take appropriate steps to spread cube literacy , But phishing on the other hand changed is methods or modus operandi frequently and the phishing incidents are high in volume. the phishers take theadvantage of their loopholes exploit the victims and the biggest loop holes in number of cases it'sfound that the phishers are using sim card and the bank account registered on fake names, this shows a failure on the part of governing institutions, this need to fixed first to develop counter measures techniques,. In India jamtara in Jharkhand became the cyber hub for crime as if it's not stopped, soon there will be more hubs will be, even studies suggests that there are establishedand dedicated call centres are nurturing

There are certain tips such as always updating the antivirus and software of mobile, don't install third party applications, use a caller id on mobile, inform police if you received any phiser call, always check the internet site you are access is secure or not , don't open any unidentified URL,don't share any account or sensitive information such as OTP , CC number ATM pin e.t.c

- Internet Crime Complaint Center. (2020). *2020 Internet Crime Report*. FBI. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
- Trend micro Inc.
- https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-power-of-the-right-message-how-phishing-works-how-to-stop-it
- Indian Penal Code, 1860. (1860). *Www.indiacode.nic.in*. https://www.indiacode.nic.in/handle/123456789/2263?sam_handle=123456789/1362
- Damodaram, R. (2016). | STUDY ON PHISHING ATTACKS AND ANTIPHISHING TOOLS. *International Research Journal of Engineering and Technology Certified*
- *Journal*, *03*(01). https://www.irjet.net/archives/V3/i1/IRJET-V3I1121.pdf
- Oladimeji, S., & Kerner, S. M. (2021, February 9). *SolarWinds Hack Explained: Everything You Need to Know*. WhatIs.com.
- https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to

ISSN: 2582-6433

- -know
- Bharucha & Partners - Kaushik Moitra. (2021, July 27). *Phishing and cybercrimes inIndia - a comparison and necessary solutions*. Lexology.
- https://www.lexology.com/library/detail.aspx?g=a6e35288-c18d-433f-83c1-4525d348d6cf-
- *Kashyap, A. & Chaudhary, M.. (2023). Cyber security laws and safety in e-commerce in India. Law and Safety*. 89. 207-216. 10.32631/pb.2023.2.19.
- *A Glance At Online Fraud – Phishing - Data Protection - India*. (2022, August 8). Www.mondaq.com.
- https://www.mondaq.com/india/data-protection/1219182/a-glance-at-online-fraud--phishing
- Livemint. (2021, September 20). *83% organizations in India saw rise in phishing attacks during pandemic*. Mint.
- https://www.livemint.com/news/india/83-organizations-in-india-saw-rise-in-phishing-attacks-during-pandemic-11632119876206.html
- *Reporting fraud and cyber crime*. Action Fraud. https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime
- *Reserve Bank of India - Draft Notifications/Guidelines*. Www.rbi.org.in. https://www.rbi.org.in/Scripts/DraftNotificationsGuildelines.aspx
- Around 5 lakh people potentially fall victim to phishing scams in India: report. (2023, March 3). *The Economic Times*. https://economictimes.indiatimes.com/tech/technology/around-5-lakh-people-potentially- fall-victim-to-phishing-scams-in-india-report/articleshow/98393025.cms?from=mdr
- **8**