TITLE

DEEP DIVE INTO PHISHING PRACTISES VIA WHATSAPP MESSENGER, ITS RELATED PENALISATION AND PROTECTION LAWS IN INDIA.

By MEGHNA R

ABSTRACT

The exponential rise in digital era not only paves way to its many advantages of networking and communication, but also many fraudulent practices to exploit the users. WhatsApp Messenger, being one of the most frequently used instant messaging service, has in recent times being used for several untold and unsubscribed advertising. User's personal details have been extracted and data is being sold to many marketing agencies. These agencies then procure data, mainly the contact details of the users, to spam chat boxes with "advertisements". In pretext of advertising and giving opportunity to the needy, WhatsApp is used to maliciously trap its users with flashy offers. These offers come with diverse applications and malignant motives, including financial scams. There has been significant growth in cyber laws and measures to protect the public from such fraud in India. The objective of this paper is to throw light on the Cyber Security and the amount of awareness provided by India to its public. This paper analyses several such Phishing practises used into duping users of various age groups, followed by its consequences. It elucidates on legal provisions relating to penalising such offenders and legislative role in providing protection to the users. The paper delves upon various prevention measures and redressal forums available in India. Conceptualizing possible ways to successfully bring down the injustice and constant invasion of privacy amongst the citizens.

Keywords: *Phishing, WhatsApp Messenger, Protection, Cyber Security, Fraud.*

1. INTRODUCTION

The robust development of science and technology and the growing population in India, may be a sign of progress but is also an opportunity for exploitation. Indian Demography is such that the country and its people of young youth, has been in upscale and has been increasing, it is expected that by 2060 the countries population is expected to reach 1.7 billion.[1] Like any country, India comprises of 3 groups of people young-age group, working-age group and the dependent group. With the rise in working-age group, India produces energetic youth who transcend the developments in several sectors. One of the popular developments around the world is the 'Digitization' of several systems in the functioning of the country. India like the rest of the world initiated several schemes which brought about the revolutionary digital trends in several sectors to help in the functioning of the country. In light of that information, we can see the growing trends in which the youth of the nation, with use of science and technology are falling into traps or setting up traps with malicious intent. Attacks made by people using science and technology are known as cyber-attacks.[2] Not one but all groups are targeted and are susceptible to these cyber-attacks. These attacks often occur through deception and malignant intentions similar to any physical attack, but the only difference being that this attack takes place in a virtual environment. Cyber-attacks give rise to the increasing cybercrime in India.[3] These cyber attacks take places in several forms for a wide variety of reasons, one such is the Phishing attack. Phishing attacks mainly occur by misrepresentation of oneself and deceiving the other who places trust in good faith. There are increasing number of platforms that are used to deceive a common man or even a huge corporate, via these phishing attacks. Focussing on the Instant Messaging platforms that target all age group, young and old, to practise their phishing attacks. One such instant messaging platform is WhatsApp Messenger. WhatsApp messenger has become one of the highly used IM services in India.[4] After Covid-19 many institutions including the educational institutes have been profusely engaging in WhatsApp Messenger services.[5] Hence with the increase in usage and attacks in the virtual forums India

---

[1] Jain N, Goli S. Potential demographic dividend for India, 2001 to 2061: a macro-simulation projection using the spectrum model. SN Soc Sci. 2022;2(9):171. DOI: 10.1007/s43545-022-00462-0.

[2] Aditi Singh, A Study on Emerging Issues of Cyber Attacks & Security: In India, Vol-7 Issue-1 2021, https://ijariie.com/AdminUploadPdf/A_Study_on_Emerging_Issues_of_Cyber_Attacks___Security__In_India_ijariie13501.pdf

[3] Deepa T.P., SURVEY ON NEED FOR CYBER SECURITY IN INDIA. DOI: 10.13140/2.1.4555.7768,

[4] Kumar, Naveen & Sharma, Sudhansh. (2017). Survey Analysis on the usage and Impact of Whatsapp Messenger. Global Journal of Enterprise Information System. 8. 52. 10.18311/gjeis/2016/15741.

[5] Munir, S., Erlinda, R., Afrinursalim, H. (2021). Students' Views on the Use of WhatsApp during Covid-19 Pandemic: A Study at IAIN Batusangkar. Indonesian Journal of English Language Teaching and Applied Linguistics, 5(2), 323-334

has time and again makes changes with the exponential development of technology in aspects of Data Protection laws and penalisation of different cyber-frauds and data breach occurring all over. Let us understand in detail the crux of the problem and analysis the strategy established by the Indian legislative, executive and Judiciary together to curb this problem. C: India is accepting and gearing itself to the consequence faced due to the rise of technology.

2. CYBER ATTACKS : THE PHISHING BAIT

What are Cyber-attacks? Attacks by which any person incurs any damage or loss through the actions done in a virtual environment of cyberspace, can be termed as cyberattacks. The term *'Cyberspace',* coined by William Gibson in his novels, is used to describe the social, cultural and psychological environment created by the Internet.[6] Simply put, attacks happening in cyberspace are cyberattacks and it then, when reported forms, a cybercrime to which general public need cyber protection via cybersecurity. Cyberattacks are then classified as attacks against: (a) Individuals, (b) Property, (c) Organisation and (d) Society.[7] Among many methods of attacks used such as Ransomware, ATP, Malware, BotNet attacks, Phishing attack is one such prominent method of attacking anyone ranging from huge corporates to general public at an individual level.[8]

2.1 Understanding Phishing Attacks

2.1.1 Defining Phishing Attacks

Phishing attack uses the social engineering attack techniques, by which the end user or administrator is deceived through different technological platforms to extract a spectrum of wide variety of information ranging from personal to professional credentials.[9] The term 'Social Engineering' is a technique that helps in manipulating people into talking decisions which they otherwise would not.[10] It psychologically draws people to gain trust in impersonators or manipulators convincing them to let in on their credentials. In layman terms,

---

[6] Niva Elkin-koren and Eli M. Salzberger, "Law, Economics and Cyberspace: The Effects of Cyberspace on Economic Analysis of Law.", ISBN 1 84064 669, PG 13.
[7] Choudhary, Atul & Choudhary, Pankaj & Salve, Shrikant. (2018). A Study On Various Cyber Attacks And A Proposed Intelligent System For Monitoring Such Attacks. 612-617. 10.1109/ICICT43934.2018.9034445.
[8] Alawida M, Omolara AE, Abiodun OI, Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. J King Saud Univ Comput Inf Sci. 2022 Nov;34(10):8176-8206. doi: 10.1016/j.jksuci.2022.08.003.
[9] M. Adil, R. Khan and M. A. Nawaz Ul Ghani, "Preventive Techniques of Phishing Attacks in Networks," 2020, pp. 1-8, doi: 10.1109/ICACS47775.2020.9055943
[10] Wang, Z., Zhu, H., Liu, P. et al. Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. Cybersecur 4, 31 (2021). https://doi.org/10.1186/s42400-021-00094-6

the term Phishing was closely related to the word 'fishing', wherein the fishes are lured into a trap using a bait.

2.1.2 Types and Motives of Phishing Attacks

There are various types of Phishing practices to dupe the general public, such as the Deceptive Phishing, Spear Phishing, Clone Phishing, Whaling, Voice Phishing. All these types of Phishing attacks are motivated towards wide range of target users.[11] The motives behind the Phishing attack for either monetary benefit that comes from coning or selling the data collected or the identity theft or data breach that leads to the loss or damage to the victim.[12]

2.1.3 Potential Targets for Phishing Attacks

The targets to Phishing attacks are classified based on three of the mentioned characteristics: (a) Curiosity, (b) Fear and (c) Empathy. A person becomes a target when they are curious as to what the flashy link or redirected offer stands for or when they are subjected to some kind of fear that someone or something of their possession is in danger or when they empathically trust some source that ultimately deceives them.[13] Targets to Phishing attacks are spectrum of persons including artificial persons and a band of organization. Only the technique they use to different persons vary on the nature and characteristics of the class of persons. It is to be noted that the Phishing attacks does not necessarily confide itself to the geographical boundaries of one country, but may also cross boundaries, using the power of Internet that connects people all over the world.

2.2 Phishing Techniques via WhatsApp Messenger

Instant Messaging platforms not only have advantages but also have disadvantages by connecting people from the corners of the world. WhatsApp Messenger on the other hand apart from being an IM platform, now has features that act as both a social media platform and an online payment platform. Mobile Phishing is what take place when a person receives random or spam texts from an unknown number, misrepresented organisation or impersonation of any brand, organisation or persons.[14] In WhatsApp Messenger, phishing attacks happen

---

[11] Bhavsar, Vaishnavi & Kadlak, Aditya & Sharma, Shabnam. (2018). Study on Phishing Attacks. International Journal of Computer Applications. 182. 27-29. 10.5120/ijca2018918286.

[12] Bhardwaj A, Sapra V, Kumar A, Kumar N, Arthi S. Why is phishing still successful? Computer Fraud & Security. 2020 Sep;2020(9):15–9. doi: 10.1016/S1361-3723(20)30098-1.

[13] Sotonye Kalio, Phishing Attacks: Raising Awareness and Protection Techniques In Bournemouth University, 2022, 10.31234/osf.io/uxeth

[14] Anushka Sharma, "Fraud alert! That WhatsApp message from your boss might be a phishing campaign",Feb 7, 2023, https://www.cnbctv18.com/technology/fraud-alert-that-whatsapp-message-from-your-boss-might-be-a-phishing-campaign-15869041.htm

individually targeting one person at a time and duping their information. Now, a fraudulent company or individual can target a group of people individually, but does not target society or organisation via WhatsApp Messenger. Take for example, an individual is being subjected to a phishing attack through a link coming via WhatsApp Messenger and that occurs successfully, the criminal then assumes the role of that person and then abuses the rest of the organisation entrusted to the victim. This explained, there are several cases logged involving of Phishing attacks via WhatsApp Messenger that have both criminal and civil liabilities.

3. IMPACT IN INDIA

3.1 HISTORY AND EVOLUTION OF PHISHING ATTACKS VIA WHATSAPP MESSENGER IN INDIA

Before the coming of WhatsApp Social Media phishing fraud occurred in Facebook Messenger. Though Instant Messaging was catered to by the SMS sent to the phone's inbox[15], it always lacked the personal touch in manipulating persons to create a make-believe environment, hence even though phishing occurred it was because of the victim's unfortunate timing. Moreover, the fraudsters need to acquire the victim's mobile number, which was then difficult to come by for setting predetermined and targeted traps. Whereas Social Media platforms it was enough if the victim was also a user of that platform, openly sourcing out the information that catches the eye of the predator. Hence, Facebook Messenger was a convenient platform for Phishing attacks before WhatsApp Messenger. With increase in sale of personal data of general public in dark web or even in public forums without prior consent of the victim, in addition to the large population using WhatsApp Messenger after its coming into the market, the general public have become more susceptible to Phishing Attacks.[16] WhatsApp Messenger is and has been the most convenient platform for digital marketing via texts and spams to a wide variety of targets. In a way a person's greed will looking at offers, flashy discounts, ideas of making quick money are reasons why the public in India are prime victims to Phishing Attacks in India. Multiple cases bizarre cases have been noted in what is called the 'Romance Scams', where the main targets are lonely people, who get sent romantic and flirtatious messages and duping them to make payments.[17] In many cases impersonation of a friend or a family member and

[15] S. Mishra and D. Soni, "SMS Phishing and Mitigation Approaches," 2019 Twelfth International Conference on Contemporary Computing (IC3), Noida, India, 2019, pp. 1-5, doi: 10.1109/IC3.2019.8844920.
[16] Kiran Rathee and Urvi Malvania, "Scammers target WhatsApp users with phishing attempts", May 21, 2023, https://economictimes.indiatimes.com/tech/technology/scammers-target-whatsapp-users-with-phishing-attempts/articleshow/100143463.cms
[17] Emma Fletcher, "Romance scammers' favorite lies exposed", Federal Trade Commission, February 9, 2023, https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed

causing an urgent need of money or asking them to indulge in any link or URLs sent from their accounts, this often happens with an already compromised account of a friend or family member.[18] In recent times there have been several cases where people were lured in with job opportunity or a way in to make quick money with a stock tip, by which they are subjected to monetary losses.[19]

3.2 Rise of Cybersecurity issues in India

From the standard definition of 'Cybersecurity', it is understood that they are set of rules and regulations comprising of tools and techniques to provide security and risk management policies in order to protect all, in cyberspace (ITU). Cybersecurity in India has been on the rise with the increasing number of cybercrimes occurring all over the country. Though in comparison with its global developed counterparts such as US and UK, who have separate data protection directive that meet international standards, India falls shorts in some ways of implementations and legislation aspects.[20] Cybersecurity issues in India deepened during the dark days of Covid-19, when the world was battling with the pandemic situation, on the other side utilizing the fragile state of the public there were several phishing attacks.[21] Then on frequent and regular spam message of recruitment or shopping frauds have been frequently reaching the phones of millions of public in the society.

3.3 Loss Incurred by India and its citizens

India along with its citizens is being nicked with huge economic losses due to these Phishing attacks now more than ever. This is so, as an increasing number of households of India are being digitized and mobile gadgets are being used, thanks to the digitization initiatives post-Covid. Recent incidents involving a 74-yr old retire government officer to loss of 35 rupees, in an embarrassing circumstance, where he received a nude phone call on WhatsApp, on ending the call, he then after few days receives another call of a fraudster posing a cybercrime officer and looting the money.[22] The above incident being a combination of moral and pecuniary loss

---

[18] Ankita Chakravarti, "WhatsApp friend in need scam is doing the rounds: Here is what it is and how to stay safe" Nov 13, 2021, https://www.indiatoday.in/technology/news/story/whatsapp-friend-in-need-scam-is-doing-the-rounds-here-is-what-it-is-and-how-to-stay-safe-1876308-2021-11-13

[19] HT Tech, "Man loses Rs. 43lakh in WhatsApp Scam", Sep 18, 2023, https://tech.hindustantimes.com/tech/news/man-loses-rs-43-lakh-in-whatsapp-scam-learn-how-to-stay-safe-online-with-these-5-tips-71695039544249.html

[20] Sushma Devi Parmar, "Cybersecurity in India: An Evolving Concern for National Security", https://www.academicapress.com/journal/v1-1/Parmar_Cybersecurity-in-India.pdf

[21] Al-Qahtani AF, Cresci S. The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19. IET Inf Secur. 2022 Sep;16(5):324-345. doi: 10.1049/ise2.12073.

[22] ET Online, "74-year-old in Bengaluru loses Rs 35,000 in WhatsApp nude video call scam", Aug, 2023, https://economictimes.indiatimes.com/news/new-updates/74-year-old-in-bengaluru-loses-rs-35000-in-whatsapp-nude-video-call-scam/articleshow/102897142.cms

of the victim. There are several other incidents that play with the persons dire need, also greed in some cases, wherein persons of different professions are targeted to provide with a part time jobs and showing virtual profits in order to gain trust of these persons and further asking them to reinvest their money for memberships to gain more benefits towards the end of duping them to lose money of several crores in one month.[23] The compensation to these losses in case of reporting and proper investigation proves legit, the Government has to pay from its funds depending upon the magnitude of the loss incurred. This overall causes huge economic loss, for these incidents keep recurring. Keeping aside the monetary loss faced by the public, the kind of mental distress the family and friends of the victim is of greater impact in development of the company. As in these cases not only the victim but there are graver chances of anyone in relation to the victim to suffer the same faith as him. Once a Phishing attack is done, there is no telling as to the scale of information that has been drawn from the victim, his phone and his bank.

4. JUSTICE THROUGH INDIAN LEGAL SYSTEM

4.1 LEGISLATIVE'S ROLE: LEGAL PROVISIONS

Cybersecurity Laws are majorly incorporated in the **Information Technology Act, 2000**[24] in India. This Act not only contains various sections that call for penalisation for the phishing practices but also encompasses Rules by which any misrepresented, impersonating or fraud organisation is kept in check. This Act comes into picture when an attack is done in the cyberspace along with the **Indian Penal Code**[25], which punishes fraud and identity theft in the virtual environment, as done in the real-time environment. The recent **Digital Personal Data Protection Act of 2023**[26], also ensures that the personal data that is used for lawful purposes is being protected righteously and if not to be brought before the Appellate tribunals for justice. The following legal provisions can be used to penalise the wrong-doer in case of Phishing attacks via WhatsApp Messenger:

1. **The Information Technology Act,2000**:
    - **Section 65**[27]: It deals with tampering of any computer sourced documents.

[23] ET Online, "Part-time job fraud: 3 techies, auditor, pharma worker and bank manager lose Rs 1.3 crore in one month in Hyderabad", Aug, 2023, https://economictimes.indiatimes.com/news/india/part-time-job-fraud-3-techies-auditor-pharma-worker-and-bank-manager-lose-rs-1-3-crore-in-one-month-in-hyderabad/articleshow/103175815.cms
[24] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[25] Indian Penal Code,1860, No.45, Acts of Parliament, 1860 (India).
[26] The Digital Personal Data Protection Act, 2023 No. 22, Acts of Parliament, 2023 (India).
[27] The Information Technology Act, 2000, § 65,No. 21, Acts of Parliament, 2000 (India).

- **Section 66**[28]: It deals with Computer related offences that happen either "dishonestly" or "fraudulently" by the definitions of S.24 and S. 25 of the IPC.
- **Section 66B**[29]: Deals with imparting punishment to those who dishonestly are receiving any stolen Computer Resource which includes Computer data base and Software.
- **Section 66C**[30]: Deals with punishing those who indulge in Identity Theft
- **Section 66D**[31]: This involves in punishing those who cheated by impersonation using a Computer Resource.
- **Section 67**[32]**, 67A**[33]**, 67B**[34]: Deals with punishing those for publishing or transmitting obscene material in electronic. 67A for containing sexually explicit act and 67 B for containing children in the same.
- **Section 67C**[35]: Deals with those intermediaries that retain and persevers information.
- **Section 71**[36]: Provides those who have misrepresented with themselves to give penalty
- **Section 72**[37]: Deals with those breach confidentiality and privacy of its users to give penalty
- **The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**
- **The Information Technology (Security Procedure) Rules, 2004**
- **The Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016**

2. **Indian Penal Code**:
    - **Section 420**[38]: It deals with fraudulent and dishonest practices that induces the victim to deliver property.

---

[28] The Information Technology Act, 2000, § 66, No. 21, Acts of Parliament, 2000 (India).
[29] The Information Technology Act, 2000, § 66B, No. 21, Acts of Parliament, 2000 (India).
[30] The Information Technology Act, 2000, § 66C, No. 21, Acts of Parliament, 2000 (India).
[31] The Information Technology Act, 2000, § 66D, No. 21, Acts of Parliament, 2000 (India).
[32] The Information Technology Act, 2000, § 67, No. 21, Acts of Parliament, 2000 (India).
[33] The Information Technology Act, 2000, § 67A, No. 21, Acts of Parliament, 2000 (India).
[34] The Information Technology Act, 2000, § 67B, No. 21, Acts of Parliament, 2000 (India).
[35] The Information Technology Act, 2000, § 67C, No. 21, Acts of Parliament, 2000 (India).
[36] The Information Technology Act, 2000, § 71, No. 21, Acts of Parliament, 2000 (India).
[37] The Information Technology Act, 2000, § 72, No. 21, Acts of Parliament, 2000 (India).
[38] Indian Penal Code,1860, § 420, No.45, Acts of Parliament, 1860 (India).

- **Section 419**[39]: It deals with punishment for cheating a victim by impersonation.

3. **Digital Personal Data Protection Act, 2023**

4.2 EXECUTIVES' ROLE: REDRESSAL FORUMS IN INDIA

With legislative building up legal provisions, the implementation part is left to the executives so that the justice and fair play is received by all of the citizens in India. Executives' role in Phishing attacks via WhatsApp Messenger mainly deals with providing awareness among the public, enabling redressal forum at varying levels in the society and enforcing penalising laws upon those who follow malignant or fraudulent methods to deceive people. The Following executive methods are followed in India for prevention and penalisation of Cyberattacks:

- **National Cyber Security Strategy 2020**, which focuses on providing improvised cyber awareness and security through a panel of cyber auditors, who look into all the security features of an organisation that should be in place legally.
- **National Critical Information Infrastructure Protection Centre (NCIIPC),** which was established under the IT Act, 2000 and functions as a nodal agency overlooking security and resilience of "critical information infrastructure".
- **Indian Cyber Crime Coordination Centre (I4C),** was setup in the year 2020 to deal with all types of cybercrimes. Before these initiatives such as the **Cyber Surakshit Bharat**, to provide awareness and build safety measures for all frontline IT officials of the Government departments and the **Cyber Swachhta Kendra**, which was started to clean all the viruses and malwares in all computer devices for all internet users.
- **National Cyber Crime Reporting Portal**, is open to all citizens to report any cybercriminal activity that they were a subjected to, these complaints can be made online and actions will be taken upon investigation given.
- **Computer Emergency Response Team-India (CERT-In**), is an organisation run by the MeitY, that collects, processes and alerts the general public on any recurring cybersecurity issues in the country.

4.3 JUDICIARY'S ROL E: JUDICIAL DISCRETION

Judicial Discretion in matters of such fraud that shakes the fiscal economy of the country is of greater importance as it sets precedence to matters that will come henceforth in the not-so distant future. In one case of **Amit Shah v. State**[40], wherein the applicant had applied for bail

[39] Indian Penal Code,1860, § 419, No.45, Acts of Parliament, 1860 (India).
[40] Amit Shah v. State, 2023 SCC OnLine Del 6461

which stood cancelled as he is deemed the main accused in the matter of defrauding another person of online financial scam. One complainant Oweas Khan had been frauded of money a total amount Rs. 7,99,850/- using an online portal. He had received a message in WhatsApp Messenger an offer of earning online part-time income, by rating on Google Platform. He was then sent links to perform his pre-paid tasks by which he was promised profits and he was receiving the same until a point where he stopped receiving the amount and was told he had completed a task wrongly and hence he needs indulge in another pre-paid task in order to retrieve the same. In this case one can observe a clear case of Phishing practice via WhatsApp Messenger as a technique to dupe the victim.

The Court observed that these sorts of well-organized trap-laying scams conducted through online transactions, poses insecurity and corrodes public's confidence in indulging over financial transactions in digital platforms. It also made a note that, at core these scams lead to causing instability in the nation's economy, as these activities leads to a cascading effect, as online transaction have become the very 'lifeblood of commerce, finance and communication' in the modern times. The Court has probed such issues to be taken seriously to protect not only the individuals but also the vitality of online financial systems.

5. RECOMMENDATIONS

India with its large, rich and diverse population, is doing an exceptional job in by way of making laws and pushing them at par with their global developed counterparts. Given like in every law there are loopholes and gaps in the law when compared to the Protection Directives and laws that are provided internationally. It is with the implementation that it taking a back seat, taking into account the vastness of the country. In terms of how India can better proceed to deal with recent trends of Phishing Attacks that are happening through IM platforms such as the WhatsApp Messenger is as follows:

- Focusing of the legal provisions in India, cyber laws are mainly sourced from the IT Act, which again fails to distinguish between the computer resourced data and the sourced data from the smart communication mobile devices, though in the recent insertion of 2(ha) communication devices is listed in the definitions, the mention of it in the entire Act is nearly nil. The mention of smart devices should be present considering the fact that there are growing smart things ranging from household articles to wristbands one uses.

- Again, the definitions of Cybersecurity and Cyberattacks need to improved, though there is a mention of Cybersecurity in Section 2(nb), when read in detail adds no value to the current rise in Criminal activity in Cyberspace, as these intricacies would carry weightage in upcoming future.
- To improve protection towards not receiving such unsolicited communication from spam numbers and unsubscribed individuals there should a strict law that restricts such messages from being repeatedly getting posted in the inboxes of the users. Though there is slight mention of this is Section 66A(c), where it was stated that 'causing annoyance' is punishable, at any rate this is only when interpretated in our cases. There should be separate mention of this law when in real world public are facing issues due to unwanted spams leading into cyberattacks. This provision can be viewed in the Privacy and Electronic Communication (EC Directive) Regulation, 2003(PECR) in the UK and in e-privacy and Electronic Communication in the EU's e-Privacy Directives.[41] These also avails strict provisions of Confidentiality and Transfer of data bans, along with the provision to Opt-Out from receiving any Marketing emails or texts.
- Like mentioned above, these directives and laws strictly follow methods such that any personal data collection or transfer or even receiving any said information happens purely on the basis of the consent of the users. These is minimally followed in India when put to practical application. Laws should enforceable in such manner that public of India maintain their privacy and still be able to indulge in activities of business.
- Executives' role to capturing the fraudster of a huge or a small cyber incident must be magnified several folds, when compared to the current trends of exploitation to their functioning in capturing the wrong-doer. Though India is doing great work in proving awareness to the society, it would be far more helpful if the executive act in accordance to prevent and protect the society from any kind of cyberattack by the same wrong-doer.

[41] Paul Lambert, "A user's Guide to Data Protection: Law and Policy", Third edition, Bloomsbury Professional.

6. CONCLUSION

It is well-known fact that every coin has two sides, likewise every scientific development has two sides of pros and cons that the public is subjected to time and again, since the days Man started inventing. India is as fast growing country and proved its excellence in several fields, and is still deemed to be a developing country, the major reason as observed can be enforcing such said law over the vast population of our country. Cyberattacks mainly phishing attacks can be put to stop with the vigilant nature of both the victims who are being scammed and the authorities who need to act immediately as soon as the said case has been reported. WhatsApp Messenger is a widely used IM as well as social media platform that currently exists with everyone who possess a smartphone in India. Due to its extensive use, even in the educational institutions, everyone ranging from the young kids to old community of our society is being affected and are terrorised to use and indulge in any online activity. India is strong and needs to grow stronger in terms of protecting its public with the new age issues arising in the Cyberspace. As the future holds more such complexities and complications with the further developments in the society.