Library Progress International
Vol.44, No.3, Jul-Dec 2024: P.210-214

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Investigating Cybercrime News Reporting in Indian Online News Media

Dr. Sumedha Dhasmana[1], Dr. Sunil Kumar Mishra[2], Dr. Atul Upadhyay[3], Dr. Sunny Kumar Gond[4]

[1]Assistant Professor, Vivekananda Institute of Professional Studies- TC
sumedha.dhasmana@gmail.com
[2] Associate Professor, Vivekananda Institute of Professional Studies
mishrasunil02@gmail.com
[3] Assistant Professor, Vivekananda Institute of Professional Studies- TC
upadhyay.atul1985@gmail.com
[4] Assistant Professor, Vivekananda Institute of Professional Studies- TC
sunygond@gmail.com

How to cite this article: Sumedha Dhasmana, Sunil Kumar Mishra, Atul Upadhyay, Sunny Kumar Gond (2024). Investigating Cybercrime News Reporting in Indian Online News Media 44(3), 210-214

ABSTRACT

Internet is being actively used world over. Covid 19 pandemic have brought a steep rise in internet use by users of all age groups. In India specifically, there are total 692 million active internet users that includes 351 million users from rural India and 341 from urban India. Without a doubt, the advantages of internet use are numerous. It is but obvious that with such a high rate of internet use, online world also opens up platforms for ever increasing cybercrimes in country. Increased online time, lack of awareness among internet users are popular reasons for the increased cybercrime trends. Moreover, lack of technical knowledge among professionals adds to the complications in solving cybercrime cases. Hackers, on the other hand, are coming up with new and innovative modus operandi to scam more and more people. This paper analyses the cybercrime related news content of leading news websites in India. The research is conducted to investigate cybercrime news reporting, identify the increase in cybercrimes and to understand the types of cybercrimes taking place in the country. It attempts to understand the most popular strategies being adopted by online attackers for luring online users. This paper attempts to create necessary mindfulness while using the internet. It is analyzed that cybercrime awareness campaigns of government are unable to make an impact at a larger level.

Keywords: Cybercrime, Cyber Security, Hacking, Phishing, Trojan, Malware, Virus, Cybercriminals.

Introduction

Life is made easy with the ever-increasing use of technology in almost every sphere (Wall, 2008). Among the new technologies, use of gadgets like tablets, computers and smartphones have become essential part of daily life. Almost all users connect their devices to the internet to navigate and explore the online space, called the cyber-space. However, just like any new advancement that comes with its own advantages and disadvantages, the creation of this space has also led to the emergence of a new kind of lawbreaking known as cybercrime. Bidgoli et al. (2019) calls cybercrimes as a threat to present day society that can lead to information breach, financial loss or damaged reputation.

Cybercrime in many ways is similar to the crimes that takes place in real-life situations. It is actually the mode of crime that has shifted from the traditional physical space to online space. Thus, we see an emergence of newer types of crimes in this cyberspace that breaks-away the hindrances of geographical barriers (Gordon & Ford 2006). Cybercrime is the dark side of cyberspace and what may look otherwise be true can be ugly in reality. Cybercrime can be defined as any criminal activity performed through cyberspace or the Internet. It is conducted through the use of computer, network or any other digital device. Cybercriminals target the users of various digital devices for reasons like financial fraud, unauthorised information access, reputation damage, physical or mental torment and sexual abuse to name a few (Patel et al., 2017).

Today, every individual is dependent heavily on internet use in various spheres of life. This has led to the

emergence of cybercrime as the criminals, just like every internet user, have started to use online space for their benefit. Criminals are now able to commit crimes, sitting in their comfort zones (Jhaveri et al. 2017). Moreover, features like high-speed internet connectivity, anonymity and lack of cyber security have increased cybercrime manifolds. Weijer (2020) brought cybercrimes under two categories, first being cyber-enabled crimes which are traditional crimes committed through the use of IT but not aimed at IT and cyber-dependent crimes that committed through the use of IT and also aimed at IT.

The government of India has come up with National Cyber Crime Reporting Portal called www.cybercrime.gov.in. This site enables the public to report incidents pertaining to all types of cybercrimes, with a special focus on those against women and children. In case of a cyber financial fraud, citizen can immediately call 1930 and report their complaint.

Filing a complaint on National Cyber Crime Reporting Portal is relatively easier as victims don't have to physically go to the police station for reporting the case. National Cyber Crime Reporting Portal is an initiative of Government of India to facilitate victims/complainants to report cybercrime complaints online. It has a dedicated team who works on cybercrime against women and children. The platform also promises anonymity to victims whenever desired. Moreover, a tracking number is provided to the victims after a complaint is filed. The victims can check the work progress in their case.

The cybercrime unit of Delhi Police has enlisted 23 different methods through which cybercrimes could take place. These include: E-mail frauds, Social media crime, Mobile app cries, Compromise of Business Email, Data Theft, Ransomware, Net Banking/ATM Frauds, Fake Calls Frauds, Insurance Frauds, Lottery Scam, Bitcoin Fraud, Cheating Scams, Online Transactions Frauds, Gift Card Frauds, Fake Shopping Site Frauds, Fake Government Website Frauds, Herbal Oil Frauds, Job Frauds through Call Centres, OLX QR Code Frauds, KBC Lottery Frauds, PayTM KYC Frauds and Sextortion Frauds Phishing-Vishing Frauds

Bidgoli & Grossklags (2016) emphasize that the reporting of cybercrime is essential as almost computer device is susceptible to cybercrime. It can generate awareness and can provide a variety of information to the readers or audience. For instance, it becomes easier to understand the frequency of its occurrence and examine the manner through which cybercrime takes place.

Review of Literature

Connolly & Piper (2022) pinpoints that media holds the responsibility of creating awareness about cybercrime. It is important that media reporting should be done sensitively and accurately so that negative consequence on the victim can be avoided. Alansari, Aljazzaf, & Sarfraz (2019) has proposed for the creation of models in the near future that possess the capability of measuring the influence of demography and technology. These should be used to identify the factors of e-crimes leading political, cultural, financial, and sexual aspects in societies, both locally and globally. The authors highlighted that without a doubt there several pros of technology, but it also poses great danger. Technology is needed to be carefully handled otherwise it can even become threat to one's lives. It is essential that the users stay cautious while using technology and be aware of the cyber-crimes that are taking place in the society. Smith et al. (2018) brings to light that a report of cybercrime pulls down a company's stock prices as well. Millions of users are impacted negatively when they get to know about identity thefts like credit card information acquired by cybercriminals illegally. Sarmah et al. (2017) classified cybercrime as cybercrime against individuals, cybercrime against organisation, cybercrime against property and cybercrime against society. Gupta (2016) presented a commentary of the Information and Technology Act which provides legal recognition to online transactions. Bohme & Moore (2012) identified that the experience of cybercrime leads to decreased participation online. Lamber et al. (2012) talked about the trade of pornographic content that is provided easily to the users on online platforms. Desai and Jayashankar (2007) highlighted cybercrime like cyber stalking and cyber bullying which is increasing day by day. The authors also focussed on the unwarranted physical contact and violence if ignored for a period of time. Gorman & McLean (2002) highlighted how pornographic material is easily distributed because of the arrival of the internet age. Goudriaan et al. (2005) pinpoints reporting of cybercrime can come with benefits like decreased crime rates plus the chance of becoming a victim again also decrease considerably.

Methodology

Content Analysis method has been utilized to understand the case reported on cybercrime cases in India. Popular news websites were scanned for a duration of 15 days. A total of 21 news stories were found relevant to the understanding of cybercrime scenario in India. The results depict a very high cybercrime rate because 21 different cybercrime stories and reported in a span of 15 days. These stories are reported in the following online publications: www.hindustantimes.com, www.timesofindia.com, www.economictimes.com, www.timesnownews.com, www.news18.com, indianexpress.com, www.newindianexpress.com, www.telegraphindia.com, www.siasat.com, www.expresscomputer.in and www.latestly.com.

Analysis of Online News Stories on Cybercrime

A case was reported where a woman from Patna, Bihar was duped by cybercriminals who threatened her by using Dawood Ibrahim's name. The criminals managed to cheat woman by taking about Rs 20 lakhs from her bank. These criminals took advantage of the anonymity feature and terrorized her in the name of underworld don Dawood Ibrahim. In this case, the victim reported the issue only after an inquiry was made by Income Tax Department about the reasons for huge amount of transaction. The woman, then narrated how cybercriminals threatened to kill her sons, in case the transactions is not done by her

A case of online fraud was reported where a man from Bengaluru city who lost Rs 50,000 after placing an online order of diapers for his newborn. After the online order was placed by him, he received a call from fraudsters, requesting him to confirm his order by filling some details of the order placed by him. Since the fraudsters knew the details of the order, the victim trusted them ad filled the form as requested. This unfortunately led to transfer of Rs 50,000 through UPI transaction.

In yet another episode of online fraud, a senior citizen from Maharashtra was cheated of 23.35 lakh. The criminals convinced him to transfer money on the pretext of earning high returns through investing in mutual funds.

India's premier medical institute, All India Institute of Medical Sciences (AIIMS) is no far from becoming a victim. In a major cyberattack, the systems of the institute went absolutely dead which hampered the daily working. Crucial services like digital hospital facilities, appointment, billing and reported was affected. This appeared to be a ransomware attach Indian Computer Emergency Response Team (CERT-In) and National Informatics Centre (NIC) had to support AIIMS in order to get back to digital service as soon as possible.

In a remarkable report submitted by the intelligence agencies to the police, cybercriminals were caught by the crime branch. Two published news stories highlighted how cyber cheaters used identity information of Army personnel for duping people. These criminals first collected data from Army men by providing lucrative offers of free SIM purchase recharge. The data collected was then used to cheat people by calling the on the pretext of being army men. Almost a dozen of incidents was reported where a cybercriminal posed as army man sent an identity proof before duping people. For instance, Mudit Agarwal of South Malaka narrated how 2.5 Lakhs were looted from his bank account. These cybercriminals, perhaps inspired from Jamtara series duped innocent people.

Online fraud case was reported by a 58 years old woman from Mumbai who was looted of money by a cyber fraudster. She was attempting to transfer money from the mobile app of her bank. On failure of her attempt, she searched for the customer care number on the internet. Much to her horror, she called up a fraudulent number where the person assured her that she is talking to the bank representative. The person then convinced her to download a remote access application on her mobile phone. A total of 11.69 lakhs were drawn off from her bank account. The same news reported also highlighted another prominent cybercrime where a 49-year-old mechanical engineer who was cheated for Rs 80,000.

The new breeds of cybercriminals take advantage of the anonymity feature for looting the hard-earned money of innocent people. This was an example of a matrimonial fraud where the Hyderabad cybercrime branch reported the case of a woman who lost of Rs 18 lakh. She was approached through a matrimonial website by a fraudster who impersonated as a civil engineer. It is identified in the same report that the crooks especially target women on matrimonial website.

Call centre fraud case was reported from Salt Lake in which the cybercrime branch raided an office with around 50 people working and making international calls through VOIP making the tracing of call difficult. These tele-callers attempted to call the victims and threaten them about a virus attack. They further offered to repair victims' operating system on a nominal fee. All those victims who were lured to click on the link provided, actually provided remote access to their computer.

In a comprehensive report published by Hindustan Times, three lakh cases have been reported in a time span of three years in Uttar Pradesh alone. Reports of criminals who offer lucrative job opportunities to job seekers and then fool them into a trap of money looting. Popular online buying and selling app OLX is also used to target both buyers and sellers of online products. The news reported also highlighted how a perpetrator pose as a female on social media and build trust with their target. In sextortion, the criminals initiate a video can and then record videos for blackmailing purposes later on.

The economic times reported how as many as 45% of Indian firms reported cases of cyber related frauds. This shows that not only the individuals become victim of cybercrime but big organizations, where a number of people work together, also become prey to cybercriminal targets.

In case of Instagram trap, a married woman from Vishakhapatnam was blackmailed through chats, emails and recorded videos. The victim was demanded money and continuously harassed. In this case the accused was found to be a local citizen. The police immediately arrested him and appealed common public to stay away from anonymous people on social media.

Popular TV actress Anjum Fakih also reported falling prey to online scam. Luckily however, she escaped by acting smart when a sales representative from online shopping website tried convince her that she won a prize and that she should choose her gift from the provided shopping application.

A retired lecturer from Pune was cheated for whooping amount of Rs 20 lakhs after she received a call from a

cybercriminal who pretended to a be a bank employee. The elderly was asked to update her KYC details or otherwise her account would get blocked. The woman immediately approached the police station after realizing the scam.

In a similar incident, an elderly man was cheated by a lady and a student of was cheated on the pretext of profit on investment the Mysore. KYC fraud case was also reported in which another senior citizen was reported of being duped.

Timesnow reported the incident of Mumbai where a steel supplier was cheated of Rs 32.7 lakhs. In this case, cybercriminals created fake company letterhead requesting of RTGS transactions. A case has been filed under IT Act in this matter

Conclusion and Suggestion

Information and Technology Act (IT Act) was formulated in 2000 for providing legal recognition to online transactions. The IT Act also clearly enlists the punishments in case of offences. Moreover, National Cyber Crime Reporting Portal (www.cybercrime.gov.in) provides an easy access to citizen to file their complains. These complains immediately get addressed as in most of the cases it is possible to catch cybercriminals through IP address. Information and awareness related to cybercrimes are also provided to users of Information and Communication Technologies through SMS reminders and caution update on various media platforms. More recently, popular actress Tabu is creating cyber security awareness through her advertisement on UPI Pin fraud. She clearly states and reminds public at large that UPI Pin is used to send money and not to receive money. UPI Pin fraud is the most used technique by cybercriminals to dupe people. Thus, we see the efforts of government in generating awareness about the possibilities of cybercrime.

It however needs to be highlighted that these campaigns of government are unable to make an impact at a larger level. The masses still remain unaware of the consequences of cyber security ignorance. The similar is highlighted through this research that identified more than twenty reported cases of cybercrime in short span of 15 days. The victims of cybercrime are reported from North to South of India, thereby depicting the increasing cybercrime rate in the entire country. On checking the age category of the victims, it is identified that in most of the recent cases where large amount of money duping is involves ranges from college going student to a senior citizen as old has 74 years. It is also very crucial to highlight here that in most of cases of cybercrimes that are reported, the victims are educated Indians as we see students, retired lecturer, TV actress, business owner and even premier organisation becoming victim of cybercrime.

It is identified that cybercriminals often pose as military and para-military personnel in order to win trust of their victims and then convince them for incorrect transactions. KYC update fraud, lottery fraud, matrimonial fraud, shopping website fraud, ransomware, UPI fraud, call centre fraud, OLX fraud and fake phone number on lookalike of banks site are some of the cybercrimes that are reported in the duration of this study. In few cases, the police were able to catch the criminal. However, in most of the reported stories the action of the police on the matter is not reported.

Since the use of cyber space is crucial in present times, this research suggests a careful note of all incidents that are covered to generate awareness about the possibilities of different types of cybercrimes that may take place with any individual or an organisation. The research emphasises the need by the government to created continuous awareness campaigns on cyber security. This should be done not only through various online platforms but also through traditional publicity methods like banner/billboard advertisement, newspaper stories and columns and TV advertising. This will ensure that the public at large stay updated about safe ways of performing online transactions.

It is commendable that the University Grants Commission has launched cyber security and data protection programmes at both undergraduate and post graduate level. This step will help in raising awareness against cybercrime and will provide the youth of the country to develop a considerate understanding of cybercrime and cyber security.

References

Alansari, M. M., Aljazzaf, Z. M., & Sarfraz, M. (2019). On Cyber Crimes and Cyber Security. In M. Sarfraz (Ed.), Developments in Information Security and Cybernetic Wars, pp. 1-41. IGI Global, Hershey, PA, USA. doi:10.4018/978-1-5225-8304-2.ch001.

Bidgoli, M., & Grossklags, J. (2016). *End user cybercrime reporting: what we know and what we can do to improve it. 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF).* doi:10.1109/icccf.2016.7740424.

Bidgoli, M., Knijnenburg, B. P., Grossklags, J., & Wardman, B. (2019*). Report Now. Report Effectively. Conceptualizing the Industry Practice for Cybercrime Reporting. 2019 APWG Symposium on Electronic Crime Research (ECrime).*

Bohme, R., & Moore, T. (2012). *How do consumers react to cybercrime? 2012 eCrime Researchers Summit.* doi:10.1109/ecrime.2012.6489519

Connolly, L. Y., & Piper, D. C. (2022). *Thirtieth European Conference on Information Systems (ECIS 2022), Timisoara, Romania*.

Desai, M., & Jaishankar, K. (February 2007). Cyber stalking victimization of girl students:
An empirical study. Paper presented at the second International and Sixth biennial
Conference of the Indian Society of Victimology at Chennai, India (pp. 1-23).

Gupta, A. (2016). *Commentary on Information Technology Act– With rules,regulations, orders, guidelines, reports and policy documents*. .Lexis Nexis

Gordon, S., & Ford, R. (2006). *On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), 13–20.* doi:10.1007/s11416-006-0015-z

Gorman, L., & McLean, D. (2002). *Media and society in the twentieth century*. Wiley-Blackwell.

Goudriaan, H., Nieuwbeerta, P. and Wittebrood, K. (2005), "Overzicht van onderzoek naar determinanten van aangifte doen bij de politie. Theorie€en, empirische bevindingen, tekortkomingen en aanbevelingen", Tijdschrift voor Veiligheid, Vol. 4 No. 1, pp. 27-48.

Jhaveri, M. H., Cetin, O., Gañán, C., Moore, T., & Eeten, M. V. (2017). *Abuse Reporting and the Fight Against Cybercrime. ACM Computing Surveys, 49(4), 1–27.* doi:10.1145/3003147

Lambert, N. M., Negash, S., Stillman, T. F., Olmste
ad, S. B., & Fincham, F. D. (2012). A love that doesn't last: Pornography consumption and weakened commitment to one's romantic partner. *Journal of Social and Clinical Psychology*, *31*(4), 410-438. https://doi.org/10.1521/jscp.2012.31.4.410

National Cyber Crime Reporting Portal. (2024, August 8). *Register a Complaint*. https://www.cybercrime.gov.in/

Patel, P., Kannoorpatti, K., Shanmugam, B., Azam, S., & Yeo, K. C. (2017). *A theoretical review of social media usage by cyber-criminals. 2017 International Conference on Computer Communication and Informatics (ICCCI).* doi:10.1109/iccci.2017.8117694

Sarmah, Sarmah, & Baruah. (2017). A brief study on Cyber Crime and Cyber Law's of India. *International Research Journal of Engineering and Technology*, *4*(16).

Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2018). *Examination of cybercrime and its effects on corporate stock value. Journal of Information, Communication and Ethics in Society.* doi:10.1108/jices-02-2018-0010

Van de Weijer, S., Leukfeldt, R., & Van der Zee, S. (2020). *Reporting cybercrime victimization: determinants, motives, and previous experiences. Policing: An International Journal, 43(1), 17–34.* Van de Weijer, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. Policing: An International Journal, 43(1), 17–34. doi:10.1108/pijpsm-07-2019-0122

Wall, D. S. (2008). *Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime1. International Review of Law, Computers & Technology, 22(1-2), 45–63.* doi:10.1080/13600860801924907