GRADUATE SCHOOL OF BUSINESS AND ADVANCED TECHNOLOGY MANAGEMENT

Co-hosted by

Au Hybrid International Conference 2024
Entrepreneurship and Sustainability in the Digital Era
Assumption University of Thailand
April 26, 2024

A Study on Cybercrime Awareness among Youth in Maharashtra

Navin Punjabi

Abstract

Every minute in India a new user is using the internet. The increasing integration of digital platforms and devices presents a challenge in protecting the youth from cybercrimes. Moreover, the stark truth is that internet users are not updated with the latest cyber threats and security concerns. Therefore, the primary question about this research paper is to know to awareness level of youth in Maharashtra. Primary and secondary data has been collected through questionnaire and journals, newspaper articles, Government reports respectively. Chi square test is used to test the hypothesis. Questionnaire was sent to 110 individuals out of which 85 respondents replied effectively. To collect data non-probabilistic convenient sampling method is used. According to the research paper, almost 37% of the respondents have fallen victim to these scams, yet 51% of them are either unaware of them or have never attended a session on the subject. Furthermore, there is no correlation between the awareness level of Maharashtra's youth and age or gender.

Keywords: Cybercrime, Cybersecurity, Awareness, Youth

1.1. Introduction

There is a huge rise in number of individuals using digital payment infrastructure in the recent years. Covid-19 made people learn and use digital technology at a rapid speed. According to a press release by Government of India dated 19th December 2023 digital payment transactions have increased from 2071 crore in financial year 2017-18 to 13462 crore in the financial year 2022-23. With this enormous rise the risk of cybercrimes has also increased.

As per the report 'Crime in India', registration of cybercrime cases was 65,893 cases which showed an increase of 24.4 per cent in comparison to 52,974 cases in 2021. According to National Crime Records Bureau, in India the highest rate in increase of crimes is cybercrimes (24%) in comparison to economic offences (11%), senior citizens crime (9%), and crimes against women (4%).

The report "Cyber security and rising incidents of cyber/white collar crimes" by Parliamentary standing committee on Finance reported a loss of ₹2537.35 crore in domestic fraud .As per a study by IIT Kanpur-incubated start-up, 75 % of financial frauds were cybercrimes from January 2020-June 2023. Hence, its important to create cybersecurity awareness for protection against these new types of financial frauds. This study attempts to study awareness of people in Maharashtra towards cybercrimes and its security.

Evolution of Cybercrime:

Cybercrime has evolved significantly since the beginning of computing. Initially, cybercriminal activities were relatively simple, often involving hacks or pranks. However, with the rapid advancement of technology, cybercrime has become more sophisticated and organised. Cybercrime has evolved through several key milestones, including the proliferation of viruses and worms in the 1980s and 1990s, the rise of financial cybercrime in the early 2000s, and the emergence of ransomware and nation-state-sponsored attacks in recent years.

The Morris Worm in 1988, the Code Red and Nimda worms in the early 2000s, and the Stuxnet worm targeting Iran's nuclear programme in 2010 have all demonstrated the destructive potential of cyber threats. These incidents resulted in significant financial losses, disruptions to critical infrastructure,

and breaches of national security. Individuals, businesses, and governments around the world face new challenges as cybercrime evolves, necessitating ongoing efforts to strengthen cybersecurity defences and effectively combat cyber threats.

Cybercrime

Cybercrime refers to a wide range of illicit activities carried out using digital means. This includes, but is not limited to:

- Malware attacks include viruses, worms, trojans, and ransomware.
- Phishing and social engineering are deceptive techniques for obtaining sensitive information.
- Identity theft and fraud are the unauthorised use of personal information for financial gain.
- Cyberbullying and online harassment: Harassment, intimidation, or defamation through digital means.

Any criminal behavior involving a computer or network is referred to as cybercrime. Hacking, virus distribution, identity theft, online fraud, phishing schemes, cyberbullying, online harassment, copyright infringement, and more are just a few of the numerous forms it can take. Cybercriminals frequently take advantage of holes in computer systems or utilize technology to carry out illegal activities including extorting money, stealing confidential data, or damaging computer networks. Because we depend more and more on digital technologies in our daily lives, cybercrime is becoming a major worry for governments, corporations, and people all around the world.

Types of Cyber crime

Malware Attacks: Malware is a general term for harmful software that covers, among other things, Trojan horses, worms, viruses, and ransomware. While worms propagate on their own over networks, viruses affix themselves to trustworthy programs and multiply when they are run. Trojans pose as trustworthy programs to fool users into installing them, giving hackers access to systems without authorization. Ransomware frequently targets both individuals and organisations, encrypting files and demanding payment to recover them.

Phishing and social engineering: Phishing is the practice of deceiving people via phoney emails or websites into disclosing private information, such passwords or bank account information. Social engineering techniques take use of psychological vulnerabilities in people to coerce them into divulging private information or acting in ways that will help the attacker. Pretexting, baiting, and tailgating are common strategies that take advantage of victims' confidence and authority to deceive them.

Identity Theft and Fraud: Identity theft is the practice of cybercriminals using credit card numbers or social security numbers to obtain personal information in order to commit financial fraud or impersonate real people. Creating illegal accounts, making unauthorised transactions, or requesting loans in the victim's name are examples of fraudulent activity. Victims of identity theft may suffer greatly as a result, including monetary loss, harm to their reputation, and psychological suffering.

Cyberbullying and Online Harassment: Cyberbullying is the practice of harassing, intimidating, or dehumanising someone via the use of digital platforms like social media, messaging applications, or online forums. Cyberbullies may target their victims with targeted harassment campaigns, disseminate rumours, or post embarrassing images or videos. Threats, stalking, and hate speech are just a few of the negative actions that fall under the larger category of "online harassment," which can have a serious negative psychological and emotional impact on its victims.

Cybersecurity

Cybersecurity is the protection of computer systems, networks, and data against cyber threats. The measures include implementing strong security

protocols and encryption to ensure data integrity and confidentiality.

- Setting up firewalls, antivirus software, and intrusion detection systems to detect and prevent unauthorised access.
- Conducting regular security audits and risk assessments to identify and address vulnerabilities.
- Developing incident response plans and procedures to address cybersecurity incidents quickly.
- Creating a culture of cybersecurity awareness and training for employees to reduce human error.

Cyber security measures

A variety of techniques are included in cybersecurity, which is intended to shield data, networks, and PCs against online dangers. Confidentiality, integrity, and availability are three fundamental cybersecurity concepts that work to maintain the security, accuracy, and accessibility of information. Firewalls, which monitor and manage network traffic, antivirus software, which finds and eliminates harmful software, and encryption, which secures data by encoding it in a format that can only be accessed with the right key, are examples of common cybersecurity technologies and tools.

Defence-in-depth techniques, which combine several tiers of security measures to successfully reduce risks, are employed in strategies for protecting networks, devices, and data against cyber threats. These could include intrusion detection systems, network segmentation, access limits, and employee security awareness training. Frequent vulnerability scans, penetration tests, and security assessments help find and fix holes in systems and apps, which lowers the chance of successful cyberattacks.

Defence-in-depth tactics are used in plans to safeguard devices, networks, and data from cyber threats. These tactics combine many security tiers to effectively lower risks. These could consist of access controls, network segmentation, intrusion detection systems, and security awareness training for staff members. Regular penetration testing, vulnerability scans, and security evaluations assist in identifying and addressing weaknesses in systems and applications, hence reducing the likelihood of successful intrusions.

Cybersecurity Market

The global cybersecurity market has grown significantly in recent years, owing to the increased frequency and sophistication of cyber threats. Key market trends include increased demand for cybersecurity solutions in industries like finance, healthcare, and government.

- Use advanced technologies like artificial intelligence and machine learning to improve threat detection and response capabilities.
- The emergence of cloud-based security solutions to meet the challenges of securing distributed and remote work environments.
- Governments and regulatory bodies are increasing their investments in cybersecurity to improve national security and protect critical infrastructure.
- Strengthening collaboration among cybersecurity vendors, industry partners, and government agencies to combat cyber threats together.

Cybersecurity Trends

Current cybersecurity trends reflect the changing nature of cyber threats and defensive strategies. The proliferation of Internet of Things (IoT) devices raises security concerns, including vulnerabilities in connected devices and networks.

- The rise of ransomware-as-a-service (RaaS) models, which allow cybercriminals to carry out sophisticated ransomware attacks with little effort.
- The growing importance of data privacy and compliance regulations, such as GDPR and CCPA, is prompting organisations to prioritise data protection and governance.
- The convergence of cybersecurity and physical security, as organisations strive to protect both digital and physical assets from evolving threats.

- A growing emphasis on proactive threat hunting and intelligence-driven security operations to detect and mitigate emerging cyber threats before they become widespread.

Cybersecurity Law

Cybersecurity laws and regulations play an important role in developing legal frameworks and standards for cybersecurity. These laws aim to establish legal obligations for organisations to protect sensitive information and reduce cyber risks.

- Create penalties and enforcement mechanisms for cybercrime, including hacking, data breaches, and identity theft.
- Encourage information sharing and collaboration among government agencies, industry stakeholders, and law enforcement agencies to effectively combat cyber threats.
- Promote international cooperation and coordination on cybersecurity issues, such as cross-border data sharing and cybercrime extradition.
- Promote transparency and accountability in cybersecurity practices, encouraging organisations to adopt best practices and cybersecurity governance standards.

Cybersecurity Awareness

Cybersecurity awareness campaigns aim to educate individuals and organisations about the importance of cybersecurity and empower them to practise safe online behaviour. Examples of such initiatives are:

- Government-sponsored cybersecurity awareness campaigns, such as National Cyber Security Awareness Month (NCSAM) in the United States, which offers resources and educational materials to help people understand cybersecurity risks and best practices.
- Corporate training programmes and workshops that teach employees about cybersecurity threats and how to identify and respond to them effectively.
- Non-profit organisations and industry associations that provide cybersecurity training and certification programmes to professionals looking to improve their skills and knowledge of cybersecurity.
- Held community outreach events and workshops to educate children, parents, and educators on safe online behaviour and digital literacy.

Collaboration among government agencies, industry partners, and non-profit organisations to create and distribute cybersecurity awareness materials and resources for specific audiences and demographics.

- Indian Cybercrime Coordination Centre (I4C) is an initiative of the Ministry of Home Affairs, Government of India to deal with cybercrime in the country in a coordinated and comprehensive manner.
- The 'National Cyber Crime Reporting Portal' (https://cybercrime.gov.in) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cyber crimes against women and children.
- The 'Citizen Financial Cyber Fraud Reporting and Management System', under I4C, has been launched for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. So far, financial amount of more than Rs. 1000 Crore have been saved in more than 4 lakh incidents. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber incidents.
- The Massive Open Online Courses (MOOC) platform, namely 'CyTrain' portal has been developed under I4C, for capacity building of police officers/judicial officers through online course on critical aspects of cyber crime investigation, forensics, prosecution etc. along with certification. More than 72,800 Police Officers from States/UTs are registered and more than 50,000 Certificates issued through the portal.

-I4C has imparted cyber hygiene training to 5,600 officials of various Ministries/ Departments of Government of India.

-To spread awareness on cybercrime, the Central Government has taken steps which, inter-alia, include; dissemination of messages through SMS, I4C social media account i.e. X (formerly Twitter) (@Cyberdost), Facebook (CyberDostI4C), Instagram (cyberdostI4C), Telegram(cyberdosti4c), Radio campaign, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, etc. The States/UTs have also been requested to carry out publicity to create mass awareness.

-The Indian Computer Emergency Response Team (CERT-In) conducts regular training programmes for network/system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organizations regarding securing the IT infrastructure and mitigating cyber-attacks. A total of 42 training programmes have been conducted, covering 11,486 participants, during the years 2021 and 2022. In 2023, up to October, a total of 7007 officials from Government, critical sectors, public and private sector have been trained in 21 training programs in the area of cyber security.

-CERT-In regularly disseminates information and shares security tips on cyber safety and security through its official social media handles and websites. CERT-In organized various events and activities for citizens during Safer Internet Day on 7.2.2023 and Cyber Security Awareness Month in October 2023, by posting security tips using posters and videos on social media platforms and websites. CERT-In, in association with Centre for Development of Advanced Computing, conducted an online awareness campaign for citizens, covering topics such as general online safety, social media risks and safety, mobile related frauds and safety, secure digital payment practices, etc., through videos and quizzes on the My Gov platform.

1.2. Literature Review

Research papers on sans cyber security: The sans technology institute provides papers on a range of cybersecurity subjects, including cyber biosecurity, a newly emergent field that straddles the boundaries of biosecurity, cybersecurity, and biological sciences.

An Analysis of cybercrime Scenario in Pune: the primary objective of this research paper is to scrutinize the cybercrime situation in Pune, and to assess the awareness of various types of cybercrimes in the city. Researcher has analyzed various cybercrimes based on IPC and IT act,

Awareness Concerns of Cyber Security for citizens in Navi Mumbai and Panvel Zone: this research paper has helped in developing and implementing enhanced cybersecurity protocols and procedures, with future investigations proving beneficial for all stakeholders.

A Study on Awareness of Cyber Crime and Security: the aim of the study is to raise awareness about the prevalence of cybercrimes in the modern world and to promote cybersecurity measures. The finding reveals a correlation between respondents age groups and educational qualifications. Therefore, it is imperative for all internet users to remain vigilant about cybercrimes and security and to actively educate others to foster a safer online environment.

Rackspace 2023 cybersecurity research report: This report highlights the critical concerns and adaptive strategies in cybersecurity, emphasizing the increasing importance of cybersecurity as a primary business concern and a major focal point of it investment among it professionals globally

Accenture cybersecurity state of play report 2023: The report from Accenture focuses on how enterprise innovation is boosted by cybersecurity to increase company resilience. It demonstrates that businesses that closely match their cybersecurity initiatives to

their operations gain market share and enhance customer happiness, staff productivity, and trust.

Research from cybersecurity ventures: Cybersecurity ventures offers an extensive compilation of cybersecurity research, including data, forecasts, and analyses of cybersecurity and cybercrime.

International journal of trend in scientific research and development: -
Internet consumers' ignorance about cybersecurity and cybercrimes. The requirement for a structure to maintain internet users' awareness campaigns to reduce cybercrimes.

International journal of current science: - The necessity of educating new and rural internet users on cybersecurity and digital literacy because they are more susceptible to online attacks. A thorough legislative framework is required to successfully combat the issue of cybercrime.

International journal of mechanical engineering and technology: - the significance of government agencies' and cybersecurity experts' capacity-building and training initiatives.

Review of cybercrime in India: an overview

The requirement for focused, regional cyber awareness training to optimize security culture and reduce the consequences of a cyberattack. The necessity for leaders at the board level to comprehend cybersecurity risks and threats.

1.3. Objectives

- To study Cybercrime in India
- To explore the awareness level among youth regarding Cybercrime.
- To evaluate the impact of demographic factors on the awareness level.

1.4. Research Methodology

This research paper aims to evaluate the awareness level of youth in Maharashtra regarding cybercrime. The foremost objective of the research is to know about cybercrime and to assess the awareness level in Maharashtra. Primary and secondary data has been collected through questionnaire and journals, newspaper articles, Government reports respectively. Chi square test is used to test the hypothesis.

1.5. Data Collection

To know the awareness level of youth in Maharashtra, Primary data has been collected in questionnaire form through google forms, Structured questionnaire was sent online. Questionnaire was sent to 110 individuals out of which 85 respondents replied effectively. Non-probabilistic convenient sampling method was used to collect data. To analyze the data chi square test, various graphs and tables are used.

Research Limitation

- 85 sample size is way too small for entire representation of Maharashtra.
- Study is restricted only to Maharashtra state.
- Non probabilistic, convenience sampling is used.
- Time and cost are the constraints.

1.6. Data Analysis & Interpretation

Respondent Profile

Items	Categories	Frequency
Gender	Male	45
	Female	40
	Total	85

Age Group	15-18	26
	19-24	42
	24 and above	17
	Total	85

Table 1: Respondent's Profile

Are you aware about cybercrime?

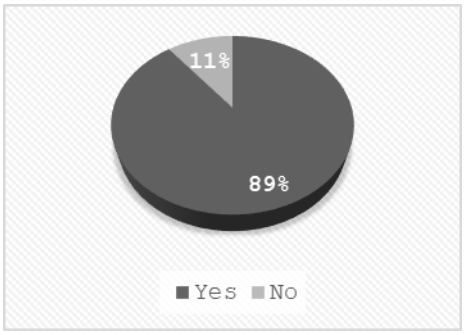

Figure 1: Awareness Regarding Cybercrime

Hypothesis Testing

Null Hypothesis (H0) - There is no significant relation between gender and awareness level for cybercrime.

Alternate Hypothesis (H1) - There is significant relation between gender and awareness level for cybercrime.

	Aware About Cybercrime	**Not Aware about Cybercrime**	**Total**
Male	40	3	43
Female	36	6	42
	76	9	

Table 2: Awareness level in Male and Female

Observed Count (O)	**Expected Count (E)**	**(O-E)**	**$(O-E)^2$**	**$(O-E)^2/E$**
40	38.447	1.55	2.40	0.062
3	4.55	-1.55	2.40	0.52
36	37.55	-1.55	2.40	0.06
6	4.44	1.55	2.40	0.54
X^2				1.182

Table 3: Chi Square Calculation

X2 (1, N=85) = 1.182, p = 0.273536. Calculated chi square value is less than the chi square critical value. Therefore, the **researcher fails to reject the null hypothesis (H0)**. Hence, there is no significant relation between gender and awareness level for cybercrime.

Null Hypothesis (H0) – There is no significant relation between age and awareness level for cybercrime.

Alternate Hypothesis (H1) – There is significant relation between age and awareness level for cybercrime.

	Aware About Cybercrime	**Not Aware about Cybercrime**	**Total**
15-18	23	3	26
19-24	38	4	42
Above 24	15	2	17
Total	76	9	85

Table 4: Awareness level in different age groups

Observed Count (O)	**Expected Count (E)**	**(O-E)**	**(O-E)2**	**(O-E)2/E**
23	23.24	-0.24	0.057	0.002
3	2.75	0.24	0.057	0.020
38	37.55	0.45	0.202	0.005
4	4.44	-0.45	0.202	0.045
15	15.2	-0.20	0.040	0.002
2	1.8	0.20	0.040	0.022
X^2				0.096

Table 5 Chi square calculation

X^2 (1, N=85) = 0.096, p = 0.951269. Calculated chi square value is less than the chi square critical value. Therefore, the researcher **fails to reject the null hypothesis (H0)**. Hence, there is no significant

relation between age and awareness level for cybercrime.

Primary Online Activities

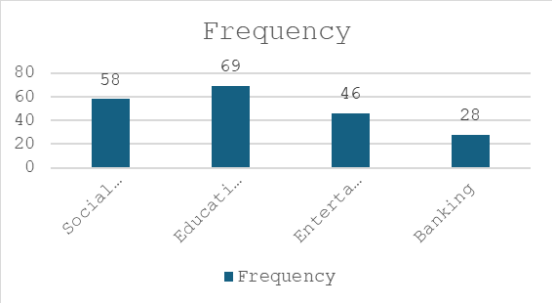

Figure 2 Primary online activities

Have you ever been a victim of cyber-attack or online fraud?

Figure 3 Victim of cybercrime

66% of respondents have never been a victim of cybercrime. Whereas, 34% of respondents are victim of cybercrime.

Have you ever reported a cybercrime?

Only 23.5 % of respondents have reported a cyber crime to concerned authorities.

Are you aware of grievance redressal mechanism (consumer support) in your area ?

55% of respondents are aware about the grievance redressal mechanism for cybercrimes. Whereas 45% of respondents are not aware about the same.

Have you participated in any cyber security awareness program by an authority?

49% of respondents have participated in cyber security awareness programs conducted by the authorities. On the other hand, 51% of respondents have never attended such events.

1.7. Conclusion

The smallest of transactions of a vegetable seller to Reserve Bank of Bangladesh or any other country using SWIFT technology, cybercrimes have been reported everywhere. From password and OTP sharing to hacking social media accounts, emails of individuals and corporations, the biggest protection required is against cybercrimes. The only way is to be aware and take precautionary measures while doing the smallest of the transactions. The study shows almost 37% of the victims have fallen prey to these frauds but on awareness level 51% have no idea on or never attended any workshop for the same. Moreover, there is no relation between age and gender with the awareness level of youth in Maharashtra. It is extremely important to create more and more cybersecurity awareness programs across the globe to protect the world from the new age crimes

References

Anupreet Kaur Mokha. A Study on Awareness of Cyber Crime and Security. Research J. Humanities and Social Sciences. 8(4): October -December, 2017, 459-464. doi: 10.5958/2321-5828.2017.00067.5

How to increase cybersecurity awareness. (n.d.). ISACA. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/how-to-increase-cybersecurity-awareness

CISA Cybersecurity Awareness Program | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/resources-

tools/programs/cisa-cybersecurity-awareness-program

Cybersecurity Awareness Month | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/cybersecurity-awareness-month

Vajagathali, M., Navaneeth Kumar, S., B Balaji, N., & Department of Criminology and Forensic Science, School of Social Work, India. (2019). Cyber Crime Awareness among College Students in Mangalore. J Forensic Sci & Criminal Inves. https://doi.org/10.19080/JFSCI.2019.12.555828

Kamble, Rakshit, & Sharma. (2023, February). Awareness concerns of Cyber Security for citizens in Navi Mumbai and Panvel Zone . International Journal of Advances in Engineering and Management (IJAEM) , 5(2), 706–712.

Kothawade, M. R., & Agarwal, P. (2016, March 17). An Analysis of Cybercrime Scenario in Pune. International Journal of Computer Applications. https://doi.org/10.5120/ijca2016908794

Research overview: Cybersecurity. (2024, March 27). ARCH-India. https://arch-india.org/research-areas/cybersecurity

India Cybersecurity market Insights. (n.d.). https://www.mordorintelligence.com/industry-reports/india-cybersecurity-market

Topic: Cyber security in India. (2023, December 19). Statista. https://www.statista.com/topics/8251/cyber-security-in-india/

Saraswat, V. & NITI Aayog. (n.d.). Cyber Security. https://www.niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf

Juyal, T., Thapliyal, S., Garg, N., & Singh, D. (2023). A Study on Cyber Security and its Challenges in India. In Lecture notes in networks and systems (pp. 151–159). https://doi.org/10.1007/978-981-99-3761-5_15

Cyber Security Research Papers | SANS Technology Institute. (n.d.). https://www.sans.edu/cyber-research/

State of Cybersecurity Report 2023 | Accenture. (n.d.). https://www.accenture.com/us-en/insights/security/state-cybersecurity

Freeze, D. (2023, January 11). Cybersecurity research: all in one place. Cybercrime Magazine. https://cybersecurityventures.com/research/