DIGITAL EMPOWERMENT AND CYBERSECURITY: UNDERSTANDING PUBLIC AWARENESS OF DIGITAL INDIA INITIATIVES

RICHA SHARMA[1], ASTHA GOYAL[2], ROLI BANSAL[3#], CHETAN YADAV[3], LIPIKA[3], ESHAAN R JAMES[3]

[1]Professor, Department of Computer Science, Keshav Mahavidyalaya, University of Delhi, India

[2]Assistant Professor, Department of Computer Science, Keshav Mahavidyalaya, University of Delhi, India

[3]Associate Professor, Department of Computer Science, Keshav Mahavidyalaya, University of Delhi, India

[3]Student, Department of Computer Science, Keshav Mahavidyalaya, University of Delhi, India

Corresponding Author: [#]roli.bansal@keshav.du.ac.in

ABSTRACT

Digitalization refers to the process of adopting digital technologies to streamline and enhance everyday activities, thereby making life easier. This includes the use of digital tools to facilitate communication, access to information, transactions and service delivery, which improves the efficiency, convenience and overall user experience. This study primarily examines the daily usage of digital technologies and cyber awareness among individuals in general, across different age groups and other demographics in the Indian context. In this research, we examined the adoption of digital technology, by focusing on the usage of financial services, online payment portals, and involvement in government initiatives. A survey was conducted to collect data about the digital awareness and cyber-attack experiences of the participants. A thorough analysis of the response data shows that there is a stronger level of interaction with digital platforms and cyber awareness within urban adults in comparison to other age groups and areas of residence. It has also been observed that digitalization of basic services has made life easier for a large section of society, still there is a need for extensive promotion of government initiatives and online resources available in specialized domains like education, healthcare and business. Also, there is a scope for improvement regarding spreading digital awareness through educational initiatives and training programs and effective and timely redressal of complaints pertaining to cybercrimes.

Keywords: *Digitalization, Digital Literacy, Technology Access, Digital India, Cybersecurity, Cyber Awareness, Digital Adoption*

1. INTRODUCTION

In recent years, the use of internet has witnessed significant growth in the number of users connected globally. In 2010, the number of internet users was 2 billion [1] with a significant increase to 4.5 billion by 2020 [2] and 5.3 billion by January 2024 [3]. But in India alone, about 7.5% of the population was using the internet in 2010 [4] which increased to about 43.4% in 2020. Currently, as of January 2024, India has over 751.5 million internet users which is 52.5% of the total population [5]. Smart devices have become a significant part of day-to-day lives. With an increase in the usage of smart devices from just surfing the web, or using social media apps to using the same for digital payments called Unified Payments Interface (UPI), net-banking, online shopping via e-commerce apps, the shift is evident. India is one of the fastest developing countries with its digital realm way more advanced than many leading nations. The government of India has launched multiple national public digital platforms such as DigiLocker, Digi Yatra, Unified Mobile Application for New-age Governance (UMANG), Rapid Assessment System, OpenForge, Application Programming Interface (API) Setu, Poshan Tracker, National AI Portal, MyScheme, India Stack Global and many more [6].

While the use of internet in India has drastically increased, many netizens are still unaware of potential information leaks and cybersecurity risks and apply only minimal and relatively basic protective measures [7]. Figure 1 depicts some common cybersecurity threats, which sometimes people even fail to have a basic

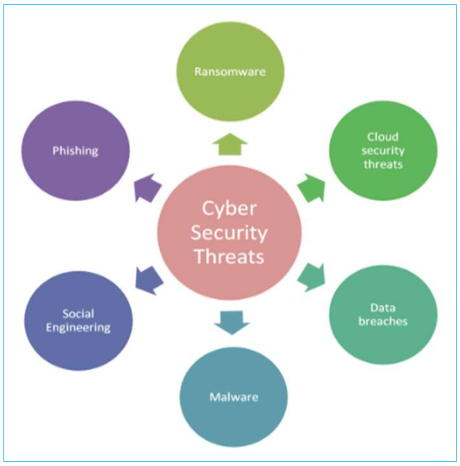


Figure 1: Cybersecurity threats

knowledge of which leads to a total lack of cyber awareness. As technology evolves, cybersecurity awareness among users becomes significant to secure personal and sensitive information from malicious attacks. To secure devices it is necessary to follow certain security frameworks and protocols to minimize the risk by taking certain precautions like- creating different passwords for different accounts, applying 2-factor authorization, using a VPN service when connecting to a public network, maintaining social media, and avoiding uploading sensitive information on these platforms. However, the levels of cyber security awareness among individuals differ across different demographic dimensions.

In light of the above, this study attempts to- a) raise awareness of digital services provided by the Indian government under the mission of *Digital India*, b) inform the readers about cyber security measures that would keep them safe while using the above services and c) determine the extent to which users know about government initiatives and cyber security at present. The authors feel that this study would impart robust information to the readers about the extensive digitalization happening in India and facilitate them to make informed decisions while moving in digital spaces.

The paper is structured in the following way. Firstly, section 2 discusses about the digital initiatives taken up by the government for the ease of users and cybersecurity measures for their safety. It also sheds light on the background knowledge in the same field establishing a foundational understanding of previous work and identifying gaps in current knowledge. Section 3 outlines the research methodology to design and launch the survey that addresses digitalization and cyber awareness among Indian users. The questionnaire adequately includes a wide variety of questions that focus on the above factors. The survey was launched and responses were collected. Section 4 discusses the responses and analyses the results to understand different knowledge levels among the users. Finally, the conclusion in section 5 gives the summary of key findings, indicating their significance and presents direction for future research and ways to increase cyber-awareness among the users.

2. BACKGROUND

As we advance further into the digital age, it becomes increasingly important to develop a foundational understanding of key concepts. The following sections underscore the critical elements of digitalization, cybersecurity and associated services. In addition, the literature review of the studies done in this domain is also presented.

Digitalization refers to the process of imposing digital technologies to transform existing businesses, processes, and services digitally. This involves the integration of information and communication technologies, digital transformation and automation to provide increased opportunities for developing countries like India. The rapid adaptation of digital solutions for traditional tasks and processes has increased efficiency and reduced operational costs [8]. The delivery of services through digital platforms and the use of appropriate technologies to do so results in digital services. These services range from simple information websites to complex transition processing applications.

The Digital India initiative is a pan-nation program launched by the Government of India to ensure that policies and schemes of the government are made available to the citizens through electronic medium by improving current infrastructure and increasing internet connectivity. This program includes DigiLocker, UMANG, Aadhaar, electronic Know Your Customer (e-KYC), e-Kranti, etc.

2.1. E-Governance

E-governance involves the use of digital platforms and techniques to digitize government services and make them accessible to citizens, businesses, or other government bodies. The main aim of e-governance is to increase efficiency, transparency, and accountability in government functioning by using information and communication technologies. To implement e-governance in India the government of India launched the Digital India initiative. Some of the services are highlighted as follows.

UMANG - (Unified Mobile Application for New-age Governance)- A centralized application that offers e-governance services to citizens from Central, state, and local government bodies. UMANG is developed by the Ministry of Electronics and Information Technology (MeitY) and Natural e-Governance Division (NeGD) to drive India into e-governance services [9].

E-Kranti - Also known as e-Governance Plan 2.0, it focuses on the delivery of services to citizens digitally. It aims to transform India into a digitally empowered nation by delivering services across various domains like health, education, agriculture, and more [10].

Aadhaar - It is a unique identification number issued to the citizens of India by UIDAI [11], an undertaking of the Government of India. It stores biometric and demographic data and is used to access services, subsidies, and other benefits and schemes provided by the government.

e-KYC (Electronic Know Your Customer) - e-KYC is the process of electronically verifying the identity of a person or a business. It is crucial for onboarding customers in various sectors. For example, in banking, telecom, and financial services E-KYC is a vital verification measure [12].

DigiLocker - It is a cloud-based service launched by the Government of India as a part of the Digital India initiative. It allows citizens to store access and share their important documents and certifications. These documents can include PAN (Permanent Account Number) cards, Aadhaar cards, school transcripts and marksheets, domicile certificates, and more [13].

Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA) - This scheme was launched by the government of India to impart digital literacy to citizens in rural areas. The goal of this scheme is to make at least one person, in each housing category, digitally literate by providing basic digital literacy training [14].

2.2. Financial Services and Technology

For the developing nations like India, finance sector plays a key role in the economic development. This sector has to be the strongest and since digitization is adapted worldwide and seen as a very important factor for economic growth, the government of India has taken some initiatives in finance sector under the Digital India scheme, as discussed in the following subsections.

Unified Payments Interface (UPI) - A payment **system** developed by the National Payments Corporation of India (NPCI) [15] that makes instant money transfers between bank accounts through mobile phones possible. To increase the usage of UPI technologies, banks are taking the initiative to accomplish the motive of Digital India. UPI became popular during the demonetisation phase [16].

National Electronic Funds Transfer (NEFT) - Another development by the government under the Digital India initiative is NEFT. It is an online retail payment system managed by the Reserve Bank of India (RBI). Unlike UPI, NEFT transactions are not processed in real-time but they are processed in 48 half-hourly batches throughout every day. Since its beginning, RBI witnessed the highest number of transactions on February 29, 2024. NEFT system achieved a milestone of 4.1 crore transitions in a day so far [17].

Mobile Wallets - Mobile wallets are, in one way or more, similar to our regular wallets which we carry in our day-to-day lives. It is an application that allows users to make mobile payments [18]. According to a report by Business Standard [19], mobile wallet payments in India are likely to surpass Rs 531.8 trillion ($2.5 trillion) in 2028. They believe it is mainly due to the government's concerted efforts to make India, Digital Bharat.

2.3. Cyber Literacy and Cybersecurity

Cyber literacy refers to the knowledge or skills required to understand and use the digital world safely. It includes understanding online services, recognizing cyber threats, and knowledge of how to protect personal information online. Cybersecurity refers to the application of technologies, prevention and control measures to protect systems, networks, and data from digital attacks. It involves the implementation of rules and protocols to defend against cyber-attacks, unauthorized access, and data breaches. According to studies it has been found that there are more than 4000 global ransomware attacks daily, reflecting the situation of the digital domain and internet world [20]. The topic of cybersecurity primarily concerns individuals making the human factor one of the largest elements in developing effective cybersecurity [21]. Figure 2 illustrates some major events in the timeline of the cybersecurity domain in India.

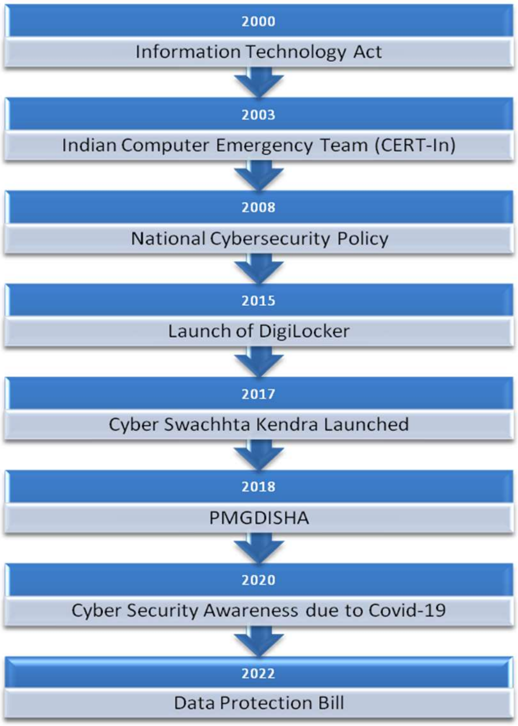

2000
Information Technology Act
2003
Indian Computer Emergency Team (CERT-In)
2008
National Cybersecurity Policy
2015
Launch of DigiLocker
2017
Cyber Swachhta Kendra Launched
2018
PMGDISHA
2020
Cyber Security Awareness due to Covid-19
2022
Data Protection Bill

Figure 2: Timeline of cybersecurity events in India

Cyber awareness includes the awareness of how to recognize cyber threats and avoid getting scammed. A study focusing on the relationship between cyber security awareness, knowledge, and behaviour in the general public found that most internet users have enough knowledge about cyber threats but ironically deploy minimal protective measures [22]. Another study [23], conducted on students of undergraduate teachers' education programs to investigate the cybersecurity awareness and protective behaviors of students during the shift to remote learning due to COVID-19, found that students have average threat knowledge and employ moderate protective behaviors online. A key finding was that there was no significant relationship between the two. The paper suggested the need for awareness campaigns and incorporating cyber security discussions in orientations and course frameworks to address this gap. In the occurrence of a cybersecurity attack both internal and external factors contribute to the vulnerability of an institution's information systems.

Social engineering is a technique that exploits weaknesses of human nature to gain unauthorized access or information and hamper the security of individuals or organizations [24]. It involves taking advantage of people's natural tendencies to trust and be helpful. The key findings were on the factors influencing the effectiveness of cybersecurity awareness and training programs, presenting that a combination of business, social, cultural, governmental, organizational, and individual level dynamics are needed for the success of such programs. Additionally, it was identified that factors such as limited training budgets, employee behavioural biases, and the evolving nature of social engineering attacks pose a challenge in the implementation of effective training and awareness programs.

Studies have repeatedly demonstrated the significance of human behaviour and its impact on data breaches, indicating that around 50% of major data breaches in recent times were caused due to unintentional human errors such as misconfiguration, poor patch management, and the use of weak or repeated passwords [25]. On the contrary, overconfidence and cognitive biases can also impair an individual's security status and lead to suboptimal decisions regarding cyber threat protection. The paper also identifies four anti-patterns: (a) security decisions based on mere intuition rather than data and evidence; (b) failure to implement basic security controls; (c) over-reliance on static threat knowledge such as basic virus scanner tools and (d) weaknesses in security governance [26].

A large number of attacks on current digital systems are made possible by exploiting the weaknesses inherent in the underlying design of the technology or the hardware components. Hence, there also needs to be a shift of attention to the Digital Security by Design (DSbD) concept [27]. According to a research report [28], a significant portion of cybersecurity vulnerabilities stem from human error. Common mistakes include inadequate device supervision, unauthorized sharing of access credentials, improper storage of login information, interaction with suspicious digital content from unfamiliar sources, and general carelessness.

According to yet another study conducted on Saudi Arabian university students, it was determined that students had an average level of cybersecurity awareness, irrespective of their gender and qualification. However, a noticeable finding was that females showed more concern about topics related to cyber security. The area of residence also has an impact on students' awareness level, students from urban residencies possess more understanding and knowledge of cyber security and digital concepts as compared to students from remote areas. The recommendations of the study included policy measures to be taken by university authorities to make students aware of the importance of cybersecurity and teach measures to prevent cyber-attacks from an early stage [29].

Today, cybersecurity curricula are available across multiple educational institutions, including a vast array of programs and modules for specific institutions and individuals. Nonetheless, a general agreement on the best measures for cybersecurity training is yet to be reached. Simulation-based solutions have gathered the most attention and confidence in terms of research due to their effectiveness. However, there is still ongoing debate among researchers regarding the optimal training delivery methods and the design of cybersecurity exercises [30].

2.4. Privacy and Data Protection Measures

Privacy and data protection includes safeguarding personal and sensitive information from threat actors. Data important enough needs to be protected from unauthorized access for the privacy, and security of an individual or an organization, for example, financial data, health records, and Personally Identifiable Information (PII), such as names, addresses, financial details, etc.

Authors in [31] discussed Information Security Risk Assessment (ISRA), a tool of cybersecurity measurement, and opined that it could help discover underlying systemic problems, and thus safeguard future cyber security concerns. They also observed that high breach costs result in greater attention to cybersecurity, and subsequently carrying out an ISRA.

The advancement in technology has provided several technical measures that can be implemented for data and privacy protection. Some of these are discussed as below.

Virtual Private Network (VPN) - Virtual Private Network is a service that hides users' IP addresses over a network, providing a secure connection over the internet. VPNs are used to protect privacy. According to a report by Business Standard India's data centres faced over 51 million cyber-attacks in 2021 within a span of 9 months [32]. The threat actors used 40,000 unique IP addresses to commit this attack. Hence protecting oneself from these kinds of attacks is important.

Two factor Authentication (2FA) - According to Ashlee Vance, 20% of passwords used by people can be concluded by a list of only 5,000 passwords [33] Hence we need a new security process that requires two levels of identification before granting access to someone's account or system. 2FA aims to enhance the resilience of password-based authentication processes by requiring the user to provide additional authentication processes, e.g., One Time Passwords (OTP), a security token, etc.

Digital Footprint - It is a trail of data that individuals leave behind when they use internet. It can include anything from comments, likes, etc, on social media, websites visited, and online purchases. Nowadays it is beneficial to maintain a decent digital footprint as reports show that 70% of employers use social networking platforms to look for potential candidates for recruitment [34]. Every aspect of an individual's life like social, political, economic, etc has been influenced by the modern digital age. This trend of increase in digital services also comes with equal threats and an increase in cybercrimes.

According to the Cyber Security Breaches Survey conducted in 2022 [35], it was revealed that around 39% of businesses have been a victim of cybercrime at least once. Cybercrimes are on the rise in India as well, with the state of Uttar Pradesh reporting a maximum number of cybercrime cases. Cybercrime affects nearly every domain like Business, consumer behavior, sexual solicitation, socio-eco-political domains, etc.

While these studies provide valuable insights into the landscape of cybersecurity awareness and the digital literacy world, there remains a gap in our understanding of the specific situation in India. Further, it was observed that most of the existing studies focused on specific strata of the population and so their results are relevant to those domains only. The present study however, covers multiple demographics and digital services specific to India. The participants included students, teachers, working professionals and people of different background, age and region. This made the study inclusive of diversified data. The rapid digital transformation of the country that has happened in the past few years, coupled with its immensely diverse population and unique socio-economic structure, drives us to a closer examination of the current cybersecurity awareness among Indian citizens. We seek to uncover critical insights that can help in more effective strategies and policy-making.

This research thus contributes to the current knowledge by providing an updated information on the state of digital awareness and cybersecurity practices in an Indian context. The knowledge gained from this study is valuable for improving the

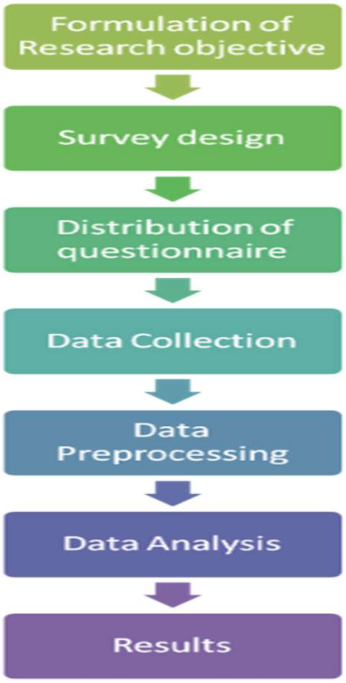


Figure 3: Flowchart of the research methodology

level of cyber awareness among Indian citizens which can be accomplished by better policy making and awareness campaigns inspired by the findings and insights of this study. The following section details the design of the research and the methodology used to gather data.

3. Research Methodology

In present times, when the use of the internet is rapidly growing, it has become crucial to understand the level of cybersecurity awareness among the general public. This study aims to evaluate the current state of digital literacy and cybersecurity knowledge across varied demographic groups in the society. The research examines in what ways factors like age, gender, area of residence, occupation, and level of education influence an individual's level of cybersecurity awareness.

The following subsections describe our research methodology comprising design, data collection methods, analysis techniques, ethical considerations, and study limitations, as shown in Figure 3.

The approach ensures that the study is transparent, comprehensive, and well-structured providing a clear framework for future decision and policy making.

3.1 Research Questions and Objectives

The study addresses the following multifaceted research questions, by employing a broad qualitative and quantitative approach.

RQ1: Does an individual’s age, gender, area of residence, occupation, and level of education impact their cybersecurity awareness level?

RQ2: Do people commonly use digital services/ platforms in their daily lives aware of possible threats/ concerns/ safety measures?

RQ3: How many people are aware of the Government of India’s initiatives like DigiLocker, Unified Mobile Application for New-age Governance (UMANG), and Unified Payments Interface (UPI), and do they actively use them?

RQ4: Do only people using digital services fall prey to cyber security issues?

3.2. Research Design

We have used a mixed method approach for the study, to analyze both qualitative and quantitative aspects of the response data and present results more comprehensively. The questionnaire was initially distributed through personal networks. The primary source of data was a questionnaire circulated online through various platforms to reach a diverse audience. The questionnaire is available at: https://forms.gle/eXaKRnMNHBJPHwVS9. They were also prompted to share the survey link with their own contacts, allowing the sample to expand and reach a wider population. To ensure a good response rate we sent frequent follow up reminders.

The authors understand that there could have been a sampling bias due to the use of online channels only for the dissemination of the survey questionnaire. As a result, people who are more active on the internet or digitally literate could be overrepresented. However, this only strengthens our study as our inherent aim was to analyse the cyber awareness amongst the digitally active population. The response data was pre-processed and analysed using Python to generate graphs for various categories discussed in section 4.

The qualitative aspects of the research design allowed for a deeper insight into respondents' understanding and experiences related to cybersecurity awareness. The questionnaire was divided into three sections as represented in Figure 4.

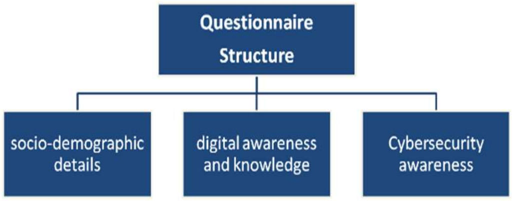


Figure 4: Questionnaire Structure Diagram

- The first section included socio-demographic details like name, age, gender, occupation, and education level.
- The second section contained questions evaluating participants' digital awareness and knowledge about digital initiatives and platforms. The choice statements were presented in an ordinal frequency scale with three options: always, sometimes, and never.
- The third and last section contained questions on a 3-point Likert scale, determining the level of cybersecurity awareness, involving questions related to online frauds and scams. The response options were: yes, no, cannot say.

The survey was completely voluntary in nature. Participants were provided with complete instructions and information before taking the survey. They were also assured regarding the privacy and safety of their data. The collected information was used for academic purposes only. The data collection process was ensured to be conscientious and adhered to ethical research practices.

4. RESULT AND DISCUSSION

The response data collected by the google forms is further analyzed and presented in a well-structured manner. This section gives the deep analysis of the response data using graphs and textual detail, in a more understandable form.

4.1 Demographic Data

Demographic data in this research are in the form of respondent data: name, email, age, gender, area of residence, occupation, and education level completed/pursuing. Gender have been categorized as male, female and other as depicted in Table 1. Age groups have been categorized as categories 1, 2, and 3 having ranges of 10-18 years, 19-44 years and 45-80 years respectively, as depicted in Table 2. Area of residence have been categorized as urban, suburban and rural depicted in Table 3. The distribution of age groups of the sample is depicted in Figure 5 and the distribution of age categories among male, female and other respondents is shown in Figure 6.

Table 1: Demographics of gender

Gender	Number of respondents	Percentage
Male	135	50.4%
Female	132	49.3%
Other	1	0.3%

Table 2: Demographics of age groups

Group	Age group (in years)	Number of respondents	Percentage
Category 1	10-18	86	32.1%
Category 2	19-44	99	36.9%
Category 3	45-80	83	31.0%

Table 3: Demographics of area of residence

Area of residence	Number of respondents	Percentage
Urban	162	60%
Suburban + Rural	106	40%

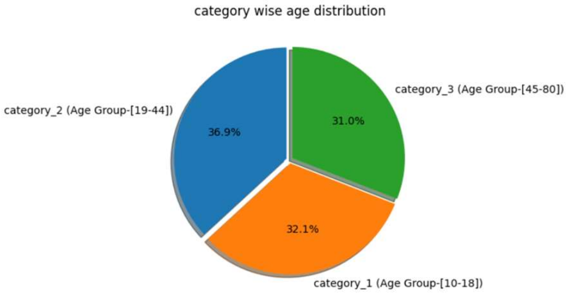


Figure 5: Distribution of age categories

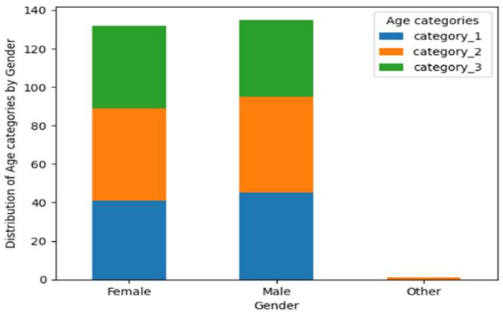


Figure 6: Distribution of gender wrt age

The number of participants from urban area was slightly more than suburban and rural areas combined. This probably reflects the higher population density and greater access to channels of survey distribution in an urban area, where people are more likely to be engaged either in online activities or community programs. In contrast, rural areas are often less well-connected and have fewer opportunities to take part in surveys, whereas suburban areas fall somewhere in between. Now, engagement in online activities or community programs also relies on academic qualification of the respondents. Figure 7 presents the distribution of age category with respect to qualification.

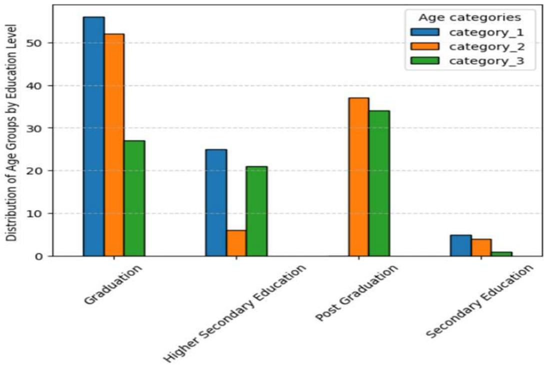


Figure 7: Distribution of education level wrt age

From the above distribution, it appears that for category 1 (age group 10-18), the highest proportion of respondents are currently pursuing under graduation. The relatively low numbers of those with secondary and higher secondary education may reflect the targeting of active engagement in online activities or community programs. For category 3 respondents, there is a wider range of educational backgrounds.

In the next subsection 4.2, we discuss the questions related to online digital platforms, while subsection 4.3 discusses the questions concerning cyber-attacks.

4.2 Online Digital Platforms Data

The questions in this section target awareness of digital platforms and online services provided by the government to ascertain more popular platforms among the participants. The response data charts for each question are depicted in Table 4. The columns present distribution of responses with respect to (a) age and (b) area of residence (urban / suburban + rural).

Question 1: *I use Unified Payments Interface (UPI) for payments regularly.*

In India, UPI has become a popular digital payment method. Response data charts of Q1 in Table 4 present the distribution of UPI usage, reflecting a very interesting and clear trend in the adoption of digital payments across different sections of society. It can be clearly seen that UPI usage is extremely popular in all age groups. Very few people in all age groups have responded as having never used it. UPI offers a very convenient mode of payment, especially to the elderly. Also, the urban usage is slightly more as compared to sub urban and rural usage taken together due to more exposure to technology in urban area.

Question 2: *I use DigiLocker for storing, sharing, or verification of documents/certificates. I use them to produce documents in official situations, for example, showing your Driving license (DL) to traffic police.*

Q2 response data charts in Table 4 depict that the usage of DigiLocker is more popular in younger population for the purpose of storing their transcripts. It is slowly picking up among the elderly for storing their important documents like Aadhaar, PAN cards, driving licence etc. As depicted in Q1, here also the rural and suburban population needs to be educated regarding benefits of DigiLocker service.

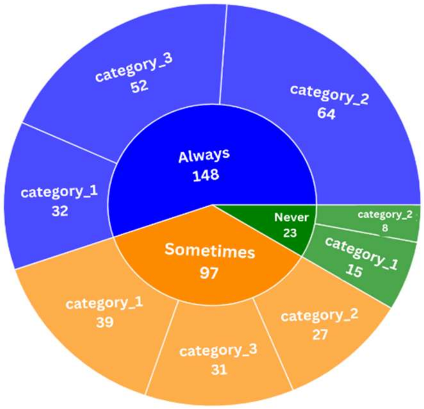
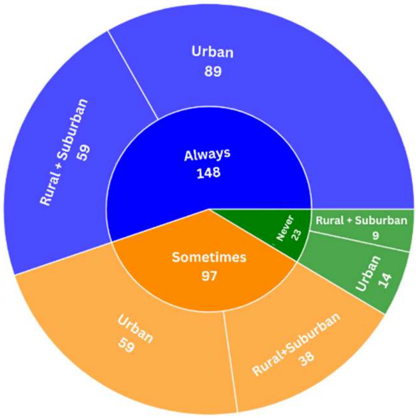
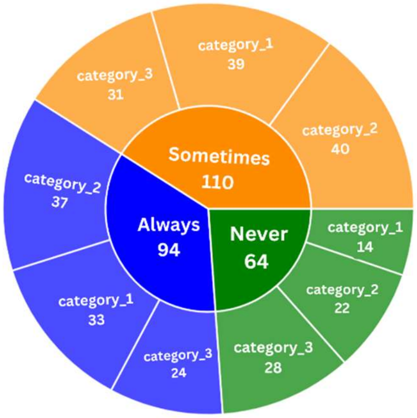
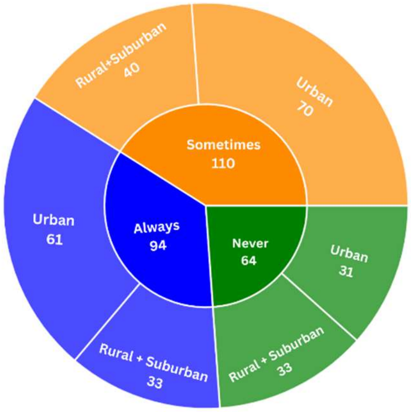
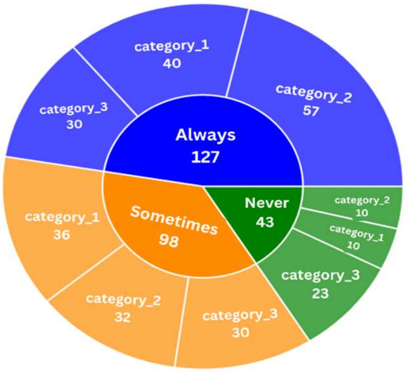
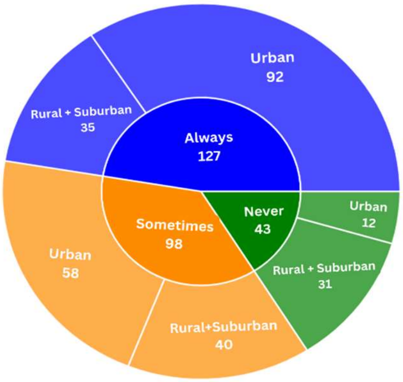
Question 3: *I use online services to apply for government documents like Aadhaar, Voter ID, PAN card, Ration card, and Certificates (caste/ income/ death/ disability/ domicile).*

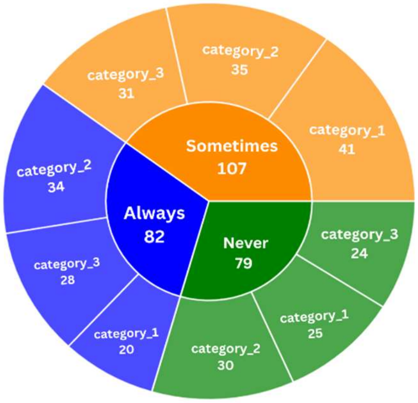
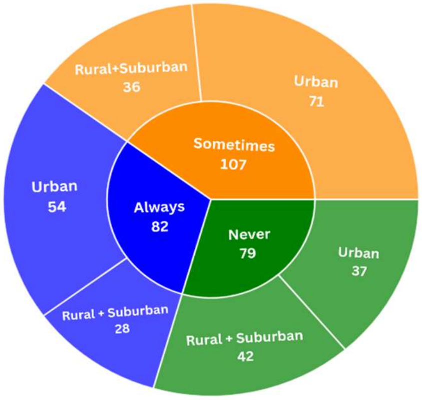
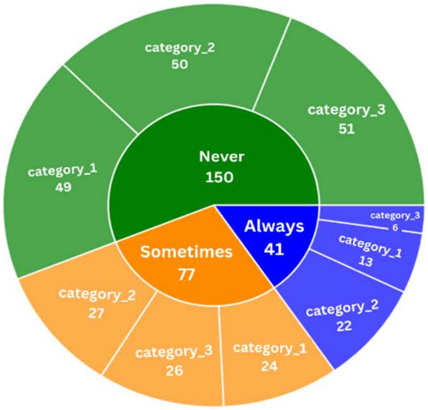
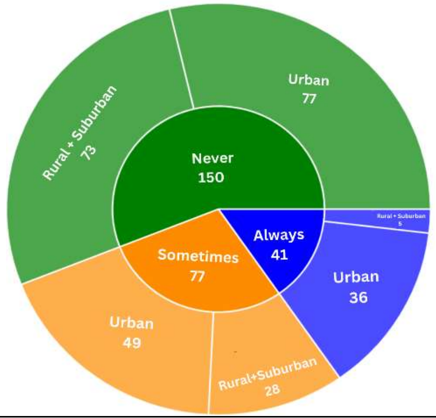
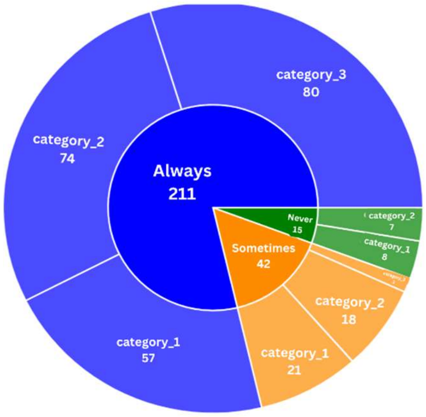
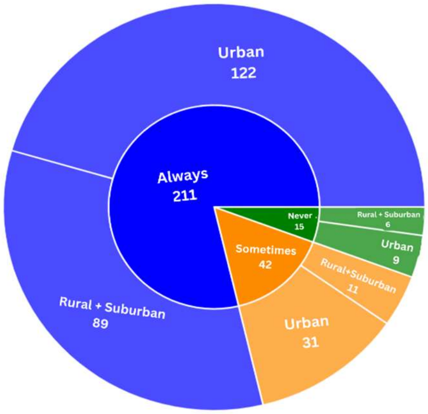
The popularity of online applications for government documents like Aadhaar, Voter ID, and PAN cards has been on the rise. Q3 response data charts in Table 4 depict that a large percentage of people belonging to the age group of 19-44, especially the urban population may be slightly more inclined toward the use of digital platforms for receiving and paying for government services. Moreover, they are able to track the status of their application also online. Hence, they prefer to apply for government documents online as the process is transparent, hassle free and time saving.

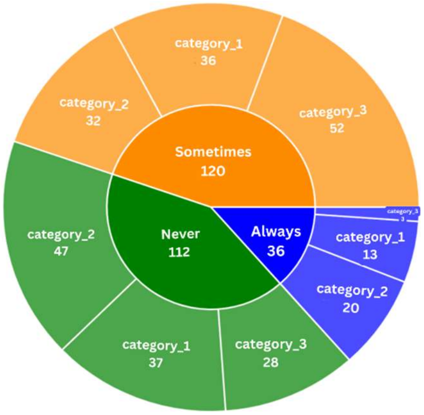
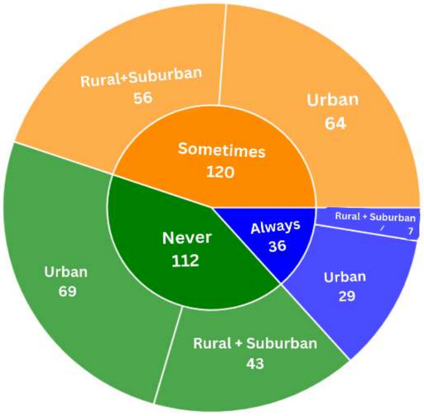
Question 4: *I am aware of digital portals for banking services, such as Aadhaar Enabled Payment System (AEPS), Aadhaar Pay, Cash Deposit, Opening Bank accounts, Money transfer, and Micro ATM and I use these services.*

This survey question shows a similar trend of engagement across different age groups. Response data charts of Q4 in Table 4 show that the opinion of people across all ages seem scattered along “always”, “sometimes” and “never” categories. However, a large share of rural + suburban responses in “never” category in comparison to “always” and “sometimes”, makes it evident that developing focused education and support is necessary for improving awareness and

Table 4: Graphical distribution of response data for survey questions regarding digital initiative awareness

Question	Age Category (a)	Area of Residence (b)
Q1. UPI usage		
Q2. DigiLocker usage		
Q3. Online service usage to apply for government documents		

Q4. **Awareness about digital portals for various banking services**		
Q5. **Awareness about process of obtaining business permits, licenses, and GST**		
Q6. **Familiarity with online platforms for recharging services and making utility bill payments**		

Q7. **Knowledge about digital health and education campaign**		

encouraging the use of digital banking across all age groups of rural and suburban population.

Question 5: *I use the process of obtaining business permits, licenses, and Goods and Services Tax (GST)-related payments/returns online.*

Q5 response data charts in Table 4 depict that a majority of representatives from all age groups simply have no habit of conducting these operations online. This may be due to the fact that most of the respondents were either students or employed persons and these are specialized services falling in the domain of business and trade.

Question 6: *I am familiar with online platforms for recharging services (such as Mobile and Direct-to-Home (DTH)) and making utility bill payments like gas, water, electricity, landline, credit card, etc., and use them.*

Q6 response data charts in Table 4 depict that more than 75% of respondents claimed great familiarity with online platforms for recharge services and utility bill payments. This implies that the usage of such digital services is an extremely popular segment of services. This trend is similar across all age groups irrespective of their area of residence.

Question 7: The response distribution to the survey question Q6 in Table 4 shows that *I know about digital health and education campaigns like e-Pathshala, e-Hospital, and the National Digital Library of India (NDL) and I participate in them.*

The statistics related to the survey question Q7 in Table 4 show that a fair share of population irrespective of their age groups or area of residence, responded as "never" to this question. The percentage of participants knowing about these platforms came out to be very low. In this regard, it is clear that barring a small section of society using digital platforms for health promotion and education, a significant percentage of this cohort is not aware of the government-initiated campaigns about e-health and education.

4.3 CYBER SPHERE DATA

The questions in this section target awareness of cybercrime and cybersecurity.

Question 8: *Have you ever been a victim of a cyberattack/cybercrime and experienced monetary loss due to cyber fraud?*

Figures 8(a) and 8(b) show that a greater proportion of the respondents reported not having experienced cybercrime or money loss due to cyber fraud. This trend would mean that a good proportion of adult people have not been victims of cybercrime. A smaller number of victims among all age groups indicate more cautious online behaviour. The urban population faced more cybercrime incidences as compared to other sections. It is speculated that these variations arise because of variations in exposure and usage levels of digital platforms between these two groups.

Question 9: *I feel it is safe to apply for services online or use digital platforms.*

Figures 9(a) and 9(b) show that a majority of the respondents felt confident about the digital interaction. However, some of them did not find it safe to use these online platforms and that they did not trust online services. The percentage of respondents being uncertain about the possibility asked in the question was higher in comparison to that of responses in other questions. Such a trend is indicative that, though the majority of people believe that online services are safe, there are still a considerable number of respondents who either doubt it or do not know anything about it. General

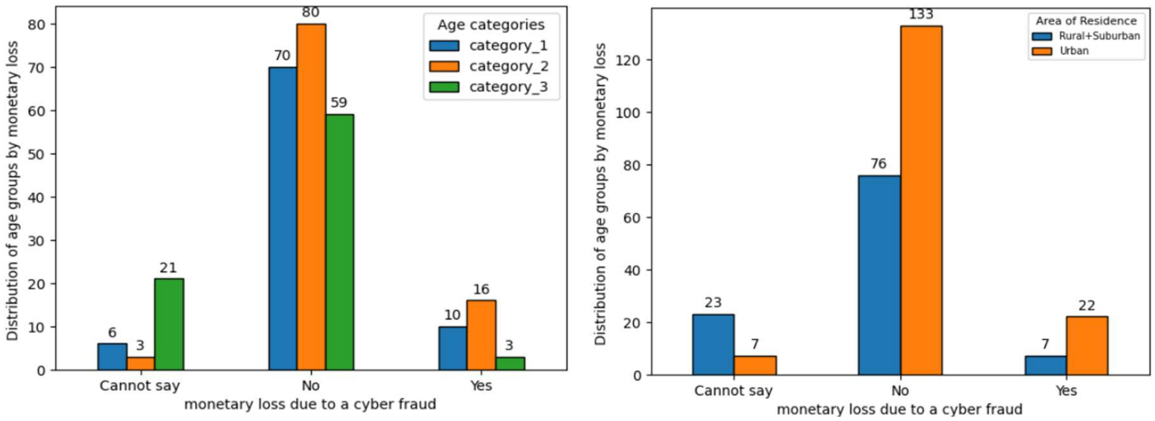


Figure 8: Response distribution regarding victimization of a cyberattack/cybercrime and experiencing of monetary loss due to cyber fraud wrt (a) age and (b) area of residence

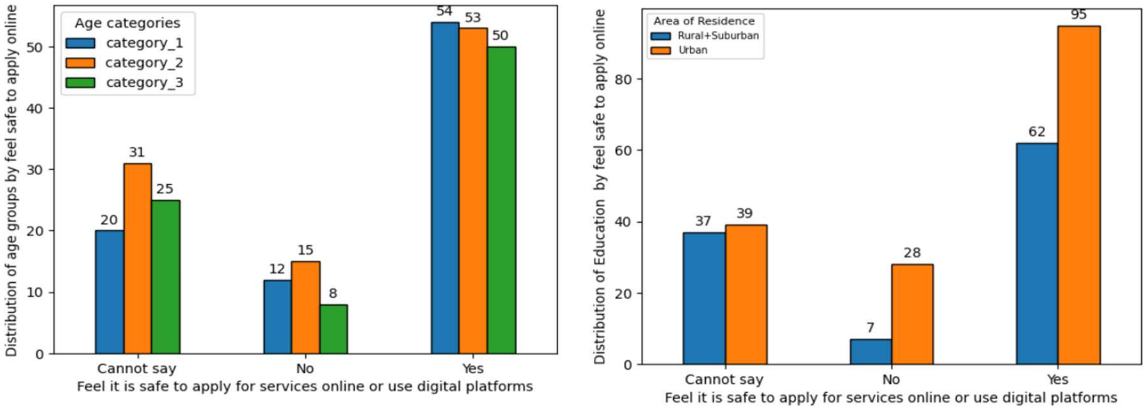


Figure 9: Response distribution regarding feeling safe about applying for services online or using digital platforms wrt (a) age and (b) area of residence

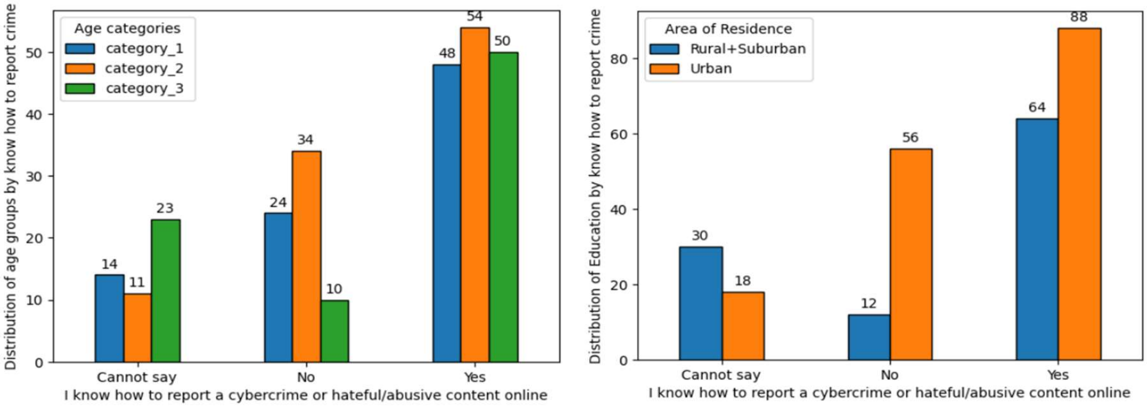


Figure 10: Response Distribution Regarding Awareness About Reporting A Cybercrime Or Hateful/Abusive Content Online Wrt (A) Age And (B) Area Of Residence

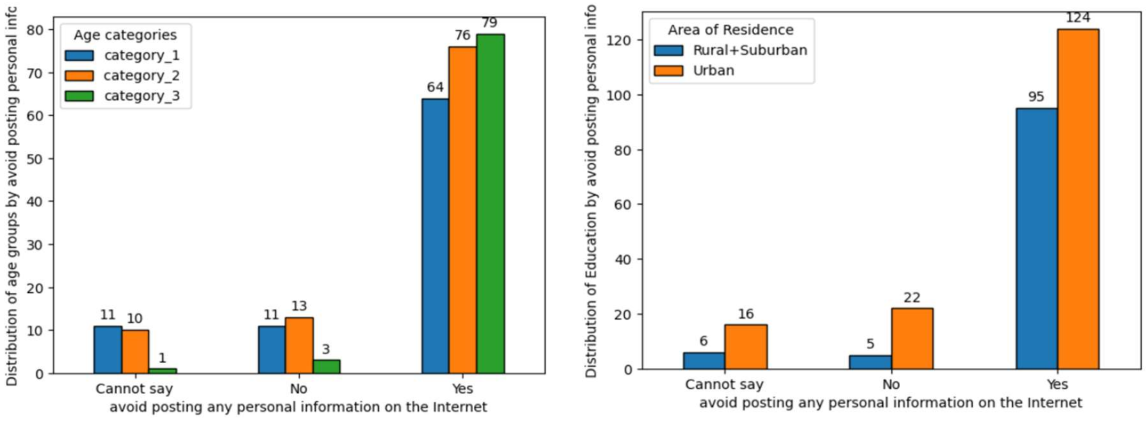


Figure 11: Response distribution regarding avoiding posting any personal information on the internet wrt (a) age and (b) area of residence

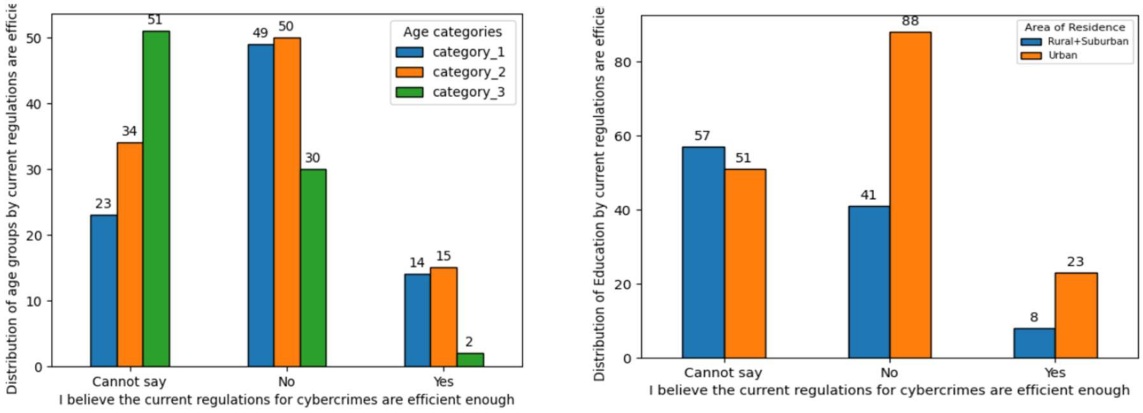


Figure 12: Response distribution regarding believing if current regulations for cybercrimes are efficient enough wrt (a) age and (b) area of residence

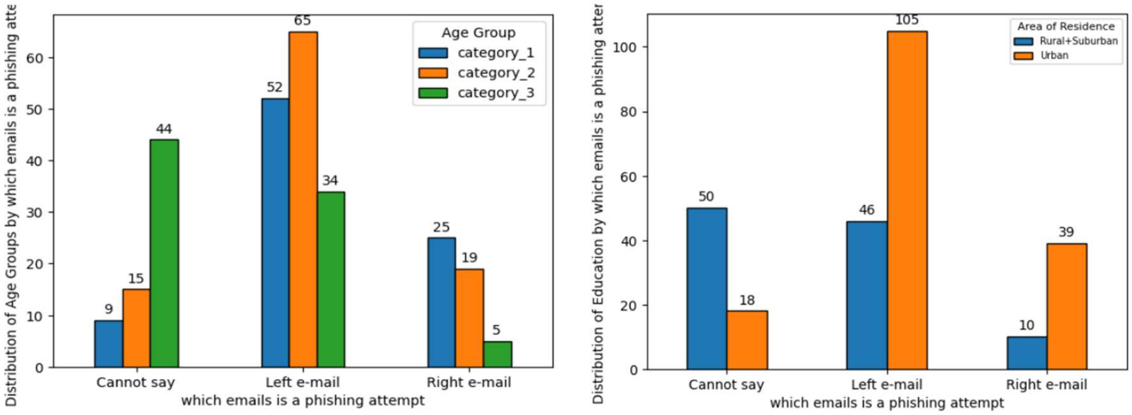


Figure 13: Response Distribution Regarding Phishing Email Recognition Wrt (A) Age And (B) Area Of Residence

digital security awareness and user education may help in improving perceptions of safety across the majority of age groups.

Question 10: *I know how to report a cybercrime or hateful/abusive content online.*

Figures 10(a) and 10(b) show that a majority of respondents are aware of the process of reporting a cybercrime or hateful/abusive content online. It thus comes out that while many people have been exposed to various mechanisms of reporting, there is still a significant portion of the sample of the respondents with limited exposure to those mechanisms. Although the government has setup a helpline mechanism with several modes by which one can report an untoward cyber incident, yet there is still room for popularizing the solutions and making them more user friendly, especially among the rural and suburban population.

Question 11: *I avoid posting any personal information on the internet.*

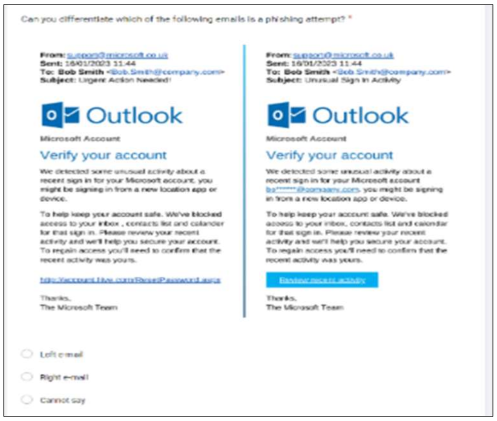
The habit of abstaining from posting personal information on the internet is significantly followed, as Figures 11(a) and 11(b) indicate. The majority of the respondents claimed that they do not post personal information on the web. At this point, it has been established that most of them are aware and would want to protect personal information on the net. With increasing age, generations are more private, meaning the older, the better when it comes to understanding digital risks. In any case, continuous education about online safety is good for all age groups, especially the less digitally aware.

Question 12: *I believe the current regulations for cybercrimes are efficient enough.*

The responses on the efficiency of the existing regulations for cybercrimes present a division based on the ages and area of residence of the participants in Figures 12(a) and 12(b). A majority of the respondents were of the opinion that the current regulations are not efficient and the redressal of reported cybercrimes is poor. Also, a lot of people are uncertain about the action taken after reporting an incidence. Efficient redressal would have been achieved with a better regulatory framework and keeping the process transparent, which would have contributed to helping address concerns and improve satisfaction among all sections.

Question 13: *Can you differentiate which of the following emails is a phishing attempt?*

Figure 13(a) and 13(b) show that while a sizable portion of respondents correctly identified phishing attempts, fewer could not identify the same. Awareness and training in email security wisely applied will help in developing detection skills in all age sets. The results show that the age group 19-44 and those residing in urban areas are more knowledgeable about discerning between phishing and genuine emails. Figure 14 shows two sample emails where the left one is a phishing attempt and the right one is a genuine email.



Can you differentiate which of the following emails is a phishing attempt? *

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Urgent Action Needed!

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account, you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox , contacts list and calander for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

http://account.live.com/ResetPassword.aspx

Thanks,
The Microsoft Team

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Unusual Sign In Activity

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account ba*****@company.com, you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

Thanks,
The Microsoft Team

○ Left e-mail
○ Right e-mail
○ Cannot say

Figure 14: Question Showing Phishing Attempt On The Left And Vs Genuine Email On The Right Side

The overall results of the survey underscore that the use of digital platforms, cybersecurity, and online services are more popular among the age group 19-44 than the age groups 10-18 and 45-80. The young and middle-aged adults feel more confident in using digital tools, know more about the government's initiative in digitization, and can easily recognize phishing attempts. While children under 18 report strong engagement, their confidence is particularly lacking in areas like reporting of cybercrimes and understanding up-to-date regulations. As one might anticipate, elderly citizens have shown slightly lower levels of familiarity and usage of digital services, cybersecurity practices, and online privacy tools, even while showing signs of engagement.

The findings thus highlight many benefits in terms of efficiency and ease, adoption differs depending on the context. Although the findings concur with former research in some aspects, they also reveal unique trends that further need to be investigated. Such insights not only help in understanding digital behaviour but also suggest areas that could be used for further research and public awareness.

5. CONCLUSION

The present study explored various digital initiatives launched by the government of India under the Digital India mission. While going through the same, it was observed that though some of the services are very popular among the citizens, yet some others are not which might prove to be quite beneficial if promoted. With this motivation, this study lists and discusses varied digital services available to the citizens of India and inform them about cyber security measures that would keep them safe while using the above services.

This study further investigated the level of adoption and usage of digital technologies, specifically regarding the usage of financial services, web-based payment gateways, and enrolment in government initiatives across various age groups and other demographics in the Indian context. A survey was thus conducted to assess the digital literacy and awareness regarding cyber-attacks among the participants. This analysis showed greater interaction with online platforms and a sense of cyber awareness within mostly adults in the category of 19-44 years. The findings also indicated that digital services like UPI and DigiLocker, applying for government documents, paying of utility bills, etc. are quite popular, while some online resources in the health, education and business domains were less popular. This may be attributed to the fact that these are domain specific and might be of interest to some professional fields. To achieve better adoption rates, education and training efforts on digital literacy need to be stepped up and popularized among masses. According to the survey results, there remains a necessity to continue increasing people's awareness about cybersecurity practice, reporting system, and the efficiency of the law that will further support a safer and more effective digital space.

There are some limitations about this research that are to be acknowledged. Although respondents were of different ages and professions, this may not necessarily reflect the bigger population. For the purpose of strengthening the study, future research could require a much larger sample to provide closer approximations to the demographics constituting the general populations. Findings of the work outlined in this paper will provoke and steer future research questions in the quest for further discovery and understanding in this area.

REFERENCES

[1] “Internet 2010 in numbers- Pingdom.” [Online]. Available: https://www.pingdom.com/blog/internet-2010-in-numbers/

[2] “Digital 2020: Global Digital Overview, DataReportal – Global Digital Insights.” [Online]. Available: https://datareportal.com/reports/digital-2020-global-digital-overview

[3] “Internet use in 2024, DataReportal – Global Digital Insights.” [Online]. Available: https://datareportal.com/reports/digital-2024-deep-dive-the-state-of-internet-adoption

[4] “India - internet penetration 2017, Statista.” [Online]. Available: https://www.statista.com/statistics/255135/internet-penetration-in-india/

[5] “India: internet penetration rate 2024 | Statista.” [Online]. Available: https://www.statista.com/statistics/792074/india-internet-penetration-rate/

[6] Sharma J. (2016). Digital India and its Impact on the Society. *International Journal of Research in Humanities & Soc*. Sciences. 4(4):64-70. [Online]. Available: www.raijmr.com

[7] Zwilling M, Klien G, Lesjak D, Wiechetek Ł, Cetin F, Basim HN. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*. 62(1):82-97. doi: 10.1080/08874417.2020.1712269.

[8] Maiti, D., Castellacci, F., Melchior, A. (2020). Digitalisation and Development: Issues for India and Beyond. In: Maiti, D., Castellacci, F., Melchior, A. (eds) Digitalisation and Development. Springer, Singapore. [Online]. Available: http://link.springer.com/10.1007/978-981-13-9996-1_1

[9] Sekar K, Rao VK. (2018). UMANG MOBILE APP Digital India Knowledge Indicators Towards Sustainable Development: An Overview. *International Journal of Information Movement*. 2(12):156-161 [Online]. Available: www.ijim.in

[10] Sharma RK, Priti. (2021). E-Kranti: Overview of electronic service delivery. In2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) 2021 pp. 1-4. IEEE. doi: 10.1109/icrito51393.2021.9596484.

[11] Raju RS, Singh S, Khatter K. Aadhaar Card: Challenges and Impact on Digital Transformation. Arxiv preprint [Online]. Available: https://arxiv.org/abs/1708.05117v1

[12] Fugkeaw S. (2022). Enabling Trust and Privacy-Preserving E-KYC System using Blockchain. *IEEE Access*. 10:49028-49039. doi: 10.1109/ACCESS.2022.3172973.

[13] Petare P, Mohite P, Joshi M. (2015). DigiLocker (digital locker-ambitious aspect of Digital India programme.). *GE-International Journal of Management Research*. 3(6):299-308. [Online]. Available:http://ssrn.com/abstract=2786499

[14] Gahlot A, Gahlot S. (2020). Changing the state of literacy in the Digital Age in India. *EPiC Series in Education Science*.3:98-107.

[15] Neema K, Neema A. (2016). UPI (Unified Payment Interface)– A new technique of Digital Payment: An Explorative study. *International Journal of Current Research in Multidisciplinary*. 3(10):1-0.

[16] Rastogi S, Panse C, Sharma A, Bhimavarapu VM. (2021). Unified Payment Interface (UPI): A digital innovation and its impact on financial inclusion and economic development. *Universal Journal of Accounting and Finance*. 9(3):518-530. [Online]. Available: https://www.india-briefing.com/news/growth-of-digital-payments-systems-in-india-

[17] NEFT processes highest-ever 4.1 crore transactions per day on February 29, 2024. B. L. M. Bureau. [Online]. Available: https://www.thehindubusinessline.com/money-and-banking/neft-processes-highest-ever-41-crore-transactions-per-day-on-february-29/article67904711.ece

[18] G. Aydin, "Adoption of mobile payment systems: a study on mobile wallets," *Pressacademia*, vol. 5, no. 1, p. 73, 2016, doi: 10.17261/Pressacademia.2016116555.

[19] "Mobile wallet payments in India to surpass Rs 531 trn in 2028: GlobalData | Economy & Policy News - Business Standard." Accessed: Sep. 10, 2024. [Online]. Available: https://www.business-standard.com/industry/news/mobile-wallet-payments-in-india-to-surpass-rs-531-trn-in-2028-globaldata-124040800139_1.html

[20] M. Keshavarzi and H. R. Ghaffary, "An ontology-driven framework for knowledge representation of digital extortion attacks," *Comput Human Behav*, vol. 139, p. 107520, 2023, doi: 10.1016/j.chb.2022.107520.

[21] I. Corradini and E. Nardelli, "Developing Digital Awareness at School: A Fundamental Step for Cybersecurity Education," 2020, *Springer International Publishing*. [Online]. Available: http://link.springer.com/10.1007/978-3-030-52581-1_14

[22] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82–97, 2022, doi: 10.1080/08874417.2020.1712269.

[23] Rotas E, Cahapay M. (2021). Does threat knowledge influence protective behaviors of students in the context of cyber security in remote learning amid COVID-19 crisis? *Journal of Pedagogical Sociology and Psychology*. 3(1):45-53. doi: 10.33902/JPSP.2021167595.

[24] Aldawood H, Skinner G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future internet*. 11(3):73. doi: 10.3390/fi11030073.

[25] Evans M, Maglaras LA, He Y, Janicke H. (2016). Human behaviour as an aspect of cybersecurity assurance. Security and Communication Networks. 9(17):4667-79. doi: 10.1002/sec.1657.

[26] Arogundade OR. (2023). Network security concepts, dangers, and defense best practical. *Computer Engineering and Intelligent Systems*. 14(2). doi: 10.7176/CEIS/14-2-03.

[27] Furnell S, Bada M, Kaberuka J. (2023). Assessing Organizational Awareness and Acceptance of Digital Security by Design. *Journal of Information Systems Security*. (1):3-18. [Online]. Available: www.security-conference.org]

[28] Caldwell T. (2016). Making security awareness training work. Computer Fraud & Security. 2016(6):8-14. doi: 10.1016/S1361-3723(15)30046-4.

[29] Aljohni W, Elfadil N, Jarajreh M, Gasmelsied M. (2021). Cybersecurity awareness level: The case of Saudi Arabia university students. *International Journal of Advanced Computer Science and Applications*. 12(3):276-81. doi: 10.14569/IJACSA.2021.0120334.

[30] Chowdhury N, Gkioulos V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*. 40:100361. doi: 10.1016/j.cosrev.2021.100361.

[31] Shaikh FA, Siponen M. (2023). Information security risk assessments following

cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*. 124:102974. doi: 10.1016/j.cose.2022.102974.

[32] B. Standard, “Data centres in India faced 51 million cyber-attacks in 9 months,” 2022. [Online]. Available: https://www.business-standard.com/article/current-affairs/data-centres-in-india-faced-51-million-cyber-attacks-in-9-months-122032500331_1.html

[33] Vance A. (2010). Simple Passwords Remain Popular, Despite Risk of Hacking. *NY Times*. 1. [Online]. Available: https://www.nytimes.com/2010/01/21/technology/21password.html

[34] Kumar H, Raj P. (2020). An indagation on experiences and awareness of digital footprint among pupils of higher education. *Acad Res Int*. 11(3):16-31.

[35] Gupta, T. (2023). Emerging Trends of Cyber Crime in India: A Contemporary Review. *Journal of Law and Policy Transformation*, 8(1):57-65.