

Original Article

Digital Privacy Awareness among College Students

Dr. Nguyen Thi Lan

Department of Information Technology, Vietnam National University, Hanoi, Vietnam.

Received: 11-02-2018

Revised: 11-27-2018

Accepted: 12-03-2018

Published: 12-05-2018

ABSTRACT

The rapid growth of digital technology and internet services has transformed communication, learning, and interaction. College students frequently use social media, online learning platforms, cloud storage, and mobile apps in their daily lives. However, this extensive use also raises concerns about data security, privacy violations, identity theft, and online surveillance. This study examines the level of digital privacy awareness among college students, including their knowledge of online threats, privacy protection practices, and attitudes toward safeguarding personal data. Data was collected through a structured questionnaire from undergraduate and postgraduate students. The findings show that while many students have basic awareness of digital privacy, they often lack knowledge of advanced protection measures and sometimes share sensitive information online. Students with higher digital literacy or technology-related education tend to have better awareness of privacy risks. The study highlights the need for digital privacy education, awareness programs, and training in educational institutions to promote responsible internet use and strengthen data protection among students.

KEYWORDS

Digital Privacy, Data Protection, Cybersecurity Awareness, College Students, Online Security, Social Media Privacy, Information Security.

1. INTRODUCTION

1.1. Background

The use of digital technology has now been a must in the daily lives of a person and a college student who depends on the use of internet based systems to learn, communicate and socialize is no exception. The use of smartphones, laptops and high-speed internet has facilitated students to access online resources, use virtual classrooms, and interact through social media besides other activities such as digital banking and cloud-based collaboration. Convenience, connectivity and- access to information have tremendously been enhanced through these technological developments. But with these advantages, there are also a number of digital privacy threats that are caused to the students. There has been sharing of personal information online which can be exposed to things like unauthorized access, identity stealing, phishing attacks, and cyber surveillance. The safety of their personal data has become more of an issue as students dedicate much of their time on digital platforms. Digital privacy is the safety and adequate handling of individual information disseminated via digital mediums and online service providers. It entails keeping sensitive information secret, regulating the manner in which personal information is acquired and kept and that the user has freedom to determine how their data is used by websites, applications, and other organizations. Digital privacy is especially important to college students since their academic, personal, and, in some cases, financial data is often shared in numerous online platforms of different forms, including learning management systems, social networking services, and online services application. Mishandling or exposure to such information may have severe repercussions such as misuse of personal information or online account intrusions.

Over the past few years, the rising cases of cyber-crimes and massive information breaches in the global scene have caused major concern regarding digital privacy and data security. In spite of these increasing threats, a lot of students are not well aware of the privacy protection systems and safe internet habits. They can also know about some risks, yet they tend to underestimate the possible outcomes of the action to share their personal information or forget about privacy settings. The lack of awareness and actual behavior results in both problems with education institutions and policymakers who want to make digital environments safe. Consequently, the study aims to study the extent of digital privacy awareness in college students and evaluate their policies and behaviors on the issue of personal data protection. The perception and behaviors of students along with the understanding of the students will assist in revealing several areas where a better digital literacy and educative effort will be needed to increase online privacy and security.

1.2. Importance of Digital Privacy

In the contemporary digital world, digital privacy is important in safeguarding the individual. With the use of online sources of communication, education, money transactions, and socialization, tons of personal information are regularly being stored and shared. Unless adequate privacy is guaranteed, such information can be abused, stolen, or accessed by people in unauthorized ways. As a college student, one should realize the need to realize the significance of digital privacy as many of their activities and data, including academic, personal, and even financial, are processed digitally. Personal data protection guarantees security, encourages trust, and responsible online conduct.

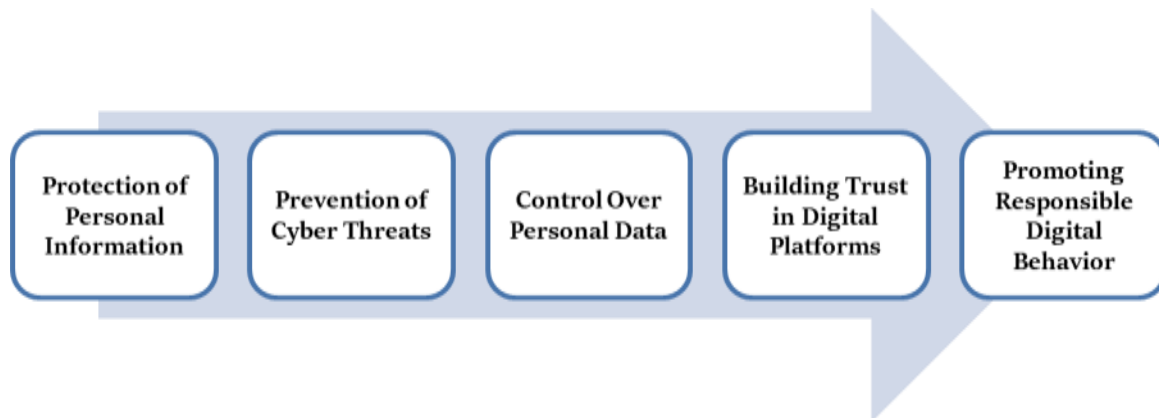


Fig 1 - Importance of Digital Privacy

1.2.1. Protection of Personal Information

Among the main factors to make digital privacy matter is to secure the availability of personal information against unauthorized access. Individual information including names, addresses, phone numbers, academics and even financial information is extensively provided on the Internet. In case such information is leaked or retrieved by malevolent people, it can be misused in other ways including identity theft, fraud or even cyber bullying. Upholding digital privacy serves the purpose of keeping the sensitive data safe and inaccessible to unauthorized users.

1.2.2. Prevention of Cyber Threats

The digital privacy is also important in the prevention of a number of cyber threats. Hackers commonly strive to use personal data by means of phishing and hacking systems and malware attacks. Knowledge about digital privacy practices will lead individuals to engage in more security practices, like good passwords, two-factor authentication, and mistrusts. Such measures minimize the threat of cyberattacks drastically and contribute to a safer and more secure online environment.

1.2.3. Control Over Personal Data

The other privacy issue that is critical about digital privacy is that an individual has control over his personal information. There are numerous online platforms, which gather the information about users to use it in advertising, analytics, and services enhancing. Having privacy settings and data policies, the users can determine the extent of sharing the information and with whom they can share the information. This control enables the user to secure his or her digital identity and manage his or her presence on the web in a responsible manner.

1.2.4. Building Trust in Digital Platforms

The aspect of digital privacy is also significant to create the trust in users and digital platforms. Users will get more confident in sharing information and using online services when they see that the companies show great data protection practices and transparent privacy policies. Trust On the part of the student, trust is required in the system because he or she uses it to study and interact with others.

1.2.5. Promoting Responsible Digital Behavior

Lastly, awareness of digital privacy promotes responsible digital practices by the users. As soon as the students are made aware of the possible dangers of reckless data disclosure, they would be responsible when it comes to the data that they share on the Internet. This awareness enhances

safer internet practices, lowers susceptibility to the cyber threat, and consequently assists in establishing a more secure online world to people and communities.

1.3. Privacy Challenges in the Digital Era

The numerous existing challenges associated with the protection of personal data and online privacy in the contemporary digital era are due to the fast development of online technologies and web-based services. Since human beings are becoming more and more reliant on digital communication, education, shopping, banking, and entertainment, several volumes of personal data are always being shared and stored over the internet. Digital systems are convenient and efficient but are vulnerable to numerous privacy risks that can jeopardize the security of the data of its users. Among the largest threats to online privacy is the data mining by social media networks. There are numerous social networking infrastructures that capture large quantities of user information such as preferences, geographical position, web browsing, and access habits. This information is usually applied in targeted advertisement, content promotion and business analytics. Even though the given practice may result in a better user experience, it also leads to concerns regarding the extent of personal information gathering and the ways it is utilized or given to third parties. Cookies and analytics systems are also another major problematic hurdle to be overcome. To track user behavior, websites usually employ cookies and tracking systems to keep track of the visits and the duration spent in the websites and online buying habits. Although these tools assist websites to personalize websites and enhance functionality, it also allows the websites to continually monitor the activities of their users online without even their full knowledge. In the long run, this tracking is able to build comprehensive profiles of interests and behaviors of people, bringing up privacy and consent issues. Moreover, the information security of digital privacy is highly threatened by data breach in cloud storage services. Most organizations are warehousing bulk of personal and institutional information in the cloud-based systems. Unless these systems are secured properly, hackers can have unauthorized access to sensitive data such as personal records, financial data, as well as, login credentials. Identity theft, financial fraud, and great loss of trust may occur as a result of such breaches. Lastly, another big challenge to digital privacy is cybercrimes and phishing attacks. To steal personal information, such as passwords, banking information or personal identification numbers, cybercriminals resort to hacking tricks, such as counterfeit emails, web sites, or messages, to determine confidential information. Such attacks take advantage of ignorance or caution on the side of the user thus leaving an individual at the mercy of loss of privacy and money as a result. Collectively, these issues underscore the increasing necessity of a higher level of digital privacy awareness, as well as better security behaviors in the online setting.

2. LITERATURE SURVEY

2.1. Digital Privacy Awareness Studies

Digital privacy awareness studies reveal that a significant portion of young adults, and especially college students, have been very prolific in expressing personal information in the online platforms without taking full cognizance of the risks involved. Students do not have a clear picture of the practice of cyber threats, including identity theft, phishing, and data misuse, but in most cases, the lack of this understanding is more theoretical than practical. Research indicates that such discrepancy between knowledge and action is occasioned by the fact that the users of the technologies emphasize on convenience, socialization, and peer socialization more than privacy protection. Consequently, students often share such sensitive data as their location, contacts, and personal favoritism, which can make them more vulnerable to cyber threats.

2.2. Social Media and Privacy Concerns

The social media sites are majorly influential in defining the way the students communicate and exchange information via the internet. Nonetheless, such sites may turn out to be big providers of privacy invasion especially when a user miserably manages the privacy settings. Most college students do not know how to make their profiles, posts, and personal information private. To meet the unintentional sharing of data, there is some insufficient understanding of controls of privacy on the platform or that frequently, the privacy policies are updated. Thus, strangers, advertisers, or third-party applications could see personal information, which can be a cause of concern due to the vulnerability of data and privacy of identity.

2.3. Cybersecurity Education

The value of cybersecurity education has extensive support regarding the increase of digital safety among the students. Schooling, training, and sensitivity sensitization on the part of learning institutions make students appreciate the need to safeguard their personal information and engage in secure internet use. Such campaigns usually target issues like password strength, fraudulent fishing, safe surfing behavior, and privacy configurations on the online platforms. According to the results of the research, students with well-organized cybersecurity education are more likely to demonstrate responsible online behavior and demonstrate a better understanding of possible online privacy threats.

2.4. Research Gap

Although the literature on cybersecurity awareness has been swelling, a significant loophole in the literature that has considered the digital privacy awareness among the developing country college students is apparent. Most of the current researches are held in developed places where digital infrastructure, policies and awareness are very different compared to developing countries. The perception of privacy risks among the students might be affected by cultural considerations, the differences in their level of technology adoption, and their level of digital literacy. Thus, a greater degree of specific research is required to investigate the extent of digital privacy awareness in developing countries among college students and to find out ways of enhancing the online safety behaviors of the latter.

3. METHODOLOGY

3.1. Research Design



Fig 2 - Research Design

3.1.1. Demographic Information

The demographic ratings about the respondents were taken in the first part of the questionnaire. This contained the age, sex, grade year and the discipline. Collected demographic data will provide all relevant information to the researcher about the background nature of the respondents and the nature of the data how an age or education level impacts the awareness of digital privacy. The information can also be used in grouping the respondents to continue analysing the statistical data.

3.1.2. Digital Usage Patterns

The second part was dedicated to the patterns of digital consumption of the participants. The questions in this questionnaire were to establish the prevalence of using the internet by them, the kind of digital devices they utilize to use the internet, and the web-based sites they frequent. It also discussed the nature of time consumed by the students on social media, browsing and online learning, and other activities involving the internet. Awareness of the patterns of digital use will offer an insight into how the exposure to online environments can be an interference to the awareness of digital privacy issues in students.

3.1.3. Privacy Awareness Knowledge

The third part of the questionnaire measured the level of knowledge of the respondents about the digital privacy and cybersecurity concepts. It consisted of questions aimed to assess the level of knowledge of the participants in issues like data protection, privacy policy, phishing attacks and dangers to privacy of online sharing of personal information. This section was to establish the degree of awareness about digital privacy threats among students and whether they have knowledge of the simplest cyber practices.

3.1.4. Privacy Protection Behavior

The last section was looking at the privacy protection behaviour among the respondents. It paid attention to the application of the students to the digital privacy they have in their daily online actions. Some of the questions covered the use of strong passwords, two-factor authentication, review of privacy settings in social media, and carefulness with the disclosure of personal information in the internet. This part also aided in reviewing the relationship between students becoming aware of the dangers surrounding privacy and taking relevant steps to secure personal information.

3.2. Data Collection

The information to be used in this study was also gathered by use of an online survey form on college students in various academic departments. The online survey approach has been chosen due to the fact that it enables a researcher to access many respondents quite quickly and gather the answers in a systematic and systemized way. The survey questionnaire was created based on a digital platform and was given to the students using different online mediums including email, student groups and social media that is popular in academic communication. This approach made sure that the respondents could fill their questionnaire at their convenience and with their smartphones, tablets, or computers. College undergraduate and postgraduate students of various disciplines like science, arts, commerce, technology-related programs were the target respondents of the study. The analysis of students in different departments has helped the study attain a wide range of answers that could be more appropriate to represent the general level of awareness of digital privacy to the student population. The use of the questionnaire was voluntary and the respondents were told the aim of the study prior to filling the questionnaire. They also got an assurance that their responses would be held in confidence and they would only use them in academic research. The

online survey had several items that collected data about the demographic attributes, the usage habits regarding digital use, awareness of privacy threats, and individual behaviors regarding privacy protection. Majority of the questions were designed in multiple choice or Likert scale format so that the participants would find it easy to respond and the researcher may easily utilize the data obtained. The process of data collection was carried out in a particular time frame giving adequate time to the students to be part of the process. After the collection of the responses the data was revised and was to be analyzed further. This method contributed to making sure that the obtained data was applicable, valid, and applicable to assess the degree of digital privacy awareness of college students.

3.3. Privacy Awareness Model

In order to determine how well college students understand the aspect of digital privacy, this study utilized a theoretical framework called Privacy Awareness Index (PAI). This model is intended to bring in several elements of privacy awareness into a single quantifiable value that demonstrates the level of knowledge and application of digital privacy protection among the students. Privacy awareness cannot be defined based on knowledge alone; it has to be based on the attitudes of people towards privacy and the actions they exhibit when utilizing digital platforms. Consequently, three significant elements, i.e. knowledge, behavior, and attitude, are associated with the model. The Privacy Awareness Index was determined as an evidence of the mean of the three scores; the Knowledge Score, the Behavioral Score, and the Attitude Score. Stated simply the Privacy Awareness Index can be defined as a result of Knowledge Score, Behavioral Score and Attitude Score divided by three. This approach makes a well-balanced assessment since it assures that all its components bear the same contribution to the total level of awareness. The Knowledge Score (K) will be the awareness of the respondent on the notion of digital privacy and cybersecurity risks. It was perceived via questions in which the familiarity with the students of problems like data protection, privacy policy, phishing attacks, and the danger of personal information online sharing were evaluated. A better score on the knowledge category shows a greater awareness of the threats and protection mechanisms of digital privacy. The Behavioral Score (B) is based on the real behavior of the students to defend themselves when utilizing the internet. These will involve things like the use of a hard-to-crack password, changing the privacy settings in social media networks, having a two factor authentication system activated, and careful use of personal information in the internet. The Attitude Score (A) is the intensity at which students take digital privacy and their degree of concern over safeguarding their personal information. It establishes their views, beliefs and how much they are concerned about privacy risks in the cyber space. A combination of all these three dimensions, the Privacy Awareness Index allows seeing the global digital privacy awareness of students and defines the areas where the private matters ought to be used better.

3.4. Research Flowchart



Fig 3 - Research Flowchart

3.4.1. Problem Identification

Problem identification was the first activity of the research process. At this phase, the investigator determined the emerging issue about the privacy of college students on the internet and social media as a result of using the internet and social networks more. A great number of students exchange personal data on the internet without being much informed about the dangers of misusing data, stealing identities, and cyber-attacks. The acknowledgment of this problem contributed to establishing the central purpose of the study that was to investigate the amount of digital privacy awareness among college students and to get to know the behavioral patterns of online privacy protection of the chosen students.

3.4.2. Literature Review

The literature review phase included reviewing the past published researches, scholarly articles and reports concerning digital privacy, cyberspace awareness, and internet behaviour. This move assisted the researcher to appreciate the existing information in the area and conceive crucial notions, theories, and results regarding the concept of privacy awareness. Through the literature review, the researcher was also able to detect weaknesses in the current literature, especially the little attention an awareness of digital privacy amongst college students in developing countries.

3.4.3. Questionnaire Design

A structured questionnaire was crafted based on the literature analysis to gather the pertinent information out of the respondents. The questionnaire was done very well to address various areas including demographic characteristics, online usage behavior, knowledge of privacy awareness, and the protection of privacy behavior. The questions were conveniently and straightforwardly phrased to make the survey participants find it easy to answer them. The questionnaire was designed in such a way that it would gather the right information about the students concerning their digital privacy awareness, attitudes, and practices.

3.4.4. Data Collection

The questionnaire was administered to the students in colleges through an online survey programme in the data collection phase. Students representing various departments were also invited to take part in the survey in a bid to have diversity in responses. The online approach provided the participants with the convenience to fill in the questionnaire at their computers. Respondents were gathered within a given time period, and there were enough respondents that were mobilized in the study.

3.4.5. Data Analysis

The data analysis and structuring was the next step to organize the responses after the data had been collected. The responses obtained were tabulated and sub grouped according to the various sections of the questionnaire. The patterns, trends and relationship in the data were analyzed statistically. This analysis assisted in computing the Privacy Awareness Index and knowing the general rate of privacy awareness of the respondents.

3.4.6. Result Interpretation

Once the data was analysed, the findings were interpreted to know what the results reveal about the awareness of the students concerning their digital privacy. The interpretation was done by comparing knowledge levels, behavior and attitude of the respondents. It aided in determining whether students know sufficient information concerning online privacy as well as whether they use that knowledge to ensure privacy in their online activities.

3.4.7. Conclusion and Recommendations

The concluding phase of the study was a conclusion of the research in accordance with the data analyzed and interpreted. This was an overview of the main results of the research and a spotlight to the general state of the digital privacy awareness among the college students. Upon the findings, it has recommended to increase awareness in order to promote safer online behavior. These guidelines can incorporate the introduction of cybersecurity awareness campaign, operations of workshops and incorporation of digital privacy education into schools curricula.

4. RESULTS AND DISCUSSION

4.1. Student Awareness Level

The obtained results of the survey indicate that college students are characterized by various degrees of their awareness as to digital privacy concerns. Although many students demonstrate a minimum level of perception of the need to secure personal information on the Internet, the need level of awareness is variable based on such parameters like academic level, degree of exposure to the concept of digitalization, and prior experience of cybersecurity measures activities. Most of the students are conversant with the ordinary digital privacy ideas like the use of passwords, privacy settings in social media, and the dangers of disclosing personal details online. This means that the use of digital technology has led to certain degree of awareness among the student population. The survey findings however also indicate that this awareness is not necessarily all inclusive. In as much as students might have noticed the significance of digital privacy, some of them do not have an in-depth understanding of more complex privacy protection techniques. As an illustration, although most respondents know that they need strong passwords to ensure that they are secure going online, the lower number of students consistently apply other security features, like two-factor authentication, or adjust their privacy settings to ensure maximum safety. Moreover, not all the students might think about the possible consequences of sharing personal information on the Internet, as there is a threat of identity theft, online fraud, and the use of the information by other individuals. The other critical observation that the answers emerged is that the students who use digital platforms mostly in academic advancements, internet-based courses, or the online learning course appear to exhibit a higher standard of digital privacy awareness than those students who usually use the digital medium to socialize or enjoy themselves. This is to imply that access to learning materials and e-literacy classes have the potential to greatly impact the awareness of the students on privacy matters. On the whole, the analysis revealed that as much as students already have an overall understanding of online privacy issues, more education and practical advice would be necessary to allow them to effectively implement privacy protection practices in their everyday internet lives. Enhancing awareness initiatives and responsible digital conduct may have significant value in boosting awareness of privacy in general and the digital safety of students.

4.2. Privacy Awareness Percentage

Table 1: Privacy Awareness Percentage

Privacy Factor	Percentage (%)
Awareness of Data Privacy	72%
Use of Strong Passwords	64%
Knowledge of Privacy Settings	58%
Awareness of Phishing Attacks	67%
Understanding of Data Tracking	49%
Reading Privacy Policies	35%
Concern about Data Misuse	76%

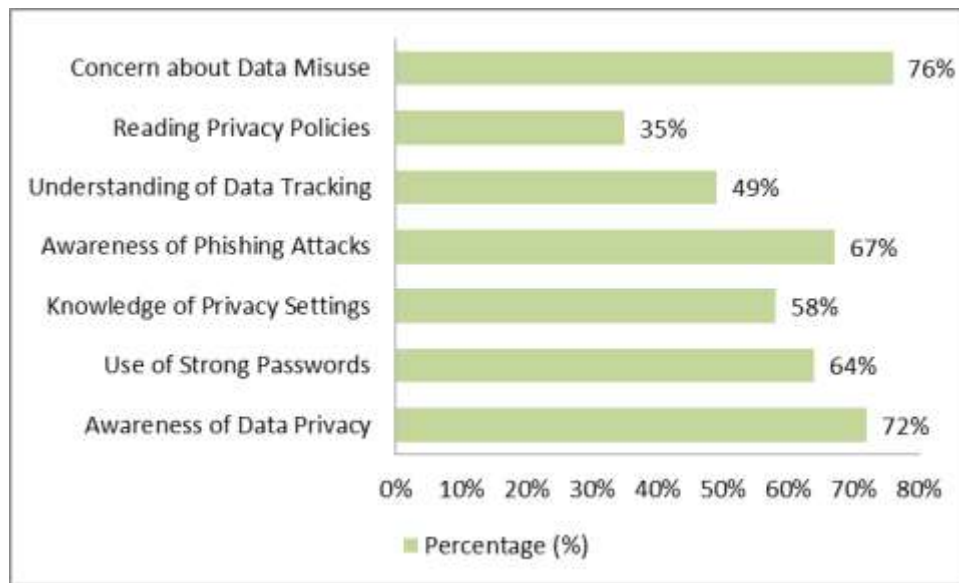


Fig 4 - Privacy Awareness Percentage

4.2.1. Awareness of Data Privacy (72%)

According to the outcomes of the survey, it shows that about 72 per cent of the students have some knowledge of what the nature of data privacy entails and the importance of personal information in the usage of digital platforms. This is an indication that most students understand the need to protect sensitive data including personal information, contact details, and online passwords. Nevertheless, although most students are informed about data privacy in general, their knowledge on this subject can be subject to limitations in certain instances, which spans to particular practices that are needed in order to make their information safe on the Internet.

4.2.2. Use of Strong Passwords (64%)

Approximately, 64 percent of the respondents stated that they use very strong passwords to lock their internet accounts. The passwords are usually encoded with a mix of letters, numbers, and special characters, thus are harder to crack or guess by the attackers. Such a finding indicates that many students are making simple measures to secure their online accounts. However, the percentage is also used to show that a considerable number of students might continue using weak or guessable passwords, thus predisposing them to having their accounts accessed in an unauthorized manner.

4.2.3. Knowledge of Privacy Settings (58%)

According to the survey results, one out of five students knows how privacy settings can be found on digital platforms, including social media applications and websites. These environments have enabled the user to manage the people who have access to their personal data, postings and profile data. Though it covers over fifty percent of the respondents who have knowledge on these features, still the indication is that most of the students might not be fully informed on how to set and update these settings more frequently to ensure that their privacy is well secured.

4.2.4. Awareness of Phishing Attacks (67%)

Only some 67 percent of the students replied that they knew about phishing attacks, which are attempts to extract sensitive information falsely impersonating reliable sources (in this context, a bank, a company, online service). Such awareness shows that there are a lot of students who are aware of common threats on the Internet, and they might be more wary when responding to

suspicious e-mails and messages. Nevertheless, further training is required so that students should be able to determine and prevent more advanced phishing attacks appropriately.

4.2.5. Understanding of Data Tracking (49%)

The results show that awareness of the concept of data tracking is only 49 percent, and in this case, websites and apps gather information about users to understand their behavior or deliver them specific advertisements. Such a comparatively low percentage of the population indicates that a good number of students have no understanding of how their online activities can be tracked or how the information can be utilized by companies and third parties. Awareness creation regarding the issue of tracking data should be increased to assist students to make better choices regarding their online behavior.

4.2.6. Reading Privacy Policies (35%)

According to the survey, merely every three out of five students are known to read privacy policies before they use Web sites or online services. Privacy policies are mindful of important information related to collection, retention, and utilization of personal data by organizations. This low percentage implies that majority of the students are likely to omit such documents, and the reason is in most cases these documents are voluminous or they are not easy to comprehend. Subsequently, users will unwillingly enter into the agreement that will permit them to use their own information extensively.

4.2.7. Concern about Data Misuse (76%)

The most significant percentage of 76 given in the survey indicates that students care about the possibility of their personal data being misused. In this observation, a huge percentage of the respondents express concern over the manner in which their information can be accessed, shared or used by unscrupulous persons or groups. This kind of worry shows that students are aware of the real danger of breaches of privacy within the online space. Nonetheless, not all students will be well knowledgeable or motivated to embrace good privacy protection habits despite this issue.

4.3. Discussion

Findings of the research allow concluding that college students have the moderately good level of awareness on digital privacy, yet there are a range of gaps in their awareness and behaviors. A lot of the respondents showed their general knowledge about various concepts of privacy and indicated the fear of insecurity of their personal information on the Internet. Many students have confirmed that the possible threats of sharing personal information on digital platforms are data misuse, identity theft, and cyber threats. This issue indicates that the students have recognized the increasing role of guaranteeing their privacy in the more digital world. Nevertheless, despite the concerned understanding, this awareness does not implicate that a considerable number of students are always equipped with effective privacy protection practices in their everyday online operations. The lack of attention in terms of privacy policies is also found to be one of the key gaps in the results. Even though these policies have fundamental information in terms of collecting, storing and using personal data by digital platforms, a small percentage of the students claimed to have read the policies frequently. This is possible because sometimes the privacy policy documentation is too complicated and long and in this case, the user is not motivated to read the work thoroughly. Due to this fact, a good portion of students can accept the conditions under which organizations can collect or distribute their personal information without their knowledge. Also, although the students are usually knowledgeable about the simple measures of keeping themselves safe, like passwords, a lower percentage of participants indicated that they applied more sophisticated privacy measures,

like two-factor authentication, regularly changing security settings, or relying on privacy-related tools. The research also found the variation in the awakening of privacy, according to academic background. Students that are undertaking courses in technological related disciplines, e.g. computer science or information technology are more likely to have greater digital privacy awareness in relation to students in non-technical disciplines. This disparity can be explained by the fact that they are exposed to technical know-how, cybersecurity principles, and digital literacy education as part of the curriculum in school. Conversely, learners in non-technical fields in general will likely lack the chance to be informed about the danger of online privacy and the ways to stay secure. These results indicate a wider educational program that would advance awareness of digital privacy in all the academic areas to ensure that any student acquires the knowledge and skills necessary to advance their personal data online.

5. CONCLUSION

The digital awareness of privacy among the college students has assumed an imperative role in the digital literacy of the day. As the online technologies develop fast and the personal use of the web as an academic, social, and personal activity increases, the students are active in communication with online resources, which accumulate and process a lot of personal data regularly. Consequently, it has been of high significance to learn how to guard personal data and remain private in the online space. The results of the current study point to the conclusion that students tend to have the rudimentary level of awareness in the context of digital privacy threats. Typical issues that many students would be conversant with include the need to keep their personal information safe, use passwords as a means of securing their accounts, and to be weary when sharing their information on the internet. The findings, however, also point to the fact that they have poorer understanding of more advanced privacy protection practices. Although students are aware of possible dangers like the abuse of personal data, phishing, or intrusion to individual accounts, they do not always provide regular and effective precautions to protect their online data. All students do not adopt such practices as checking out privacy policies, using advanced security features like two-factor authentication, and regularly updating their privacy settings.

There is also an implication in the study on how educational institutions can be instrumental in enhancing student awareness of the importance of digital privacy. Colleges and universities can include cybersecurity and cyber privacy issues in their educational programs and make sure that students regardless of their major studies would develop necessary knowledge on cyber security. Alongside official study, awareness campaigns, seminars, workshops and training programs organized by the institutions may be aware of the practical ways to defend personal information in the digital space. These initiatives are capable of making the students be responsible in their online conduct and motivate them to engage in safer online habits in their day-to-day endeavors.

Moreover, the future work can be based on this study, with the increase in the sample size and the introduction of participants of a more diverse set of institutions and geographic areas. There is also a possible prospect of additional research that investigates the display of emerging technologies like artificial intelligence, big data analytics, and the Internet of Things on the understanding of digital privacy and methods of personal data protection in the population of students. Those disciplines would potentially offer further details on the effect of changing technological conditions on privacy issues and user actions.

REFERENCES

- [1] Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514.
- [2] Barth, S., & de Jong, M. D. T. (2017). The privacy paradox - Investigating discrepancies between expressed privacy concerns and actual online behavior. *Telematics and Informatics*, 34(7), 1038-1058.
- [3] Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, 40(2), 215-236.
- [4] Tufekci, Z. (2008). Grooming, gossip, Facebook and MySpace: What can we learn about these sites from those who won't assimilate? *Information, Communication & Society*, 11(4), 544-564.
- [5] Boyd, D., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, 15(8).
- [6] Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1), 83-108.
- [7] Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1), 153-160.
- [8] Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, 25(2), 109-125.
- [9] Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 10(3), 393-411.
- [10] Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. *Journal of Consumer Affairs*, 38(2), 217-232.
- [11] Ng, W. (2012). Can we teach digital natives digital literacy? *Computers & Education*, 59(3), 1065-1078.
- [12] Pusey, P., & Sadara, W. A. (2011). Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge and preparedness. *Journal of Digital Learning in Teacher Education*, 28(2), 82-88.
- [13] Choi, D., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81, 42-51.
- [14] Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L., & Hong, J. (2007). Getting users to pay attention to anti-phishing education. *Proceedings of the ACM Workshop on Privacy in the Electronic Society*, 70-81.
- [15] Bansal, G., Zahedi, F. M., & Gefen, D. (2016). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, 49(2), 138-150.