IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, October 2026
Impact Factor: 8.2

A Study on Online Privacy Awareness, Security Risks and Data Protection

Miss. Thorat Puja Krushnangar[1] and Prof. Pravin S. Pawade[2]
MCA Student, Agasti Institute of Management, Computer Application and Research (AIMCAR), Akole[1]
Assistant Professor, Agasti Institute of Management, Computer Application and Research (AIMCAR), Akole[2]
pujathorat242003@gmail.com and pravin.pawade123@gmail.com

Abstract: *In the modern digital era, the use of the internet, social media platforms, smartphones, and online services has increased significantly. People share their personal information through various digital platforms for communication, education, online transactions, and other activities. However, a lack of awareness about data privacy and security risks can expose individuals to threats such as data breaches, identity theft, phishing attacks, and unauthorized access to personal information. Therefore, understanding online privacy awareness and data protection practices has become essential.*
The present research project, entitled "A Study on Online Privacy Awareness, Security Risks and Data Protection," aims to study the level of data privacy awareness among college students and understand their knowledge, attitudes, and practices regarding the protection of personal information. The study focuses on privacy policies, website cookies, application permissions, online tracking, password security, two-factor authentication, phishing attacks, and safe internet usage practices. It also examines users' concerns about sharing personal information on social media and other digital platforms.

Keywords: Online Privacy Awareness, Data Privacy, Security Risks, Data Protection, Personal Information, Cybersecurity, Digital Privacy, Privacy Policies, Data Breaches, Identity Theft, Phishing Attacks, Password Security, Two-Factor Authentication, Social Media Privacy, Digital Literacy

I. INTRODUCTION

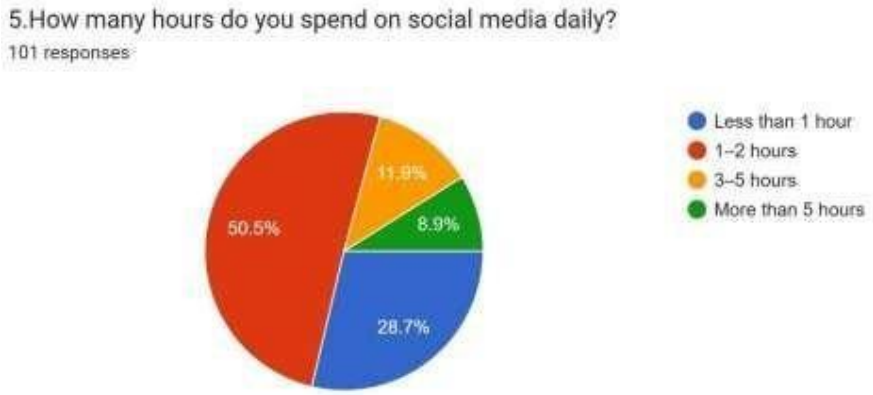
In today's digital world, the use of the internet, smartphones, social media, online banking, e-commerce, and various digital applications has increased significantly. People use these services for communication, education, shopping, financial transactions, entertainment, and many other daily activities. While these technologies make our lives easier and faster, they also involve the collection, storage, processing, and sharing of personal information. Therefore, data privacy has become an important concern for individuals, organizations, and society.

Data privacy refers to the proper handling, protection, and use of personal information. Personal data may include a person's name, address, phone number, email address, photographs, location, financial details, login credentials, and other information that can identify an individual. Data privacy ensures that such information is collected and used appropriately, with proper authorization and in accordance with applicable rules and regulations.

Research Objectives: To study the level of data privacy awareness among college students and understand their knowledge, attitudes, and practices regarding the protection of personal information in the digital environment. To assess the level of awareness among college students regarding data privacy and the importance of protecting personal information. To examine students' knowledge of privacy policies, terms and conditions, and consent while using websites, mobile applications, and online services. To study students' awareness of password security, two-factor authentication, and other methods used to protect online accounts. To analyze students' practices regarding sharing personal information on social media platforms and other digital applications. To investigate students' awareness of cyber threats such as phishing attacks, identity theft, online fraud, and data breaches.

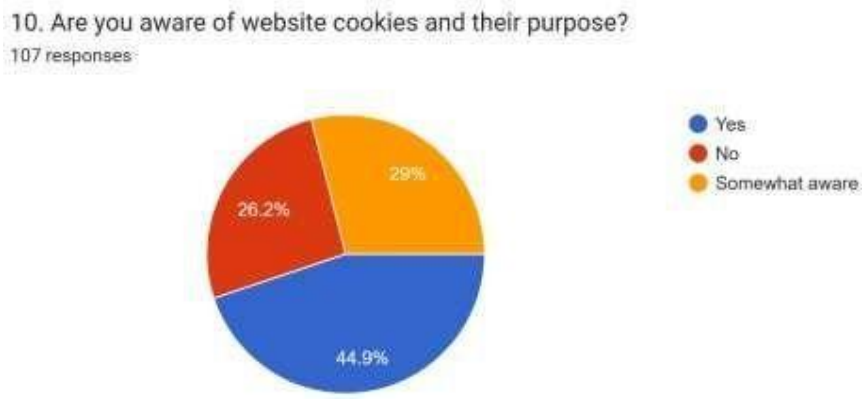
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, October 2026
Impact Factor: 8.2

Research Methodology: This study uses a survey-based research approach to examine online privacy awareness, security risks, and data protection among college students. The research primarily focuses on collecting structured responses and analyzing them using quantitative techniques. Primary data is collected through a structured questionnaire created using Google Forms. The questionnaire includes questions about respondents' demographic characteristics, awareness of online privacy, understanding of privacy policies and cookies, app permissions, online tracking, and personal data protection practices. It also explores security-related aspects such as password safety, two-factor authentication, phishing attacks, identity theft, and data breaches. The questionnaire further examines respondents' online behaviour, privacy settings, and precautions taken while using social media platforms and other digital services. The target population consists primarily of undergraduate and postgraduate students who use the internet, smartphones, social media, and online services. The final sample size and respondent characteristics are reported according to the actual survey responses collected. The chart shows that 30.2% of respondents are aged 23-26 years, 24.5% are above 30 years, 18.9% are aged 27-30 years, 14.2% are aged 19-22 years, and 12.3% are 18 years or below.The chart shows that 49.5% of respondents are female, 45.8% are male, 3.7% prefer not to say and 0.9% belong to other gender categories. The chart shows that 31.8% of respondents are graduates, 29% belong to other educational qualifications, 28% are postgraduates, and 11.2% are undergraduates. The chart shows that 27.1% of respondents are employed, 25.5% are self-employed, 23% are students, and 19% are engaged in business. The chart shows that 40.2% of respondents use the internet once a day, 24.3% several times a day, 24% a few times a week, and 12.1% rarely.

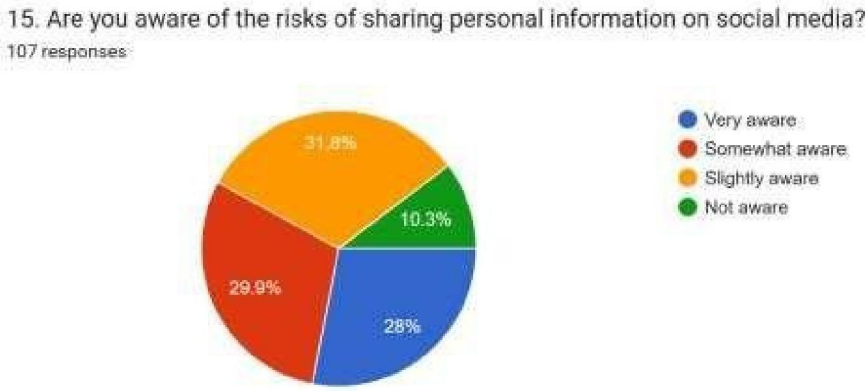


The chart shows that 34.6% of respondents are fully aware of data privacy, 27.1% are somewhat aware, 22.4% have heard the term but know little about it, and 15.9% are not aware. The chart shows that 35.5% of respondents understand data privacy as protecting personal information from unauthorized access, 26.2% relate it to protecting computer hardware, 23.4% associate it with increasing internet speed, and 15% selected none of the above. The chart shows that 34.6% of respondents identified full name and phone number as personal information, 23.4% selected email address, 19.6% selected home address, and 22.4% chose all of the above. The chart shows that 31.8% of respondents clearly know how websites collect personal data, 26.2% understand it to some extent, 26.2% have very little knowledge, and 15.9% have no knowledge. The chart shows that 44.9% of respondents are aware of website cookies, 29% are somewhat aware, and 26.2% are not aware of them.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, October 2026
Impact Factor: 8.2

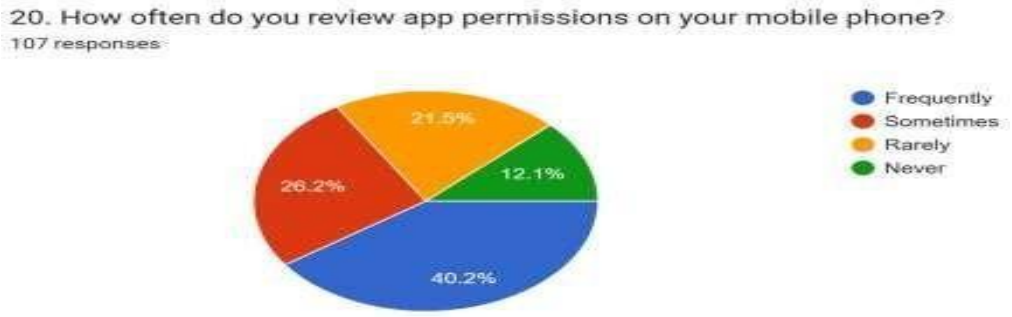


The chart shows that 34.6% of respondents sometimes read privacy policies, 25.2% always read them, 21.5% rarely read them, and 18.7% never read them. The chart shows that 29.9% of respondents usually understand mobile application permissions, 26.2% always understand, 21.5% sometimes understand, and 22.4% do not understand them. The chart shows that 38.3% of respondents are aware that their online activities may be tracked by websites, 31.8% are somewhat aware, and 29.9% are not aware. The chart shows that 42.1% of respondents have heard about a data breach, 32.7% do not know what it is, and 25.2% know what a data breach is.



The chart shows that 31.8% of respondents are slightly aware of the risks of sharing personal information on social media, 29.9% are somewhat aware, 28.0% are very aware, and 10.3% are not aware. The chart shows that 33.6% of respondents change their passwords every 1-3 months, 27.1% change them every 4-6 months, 25.2% change them only when required, and 14.0% never change their passwords. The chart shows that 36.4% of respondents always use strong passwords for their online accounts, 28.0% use them sometimes, 22.4% use them rarely, and 13.1% never use strong passwords. The chart shows that 27.1% of respondents always use the same password for multiple accounts, 26.2% never use the same password, 25.2% sometimes do, and 21.5% rarely do. The chart shows that 30.8% of respondents enable 2FA on some accounts, 28.0% enable it on all important accounts, 23.4% know about it but do not use it, and 17.8% are not aware of the feature. The chart shows that 40.2% of respondents frequently review app permissions on their mobile phone, 26.2% review them sometimes, 21.5% rarely review them, and 12.1% never review them.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, October 2026
Impact Factor: 8.2



The chart shows that 29.0% of respondents never share personal information with unknown websites or applications, another 29.0% share it sometimes, 27.1% share it rarely, and 15.0% share it frequently. The chart shows that 28.0% of respondents never use public Wi-Fi for banking or other sensitive activities, 26.2% use it rarely, 24.3% use it sometimes, and 21.5% use it frequently. The chart shows that 36.4% of respondents always check whether a website is secure (HTTPS) before entering personal information, 26.2% check sometimes, 19.6% check rarely, and 17.8% never check. The chart shows that 40.2% of respondents are not sure if they have received a suspicious emails, SMS, or link asking for personal information,30.8% stated they have not received any, and 29.0% confirmed that they have. The chart shows that 31.8% of respondents open a suspicious link without checking, 27.1% ignore or delete it, 23.4% verify the sender before opening, and 17.8% share it with others.

Findings

The study on "A Study on Online Privacy Awareness, Security Risks and Data Protection" focuses on understanding college students' awareness of online privacy, security risks, and personal data protection practices. The research aims to examine how students protect their personal information while using social media platforms, smartphones, websites, and other digital services.

• Awareness of Online Privacy: The study examines students' understanding of online privacy and the importance of protecting personal information shared on digital platforms. It aims to identify their level of awareness regarding the risks associated with sharing personal details online.

• Understanding of Privacy Policies: The research investigates whether students read and understand privacy policies and terms and conditions before using websites, mobile applications, and online services. It also explores their awareness of how digital platforms collect, store, and use personal information.

• App Permissions and Online Tracking: The study examines students' awareness of mobile application permissions, cookies, and online tracking. It aims to understand whether students check the permissions requested by applications and recognize the possible privacy risks associated with unnecessary access to personal data.

• Password Security and Account Protection: The research focuses on students' password management practices, including the use of strong passwords, avoiding password reuse, and protecting login credentials. It also examines their awareness of two-factor authentication as an additional security measure.

• Awareness of Cybersecurity Threats: The study explores students' understanding of common online threats, such as phishing attacks, identity theft, unauthorized access, and data breaches. It aims to assess whether students can recognize suspicious links, fraudulent messages, and other potential online security risks.

• Social Media Privacy Practices: The research examines how students manage privacy settings on social media platforms and control the information they share publicly. It also considers their awareness of the risks associated with sharing personal photographs, contact details, location information, and other sensitive information online.

• Personal Data Protection Behaviour: The study investigates the precautions students take to protect their personal information while browsing the internet and using digital services. These practices may include checking website

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, October 2026
Impact Factor: 8.2

security, avoiding suspicious links, limiting the sharing of personal information, and logging out of accounts on shared devices.

• Digital Literacy and Responsible Internet Usage: The research highlights the importance of digital literacy in helping students make informed decisions about online privacy and security. It aims to understand whether students possess sufficient knowledge to identify privacy risks and adopt safe online practices.

Suggestions

The suggestions emphasize the need to promote online privacy awareness and encourage responsible internet usage among college students. Users should be educated about the importance of protecting personal information while using websites, social media platforms, smartphones, and other digital services.

Students should create strong and unique passwords for different online accounts and enable two-factor authentication wherever available. Passwords and verification codes should never be shared with unauthorized individuals. Users should also avoid clicking on suspicious links, downloading files from untrusted sources, or responding to messages requesting confidential information.

REFERENCES

1. Government of India. (2023). The Digital Personal Data Protection Act, 2023. Ministry of Law and Justice, Government of India. https://www.indiacode.nic.in/

2. National Institute of Standards and Technology (NIST). (2020). NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0. https://doi.org/10.6028/NIST.CSWP.10

3. Organisation for Economic Co-operation and Development (OECD). (2002). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD Publishing. https://doi.org/10.1787/9789264196391-en

4. OECD. (2023). Explanatory Memoranda of the OECD Privacy Guidelines. OECD Publishing. https://doi.org/10.1787/ea4e9759-en

5. Pew Research Center. (2019). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/