International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Cybersecurity Awareness Among College Students - A Study Among College Students

1.Monisha N

2.Kavya Shree BJ
3.Assistant professor Balaram M
Affiliation: Bachelor Of Computer Applications (BCA) **Department of Computer Applications**
College: BMS COLLEGE OF COMMERCE AND MANAGEMENT
AUTHOR'S EMAIL:
monishan.sammu@gmail.com
jagadishkavya29@gmail.com
balaram@bmsccm.ac.in

Abstract

With the increasing use of smartphones, social media, online banking, digital learning platforms, and other internet-based services, college students are increasingly exposed to various cybersecurity risks. Cyber threats such as phishing, password attacks, online scams, malware, identity theft, and social engineering can affect students who may not have adequate awareness of safe digital practices. This study aims to assess the level of cybersecurity awareness among college students by examining their knowledge of common cyber risks, online behaviors, and preventive practices. A survey-based research methodology will be adopted, using a structured questionnaire to collect primary data from college students. The questionnaire will focus on students' awareness of cybersecurity threats, password and authentication practices, recognition of suspicious links and messages, privacy settings, software updates, use of public Wi-Fi, and responses to potential cyber incidents. The collected responses will be analyzed to identify patterns in cybersecurity awareness, risky online behaviors, and the adoption of preventive measures among students. The study is expected to provide insights into the cybersecurity knowledge and practices of young internet users and highlight the importance of cybersecurity education, digital literacy, and responsible online behavior among college students.

KEYWORDS: Cybersecurity Awareness, College Students, Cyber Risks, Online Behavior, Preventive Practices

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

1. Introduction

Cybersecurity awareness refers to the extent to which a person understands online threats and knows how to protect personal information, devices, and accounts. It is not only a technical matter. It also depends on everyday habits such as choosing strong passwords, checking links before clicking, reviewing privacy settings, and knowing what to do when something goes wrong.

College students are an important group to study. They use smartphones, social media, online banking and UPI payments, learning platforms, and public Wi-Fi almost every day, and many manage their own accounts and money for the first time. Threats such as phishing, password attacks, online scams, malware, identity theft, and social engineering can therefore reach them easily, especially when they have not had formal guidance on safe digital practices.

Awareness and behavior are not always the same thing. A student may know that public Wi-Fi is risky and still use it for banking, or may know the advice on passwords and still reuse one password everywhere. Studying knowledge, behavior, and preventive practices together gives a more useful picture than any single question could.

This paper follows a descriptive survey approach. It reports the responses as recorded and does not claim that any one factor causes better or worse cybersecurity practice. The findings are perceptions and self-reported behaviors of the students who responded, and they should not be treated as a technical audit of their devices or accounts.

2. Objectives of the Study

1. To assess college student's awareness and knowledge of common cyber threats such as phishing, malware, online scams, identity theft, and social engineering.
2. To examine student's online behaviors and preventive practices, including password and authentication habits, recognition of suspicious links and messages, privacy settings, software updates, and use of public Wi-Fi.
3. To understand how students respond to potential cyber incidents and to identify the main gaps that call for cybersecurity education and digital literacy support.

3. Review of Literature

Research on information security behavior often separates knowledge from practice. Protection motivation theory (Rogers, 1975) proposes that people protect themselves when they see a threat as serious and likely, and believe they can act effectively against it. Applying the health belief model to

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

computer security, Ng, Kankanhalli and Xu (2009) surveyed 134 employees and found that perceived susceptibility, perceived benefits and self-efficacy were determinants of email-related security behavior. Knowing about a threat is therefore only one step toward safer behavior.

Studies of employee security awareness usually treat it as multi-dimensional. The Human Aspects of Information Security Questionnaire (Parsons et al., 2014), for example, measures awareness in terms of knowledge, attitude, and behavior across several focus areas of everyday security practice. This supports examining awareness across several questionnaire items instead of a single overall question.

Common threats discussed in the literature include phishing, weak or reused passwords, malware from unverified downloads, unsecured public networks, oversharing on social media, and social engineering that exploits trust or urgency. Young and frequent internet users may be confident with technology yet still be vulnerable, because risky habits can form through convenience.

Awareness programs and digital literacy education are widely suggested as practical responses, but their effect depends on whether they change everyday habits. This paper uses these ideas as a framework for organizing the survey findings. It does not claim that the survey tests every relationship identified in earlier research.

4. Research Methodology

Research design: The study uses a descriptive survey design based on a structured questionnaire.

Data source and sample: Primary data were collected from **50** college students studying from different colleges, including the author's own college. Respondents were selected using convenience sampling, and data were collected through an online questionnaire (Google Forms). Respondent names were collected on the form but are not reproduced in this paper, and only aggregate results are presented.

Instrument: The questionnaire has two parts. Part A covers demographics: age, course or stream, and gender. Part B contains ten multiple-choice questions on password updates, reuse of passwords across accounts, two-factor authentication (2FA), handling of suspicious links, checking of social media privacy settings, use of public Wi-Fi for sensitive activities, installing applications from trusted sources, checking a website before sharing personal information, software updates, and the response to a suspected account hack. Each question offers four options, ranging from the safest practice to the riskiest.

Method of analysis: Frequency counts and percentages are used to describe the response patterns. Percentages are calculated against the total of 50 responses, and every question was answered by all respondents. The results are descriptive and do not establish causal relationships.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

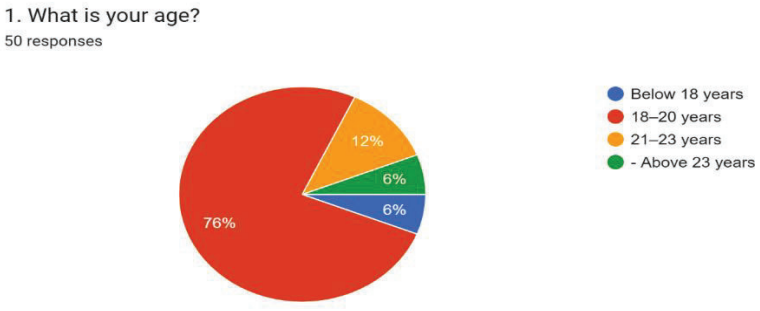
Limitations: The sample is small and was selected by convenience, so the results describe these 50 respondents and cannot be generalized to all college students. The responses are self-reported and may differ from actual behavior.

Ethical and reporting note: Participation was voluntary and the purpose of the survey was explained to respondents. Names and other identifying details are not reported, and all sources are acknowledged in the references.

5.Data Analysis and Interpretation

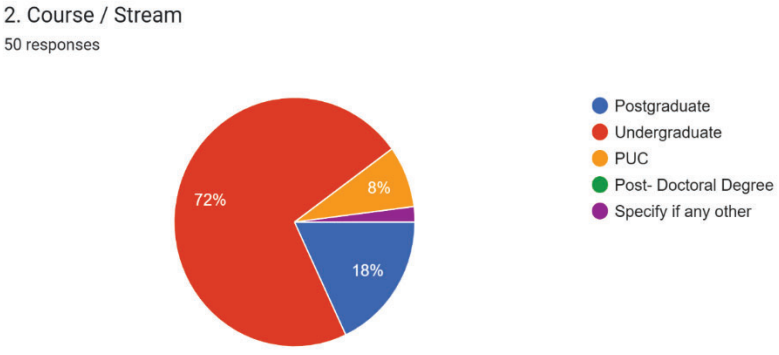
5.1 .Respondent Profile

Distribution by: Age.



Age group	Count	%
Below 18 years	3	6.0%
18–20 years	38	76.0%
21-23 years	6	12.0%
Above 23 years	3	6.0%

Distribution by: Course / Stream



(This work is licensed under a Creative Commons Attribution 4.0 International License.)

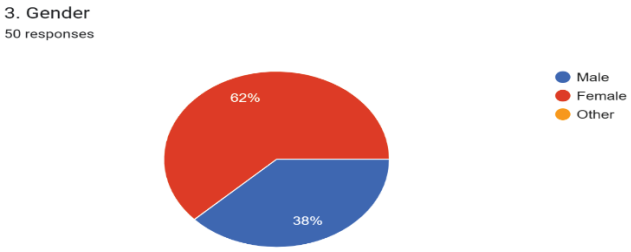
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Course	Count	%
Undergraduate	36	72.0%
Postgraduate	9	18.0%
PUC	4	8.0%
Other	1	2.0%

Interpretation: Of the 50 respondents, 76.0% were aged 18–20 years and 62.0% were female. Undergraduate students formed the largest group (72.0%), followed by postgraduate students (18.0%).

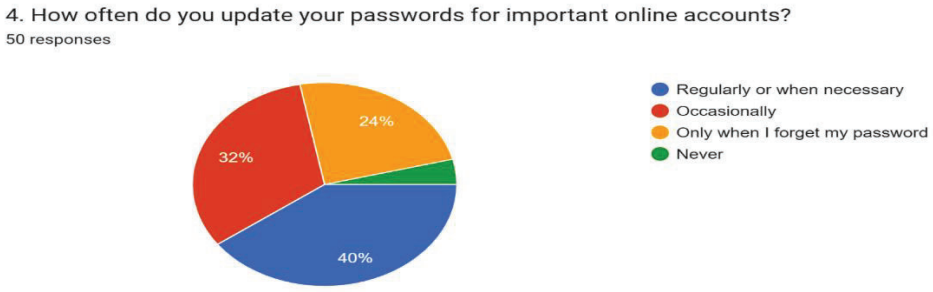
5.2 Password and Authentication Practices (Objective 1)

Distribution by: Gender.



Gender Count %	Count	%
Female	31	62.0%
Male	19	38.0%

Distribution by: How often do you update your passwords for important online accounts?

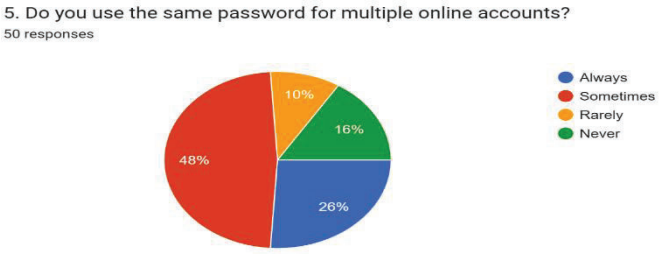


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

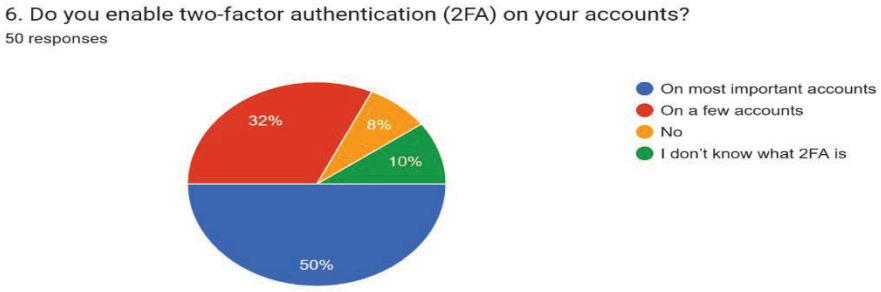
Response	Count	%
Regularly or when necessary	20	40.0%
Occasionally	16	32.0%
Only when I forget my password	12	24.0%
Never	2	4.0%

Distribution by: Do you use the same password for multiple online accounts?



Response	Count	%
Always	13	26.0%
Sometimes	24	48.0%
Rarely	5	10.0%
Never	8	16.0%

Distribution by: Do you enable two-factor authentication (2FA) on your accounts?



(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

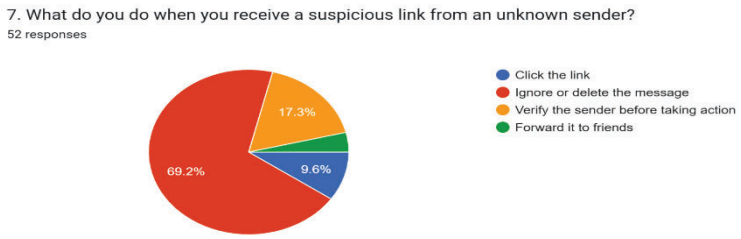
Response	Count	%
On most important accounts	25	50.0%
On a few accounts	16	32.0%
No	4	8.0%
I don't know what 2FA is	5	10.0%

Interpretation:

Only 40.0% of respondents updated their passwords regularly, while 24.0% did so only when they forgot the password and 4.0% never did. Password reuse was common: 26.0% always and 48.0% sometimes used the same password on multiple accounts, which together is 74.0%. Only 16.0% never reused a password. For two-factor authentication, 50.0% used it on most important accounts and 32.0% on a few. However, 18.0% did not use it, including 10.0% who did not know what 2FA is.

5.3 Handling of Links, Privacy, Wi-Fi, Apps and Personal Information (Objective 2)

Distribution by: What do you do when you receive a suspicious link from an unknown sender?

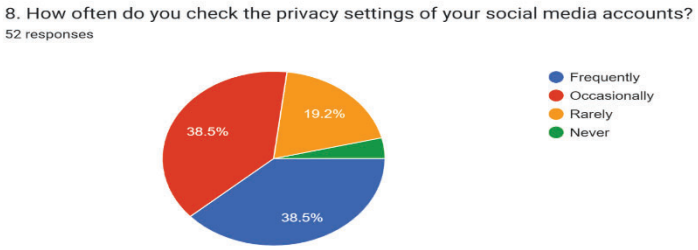


Response	Count	%
Ignore or delete the message	34	68.0%
Verify the sender before taking action	5	18.0%
Click the link	9	10.0%
Forward it to friends	2	4.0%

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

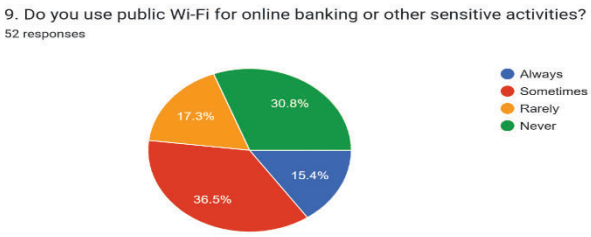
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Distribution by: How often do you check the privacy settings of your social media accounts?



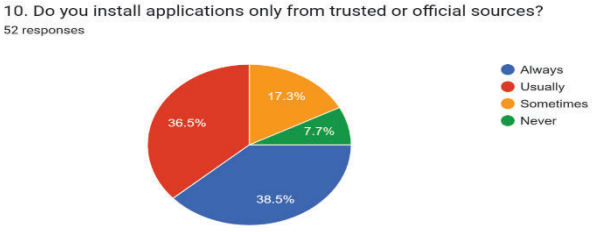
Response	Count	%
Frequently	20	40.0%
Occasionally	18	36.0%
Rarely	10	20.0%
Never	2	4.0%

Distribution by: Do you use public Wi-Fi for online banking or other sensitive activities?



Response	Count	%
Always	9	14.0%
Sometimes	19	38.0%
Rarely	8	16.0%
Never	16	32.0%

Distribution by: Do you install applications only from trusted or official sources?

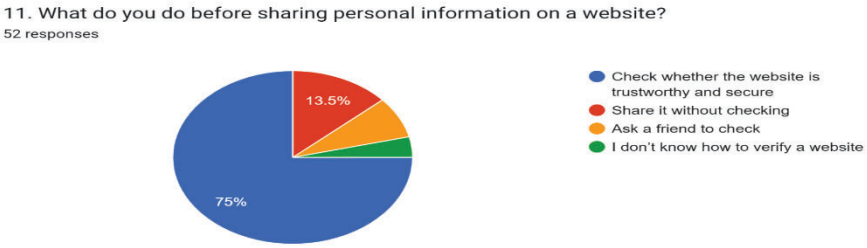


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Response	Count	%
Always	19	38.0%
Usually	19	38.0%
Sometimes	8	16.0%
Never	4	8.0%

Distribution by: What do you do before sharing personal information on a website?



Response	Count	%
Check whether the website is trustworthy and secure	38	76.0%
Share it without checking	7	14.0%
Ask a friend to check	3	6.0%
I don't know how to verify a website	2	4.0%

Interpretation:

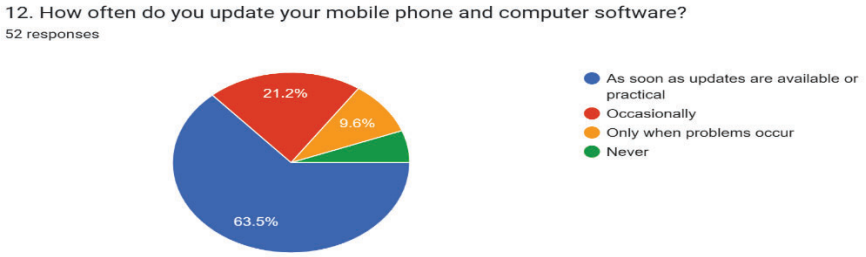
For suspicious links, 68.0% ignored or deleted the message and 18.0% verified the sender, but 14.0% took a risky action: 10.0% clicked the link and 4.0% forwarded it to friends. Privacy settings were checked frequently by 40.0%, while 24.0% checked them rarely or never. Public Wi-Fi use for sensitive activities was a clear concern: 52.0% did so always or sometimes, and only 32.0% never did. For app downloads, 76.0% installed apps always or usually from trusted sources, but 24.0% did so only sometimes or never. Before sharing personal information, 76.0% checked whether the website was secure, while 24.0% shared without checking, asked a friend, or did not know how to verify a website.

5.4 Software Updates and Response to a Suspected Hack (Objective 3)

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

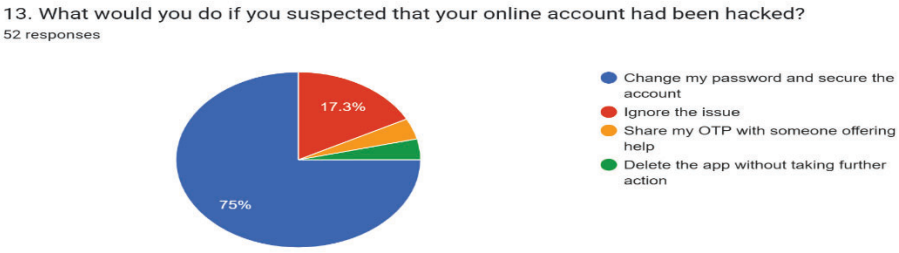
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Distribution by: How often do you update your mobile phone and computer software?



Response	Count	%
As soon as updates are available or practical	32	64.0%
Occasionally	11	22.0%
Only when problems occur	4	8.0%
Never	3	6.0%

Distribution by: What would you do if you suspected that your online account had been hacked?



Response	Count	%
Change my password and secure the account	38	76.0%
Ignore the issue	9	18.0%
Share my OTP with someone offering help	2	4.0%
Delete the app without taking further action	1	2.0%

Interpretation:

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Software updates were applied promptly by 64.0% of respondents, while 36.0% updated occasionally, only when problems occurred, or never. In response to a suspected hack, 76.0% would change their password and secure the account. The remaining 24.0% chose an unsafe response: 18.0% would ignore the issue, 4.0% would share their OTP with someone offering help, and 2.0% would delete the app without further action. Sharing an OTP with a stranger is especially dangerous because it can give an attacker direct access to the account.

5. Summary of Key Findings

1. The dataset contains 50 survey responses. Most respondents were aged 18–20 years (76.0%), female (62.0%), and undergraduate students (72.0%).
2. Password habits are weak for many students. Only 40.0% updated passwords regularly, and 74.0% reused the same password at least sometimes.
3. Two-factor authentication is fairly widely used (82.0% on at least some accounts), but 10.0% did not know what it is.
4. Most respondents handled suspicious links safely (86.0% ignored or verified), but 14.0% clicked the link or forwarded it.
5. 52.0% used public Wi-Fi for banking or other sensitive activities at least sometimes.
6. 76.0% checked a website before sharing personal information, but 24.0% did not.
7. 64.0% updated software promptly, and 76.0% installed apps always or usually from trusted sources.
8. 76.0% would change their password after a suspected hack, but 24.0% would respond unsafely, including 4.0% who would share their OTP.

6. Suggestions and Recommendations

- Teach students to use a different password for each account and to use a password manager, since 74.0% reuse passwords at least sometimes.
- Promote two-factor authentication with a short demonstration of how to switch it on, including for the 10.0% who do not know what it is.
- Run awareness sessions on public Wi-Fi risks and safer alternatives such as mobile data for banking and payments.
- Use practical exercises and simulated phishing messages so that students learn to verify senders and avoid clicking unknown links.
- Explain clearly what to do after a suspected hack: change the password, enable 2FA, and never share an OTP with anyone. Include how to report incidents on the national cyber crime portal and helpline.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

- Encourage regular review of privacy settings and checking a website's security before sharing personal information.
- Remind students to install updates promptly and download apps only from official stores.
- Repeat the survey with a larger sample to see whether practices improve.

7. Conclusion

This study examined the online safety practices of 50 college students, covering their password habits, use of two-factor authentication, handling of suspicious links, privacy settings, public Wi-Fi use, app downloads, sharing of personal information, software updates, and responses to a suspected account hack. The findings show that many respondents follow safe practices, such as ignoring suspicious links, checking websites, and updating software, but significant gaps remain. Password reuse, infrequent password updates, use of public Wi-Fi for sensitive activities, and unsafe responses to a suspected hack were common enough to be a concern.

The survey gives descriptive evidence of respondents' self-reported habits. Because the sample is small and was selected by convenience, the results cannot be generalized to all students, and the study does not establish that any single factor causes safer or riskier behavior. A practical next step is for colleges to combine awareness sessions, hands-on practice, and clear reporting channels. Future research with a larger and more varied sample, including questions that test knowledge of specific threats, could examine differences by gender, age, and course in greater depth.

References

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815–825.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165–176.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93–114.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)