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 10, March 2026
Impact Factor: 8.2

Cyber Security Awareness Among Internet Users Recent Technology Trends in Computer Technology

Rushda Osama Khanzada, Sai Sanjay Kotwal and Abdul Rehman Imtiyaz Bharoon
Department of Computer Science
Anjuman Islam Janjira Degree College of Science Murud-Janjira Raigad MS India

Abstract: *The increasing use of the internet has made cyber security awareness essential for users. This study examines the level of awareness, online behavior, and security practices among internet users through a Google Form survey of 40 respondents. The results show that most participants access the internet daily, mainly via mobile phones. Although many users are aware of cyber threats, knowledge about specific risks such as phishing and identity theft remains limited. The study also found risky practices, including password reuse, failure to verify website links, and low usage of antivirus software. A notable number of respondents have experienced cybercrime, indicating existing security gaps. However, most participants agreed that cyber security awareness programs are necessary. Overall, the research highlights the need for better education and training to improve safe online behavior and reduce cyber risks, ultimately promoting a more secure digital environment.*

Keywords: Cyber Security, Awareness, Internet Users, Cyber Threats, Online Safety

I. INTRODUCTION

The widespread adoption of the internet has transformed the way people communicate, work, learn, and access information. From online banking and shopping to social networking and digital education, internet services have become an essential part of daily life. However, this increased reliance on digital platforms has also led to a rise in cyber threats such as phishing, malware, identity theft, and data breaches. As a result, cyber security awareness has become a critical requirement for protecting personal and organizational information.

Cyber security awareness refers to the knowledge and practices that help individuals recognize potential online risks and take appropriate precautions to avoid them. Despite technological advancements in security systems, human error remains one of the leading causes of cyber incidents. Weak passwords, sharing sensitive information, clicking on suspicious links, and neglecting security software can make users vulnerable to attacks.

This study focuses on assessing the level of cyber security awareness among internet users and understanding their online safety behaviors. Using a survey-based approach, the research analyzes users' knowledge of cyber threats, password habits, use of security tools, and experiences with cybercrime. The findings aim to identify gaps between awareness and actual practices while emphasizing the importance of educational programs to promote responsible internet usage and create a safer digital environment.

II. METHODOLOGIES

1. **Research Design:** This study uses a quantitative research design to systematically evaluate the level of cyber security awareness among internet users. The approach focuses on collecting measurable data that can be analyzed to identify patterns in user knowledge, behavior, and security practices.
2. **Data Collection Method:**Primary data was collected through an online survey created using Google Forms. The questionnaire was designed to be simple, clear, and easy to understand, encouraging participants to provide accurate responses.

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 10, March 2026
Impact Factor: 8.2

3. **Questionnaire** Structure:The survey consisted of multiple-choice questions covering key areas such as:
   - Frequency of internet usage
   - Devices used to access the internet
   - Awareness of common cyber threats (phishing, malware, identity theft, etc.)
   - Password management habits
   - Use of antivirus and other security tools
   - Ability to identify suspicious links or websites
   - Personal experiences with cybercrime
   - Opinions on the importance of cyber security awareness
4. **Sample Size and Participants:**A total of 40 respondents participated in the survey. The participants represented diverse age groups and occupational backgrounds, providing a broader perspective on cyber security awareness.
5. **Sampling Technique:**Convenience sampling was used to gather responses quickly and efficiently. Participants were selected based on accessibility and willingness to complete the survey.
6. **Data Analysis:**The responses were automatically recorded in Google Forms and presented in the form of charts and graphs. Percentage-based statistical analysis was applied to interpret the data, making it easier to identify trends, common behaviors, and awareness levels among respondents.
7. **Purpose of the Methodology**: The methodology aims to assess how well internet users understand cyber risks, evaluate their safety practices, and identify gaps between awareness and actual behavior. The findings\

III. LITERATURE REVIEW

Cyber security awareness has become an important area of research due to the rapid expansion of internet technologies and the increasing number of cyber threats. Researchers have emphasized that while technological defenses are improving, users remain one of the most vulnerable points in maintaining digital security.

Studies suggest that a lack of awareness and insufficient knowledge about cyber threats often lead to unsafe online behavior. Many users fail to recognize phishing emails, malicious links, and fraudulent websites, making them easy targets for cybercriminals. According to previous research, weak password practices, such as using simple passwords or repeating them across multiple accounts, significantly increase the risk of data breaches.

Researchers have also highlighted that education plays a major role in improving cyber security awareness. Training programs, awareness campaigns, and digital literacy initiatives help users understand potential risks and adopt safer practices, such as enabling two-factor authentication and regularly updating security software.

Furthermore, literature indicates that younger internet users are generally more active online but may overlook security precautions due to overconfidence in technology. On the other hand, some studies show that individuals who have previously experienced cybercrime tend to be more cautious in their online activities.

Overall, existing research demonstrates that although awareness of cyber security is gradually increasing, there is still a gap between knowledge and actual implementation of safe practices. This study builds upon prior research by examining current awareness levels and user behavior, contributing to a better understanding of cyber security preparedness among internet users.

IV. RESULT AND DISCUSSION

The survey collected responses from **38 participants** to assess **awareness of Artificial Intelligence (AI)**, patterns of **internet usage**, and understanding of **AI-based tools and related digital risks**. The findings offer valuable insights into how users engage with AI technologies in their daily lives and their level of awareness regarding the benefits and limitations of AI.

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 10, March 2026
Impact Factor: 8.2

1. Age Distribution (Figure 1)

Figure 1 shows that the majority of respondents fall within the 18–20 years age group (67.6%), indicating strong participation from late adolescents and young adults. This is followed by respondents aged 21–23 years (16.2%) and 15–17 years (13.5%). Only a small proportion of participants belonged to the 24–25 years age group (approximately 2.7%).

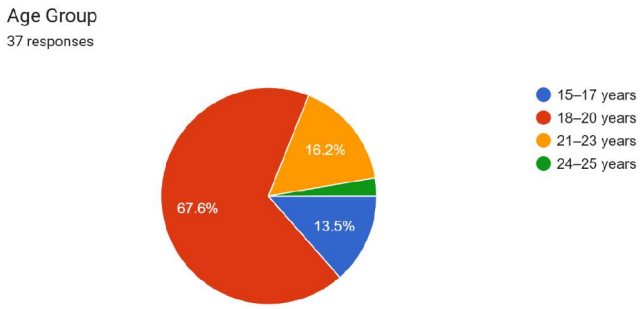


Figure 1 shows a pie chart representing the age groups of respondents, highlighting that most participants are young adults.

2. 2. Gender Distribution (Figure 2) : The gender-wise analysis shows that a majority of the respondents were female (64.9%), while 35.1% were male. No participants selected the "prefer not to say" option. This indicates higher participation from female respondents in the survey, providing a gender-diverse perspective on AI awareness and usage among youth.

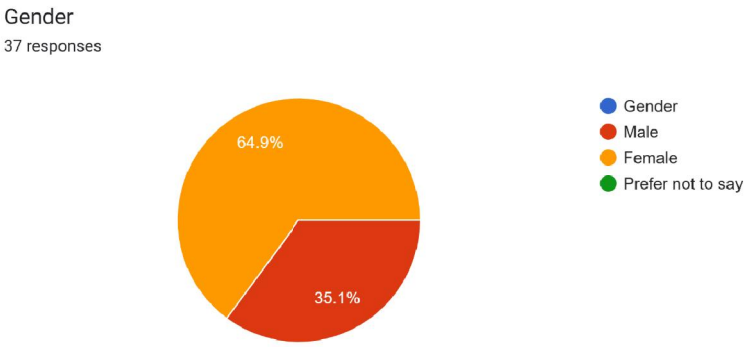


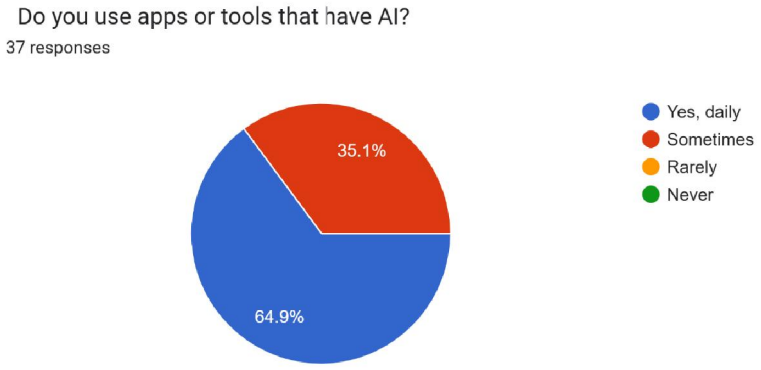
Figure 2 illustrates the occupational status of participants

V. USAGE OF AI APPLICATIONS OR TOOLS (FIGURE 3)

The results show that a majority of participants (**64.9%**) use AI-based applications or tools **daily**, indicating that AI has become a regular part of their daily activities. The remaining **35.1%** reported using AI **sometimes**. Notably, no respondents selected the options "rarely" or "never," suggesting widespread exposure to and reliance on AI technologies among the youth population.

DOI: 10.48175/IJARSCT-35027

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 10, March 2026
Impact Factor: 8.2



VI. WHICH AI APPS OR TOOLS DO YOU USE MOST(FIGURE 4)

The Social media platforms such as Instagram, TikTok, and YouTube were the most frequently used AI tools, selected by 81.1% of participants. This was followed by voice assistants and games or smart devices, each used by 29.7% of respondents. Learning applications such as Duolingo and Khan Academy were used by 10.8%, while 8.1% reported not using any AI tools

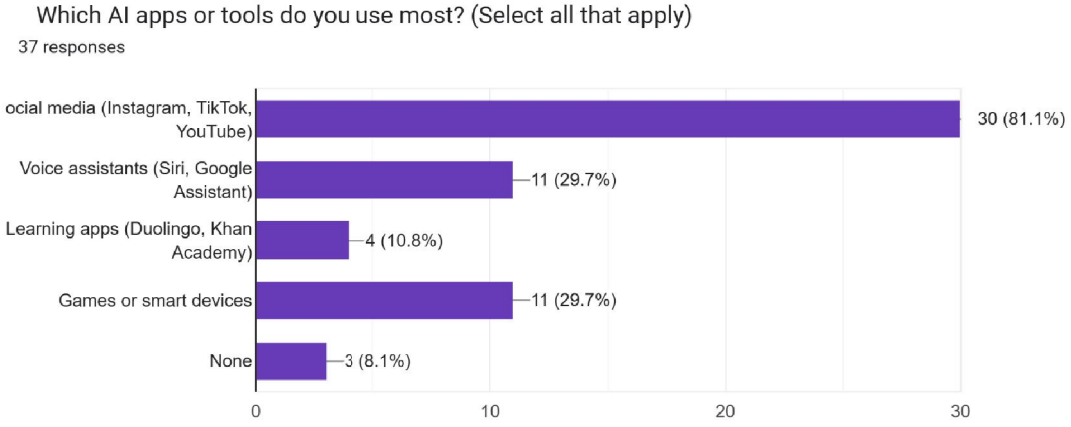


Figure 4 displays a bar chart showing mobile phones as the dominant device for internet access.

VII. AWARENESS OF AI (FIGURE 5)

About 65% of respondents reported being aware of cyber security threats, while 35% indicated they were not aware.

Discussion:

Although a majority claim awareness, the presence of a significant unaware group suggests that cyber security knowledge is still not universal. Awareness campaigns, workshops, and digital literacy programs can help bridge this gap.

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 10, March 2026
Impact Factor: 8.2

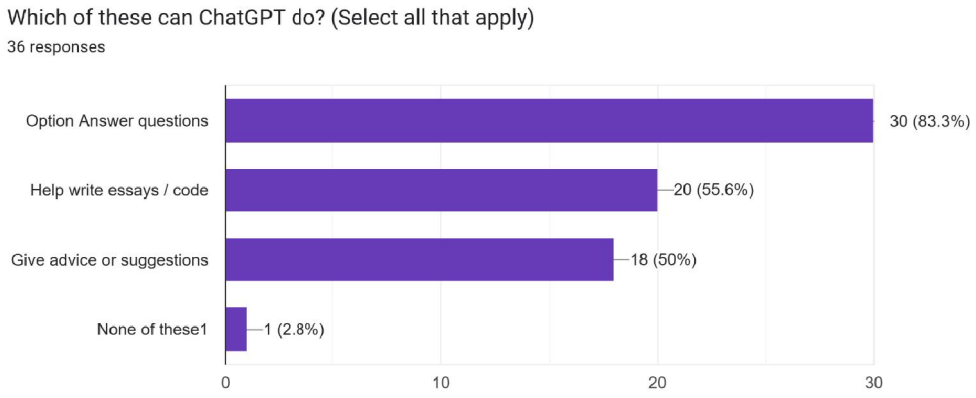


Figure 5 shows a pie chart comparing respondents who are aware of cyber threats versus those who are not.

VIII. KNOWLEDGE OF SPECIFIC CYBER THREATS (FIGURE 6)

The results show that 32.5% of respondents are aware of malware and identity theft, 25% know about phishing, and only 7.5% recognize ransomware, while 40% are not aware of any cyber threats.

Discussion:

This indicates that although some users understand common cyber risks, a large number still lack basic knowledge, making them more vulnerable to online attacks. Increasing awareness through education and training is necessary to improve cyber safety.

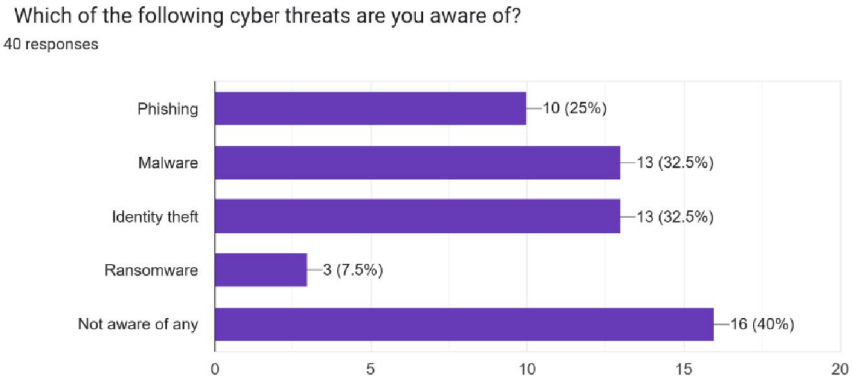


Figure 6 presents the level of awareness regarding different cyber threats among respondents.

IX. USE OF STRONG PASSWORDS (FIGURE 7)

shows that 52.5% of respondents always use strong passwords, while 25% use them sometimes and 22.5% never use strong passwords.

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 10, March 2026
Impact Factor: 8.2

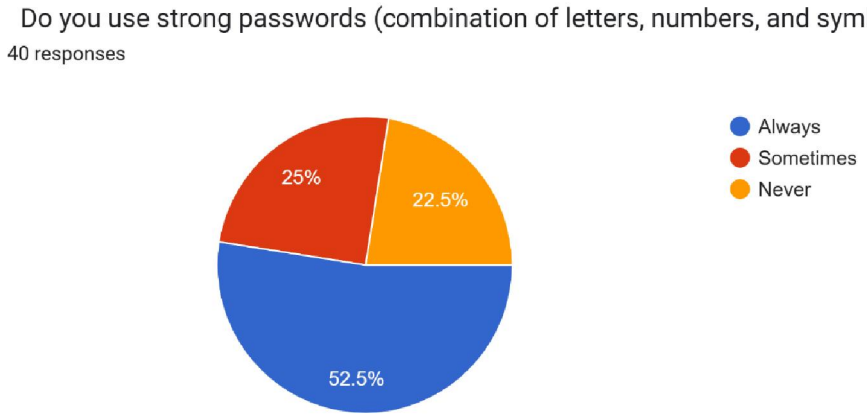


Figure 7 Password reuse across multiple online accounts

X. REUSE OF PASSWORDS ACROSS MULTIPLE ACCOUNTS (FIGURE 8)

When asked whether they use the same password for multiple online accounts, **61.5%** of respondents answered **yes**, while only **38.5%**reported using unique passwords.

This highlights a major security risk, as password reuse increases susceptibility to account compromise in the event of a data breach.

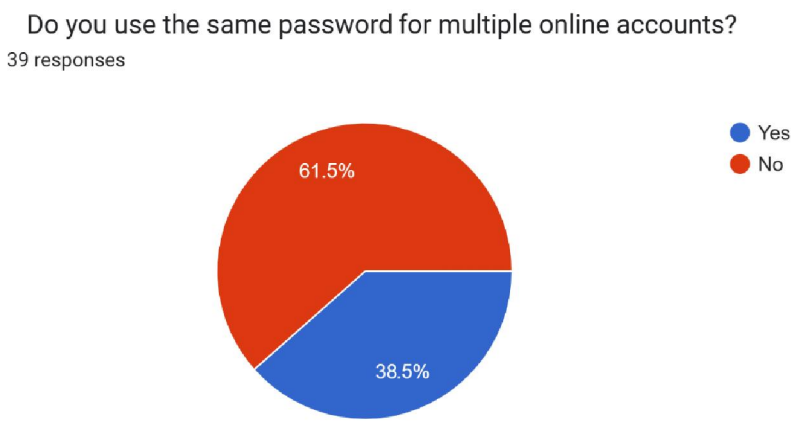


Figure 8 Use of the same password for multiple online accounts

XI. VERIFICATION OF WEBSITE LINKS (FIGURE 9)

When asked whether they verify website URLs before entering personal information, __% reported always checking, __% sometimes checking, and __% never checking. This shows that while many users practice caution, a portion of respondents remain at risk of phishing scams.

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 10, March 2026
Impact Factor: 8.2

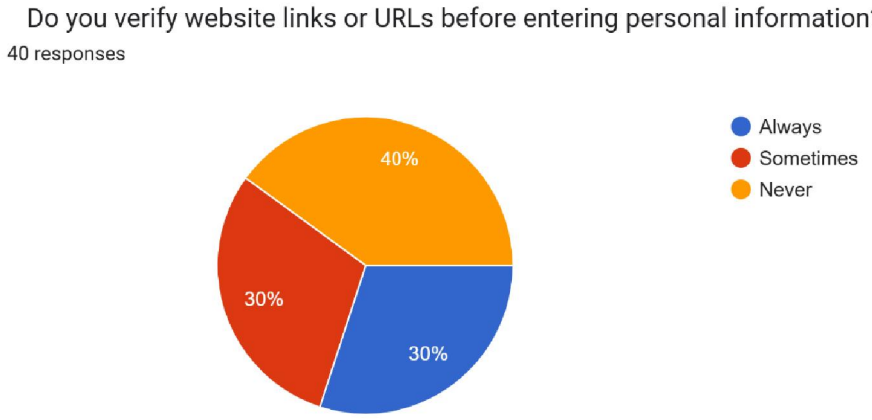


Figure 9 Verification of Website Links

Use of Antivirus Software (Figure 10):
The survey found that __% of respondents use antivirus or security software, while __% do not. This reflects a moderate level of awareness regarding device protection, though the absence of security tools among some users is concerning.

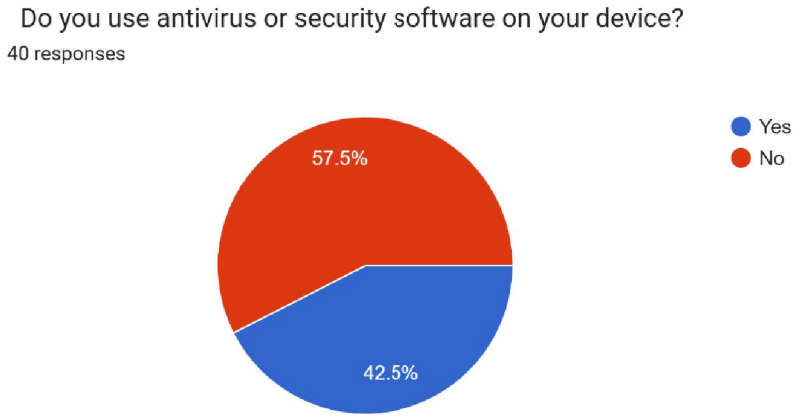


Figure 10 Use of Antivirus Software

XII. CONCLUSION

This study examined the level of cyber security awareness among internet users through a structured survey. The findings indicate that while many users demonstrate basic knowledge of online safety practices—such as verifying website links and using antivirus software—there are still noticeable gaps in secure behavior. For example, some respondents continue to reuse passwords across multiple accounts, which increases the risk of data breaches and cyberattacks.

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 10, March 2026 Impact Factor: 8.2

Additionally, the results show that a number of participants have experienced cybercrime, emphasizing the growing importance of strong security measures in today's digital environment. Encouragingly, most respondents recognized the need for cyber security awareness programs, reflecting a willingness to learn and adopt safer online habits.

Overall, the study concludes that cyber security awareness among internet users is improving but remains insufficient. Continuous education, awareness campaigns, and training programs are essential to help individuals understand potential threats and practice safer internet usage. Strengthening cyber security knowledge will not only protect personal information but also contribute to a more secure digital society.

ACKNOWLEDGEMENT

I hereby declare that all the information provided in the respected paper is authenticated , authorized and hence reliable. I would like to thanks all the viewers and readers of this paper for their precious time.

REFERENCES

1. Nagari, S. F., & Raharja, S. (2000). *Cyber security awareness, knowledge and behavior of digital banking users in Salatiga*.
2. Gahletia, K., & Upadhaya, K. (2022). *Cybersecurity awareness in the age of social media: A behavioral study*.
3. Modupe, A. O. (2017.). *Assessment of internet safety, cybersecurity awareness and risks in technology environment among college students*.
4. Dawkins, S., & Jacobs, J. (2023). *Phishing with a net: The NIST phish scale and cybersecurity awareness*.
5. Mittal, C. (2024). *An empirical study on cybersecurity awareness, cybersecurity concern, and vulnerability to cyber-attacks*.
6. Anonymous. (2018). *Cybersecurity awareness: A critical analysis of education and law enforcement methods*.
7. Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). *Cybersecurity practices for social media users: A systematic literature review*.
8. Priya, J. R., et al. (2015). *Awareness of cyber security among internet users with reference to Coimbatore district*.