Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2026): 8.748 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 13 | Issue: 3 | March 2026 -Peer-Reviewed Journal

A STUDY OF CYBER SECURITY AWARENESS AMONG STUDENTS IN VAIJAPUR TAHSIL

Abhijit Ramrao Thorat
Assistant. Professor, Vinayakrao Patil Mahavidyalaya Vaijapur, Dr. B .A. M. University. CSN

ABSTRACT
This Research Paper discussed about Awareness among College Students of Cyber Security and Cyber Crimes. It Further analyzed The Impact of Cyber Crimes on their Internet Use in vaijapur Tahsil Rural Areas. In terms of Cyber Awareness in Students prefer Safe Internet Use.
KEYWORDS : *Cyber Crimes, Internet Use etc.*

INTRODUCTION

Cyber security crimes in India increased day by day in 2025, with financial losses more than ₹22,000 core, driven by UPI fraud, investment scams, and phishing. The most common crimes include financial fraud, identity theft, cyber stalking, and deep fake impersonation. The government is responding with increased budgetary allocation, blocking fraudulent SIMs/IMEIs, and operating the 1930 cyber helpline.

This Paper Analyze how Increase Cyber crime in Society harass Students in their internet Use.how much Cyber Crime affect Students day to day Internet use , & How many Students are Aware about Safe internet Use and Various Types of Cyber Crimes.Following are The Various cyber Crimes Increase day by Day in Internet world.

Various Types of Cybercrimes in India :

- **Financial Fraud:** The most prevalent, involving UPI scams, fraudulent investment apps, and job scams that promise high returns or remote work.
- **Phishing & Identity Theft:** Stealing personal data or credentials via deceptive emails, SMS, or calls to drain bank accounts.
- **Deep fakes & AI Crime:** Rapidly growing, using artificial intelligence to create fake videos or images for extortion and defamation.
- **Social Media & Online Harassment:** Cyber stalking, bullying, and creating fake profiles to harass individuals.

Major Vulnerabilities

The rapid increase in internet connectivity (86%+ households) combined with high-speed digital payment adoption has made India a prime target for cybercriminals. High-risk areas include online banking, social media misuse, and data breaches resulting from poor cloud security.

Cyber security awareness for students is vital to prevent personal data theft, protect academic records, and secure school networks from malware and ransom ware attacks. As young users often fall victim to phishing and online scams, education on safe digital habits—such as using strong passwords and recognizing threats—is critical for protecting their privacy and fostering a culture of caution.

Key reasons for the importance of cyber security awareness in students include:

- **Protection Against Cyber Threats:** Students face risks like identity theft, cyber bullying, and phishing scams that can compromise personal and financial information.
- **Securing Students Educational Life :** Students often use personal devices, which can introduce malware to school networks, leading to major data breaches.

Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2026): 8.748 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 13 | Issue: 3 | March 2026 -Peer-Reviewed Journal

- **Data Privacy of Students :** With the rise of online learning, student records, assignments, and personal data are highly targeted, making awareness necessary for protecting privacy.

- **Developing Safe Habits among Students:** Education promotes crucial habits like using multi-factor authentication (MFA), creating strong passwords, and identifying suspicious links.
- **Academic Integrity:** Awareness helps prevent online academic dishonesty, such as plagiarism and cheating, which can occur on unsecure platforms.

Structured cyber security training and education allow students to become proactive, responsible, and secure, ensuring they can navigate the digital world safely.

Objectives of this Study

1. To study the Awareness of Cyber security among college students
2. To collect the information about Cyber security knowledge in students
3. To study the safe use of Internet in students.
4. To study the Cyber Security factor and its impact on college students.

Need of the the study

Cyber crime increase day to day in society , after the Corona period and increase the use of Internet in computer users. No of cyber crimes also increase every day , Phishing ,Hacking, Bullying, Harassment increase in society. To find out the Awareness among students about cyber security & Aware them about various cybercrimes in cyber world. And motivate them safe Browsing on the Internet.

Scope And Limitation of The Study

1. This study is related to the Vaijapur taluka college students
2. The use of Internet increase in the students ,but Awareness is not that much
3. This further leads to increase cyber crimes in society
4. The study cover various college students data.

Research Methodology

A convenience sample is type of non-probability sampling method where the sample is taken from a group of people easy to contact or reach for example , standing at a mail or grocery store and asking people to answer questions . This type of sampling or availability Sampling. There are no other Criteria to the sampling method except that people be available and willing to participate. In addition , this type of sampling method does not require that a simple random sample is generated since the only criterion is whether the participants agree to participate .B.Com 100 ,BBA 100 , BCA 100 , BCS 100. . So data is very large the total study not possible then select the convenience sampling method.

Table 1: Selection of the Sample-

Tahsil	Villege Name	No Sample
Vaijapur	Vaijapur	50
	Khandala	30
	Shivoor	20
	Total	100

Data Collection Method

Primary Data: Primary data collection involves gathering data from first-hand experiences and sources, which haven't been available in the past. Its quite simply the first information in its basic to see, we decided to go to the door of small business. Before conducting the survey, we prepared a 15 –question questionnaire in which we asked about cyber awareness . They were ready to know the drought situation.

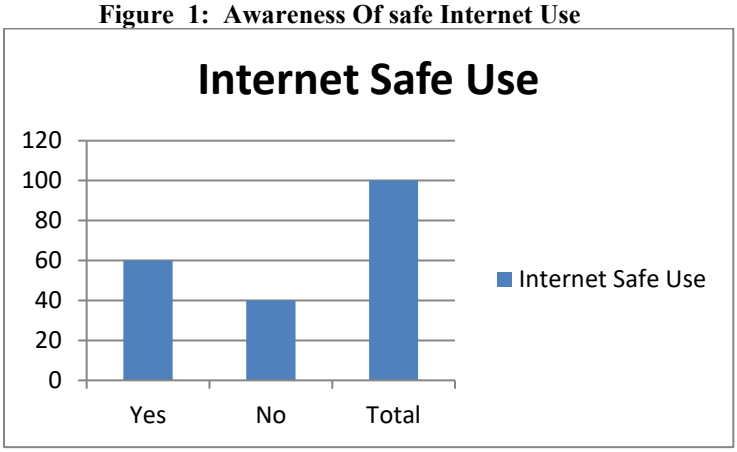
Secondary data: Secondary data is one of the main types of data, where the second types the primary data . These two data types are very useful in research and findings.

Table 2: Familiar of Safe Internet Use

Question	Yes	No	Not Exact Known	Total
Familiar of safe Internet Use	60	40		100

Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2026): 8.748 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 13 | Issue: 3 | March 2026 -Peer-Reviewed Journal

Figure 1: Awareness Of safe Internet Use



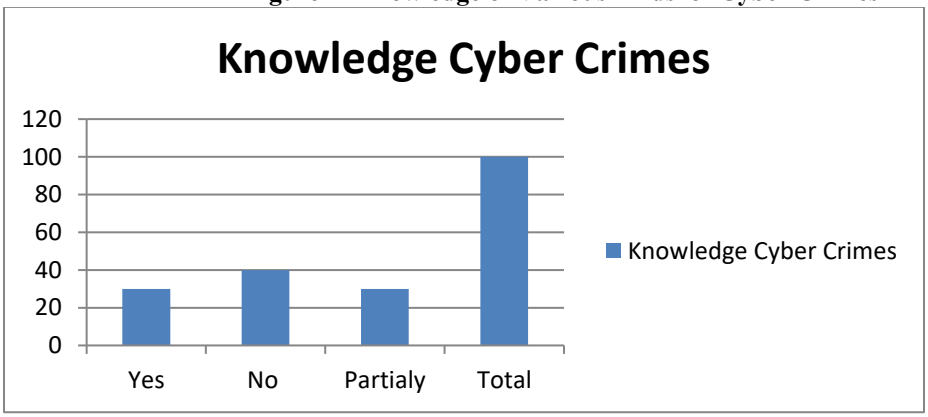
Interpretation

Among the strength of Internet users 60% say they use safely internet, 40% users say No & 30 say they don't know How to use safe Internet.

Table 3: Knowledge of Various kinds of Cyber Crimes

Question	Yes	No	Not Exact Known	Total
Knowledge of Various Cyber Crimes	33	37	30	100

Figure 2: Knowledge of Various kinds of Cyber Crimes



Interpretation

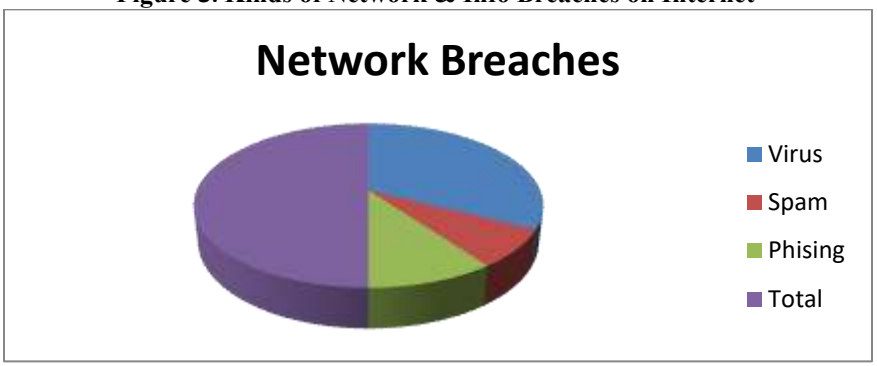
Among the strength of Internet users 33% say they known cyber crimes, 37% users say No & 30 say they know partially about Cyber Cries Internet.

Table 4: What kinds of Network & Info Breaches on Internet

Question	Virus	Spam	Phishing	Total
Knowledge of What Kinds of Network Breaches	65	15	20	100

Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2026): 8.748 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 13 | Issue: 3 | March 2026 -Peer-Reviewed Journal

Figure 3: Kinds of Network & Info Breaches on Internet



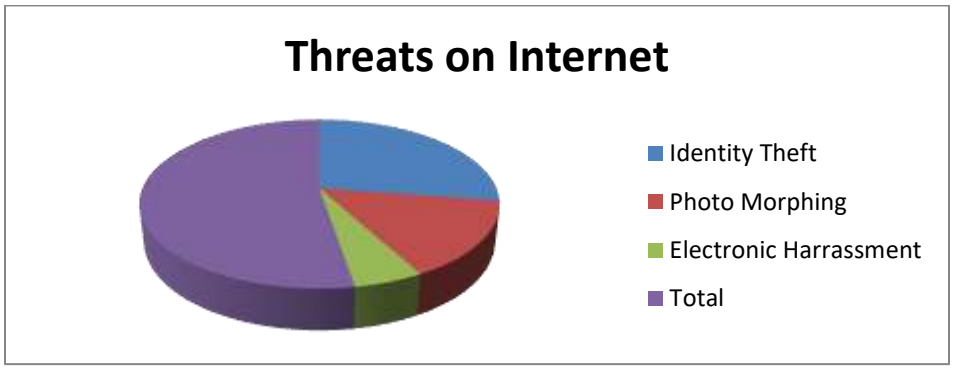
Interpretation

Among the strength of Internet users 65% say Virus is Reason Of Network Beach, 15% users say Spam & 20% say Phishing is Reason of Network Breach on Internet.

Table 5: What kinds of Threats on Internet

Question	Identity Theft	Photo Morphing	Electronic Harrassment	Total
What Kinds of Threats They Face	52	28	10	100

Figure 4: Kinds of Threats on Internet



Interpretation

Among the strength of Internet users 52% say Identity Theft Threats they Face, 28% users say Photo Morphing & 10% say Electronic Harassments Reason of Network Breach on Internet.

Findings & Conclusions

Bar chart graph 1 shows 60% users of internet Know safe Use ,then 30% say they Don't know safe use of Internet. Bar-Chart graph Show 33% Users Know Various Cyber Crimes & 37% users Say They Don't Know. Pie-Chart 3 graph Show that 65% Users Say Virus's is reason of network breach & 15 % Say Spam is reason of breach & 20 say Phishing Is reason Of network breach. Pie-Chart 4 Show that 52% Users Face Identity threats & 28% say Photo morphing Threats They face & 10 % Users Face Electronic Harassment Threats.

Conclusions

1. The study of Cyber Awareness is an extremely complex endeavor. It Requires to contact to those Internet Users Regularly. Approximately 40 % Users are Unawareness about Cyber Security.
2. The Study Show that Cyber Security awareness Among Students.
3. The Study show that any Internet Users Faces Cyber threats.
4. Due to Cyber Crimes many users Cheat in Phishing.

5. Due to Cyber Crimes many users tackle Photo Morphing Crimes.
6. For secure Internet Navigation Use Proper Anti-Virus & HTTPS Websites.

Suggestions

Administration to provide various schemes for prohibit cyber crimes ,it create Cyber Awareness among Common Citizen. It Also Create lot of Job Opportunities for Cyber securities Expert. Govt Also Provide Cyber security Education to Internet Users for Securing their Internet Navigation & Secure their Financial Transactions. Govt create CERT type Organizations for Cyber Awareness and Tackle Cyber Crimes.

BIBLOGRAPHY

Books & Journal

1. *Cyber Security Awareness Challenges And Issues- Prof. Sanjay Vaid*
2. *Cyber Awareness – Dr. Nitin Rajvanshi*
3. *Cyber Security Awareness –Michael Mullins*

Websites

https://ai overview
https://www.cert.-in.org.in
https://www.csk.gov.in
https://www.staysafeonline.org