International Journal of Engineering & Scientific Research
Vol.11 Issue 10, October 2023
ISSN: 2347-6532 Impact Factor: 7.501
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Awareness of Phishing Among Students: A Survey-Based Study on Cyber Threats *(Special Reference to Aurangabad)*

Dr. S. S. Nandnavare,
BCA Department,
College of Computer Science and Multimedia,
Satara Parisar, Aurangabad (Sambhajinagar)

Abstract:

The rapid growth of internet usage among students has brought numerous educational and social benefits, but it has also exposed them to a variety of cyber threats. Among these, phishing stands out as one of the most pervasive and deceptive forms of cybercrime. Phishing attacks exploit human trust, curiosity, and lack of technical awareness to steal sensitive information such as passwords, banking details, or personal data. This study aims to assess the level of awareness and preparedness against phishing among students in Aurangabad during the academic year 2023–24. A structured questionnaire was administered to a representative sample of school and college students. The survey examined demographic details, patterns of internet usage, familiarity with phishing techniques, and existing cyber safety practices. Findings reveal that although students demonstrate moderate internet literacy, their understanding of phishing and preventive strategies remains limited. Only 42% of respondents reported having heard the term "phishing," and a striking 63% admitted to having clicked on suspicious links, often through emails, social media messages, or fake websites. Many students lacked knowledge about verifying website authenticity or using security tools such as two-factor authentication. These results underscore the urgent need for targeted cyber safety education and awareness programs within academic institutions. Integrating digital literacy modules into school and college curricula enhance students' ability to identify fraudulent activities, avoid risky online behaviours, and build resilience against evolving cyber threats.

Keywords:

Phishing, Cybersecurity, Students, Awareness, Aurangabad, Internet Safety, Digital Literacy, Cyber Threats, Online Security etc.

Introduction:

In today's digital society, internet use has become an inseparable part of daily life, shaping the way individuals learn, communicate, and entertain themselves. For students, in particular, the internet has emerged as a powerful tool for education, offering instant access to knowledge, online courses, e-learning platforms, and global collaboration opportunities. Social media networks and messaging apps further enhance connectivity, enabling real-time communication and the sharing of ideas beyond geographical boundaries. However, along with these immense opportunities for growth and development, the internet also introduces significant risks. Among the various cyber threats that endanger users, phishing has become one of the most deceptive and damaging forms of online crime.

Phishing is a malicious activity in which attackers impersonate trusted entities through fraudulent emails, fake websites, or misleading messages to trick individuals into revealing sensitive personal information such as passwords, banking credentials, or identity details. Unlike other forms of cyberattacks that rely heavily on advanced technical exploits, phishing manipulates human psychology, exploiting curiosity, urgency, or trust to achieve its objectives. This makes it particularly dangerous because even technically aware users may fall victim if they are not cautious.

Students, as some of the most active internet users, are especially vulnerable to phishing attacks. Their frequent engagement with social media platforms, online learning systems, gaming networks, and digital communication channels creates multiple points of exposure. Many students prioritize convenience over security, often reusing passwords, clicking on unknown links, or sharing personal information without verification. Limited awareness of cyber hygiene practices and the absence of structured training programs further heighten their risk of falling prey to phishing schemes.

With India experiencing rapid digital penetration through affordable internet services and widespread smartphone usage, understanding the level of phishing awareness among students has become critically important. The student population represents a significant segment of future professionals, and their digital behaviour today will influence the overall cybersecurity landscape of the country. If students remain unaware of phishing tactics, they may compromise their personal data and endanger institutional networks, academic platforms, and even family members through secondary attacks.

Assessing phishing awareness among students is, therefore, essential to design effective prevention strategies. Surveys and studies focusing on students' knowledge of phishing techniques, recognition of suspicious links, and use of protective measures such as strong passwords or two-factor authentication reveal key gaps in digital literacy. The insights gained guide schools, colleges, and policymakers to implement targeted cyber safety programs, workshops, and curriculum-based training sessions.

Building a culture of cybersecurity awareness will empower students to identify suspicious messages, avoid fraudulent websites, and practice safe online behaviour. Educational institutions play a pivotal role in reducing phishing incidents and ensuring that the benefits of the internet are enjoyed without compromising privacy and security by promoting responsible

internet usage and strengthening digital literacy,

Objectives of the Study:

1. To assess the level of awareness of phishing among students in Aurangabad.
2. To analyse students' internet usage patterns and exposure to potential phishing threats.
3. To evaluate the adoption of cyber safety practices such as password updates and two-factor authentication.
4. To identify gaps in knowledge and suggest educational interventions for improving cybersecurity awareness.

Review of Literature:

Several studies emphasize the growing threat of phishing in India, particularly among young internet users. **Gupta and Jain (2020)** reported that phishing constitutes more than 30% of all reported cyber fraud cases in major Indian metropolitan cities, highlighting the scale and persistence of this cybercrime. Their findings indicate that phishing has surpassed other forms of online fraud such as identity theft and credit card scams, largely due to its low cost of execution and high success rate.

In a related study, **Chakraborty (2021)** observed that students and young professionals are among the most frequent victims of phishing attacks. The research attributes this vulnerability to limited cybersecurity training, over-reliance on social media, and the tendency to share personal information without adequate verification. The study also pointed out that while internet literacy is increasing among the younger population, specific awareness regarding phishing techniques remains critically low.

Further supporting this concern, **Rao and Sharma (2022)** demonstrated that structured awareness programs significantly reduce susceptibility to phishing attempts. Their experimental research conducted in selected colleges showed that after a targeted cybersecurity workshop, students' ability to identify suspicious emails and fake URLs improved by nearly 45%.

Other scholars have echoed similar findings. **Kumar and Patel (2020)** analysed phishing trends across Indian educational institutions and discovered that nearly 60% of surveyed students failed to recognize warning signs in fraudulent emails. Likewise, **Mishra et al. (2021)** emphasized that phishing attacks are evolving rapidly, with attackers using more sophisticated techniques such as spear-phishing and social engineering to bypass conventional security tools.

These studies collectively underscore the urgent need for comprehensive cyber safety education. They suggest that integrating cybersecurity awareness into school and college curricula, coupled with regular training sessions and simulated phishing exercises, substantially reduce the risk of students becoming victims of such attacks.

Research Methodology:

Research Design:

The present study employed a descriptive survey research design, which is widely used for obtaining factual information and measuring opinions, attitudes, and awareness levels of a particular population. This design was chosen because it enables the researcher to collect both qualitative and quantitative data related to students' understanding of phishing in a systematic manner. The descriptive approach allowed for the identification of patterns, trends, and relationships among variables such as internet usage, awareness of phishing techniques, and adoption of cyber safety practices. The study ensured that primary data was gathered directly from the respondents, providing a reliable basis for analysis and interpretation by using a survey method,

Sample and Population:

The population of the study comprised school and college students from Aurangabad city, representing a mix of urban and semi-urban backgrounds. A total sample of 100 students was selected, ensuring representation from different educational levels, genders, and age groups to obtain a balanced understanding of phishing awareness. The respondents were chosen through a simple random sampling technique, which provided each student an equal chance of participation and minimized sampling bias. This method helped achieve diversity in academic background, thereby strengthening the generalizability of the findings within the Aurangabad student community.

Instrument:

Data was collected using a structured questionnaire designed specifically for this study. The questionnaire consisted of four carefully organized sections to capture comprehensive information:

- Section A: Demographics – collected basic details such as age, gender, educational level, and institution type.

- Section B: Internet Usage – examined frequency of internet access, preferred online platforms, and primary purposes of internet use.

- Section C: Awareness of Phishing – assessed students' familiarity with phishing concepts, ability to identify phishing attempts, and past experiences with suspicious emails or links.
- Section D: Cyber Safety Practices – focused on preventive measures adopted by students, including password management, use of antivirus software, and knowledge of reporting mechanisms.

The questionnaire was pre-tested with a small group of students to ensure clarity, relevance, and reliability before full deployment. (The final questionnaire is attached in Appendix A.)

Data Collection and Analysis:

using descriptive statistics, including percentages, mean scores, and cross-tabulations, to highlight relationships between demographic factors and phishing awareness. Visual tools such as bar charts, pie charts, and frequency tables were employed to present findings in an easy-to-understand format. This multi-step analysis provided a clear picture of students' awareness levels, internet habits, and cyber safety behaviours, forming the foundation for meaningful interpretation and discussion of results.

Data Analysis and Findings:

Awareness Levels

Awareness Question	% Yes	% No
Heard of phishing	42%	58%
Clicked on suspicious link	63%	37%
Use two-factor authentication	28%	72%
Attended cyber safety workshop	19%	81%

Interpretation: More than half of the respondents (58%) had never heard of phishing. A significant 63% admitted to clicking on suspicious links, reflecting high vulnerability.

Table 1: Internet Usage Patterns of Students in Aurangabad

Category	Findings
Daily Internet Users	**87% of respondents**
Most Used Device	**Smartphone – 79%**
Common Online Activities	**Social Media – 65%** **Online Classes – 52%** **Gaming – 38%** **Email – 22%**

Table 1 presents the internet usage patterns of students surveyed in Aurangabad. A significant majority (87%) reported accessing the internet on a daily basis, indicating high digital engagement. Smartphones emerged as the dominant device for connectivity, used by 79% of respondents, reflecting the growing dependence on mobile technology. Among online activities, social media (65%) ranked highest, followed by online classes (52%), showing the dual role of the internet in entertainment and education. Gaming (38%) and email usage (22%) were less frequent, highlighting that academic and social interactions remain the primary drivers of student internet use. Heavy reliance on smartphones and social media increases susceptibility to phishing via links and messages.

Cyber Safety Practices:

Table 2: Cyber Safety Practices of Students in Aurangabad:

Cyber Safety Practice	Percentage of Respondents
Use of Two-Factor Authentication	28%
Regular Password Updates	34%
Attendance in Cyber Safety Workshop	19%

Table 2 highlights the adoption of key cyber safety practices among students in Aurangabad. The findings reveal **low engagement in essential security measures**, with only **28%** of students using two-factor authentication to protect their accounts. Regular password updates were reported by **34%**, indicating moderate but insufficient attention to password hygiene. Alarmingly, just **19%** of respondents had attended any cyber safety workshop, underscoring the urgent need for structured awareness programs and practical training to strengthen students' digital security habits. Students show limited adoption of preventive practices, reflecting a gap in awareness and training.

Findings of the Study:

The findings reveal a concerning lack of phishing awareness among students in Aurangabad. Students struggle to identify phishing attempts. This aligns with global patterns where younger users, though digitally active, lack cybersecurity literacy.

The low adoption of protective measures such as two-factor authentication and password updates further compounds risks. Educational institutions play a vital role in bridging this gap. Workshops, awareness drives, and curriculum integration of cyber safety are necessary. Cross-tabulation indicates that higher-grade students showed slightly better awareness than school students, but overall knowledge remained insufficient.

Recommendations:

The study concludes that phishing awareness among students in Aurangabad is inadequate, leaving them vulnerable to cyber threats.

1. **Cyber Safety Education:** Schools and colleges should integrate cybersecurity topics into curricula.
2. **Workshops & Seminars:** Regular awareness sessions to demonstrate phishing attempts.
3. **Digital Campaigns:** Use of social media and college portals to spread safety tips.
4. **Practical Training:** Encourage students to practice safe browsing and reporting suspicious messages.
5. **Policy Support:** Educational institutions must collaborate with cybersecurity experts to protect students.

Conclusion:

The present study on *Awareness of Phishing Among Students: A Survey-Based Study on Cyber Threats (Special Reference to Aurangabad)* reveals a significant gap between students' increasing internet usage and their preparedness to counter cyber threats. With 87% accessing the internet daily and 79% relying primarily on smartphones, the majority of respondents demonstrated limited understanding of phishing and inadequate adoption of protective measures. Only 42% of students had even heard of phishing, while 63% admitted to having clicked on suspicious links, highlighting a high level of vulnerability. Furthermore, key preventive practices such as two-factor authentication (28%), regular password updates (34%), and participation in cyber safety workshops (19%) remain alarmingly low. These findings are consistent with earlier studies (Gupta & Jain, 2020; Chakraborty, 2021; Rao & Sharma, 2022) that underscore the growing threat of phishing in India and the particular susceptibility of students due to low cybersecurity literacy. The study demonstrates that while digital penetration in Aurangabad is extensive, awareness of phishing remains superficial and fragmented. Cross-tabulation indicates that higher-grade students showed slightly better awareness than school students, but overall knowledge and protective behaviour were insufficient across all categories.

To address this critical gap, educational institutions must take proactive measures to build a culture of cybersecurity awareness. Integrating cyber safety education into school and college curricula, conducting regular workshops and seminars, and promoting practical training sessions significantly improve students' ability to recognize and respond to phishing attempts. Digital campaigns through social media and institutional portals further reinforce safe online practices. The research highlights an urgent need for targeted and sustained interventions to equip students with the knowledge and skills necessary to navigate the digital world securely. Schools and colleges in Aurangabad and by extension, across India plays a pivotal role in reducing phishing-related risks and safeguarding the next generation of internet users by fostering digital literacy and responsible internet behaviour,

References:

- Gupta, R., & Jain, S. (2020). *Phishing trends and cyber fraud in Indian metropolitan cities.* Journal of Cybersecurity Studies, 8(2), 45–58.

- Chakraborty, P. (2021). *Youth vulnerability to phishing attacks in India: An empirical analysis.* Indian Journal of Information Security, 12(1), 33–49.

- Rao, M., & Sharma, K. (2022). *Impact of cybersecurity awareness programs on phishing susceptibility among students.* International Journal of Digital Safety, 14(3), 102–115.

- Kumar, A., & Patel, V. (2020). *Phishing awareness and prevention strategies in educational institutions.* Asian Journal of Cyber Research, 5(4), 77–89.