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 6, October 2026
Impact Factor: 8.2

Assessing Phishing Detection Ability and Cybersecurity Awareness Among College Students: A Review

Prof. Dr. Pawar Santosh Baraku, Prof. Punam Popat Deshmukh, Atharva Vilas Gawali
Vidya Niketan Institute of Management & Computer Application, Bota

Abstract: *Phishing remains one of the most common and damaging cyber threats, targeting users through deceptive emails, websites, messages, and social media content. College students are especially relevant as a study group because they actively use digital platforms for academics, communication, banking, shopping, and entertainment, yet they may not always possess strong cybersecurity habits. This review examines the phishing detection ability and cybersecurity awareness among college students, focusing on the factors that influence awareness, common weaknesses in identifying phishing attempts, and the role of education in improving digital safety. The review highlights that while students often show moderate familiarity with cyber threats, their practical ability to detect phishing messages is frequently limited by urgency, trust in familiar-looking messages, and lack of formal training. The paper also discusses the need for continuous awareness programs, simulation-based learning, and security-focused curriculum integration to strengthen students' cyber resilience*

Keywords: Phishing, cybersecurity awareness, college students, online safety, cyber education, digital literacy

I. INTRODUCTION

The rapid growth of digital technology has made college students heavily dependent on the internet for learning and daily activities. Along with the benefits of connectivity, however, comes exposure to cyber risks such as phishing, identity theft, account compromise, and social engineering attacks. Phishing is a technique in which attackers impersonate trusted institutions or individuals to trick users into revealing sensitive information such as passwords, banking details, or personal data.

College students are attractive targets because they frequently access email, social media, e-learning platforms, and online payment systems. Many students also tend to multitask, respond quickly to notifications, and trust familiar digital interfaces. These habits can make them vulnerable to deceptive cyber messages. Therefore, assessing phishing detection ability and cybersecurity awareness among college students is important for understanding how well this group can protect itself online.

II. PHISHING DETECTION ABILITY

Phishing detection ability refers to the skill of recognizing suspicious messages, websites, links, attachments, and requests that attempt to deceive users. A student with strong phishing detection ability should be able to identify warning signs such as:

- unfamiliar sender addresses,
- misspelled domain names,
- urgent or threatening language,
- requests for confidential information,

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 6, October 2026 Impact Factor: 8.2

• unexpected attachments or login prompts,
• poor grammar or formatting inconsistencies.

In practice, many students rely on surface-level clues rather than systematically checking message authenticity. Some are able to detect obvious phishing attempts, but more advanced attacks, such as spear phishing or cloned websites, can bypass casual inspection. Attackers often use convincing logos, familiar branding, and emotional triggers such as fear, urgency, or reward to manipulate victims. This means that phishing detection is not only a technical issue but also a behavioral one.

III. CYBERSECURITY AWARENESS AMONG COLLEGE STUDENTS

Cybersecurity awareness includes knowledge of online threats, understanding safe digital practices, and the ability to respond appropriately to suspicious activity. Among college students, awareness levels vary widely. Some students are familiar with basic concepts such as strong passwords, two-factor authentication, and safe browsing.

Others may have limited understanding of social engineering, phishing, malware, or account security.

A recurring theme in research on student awareness is the gap between theoretical knowledge and actual behavior. Students may know that phishing exists, but still click on suspicious links due to curiosity, time pressure, distraction, or trust in what appears to be an official message. This shows that awareness alone does not always lead to safe behavior. Practical experience, repeated training, and reinforcement are necessary to improve decision-making.

IV. FACTORS AFFECTING PHISHING DETECTION AND AWARENESS

Several factors influence how well college students can detect phishing and practice cybersecurity:

4.1 Digital Literacy

Students with stronger computer and internet literacy usually perform better in identifying suspicious activity. However, digital literacy does not automatically mean security literacy. A student may be skilled in using apps and platforms but still fail to recognize fraud indicators.

4.2 Prior Security Training

Students who have received formal cybersecurity training are generally more cautious. Training helps them notice suspicious URLs, verify sender identities, and report threats. Lack of training often results in weak threat recognition.

4.3 User Behavior and Psychology

Phishing attacks exploit human emotions such as fear, urgency, excitement, and trust. College students may respond quickly to messages about scholarships, grades, account verification, internships, or prizes. Psychological manipulation is one of the biggest reasons phishing remains effective.

4.4 Frequency of Internet Use

Students who spend more time online are exposed to more opportunities for phishing attempts. Heavy use of email, online learning systems, and social platforms increases risk unless safety habits are strong.

4.5 Device and Platform Usage

Mobile users may be more vulnerable because smaller screens make it harder to inspect URLs and sender details carefully. Messaging apps and mobile notifications also encourage quick responses without verification.

V. COMMON WEAKNESSES OBSERVED

Studies and campus observations often show that college students struggle with the following:

• clicking links without checking the source,
• trusting messages that appear to come from university offices,
• overlooking spelling errors in URLs,
• using the same password across multiple accounts,
• not enabling two-factor authentication,
• ignoring security warnings from browsers or email systems,

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 6, October 2026
Impact Factor: 8.2

• failing to report suspicious messages.

These weaknesses suggest that phishing awareness is not just about knowing the definition of phishing, but about developing consistent protective behavior.

VI. IMPORTANCE OF AWARENESS PROGRAMS

Awareness programs are one of the most effective ways to improve phishing detection among students. These programs should not be limited to one-time lectures. Instead, they should include:

• interactive workshops,
• real phishing email examples,
• simulated phishing campaigns,
• short awareness videos,
• quizzes and practical exercises,
• orientation sessions for new students.

Simulation-based training is especially useful because it allows students to practice identifying suspicious messages in a controlled environment. Feedback after simulations helps students learn from mistakes and improve future responses.

VII. ROLE OF COLLEGES AND INSTITUTIONS

Educational institutions play a major role in strengthening cybersecurity awareness. Colleges should:

• include cybersecurity topics in student orientation,
• promote safe use of campus email and portals,
• train students to verify official communications,
• encourage strong password and authentication practices,
• establish clear reporting channels for phishing incidents,
• conduct regular awareness campaigns.

Since students frequently interact with academic systems, colleges must also ensure that official messages are easy to verify. Using consistent domain names, authentication markers, and awareness notices can reduce confusion and help students distinguish real communications from fake ones.

VIII. RESEARCH GAPS

Although many studies discuss phishing awareness, there are still important gaps. More research is needed on:

• differences in awareness between disciplines such as engineering, arts, and business,
• the role of gender, year of study, and digital experience,
• effectiveness of training over time,
• mobile-based phishing risks among students,
• comparison between self-reported awareness and actual phishing detection performance.

Future studies should combine surveys, experiments, and phishing simulations to measure awareness more accurately.

IX. CONCLUSION

Assessing phishing detection ability and cybersecurity awareness among college students is essential in today's digital environment. College students are active internet users, but their ability to detect phishing attempts varies depending on training, experience, digital literacy, and behavior. Although many students understand the basic idea of phishing, they are often vulnerable to realistic and socially engineered attacks. Continuous education, practical simulations, and institutional support are necessary to improve their cybersecurity awareness. Strengthening these skills will help students protect their personal information, academic accounts, and online identity in an increasingly risky digital world.

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/568

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 6, October 2026
Impact Factor: 8.2

REFERENCES

1. Purkait, S. (2013). Assessing Anti-Phishing Awareness among Undergraduate Students in India. International Journal of Applied Research on Information Technology and Computing, 4(1), 26–41.
2. Okokpujie, K., Kennedy, C. G., Nnodu, K., & Noma-Osaghae, E. (2023). Cybersecurity Awareness: Investigating Students' Susceptibility to Phishing Attacks. International Journal of Sustainable Development and Planning, 18(1), 255–263.
3. Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human Factors in Phishing Attacks: A Systematic Literature Review. ACM Computing Surveys, 54(8).
4. Sumner, A., Yuan, X., Anwar, M., & McBride, M. (2022). Examining Factors Impacting the Effectiveness of Anti-Phishing Trainings. Journal of Computer Information Systems, 62(5), 975–997.