Medicon Engineering Themes
Volume 9 Issue 1 July 2025
Article Type: Short Communication
ISSN: 2834-7218

Cybersecurity Awareness in Undergraduate Engineering Education: A Critical Imperative in the Digital Age

Mohit Tiwari*

Assistant Professor, Department of Computer Science and Engineering, Bharati Vidyapeeth's College of Engineering, Delhi

***Corresponding Author:** Mohit Tiwari, Assistant Professor, Department of Computer Science and Engineering, Bharati Vidyapeeth's College of Engineering, Delhi.

Received: June 27, 2025; **Published:** July 25, 2025

Abstract

In the rapidly evolving digital ecosystem, cybersecurity is no longer a specialist's concern—it is a fundamental literacy. This short communication underscores the pressing need to embed cybersecurity awareness into the undergraduate engineering curriculum across disciplines. Drawing from academic and industry observations, it outlines the key gaps, proposes integrative strategies, and calls for a pedagogical shift to prepare students for the realities of a hyperconnected world.

Keywords: Cybersecurity education; engineering curriculum; digital literacy; cyber awareness; interdisciplinary training, cyber hygiene

Main Text

The digital transformation of society has created a paradox: while our dependency on connected technologies has increased, so has our exposure to sophisticated cyber threats. From healthcare and finance to education and manufacturing, every sector today is intertwined with data networks and digital infrastructure. As a result, cybersecurity is no longer optional—it is foundational.

Yet, a critical gap persists in how cybersecurity is addressed in undergraduate engineering education in India. Despite the increasing cyber threats, many universities still treat cybersecurity as a specialization course limited to computer science students. This narrow focus excludes a large section of engineering graduates—civil, mechanical, electrical—who often end up working in digitized environments without basic cyber hygiene knowledge.

In my experience as a faculty member and cybersecurity trainer, I have frequently observed students with exceptional technical potential, yet alarmingly unaware of elementary practices such as recognizing phishing attempts, using secure passwords, or understanding data privacy regulations like India's DPDP Act. This knowledge gap is not just academic—it is a real-world vulnerability.

What is needed is not merely the addition of elective courses, but a paradigm shift that normalizes cybersecurity literacy. Just as engineers are expected to know ethics or environmental impact, cybersecurity awareness must become a cross-disciplinary requirement.

Some practical steps to implement this include

Micro-Modules Across Semesters

Short modules or workshops that introduce core cybersecurity concepts such as network safety, data integrity, and endpoint security should be delivered across all years of study. These should be scenario-based, using Indian case studies such as the Cosmos Bank SWIFT breach or the AIIMS ransomware attack to illustrate consequences.

Gamified Learning

Interactive Capture-the-Flag (CTF) exercises and simulated cyberattack response drills can create engaging learning environments. These can be conducted across departments, fostering collaborative and interdisciplinary problem-solving.

Integration with Capstone Projects

Final-year projects across all branches should include an optional cybersecurity audit or compliance check section. This will instill a habit of thinking about vulnerabilities even in non-IT domains.

Faculty Development

Teachers across engineering departments must be sensitized to cybersecurity trends. Faculty development programs can play a pivotal role in cascading this awareness to students.

Institutional Support

Colleges must collaborate with national initiatives like Cyber Surakshit Bharat, CERT-In, or NCIIPC to bring authentic content, expert talks, and real-life breach analyses to campus.

India is at a juncture where it cannot afford to produce engineers who are technically sound but digitally unaware. The next generation of professionals will be operating in industries where cybersecurity is not a department—it is a part of everyday decision-making. As educators, we must rise to this responsibility.

In conclusion, cybersecurity awareness in undergraduate engineering must be seen as an investment, not an afterthought. It is time that academic institutions treat digital safety with the same seriousness as structural safety or industrial standards. The students we teach today are the gatekeepers of tomorrow's digital India.

Acknowledgement

The author acknowledges the students, colleagues, and cyber training partners whose inputs and real-world feedback have helped shape the ideas in this communication.

Volume 9 Issue 1 July 2025