SMT. DEVKIBA MOHANSINHJI CHAUHAN COLLEGE OF COMMERCE AND SCIENCE

"CYBERSECURITY AWARENESS SURVEY AMONG STUDENTS"

Submitted By :

1.Prashant Kumar Das [53014]
2.Sanjeev Kushwaha [53024]
3.Pandey Shubham [53025]
4.Juned Shaikh [53027]
5.Pramod Lehva [53003]

Submitted To:

[Prof. Savita Lambhe]
Department of Computer Science

Cybersecurity Awareness Survey Among Students: Understanding the Risks and Realities

This presentation explores the critical findings of a survey conducted to assess the cybersecurity knowledge, attitudes, and practices of university students. As digital natives, students face an evolving landscape of online threats, making robust awareness and practical skills essential for protecting their personal and academic lives.

> A proactive approach to digital safety starts with understanding where the vulnerabilities lie.


SCHOOL BUS
GPS Map Camera
Silvassa, Dadra And Nagar Haveli And Daman And Diu, India
7298+73q Flyover Crossing, Sanjibhai Rupjibhai Delkar Marg, Bavisa Faliya, Silvassa, Dadra And Nagar Haveli And Daman And Diu 396230, India
Lat 20.26921° Long 73.014952°
Friday, 07/11/2025 12:57 PM GMT +05:30
Google


GPS Map Camera
Silvassa, Dadra And Nagar Haveli And Daman And Diu, India
7298+73q Flyover Crossing, Sanjibhai Rupjibhai Delkar Marg, Bavisa Faliya, Silvassa, Dadra And Nagar Haveli And Daman And Diu 396230, India
Lat 20.26921° Long 73.014953°
Friday, 07/11/2025 12:57 PM GMT +05:30
Google

Why Cybersecurity Awareness Matters for Students

High Exposure to Digital Threats

Data from 2022 indicates that over **55% of internet users** have encountered some form of cybersecurity issue. Students, with their constant online activity across multiple devices and platforms, represent a highly exposed demographic.

Prime Targets for Social Engineering

Students aged 18-24 are frequent targets for sophisticated social engineering scams, including phishing, online financial fraud, and identity theft. The focus on academic pursuits often means vigilance is lower, making them susceptible to time-sensitive, coercive scam messages.

Consequences of Vulnerability

A lack of foundational awareness and protective measures directly leads to severe consequences, including significant financial loss, critical privacy breaches, and long-term damage to their academic and professional reputation.

Digital fluency does not automatically equate to digital security. While students are adept at using technology, many overlook basic security hygiene, which attackers exploit relentlessly.

The Human Factor: Students as the Weakest Link

Behavioural Vulnerabilities

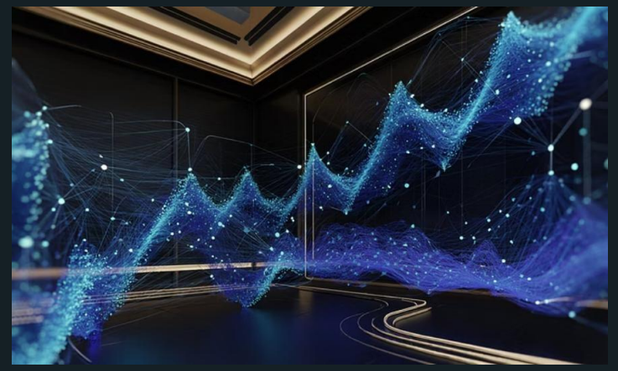
Despite advanced technical defences implemented by institutions, human behaviour consistently remains the most critical vulnerability in any security chain. Attackers understand that exploiting human error is often easier than bypassing firewalls.

- **Weak Passwords:** Reusing simple or predictable passwords across services.
- **Credential Sharing:** Sharing login details with peers or for shared services.
- **Link Clicking:** A high propensity for clicking on unknown or suspicious links, particularly within email or social media messages.

A prevalent example involves university students falling victim to highly believable online loan and part-time job scams, resulting in the theft of personal information and, in some cases, large sums of money.

Survey Snapshot: Awareness Levels Among Students

Our study collected data from a sample of 570 students, carefully selected from both technically focused (Computer Science) and non-technical (Media Studies) disciplines to provide a balanced view of cybersecurity understanding across the student body.



Key Assessment Areas

The survey rigorously assessed students across four critical dimensions of digital security:

1. Fundamental cybersecurity knowledge and terminology.
2. Personal password management hygiene and practices.
3. Understanding of online privacy settings and data sharing risks.
4. Scepticism and trust levels when encountering unknown sources or requests online.

Discipline-Specific Gaps

The findings highlighted significant, concerning gaps, particularly when comparing the two groups. While Computer Science students generally demonstrated higher theoretical knowledge, students from Media Studies (and implicitly, other non-technical fields) displayed lower overall awareness and risk-averse behaviour. This confirms that basic cybersecurity skills are not uniformly distributed and require targeted intervention.

Password Management: A Critical Weakness

78%

Do not use unique passwords

A high percentage of surveyed students admitted to reusing the same password, or variations thereof, across multiple essential services, dramatically increasing their risk profile.

15%

Use Password Managers

Despite the widespread availability and clear security benefits of password managers, adoption remains low, suggesting either a lack of trust in the tools or a perception of inconvenience.

Poor password habits are a gateway to significant security compromises. If an attacker gains access to one account due to a data breach, the reuse of that password immediately puts all other connected accounts—including university systems, banking, and social media—at risk of compromise and data breach.

Effective password hygiene is not merely a technical step; it is a fundamental pillar of personal cybersecurity.

Privacy and Trust: Misplaced Confidence Online

Students often operate under a high level of misplaced confidence regarding their online presence, leading to significant privacy risks. Their digital lives are characterised by a frequent blending of personal and public spaces:

Social Media Oversharing

The pervasive use of social media results in excessive sharing of personal details, location data, and sensitive life events, all of which can be leveraged by social engineering attacks or identity thieves.

Verification Blind Spots

Many students demonstrate a critical lack of skills to verify the authenticity of communication sources (e.g., email senders, website URLs). This inability to spot fakes makes them easy prey for phishing and whaling attempts.

Dangerous Levels of Trust

A significant finding was the dangerously high level of trust placed in unknown or unverified online sources, especially if the communication mimics an official authority figure (e.g., a university administrator or a government body).

Educational Gaps and Opportunities

The survey highlights a systemic failure in integrating essential cybersecurity education into the core academic curriculum.

1

Infrequent or Absent Training

Cybersecurity training programmes are often either non-existent, optional, or relegated to a single, brief introductory session during induction. This fails to account for the continuous and evolving nature of cyber risks.

2

Informal Learning Channels

When students do learn about cyber risks, it is primarily through informal channels—peers, social media, or, most worryingly, negative personal experience after an incident occurs. This reactive learning model is costly and ineffective.

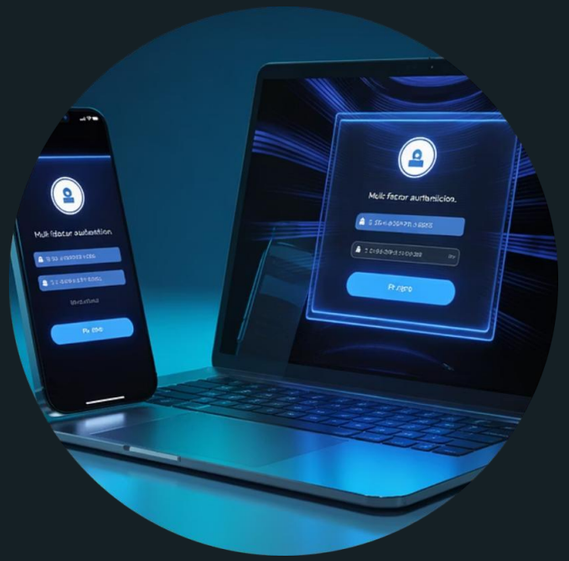
3

The Opportunity for Structure

Implementing structured, mandatory, and regular awareness programmes—tailored to specific student behaviours—can dramatically transform the overall security posture of an institution and significantly reduce student vulnerability.

Best Practices to Boost Student Cybersecurity Awareness

A multi-faceted approach combining technological enforcement with educational engagement is necessary to achieve meaningful behavioural change.



Enforce MFA Adoption

Mandate the use of Multi-Factor Authentication (MFA) across all critical student accounts (email, LMS, library systems) to provide a vital layer of defence against compromised credentials.

Promote Password Managers

Actively promote and possibly subsidise professional password manager tools, coupling this with education on the necessity of unique and complex passwords.

Interactive Workshops

Move beyond passive lectures. Conduct frequent, engaging workshops, including simulated phishing exercises, to allow students to practise identifying threats in a safe environment.

Cultivate Vigilance

Foster a continuous culture of vigilance and critical thinking. Teach students to pause, question, and verify online information and requests, treating scepticism as a core digital life skill.

Real-World Impact: Reducing Cyber Threats Through Awareness

Investment in robust cybersecurity education yields quantifiable benefits, moving institutions from a reactive security model to a proactive, preventative one.

Fewer Incidents

Universities that commit resources to comprehensive, continuous cybersecurity awareness and education programmes report a marked decrease in the number and severity of security incidents, including account compromises and system breaches.

Student Advocacy

Students who are properly empowered with knowledge become positive advocates, extending safer digital behaviour to their peers, families, and future workplaces, creating a wider security ecosystem.

Protection and Savings

Proactive awareness directly reduces financial losses associated with fraud and incident response costs, simultaneously protecting the sensitive personal and academic data essential to students' lives.

Conclusion: Building a Cyber-Resilient Student Community

The digital world presents a constantly shifting battleground of cyber threats. Our survey highlights that awareness is not a luxury; it is the fundamental, non-negotiable first line of defence against modern attacks.

The Path Forward: Continuous and Tailored Education

- Education must be **continuous**, moving beyond one-off training sessions to integrated, timely, and updated modules throughout the student journey.
- Training must be **engaging** and interactive, utilising real-world scenarios and gamification to capture attention and improve retention.
- Programmes must be **tailored** to specific student cohorts (e.g., technical vs. non-technical) and their unique risk profiles.

By embracing these principles, we can transform students from inherently vulnerable targets into informed, critical thinkers and robust **cybersecurity champions**.

> "In the digital age, cybersecurity awareness is as crucial as academic literacy. We must equip students with the skills to secure their future."

Thank you. Stay vigilant, stay secure.

“Your Security Is Our Priority”

Cyber threats evolve — so should we.Thank you for being part of the conversation on building a safer digital future.