

Cyber Awareness Program by TI at DAV Public School

Date: 29.09.2025

Venue: DAV Public School, [Insert Location]

Organizer: Town Inspector

Participants: Students (Classes _6__ to _12__), Teachers, Staff

1. Objectives

The program aimed to:

- Increase awareness among students about cyber threats (e.g. phishing, cyberbullying, identity theft).
 - Educate them on safe online behaviour, including social media etiquette, privacy protection, and secure password practices.
 - Provide guidance on how to respond to cyber incidents (reporting mechanisms etc.).
 - Empower teachers and staff to support students in maintaining cyber safety.
-

2. Program Contents

The session(s) included:

- **Introduction to Cyber Threats:** Types of cybercrimes relevant to students; real-life examples.
 - **Safe Online Practices:** How to recognize phishing, safe browsing, avoiding suspicious links, secure use of apps and downloads.
 - **Privacy and Social Media:** Settings, digital footprint, responsible use of social platforms.
 - **Security Measures:** Strong passwords, two-factor authentication (2FA), keeping software/applications up to date.
 - **Reporting and Support:** What to do if they or someone they know encounters cyber harassment or cybercrime; available resources / whom to contact.
 - **Interactive Activities:** Q&A, quizzes, maybe role-plays or demonstrations to reinforce learning.
-

3. Attendance & Participation

- Approximate number of students: [e.g. 200-300, or as appropriate].
 - Teachers and staff: [number].
 - Engagement: Students were actively involved—asking questions, sharing personal experiences, etc.
 - Many participants responded well to interactive components—quiz, demo etc.
-

4. Key Outcomes

Positive outcomes included:

- **Awareness raised:** Students reported having a better understanding of what constitutes cyber threats.
 - **Behavioral intent:** Commitments by students to adopt safer practices (e.g. not sharing passwords, being cautious with unknown links).
 - **Empowerment:** Teachers feel more equipped to guide students; staff are more informed about reporting channels.
 - **Increased confidence:** Students expressed feeling more confident in identifying online risks.
-

5. Challenges & Areas for Improvement

- Some students may still find technical terms difficult; simple, relatable language helps.
 - Limited time may restrict deeper discussion or more examples/case studies.
 - Need for follow-up sessions to reinforce learning.
 - Possibly more hands-on/practical demonstrations (e.g. safe settings changes, spotting fraud emails) could help retention.
-

6. Suggestions / Recommendations

- **Regular follow-ups:** Quarterly or half-yearly refreshers for students and staff.
- **Workshops for parents:** So that cyber safety becomes a shared home-school responsibility.
- **Integration into curriculum:** Include cyber safety topics in ICT / Computer classes.

- **Use peer-education:** Train some students as 'cyber ambassadors' who help spread awareness.
- **Continuous evaluation:** Use quizzes or surveys before & after the program to measure improvement in knowledge / behaviour.

7. Conclusion

The Cyber Awareness Program by TI at DAV Public School was successful in making students and staff more aware of cyber risks and safety practices. While there are areas to strengthen (deeper hands-on learning, ongoing reinforcement), the event has laid a strong foundation. With sustained efforts, this can contribute significantly toward creating a safer online environment for the school community.

