

1. Introduction to Digital Footprint (Advanced)

- What is a Digital Footprint
- How Online Actions Leave a Permanent Record (e.g., comments, posts, images)
- Consequences of a Negative Digital Footprint in the Future

2. Privacy Settings on Social Media

- Adjusting Privacy Settings on Social Media Platforms (e.g., Instagram, TikTok, etc.)
- Managing Who Can View Your Posts, Comments, and Personal Information
- Being Cautious While Adding Friends and Avoiding Stranger Requests

3. Understanding Online Identity

- Online vs. Real-Life Identity Presentation (e.g., fake identities, filtered images)
- Risks of Interacting with Fake Profiles and Catfishing
- How to Recognize Fake Identities and Stay Cautious
- Different forms of cyberbullying (harassment, exclusion, trolling)
- Effects of Cyberbullying on Mental Health and Self-Esteem
- Legal Consequences of Cyberbullying and How to Report It

4. Cyberbullying (Intermediate to Advanced)

5. Phishing and Scams (Advanced)

- How Phishing Scams Happen (via emails, messages, and fake websites)
- Identifying Phishing Attempts and Taking Immediate Protective Actions

6. Social CSineering Attacks (Introduction)

- What is Social CSineering and How It Manipulates People
- Common Examples of Social CSineering Attacks
- Ways to Avoid Falling for Social CSineering Tricks

7. Password Security (Advanced)

- How to create strong passwords using passphrases
- Importance of Using Unique Passwords and Enabling Two-Factor Authentication (2FA)

8. Cybercrime Awareness

- Introduction to Cybercrime (including hacking, identity theft, and online fraud)
- Ways Students Can Protect Themselves and Report Cybercrime

9. Online Safety for Gaming Platforms

- Tips for Staying Safe While Gaming Online (e.g., avoid chatting with strangers, don't share personal information)
- Recognizing and avoiding in-game scams.

10. Recognizing Fake News (Advanced)

- Introduction to fake news and misinformation.
- How to verify news sources using fact-checking tools.

11. Safe Online Shopping (Introduction)

- Safe online shopping practices (secure payment methods, reading reviews).
- Protecting Personal Information While Shopping Online

12. Risks of Public Wi-Fi

- How public Wi-Fi can expose personal data
- Steps to stay safe while using public Wi-Fi.

13. Safe Use of Email

- Managing emails safely (Avoid opening suspicious attachments or clicking unknown links)
- Filtering Spam and Reporting Unsafe Emails (Use email filters, mark suspicious emails as spam, and report phishing attempts)

14. Social Media Challenges and Trends

- Dangers of participating in viral social media challenges.
- Evaluating risks and avoiding peer pressure.

15. Understanding Misinformation and Its Impact

- How Misinformation Spreads Online and Affects Society
- Importance of Fact-Checking to Prevent the Spread of False News

16. Parental Controls and Online Safety

- Importance of using parental controls on devices.
- How to Set Up Basic Parental Controls on Browsers, Apps, and Devices

17. Data Privacy (Introduction)

- What Personal Data Is and How It Is Collected Online
- How Companies Use Personal Data and Why Privacy Matters

18. Cyber Laws and Reporting

- Basic Understanding of Cyber Laws That Protect Students

- How to Report Cybercrime and the Consequences of Committing One

