

## 1. Introduction to the Internet (Advanced)

- Deeper understanding of how the internet works (servers, browsers, and websites)
- How search engines find information
- Basic concepts of keywords and algorithms.

## 2. Safe Browsing Techniques

- Using child-safe search engines and enabling safe search filters on regular search engines.
- How can Safe Search filters be enabled on regular search engines to ensure safe browsing?
- Understanding URL structures and how to identify secure websites (https vs. http).

## 3. Phishing, Email Masquerading, and Scams

- An Overview of Phishing and Email Masquerading Techniques and Their Functioning
- How to spot phishing attempts (suspicious URLs, misspellings, unusual requests for personal info).
- Steps to take if you receive phishing emails or messages.

## 4. Cyberbullying (Intermediate)

- Understanding the different forms of cyberbullying (e.g., exclusion, harassment, flaming).
- Emotional and social impact of cyberbullying.
- Steps to take if you experience or witness cyberbullying (blocking/reporting features).

## 5. Introduction to Cybercrime

- Basic understanding of cybercrime (hacking, identity theft, online fraud)
- How to report suspicious online activities.

## 6. Creating Strong and Secure Passwords

- How to create secure passwords using letters, numbers, and special characters.
- Importance of not reusing passwords across different websites.
- Introduction to password managers and their benefits.

## 7. Recognizing Inappropriate Content

- What constitutes inappropriate content (e.g., violence, explicit content, hate speech).
- How to respond when encountering inappropriate content (reporting, seeking parental guidance).

## 8. Indian Government Platforms for Digital Safety

- i4c (Indian Cyber Crime Coordination Centre): Government platform for raising cyber crime awareness.
- Cybercrime Reporting Portal: Reporting cyber crimes and learning about digital safety.
- CEIR (Central Equipment Identity Register): Track and block lost or stolen devices.
- Sancharsathi: Platform for managing SIM cards and telecom safety.

## 9. Understanding Social Media (Introduction)

- What is social media, and why students should be cautious.
- Age restrictions and privacy concerns on social platforms
- Recognizing fake accounts and avoiding strangers online.

## 10. Privacy Settings on Devices and Apps

- How to set basic privacy settings on devices, apps, and browsers
- Importance of controlling permissions (e.g., camera, microphone, location tracking).

## 11. Safe Downloads and Apps

- Identifying safe apps and software from trusted sources.
- Risks of downloading unknown apps or files from pop-up ads or suspicious emails
- Checking reviews and permissions before downloading apps.

## 12. Digital Footprint (Introduction)

- Understanding that online actions leave a permanent trace
- Thinking before posting or sharing personal details or images online.

## 13. Online Etiquette and Digital Citizenship

- Valuing Diverse Opinions and Encouraging Online Kindness
- Importance of asking permission before sharing someone else's content or pictures
- Practicing positive digital citizenship.

## 14. Parental Supervision and Online Safety Rules

- Importance of parental controls and how they protect students online.
- Basic rules for staying safe online (e.g., not meeting strangers, avoiding risky behavior).

## 15. Online Game Safety (Advanced)

- Understanding risks like cyberbullying and in-game purchases
- Being Aware of Financial and Privacy Risks in In-Game Purchases
- How to set privacy settings in games and report inappropriate behavior
- Importance of balancing gaming with physical activity and limiting screen time.