

1. Understanding Cybersecurity Threats (Advanced)

- Introduction to Cybersecurity Threats (e.g., malware, ransomware, spyware)
- How Hackers Target Individuals and Organizations
- Preventive Measures to Stay Safe Online

2. Social Engineering Attacks

- Social Engineering Attacks Advanced understanding of social engineering (phishing, vishing, baiting) How attackers manipulate victims into sharing personal information. Real-life examples and prevention strategies.
- How Attackers Manipulate Victims to Reveal Personal Information
- Real-Life Examples of Social Engineering and Ways to Prevent Them

3. Data Privacy and Protection

- Understanding Personal Data and How It Is Collected Online
- How companies use data and why privacy is important.
- Steps to Protect Personal Data (e.g., disabling location tracking, controlling app permissions)

4. Cyber Ethics and Laws (Advanced)

- Overview of International and National Cyber Laws
- Ethical Responsibilities When Using the Internet (e.g., respecting intellectual property, privacy rights)
- How Cybercrimes Are Prosecuted and Reported

5. Advanced Phishing Techniques

- How Phishing Has Evolved (e.g., spear phishing, whale phishing)
- Recognizing Suspicious Emails, Websites, and Messages
- Immediate Steps to Take If Personal Data Is Compromised

6. Digital Identity and Impersonation

- How Online Identities Are Created and Manipulated
- Understanding the Risks of Impersonation and Catfishing
- Recognizing the Signs of Fake Profiles and How to Report Them

7. Protecting Personal Devices

- Importance of Securing Personal Devices (e.g., smartphones, laptops)
- Using Antivirus Software, Firewalls, and Regular Updates to Protect Devices
- Using Antivirus Software, Firewalls, and Regular Updates to Protect Devices

8. Digital Footprint Management

- How to actively manage and curate a positive digital footprint.
- Tools to monitor what is shared about you online.
- Long-Term Consequences of Irresponsible Online Behavior

9. Social Media Responsibility

- Exploring how social media affects mental health, personal privacy, and digital reputation.
- Interpreting social media terms of service, user agreements, and platform policies.
- Managing audience visibility and CSagement settings to protect online interactions

10. Cyberbullying and Online Harassment

- Identifying various forms of online harassment (e.g., trolling, doxxing, group targeting).
- Understanding the legal consequences associated with cyberbullying.
- How to support victims of cyberbullying and report incidents.

11. Protecting Financial Information

- Identifying secure and trusted online payment platforms.
- Detecting fraudulent financial schemes such as phishing and investment scams.
- Implementing best practices for safeguarding banking and financial credentials online.

12. Managing Digital Addiction

- Understanding the impact of excessive digital usage on mental and physical well-being.
- Identifying key signs of digital addiction, such as sleep disturbances and reduced concentration.
- Techniques for balancing online activities with offline life (e.g., digital detox, screen time tracking apps).

13. Identifying Fake News and Misinformation

- How to spot fake news and misleading information.
- Importance of fact-checking sources and using reliable platforms
- Understanding how misinformation spreads through social media and its impact.

14. Online Earning Scams

- Recognizing Fake Job Offers and Get-Rich-Quick Schemes (Identifying scams that promise high income with minimal effort.)
- Types of Online Earning Scams: From pyramid schemes to fraudulent freelance job postings.

- Protecting Personal and Financial Information: Avoid sharing sensitive data such as ID proofs, bank details, or passwords.
- Reporting and Avoiding Scams: How to report online scams and stay informed to avoid falling victim.

15. Cybersecurity Careers

- Introduction to career opportunities in cybersecurity.
- Key Skills and Certifications for Cybersecurity Professionals
- Importance of Ethical Hacking and Penetration Testing in today's world.

16. OTT Platforms

- Risks of Over-the-Top (OTT) Platforms: How subscription-based streaming services (e.g., Netflix, Amazon Prime) collect and use user data.
- Managing Privacy on OTT Platforms: Securing accounts, setting up parental controls, and understanding how viewing behavior is tracked.
- Pirated Content and Legal Consequences: The risks of streaming illegal content and how to avoid unsafe websites.

17. School Email

- Using School Email Safely: Best practices for managing, organizing, and securing your school email account.
- Recognizing Phishing Attempts Through School Emails: How to identify and avoid suspicious links or attachments in emails
- Password Protection and Two-Factor Authentication (2FA): Creating strong passwords and enabling 2FA to enhance account security.

18. Participation in Online Exams

- Online Exam Security: Ensuring your system is secure during exams, using approved tools, and avoiding cheating
- Privacy and Proctoring Tools: Understanding how online exams are monitored and your rights regarding privacy.
- Preparing Your Device for Online Exams: Steps to secure your device and connection, including antivirus and updates before exams.