

CYBER SECURITY BOOTCAMP

Goal: Develop cyber awareness, online safety skills, and ethical: hacking fundamentals, and an understanding of how AI can be used in cyber security. This matches the site's description of the bootcamp as covering online safety, ethical hacking, and AI: powered security concepts.

Module 1: Introduction to Cyber Security

- What is cybersecurity?
- Why cybersecurity matters
- Types of cyber threats
- Cyber criminals and attackers
- Ethical hackers
- Cybersecurity careers

Activity: Identify common cyber threats.

Module 2: Digital Safety

- Strong passwords
- Password managers
- Multi:factor authentication
- Safe browsing
- Software updates
- Device security
- Public Wi:Fi safety

Activity: Create a personal Cyber Safety Checklist.

Module 3: Phishing & Social Engineering

- What is phishing?
- Email phishing
- SMS scams
- Fake websites
- Social engineering
- Impersonation
- Recognizing suspicious links and messages

Activity: Phishing Detection Challenge.

Module 4: Networks & Internet Security

- What is a computer network?
- Internet basics
- IP addresses
- DNS
- Routers
- HTTP vs HTTPS
- Firewalls
- Secure networks

Activity: Understand how a website request travels across the internet.

Module 5: Encryption & Privacy

- What is encryption?
- Encryption vs hashing
- Why HTTPS is important
- Public and private keys
- Digital signatures
- Data privacy

Activity: Simple encryption/decryption exercise.

Module 6: Web & Application Security

- How websites work
- User authentication
- Common web vulnerabilities
- Input validation
- Secure coding principles
- Why software updates matter

Activity: Analyze intentionally vulnerable educational examples in a safe environment.

Module 7: Ethical Hacking Fundamentals

- What is ethical hacking?
- Hacker types
- Reconnaissance
- Vulnerability assessment
- Penetration testing concepts
- Rules of engagement
- Responsible disclosure

Important: All practical exercises should be performed only on authorized educational systems/labs.

Module 8: Malware & Cyber Attacks

- Viruses
- Worms
- Trojans
- Ransomware
- Spyware
- DDoS attacks
- Prevention and basic response

Activity: Build a Cyber Incident Response Plan.

Module 9: AI & Cyber security

- Introduction to AI in cyber security
- Threat detection
- Anomaly detection
- AI-assisted phishing detection
- Benefits and limitations of AI
- Deepfakes and AI-enabled scams
- Responsible use of AI

Activity: Evaluate examples of AI-generated scams.

Module 10: Cybersecurity Capstone

Students create:

- Cyber Safety Awareness Campaign
- Phishing Awareness Presentation
- Personal Security Checklist
- Cybersecurity Quiz
- Safe Network Design

Final Outcome: Students understand how to protect themselves online and understand the basic principles behind ethical cyber security.