

Cyber Security Training Program – Content Plan

Module 1: Welcome & Introduction (15 minutes)

- Why Cyber Security Matters
 - Current cyber threat landscape
 - Real-life cybercrime statistics
 - Icebreaker activity: "How safe are you online?"
-

Module 2: Latest Cyber Frauds (45 minutes)

- AI Voice Cloning Scam
- QR Code Fraud
- Phishing Emails & SMS
- OTP & Banking Scams
- Fake Job Offers
- Deepfake Videos
- Social Media Account Hacking
- Investment & Cryptocurrency Scams

Activity: Spot the Scam Challenge

Module 3: Password & Authentication Security (30 minutes)

- Strong Passwords
- Password Managers
- Multi-Factor Authentication (MFA/2FA)
- Common password mistakes

Hands-on: Create a strong password using a simple formula.

Module 4: Social Engineering (30 minutes)

- Psychology behind cyber attacks
- Urgency, fear, greed, and curiosity
- Real scam call examples
- How attackers manipulate victims

Activity: Role-play a scam call.

Module 5: Safe Internet Practices (30 minutes)

- Safe Browsing
 - Public Wi-Fi Risks
 - Safe Online Shopping
 - QR Code Safety
 - Mobile Security
 - App Permissions
-

Module 6: Email & Phishing Awareness (30 minutes)

- Identify fake emails
- Suspicious links
- Fake attachments
- Business Email Compromise (BEC)

Activity: Find 10 red flags in a phishing email.

Module 7: AI & Cyber Security (20 minutes)

- Deepfakes
 - AI-generated scams
 - Voice cloning
 - AI-powered phishing
 - Safe use of AI tools
-

Module 8: Digital Footprint & Social Media Safety (20 minutes)

- Privacy settings
 - Oversharing risks
 - Identity theft
 - Safe posting habits
-

Module 9: Incident Response (20 minutes)

What should you do if:

- Your phone is hacked?
- Your email is compromised?
- Your bank account is targeted?
- You receive a suspicious QR code?

- Your social media account is hacked?

Introduce the simple rule: **STOP → THINK → VERIFY → REPORT**

Module 10: Cyber Safety Toolkit (15 minutes)

Participants receive a checklist covering:

- Password checklist
 - 2FA checklist
 - Device update reminders
 - Backup strategy
 - Safe browsing habits
 - Emergency contact list
-

Interactive Activities Throughout the Session

- Scam or Safe? Quiz
 - QR Code Investigation
 - Password Strength Challenge
 - Phishing Email Hunt
 - Cyber Myth vs Fact
 - Cyber Security Kahoot Quiz
 - Case Study Discussions
-

Wrap-up & Q&A (15 minutes)

- Key takeaways
- Top 10 Cyber Safety Rules
- Questions and discussion
- Feedback

Learning Outcomes

By the end of the training, participants will be able to:

- Recognize common cyber threats.
- Detect phishing and social engineering attempts.
- Create and manage strong passwords.
- Use Multi-Factor Authentication effectively.
- Protect personal and organizational data.
- Respond confidently to common cyber incidents.
- Apply safe online practices in daily life.