Duration: As per the organization

CORPORATE TRAINING

Overview:

The comprehensive cyber security training program encompasses threat awareness, secure practices, incident response, and cultivating a security-oriented culture. Participants gain crucial skills and knowledge to mitigate risks, foster a vigilant mindset, and counter evolving cyber threats within organizational settings. With modules covering common threats, secure password management, incident reporting, and ongoing awareness, the curriculum equips employees to safeguard sensitive information, fortify defenses, and uphold cyber resilience across diverse operational landscapes.

What you'll learn

- ➢Recognize cyber threats and their impact.
- ➢Understand the importance of cyber security awareness.
- ➢Learn basic cyber security terminology.
- ➢Identify and prevent common cyber threats.
- ➢Implement best practices for security.

Benifits

- ➢**Hands-on practical:** Engage in real-world exercises to apply theoretical knowledge directly.
- ➢**Internship opportunity:** Gain practical experience through internships to enhance skills and build a professional network.
- ➢**Expert trainers:** Receive guidance and instruction from seasoned professionals with extensive experience in the field.
- ➢**Job assistance:** Access support and resources to secure employment opportunities aligned with acquired skills. and expertise.

You can reach us at:

www.cyberous.in
info@cyberous.in
cyberous_
cyberous

Course Outline:

Module 01: Introduction to Cyber Security

- Cyber threats overview
- Importance of awareness
- Basic terminology

Module 02: Understanding Common Cyber Threats

- Phishing: How it works
- Malware types and prevention
- Social engineering tactics

Module 03: Secure Password Management

- Strong password importance
- Best practices
- Introduction to password managers

Module 04: Email Security

- Recognizing suspicious emails
- Safe handling of attachments/links
- Reporting phishing attempts

Module 05: Safe Web Browsing Practices

- Identifying secure websites
- Risks of unsafe browsing
- Using HTTPS

Module 06: Data Protection and Privacy

- Understanding data classification
- Secure information handling
- Compliance with regulations

Module 07: Device Security

- Importance of updates
- Securing mobile devices
- Data encryption

Module 08: Social Media Security

- Risks of oversharing
- Privacy settings
- Avoiding social engineering

Module 09: Remote Work Security

- Securing remote setups
- Accessing corporate resources
- Risks of public Wi-Fi

Module 10: Incident Response and Reporting

- Reporting procedures
- Responding to breaches
- Timely reporting

Module 11: Cyber Security Policies and Compliance

- Corporate policies overview
- Employee responsibilities
- Consequences of non-compliance

Module 12: Cyber Security Culture

- Building security awareness
- Employee involvement
- Recognizing good practices

Module 13: Security Awareness Assessment

- Evaluating understanding
- Identifying improvement areas
- Feedback and reinforcement

Module 14: Ongoing Training and Awareness

- Continuous learning importance
- Updates on threats/practices
- Reinforcing awareness

Module 15: Conclusion and Recap

- Summary of takeaways
- Encouragement for application
- Importance of vigilance