INTRODUCTION TO CYBERSECURITY

GENTEX®
TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Introduction

Cybersecurity is now a critical field for every organization, regardless of its size or industry. With the rising frequency and complexity of cyberattacks, professionals must understand the core principles that protect systems, networks, and data. This course provides a solid foundation in cybersecurity fundamentals. It helps participants recognize vulnerabilities, apply protective measures, and develop a security-focused mindset. By exploring key concepts such as threat types, risk management, and basic security protocols, participants will gain essential knowledge to enhance organizational safety and resilience.

Introduction to Cybersecurity Course Objectives

- Understand basic cybersecurity concepts, terminology, and principles.
- Identify different types of threats, attacks, and vulnerabilities.
- Apply preventive measures to protect information and infrastructure.
- Explore network security, endpoint protection, and identity management.
- Understand the importance of incident response and disaster recovery.
- Develop awareness of cybersecurity laws, ethics, and compliance.

Course Methodology

This course combines instructor-led sessions, interactive discussions, practical scenarios, group exercises, and real-world case studies to ensure learning is engaging and relevant.

Who Should Take This Course

- IT professionals and administrators
- Managers responsible for information security
- Employees handling sensitive or digital data
- Individuals seeking foundational cybersecurity knowledge

- Risk management and compliance officers

Introduction to Cybersecurity Course Outlines

Day 1: Understanding Cybersecurity Basics

- What is cybersecurity and why it matters
- Core elements of information security (CIA Triad)
- Key terms and common security myths
- History of cyberattacks and modern-day threats
- Introduction to cybersecurity frameworks and standards

Day 2: Types of Threats and Attacks

- Malware, phishing, ransomware, and social engineering
- Insider threats vs. external threats
- Denial of Service (DoS) and Distributed DoS
- Real-life cyberattack case studies
- Techniques used by attackers and how to recognize them

Day 3: Security Technologies and Tools

- Antivirus and anti-malware solutions
- Firewalls and intrusion detection systems (IDS)
- Authentication, authorization, and encryption
- Endpoint and network protection
- Cloud and mobile security fundamentals

Day 4: Risk Management and Compliance

- Introduction to risk assessment and management
- Security policies, procedures, and governance
- Regulatory requirements (GDPR, HIPAA, etc.)
- Ethical considerations in cybersecurity
- Business continuity and disaster recovery planning

Day 5: Building a Cybersecurity Culture

- Security awareness and training for staff
- Incident response planning and execution
- Roles and responsibilities in a secure environment
- Continuous monitoring and improvement
- Final group activity: Creating a simple security action plan

Conclusion

By successfully completing this course with Gentex Training Center, participants will gain the knowledge and tools to understand and apply cybersecurity fundamentals within their organizations. They will leave with practical insights, enhanced awareness, and the ability to support cybersecurity initiatives in their workplace confidently.