Cyber Security - An Introduction Training

Duration: **1 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

As cyber threats continue to evolve, security awareness has become an essential skill for every employee—not only IT professionals. Organisations can only reduce cyber risk when their workforce understands how attacks occur and adopts secure working practices.

Cyber Security – An Introduction is a practical foundation programme designed to introduce the core principles of cyber security and information protection. Participants explore common cyber threats, attacker profiles, malware, social engineering techniques, and the essential practices required to safeguard both personal and organisational information.

Using practical examples and real-world scenarios, the course builds confidence in recognising cyber risks and responding appropriately to potential security incidents.

Prerequisites

No previous cyber security experience is required.

Basic computer literacy and an interest in learning through practical discussions and activities will help participants gain maximum value from the programme.

Who Should Attend

This course is suitable for:

- Professionals with little or no cyber security background
- Employees from non-technical departments
- Managers and team leaders responsible for protecting business information
- Individuals beginning a career in cyber security
- Anyone wishing to improve their personal and workplace cyber security awareness

What You Will Learn

Upon successful completion of this course, participants will be able to:

- Explain the importance of cyber security for individuals and organisations.
- Recognise different categories of cyber attackers and their motivations.
- Describe the typical stages of a cyber attack.
- Identify common attack techniques, including reconnaissance and social engineering.
- Understand different types of malware and their potential impact.
- Explain how organisations respond to and recover from cyber incidents.
- Apply practical cyber hygiene techniques to reduce everyday security risks.
- Identify reliable sources of cyber security information and threat intelligence.

Cyber Security - An Introduction Training

Duration: **1 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Training Outline

Module 1 – Introduction to Cyber Security

- Cyber security fundamentals
- Information security principles
- The CIA Triad
- Introduction to Information Security Management Systems (ISMS)
- Building a security-aware culture
- The role of organisational policies

Module 2 – Understanding the Threat Landscape

- Today's cyber threat environment
- Types of threat actors
- Cybercriminals
- Hacktivists
- Nation-state attackers
- Insider threats
- Common attack motivations
- Emerging cyber security trends

Module 3 – Anatomy of a Cyber Attack

- The cyber attack lifecycle
- Reconnaissance techniques
- Information gathering
- Social engineering attacks
- Port scanning
- Network sniffing
- Real-world cyber attack case studies

Module 4 – Practical Cyber Defence

- Creating strong passwords
- Multi-factor authentication (MFA)
- Antivirus and endpoint protection
- Software updates and patch management
- Data backup strategies
- Encryption fundamentals
- Responding to cyber incidents
- Recovery procedures and incident reporting