COURSE CONTENT OVERVIEW

Introduction to Cyber Security

High Speed Training™

0333 006 7000

www.highspeedtraining.co.uk

Ensuring that a high level of cyber security is maintained is every internet user's responsibility. As an employee, you must understand how to keep information safe by correctly handling and storing data.

This Introduction to Cyber Security course provides you with knowledge of the possible risks if the confidentiality, integrity or accessibility of information is compromised. You will understand how you can help improve information security and what action you must take if information is lost or stolen.

Module One: What is Cyber Security?

This module explains what information security and cyber security are. It outlines why keeping information safe is important and what your responsibilities are as an employee when it comes to handling data.

- What is information security?
- What is cyber security?
- Why is cyber security important?
- Who is at risk?
- Types of cyber attacks
- Employee responsibilities
- Case studies
- Cyber security survey

Module Two: Types of Cyber Attacks

This module describes each of the most common types of cyber attacks. You will learn what they are, how they work and the possible consequences of each.

- Phishing
- Spear phishing
- Malware - viruses, worms and Trojans
- Ransomware
- Protecting yourself from a cyber attack
- Identity theft
- Other types of cyber attacks

Module Three: Information Security

This module covers the main internal and external threats to information security. It explains how organisations can manage their vulnerabilities to these threats as well as what areas within a company are most at risk.

- Verizon's 2019 Data Breach Investigations Report
- Internal threats to information security
- External threats to information security
- Managing organisational vulnerabilities to threats
- Areas at risk of information security threats

Module Four: How to Improve Information Security - Part 1

This module suggests actions you can implement in order to improve your online security. It identifies what a potentially untrustworthy website or email looks like. You will also learn how to create a secure password for accounts and how to use social media safely.

- Sharing information
- Creating a strong password
- Password security
- Emails
- Social media

Module Five: How to Improve Information Security - Part 2

This module explains the cyber security measures that you should have in place to help prevent attacks from being successful. You will learn how to identify malicious activity, what to do if you suspect an attack and how to report lost or stolen information.

- Firewalls
- Antivirus software
- Further measures
- How to identify malicious activity
- Actions you should take if you suspect malicious activity
- Reporting lost or stolen information

Aims of the training

By the end of this course, you will understand:

- What is meant by cyber security and who is at risk from security threats.
- The different types of cyber attacks that organisations and individuals may experience.
- The internal and external threats to information security and how to manage the organisational vulnerabilities to these threats.
- How to improve information security.
- The cyber security measures that you should have in place and what action you must take if confidential information is lost or stolen.