# CYBERSEC ESSENTIALS

**DURATION: 1 DAY**

CYBER SECURITY

Cybersecurity is the practice of protecting computer systems, networks, and digital information from unauthorised access, theft, damage or disruption. With the increasing reliance on technology and the internet for business operations and personal activity, cybersecurity has become a critical issue for individuals, organisations and governments around the world. To help combat this, ALC's CyberSec Essentials course has been designed specifically for the **NON-IT people**, to understand their roles & responsibility in ensuring cyber safety and security in the workplace, home and anywhere.

## WHO SHOULD ATTEND

**General Users:** Individuals who use computers, smartphones, and the internet regularly for personal and professional purposes. They may not have a technical background but want or need to understand the fundamental concepts of cybersecurity to protect themselves and the digital assets, business operations, customer data, and intellectual property.

**Employees in Non-IT Roles:** Non-technical employees who work in various departments who may handle sensitive information or use digital tools. They need awareness of cybersecurity best practices to protect company data and prevent common cyber threats.

**Non-IT Managers and Executives:** who have oversight responsibilities for cybersecurity within their organisations. They require a basic understanding of cybersecurity concepts to make informed decisions, allocate resources, and establish cybersecurity policies and procedures.

**Government and Public Sector Employees:** Non-technical government employees and public servants who handle sensitive data.

## LEARNING OUTCOMES

ALC's CyberSec Essentials course is designed to cater to individuals without a technical IT background, providing clear explanations of cybersecurity concepts, common threats, best practices, and practical tips for securing personal and professional digital environments.

This 1-day course focuses on raising awareness, fostering a security mindset, and empowering participants to take proactive steps to enhance their cybersecurity posture and understanding their responsibilities in cyber security.


CYBER SECURITY
**WE HAVE YOU COVERED**

**1300 767 592**
**customerservice@alc-group.com**
**alctraining.com.au**

ALC.Training
@alcgroup
alc-training


## COURSE CONTENTS

### INTRODUCTION TO CYBER SECURITY

- Overview of cyber security and its importance
- Types of cyber security threats and attacks
- Impact of cyber security breaches
- Importance of good cyber security practices

### THREATS TO CYBER SECURITY

- Overview of common cyber security threats
- Malware: types and how they spread
- Phishing: what it is and how to identify it
- Social engineering: what it is and how to avoid it
- Password attacks: Types and prevention
- Denial of service attacks: what they are and how to prevent them

### PROTECTING YOUR COMPUTER AND NETWORK

- Overview of computer and network security
- Firewall basics and configuration
- Antivirus software: what it is and how to use it
- Secure web browsing: best practices and tools
- Wireless security: securing your Wi-Fi network

### PROTECTING YOUR DATA

- Overview of data security
- Encryption: what it is and how to use it
- Backup and recovery: why it's important and how to do it
- Monitoring Data Security: why it's important and how to do it
- Cloud security: how to keep your data safe in the cloud Threats to cyber security

### BEST PRACTICES FOR CYBER SECURITY

- Creating strong password
- Multifactor authentication: what it is and how to use it
- Keeping software up to date
- Avoiding risky online behavior

### COMMON CYBER SECURITY STANDARDS AND FRAMEWORKS

- ISO 27001
- ACSC Essential Eight
- The Essential 8 Maturity Model
- NIST Cyber Security Framework
- GDPR

### CONCLUSION & NEXT STEPS

- Recap of cyber security basics
- Importance of ongoing cyber security education
- Additional resources for additional learning