CYBER SECURITY AWARENESS FOR GENERAL STAFF

DURATION: 1-2 HOURS

CYBER SECURITY

Cyber incidents big or small can dramatically impact your business. Unfortunately, people, even those with the best intentions, can be the cause of some of these incidents. An accidental click of a link, working from a public WIFI, oversharing on social media, can all lead to a potential breach.

In order to empower our people, we believe the best cyber awareness training uplifts a person's overall cyber safety knowledge and not just best business practice. We've created a 90 minute session that is both engaging and informative. We cover the key security areas such as Password, Phishing, Social Media and Physical Security, but we ensure the examples are relatable and part of people's every day experiences. By helping your staff protect their personal security you enable them to protect your business security.

LEARNING OUTCOMES

- **Full & Part-Time Employees:** All staff members, regardless of their employment status, should attend to ensure a consistent level of cybersecurity awareness throughout the organisation.
- **Contract and Temp Workers:** Extend the training to include contractors or temporary employees who have access to the organisation's systems and data.
- **Admin Staff:** Including receptionists, administrative assistants, and office managers.
- **IT and Technical Teams:** IT personnel, software developers, network administrators, and technical support staff.
- **Human Resources:** HR staff responsible for employee data and confidential information.
- **Finance and Accounting:** Finance and accounting teams handling financial transactions and sensitive data.
  Operations and Facilities: Staff responsible for the physical security of premises and equipment.

LEARNING OUTCOMES

Equip employees with the knowledge and skills to recognize and respond to cybersecurity threats effectively. Empower staff to protect sensitive data, customer information, and intellectual property. Promote a culture of security and responsible online behavior throughout the organisation. Help prevent security incidents, data breaches, and potential financial and reputational damage. Ensure compliance with industry regulations and safeguards the organisation's reputation.

CYBER SECURITY
WE HAVE YOU COVERED
1300 767 592
customerservice@alc-group.com
alctraining.com.au

ALC.Training
@alcgroup
alc-training

COURSE CONTENTS

Our Cybersecurity Awareness content is designed to tackle key security concepts as covered below. Some of the below content can also be adjusted based on company specific policies and guidelines.

PASSWORD
- Strong Password Practices
- Using a Password Manager
- Multi Factor Authentication
- Clearing Saved Passwords

SECURITY AROUND THE OFFICE
- Social Engineering Tactics
- Cloning RFID Access Cards
- Clean Desk Policy
- Locking the Workstation
- Secure Laptop & Document Storage
- Destruction of Records
- Filtering Phone Calls

SOCIAL MEDIA & DATA PRIVACY
- Geolocation Risks
- Preventing Information Disclosure
- Privacy Settings

PHISHING
- How to Spot a Phishing Email
- Common Phishing Tactics
- Detecting Threatening Hyperlinks
- How to Read a URL
- Safe Internet Browsing
- Visiting Secure Websites

BAD USB/PUBLIC WIFI
- Dangers of Foreign USB Devices
- Safely Connecting to Wi-Fi Networks
- Using the Internet when Travelling
- Bluetooth and Wi-Fi Dangers