

Introduction

Providing cybersecurity awareness training for employees is important for ensuring that they have the necessary knowledge and understanding of the best security practices to safeguard the business from cyber-related risks and threats.

Key awareness training topics

While the content of cybersecurity training should be tailored to the specific needs of each business and the challenges they might face, some cybersecurity awareness topics that employee training should cover include:

- ☐ **Password Management:** The importance of unique passwords (minimum 10 characters) for each account, using password managers and never saving passwords in browsers or physically.
- ☐ **Email security:** How to identify and handle phishing emails, as well as advising employees to only open attachments from trusted contacts and to never respond to emails requesting personal or sensitive information. Restrict usage of emails for work purposes and don't allow employees to register their work email address for personal online account usage.
- ☐ **Safe browsing:** Best practices for internet use and avoiding malicious websites.
- ☐ **Data protection:** How to handle and store sensitive information or data securely. For instance, understanding the risks of externally storing information outside internal business storage systems, such as transferring data to non-work devices.
- ☐ **Securing work devices:** Installing reputable anti-malware applications, only obtaining applications or software from trusted sources (such as your device's application store), as well as utilising access control functions, such as passwords and multi-factor authentication across the operating environment.
- ☐ **Guidance for working remotely:** Best practices when working outside of the regular workplace. For instance, to avoid connecting business devices to unknown or unsecure networks, employees can tether connectivity from their mobile phone. Further, ensuring documents containing sensitive information are never left unattended in public areas and are securely stored or destroyed when no longer needed.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document,

IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

- **Incident response:** Steps to take if a compromise or cyber incident occurs, such as resetting passwords, securing vulnerabilities and where to report.

Additional guidance for training employees on cybersecurity

Develop a cyber security policy

- While a cyber security policy may sound unnecessary for smaller businesses, creating thorough guidelines for how your online systems and operations should be executed safely can minimise risk. It can help employees understand their role in protecting the technology and information assets of the business. This policy should be easily accessible to all employees and continuously updated to address new and emerging vulnerabilities. For support on what information a cyber security policy should include, visit business.gov.au.

Provide regular cyber training and updates

- While all employees should undergo cybersecurity training during their onboarding process, periodically providing additional training for employees is important to maximise their awareness of potential threats. Employers should take advantage of online cybersecurity courses and resources for training employees, either paid or unpaid.

Promoting a culture of security awareness

- Making cybersecurity awareness an ongoing conversation involves positioning cybersecurity as an important consideration in the business's operations and discussions, as opposed to being an occasional training topic. Employers can promote this by sharing updates about recent threats that may be relevant for the business and regularly discussing the importance of good security practices.
- IDCARE's [free monthly newsletter](#) is a great way to be informed of the latest scam trends.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Encourage reporting of vulnerabilities and suspicious activity

Employers should encourage employees to report any observed areas of weakness, or opportunities for improvement of information security management within the business. Employers should also encourage employees to report signs of suspicious activity or indicators of compromise, such as the sudden appearance of unrecognised apps or programs on their devices or strange pop-ups.

IDCARE's free Cyber Advisory Sessions are designed to help small businesses (<20 FTE) improve their cyber security knowledge and practices. Complete the short Cyber Health Check survey which will provide your business an independent and confidential appraisal of your resilience in relation to privacy and cyber security. Start the health check and book your Cyber Advisory Session [here](#).

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 170 (Aus) | 0800 121 068 (NZ)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.