NEW COURSES | GENERAL SECURITY

87% learnt something new during this course

1 Vendor Email Compromise

This course focuses on Vendor Email Compromise (VEC) and the risk associated with vendors becoming compromised within the supply chain.

⭐ **Learner Feedback** ⭐
88% learnt something new during this course saying it was well paced and was engaging.

2 Anatomy of a BEC Attack

This course will outline the different levels of risk associated with BEC attacks, focusing on the different types of tactics used by cybercriminals to compromise accounts.

3 Online Gaming

This course equips gamers with the knowledge to stay safe online.

I loved the facts about the gamer and how applicable the information is and what to look out for.

4 Multi-Factor Authentication (MFA)

MFA provides an additional layer of security for your accounts, to prevent unauthorised access. Understanding MFA will equip you with the knowledge and skills to secure your digital assets effectively.

Love the animations. Nice and simple and easy way to absorb phishing information.
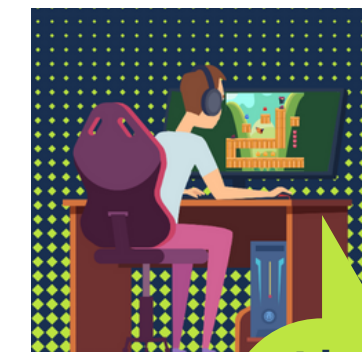
5 Scams & Social Engineering

This course identifies some common signs of scams via social engineering. You will learn how to protect the organisation, yourself and your family from social engineering.

6 QR Code Scams

QR codes are meant to be convenient and efficient, and this is precisely what scammers prey on. Scammers can send QR codes digitally using social media, text messages, or emails.

88% learnt something new during this course

7 Investment Scams

This course aims to empower you with the knowledge and skills needed to protect yourself and others from falling victim to fraudulent investment schemes.

8 Supply Chain Risks

The digitisation of supply chains makes them a big target for threat actors. The security of every business partner in the supply chain is only as strong as the weakest link.
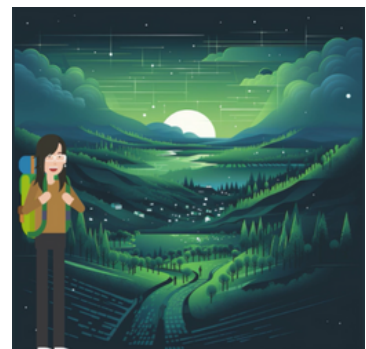
9 Passwords & Passphrases (NZ)

Ensure you understand the important role of passwords in keeping information safe and secure.

Great way to present the information

10 Remote Working

In today's digital age, more and more people are working remotely or travelling for work. While this can be convenient, it also poses a risk to the security of sensitive information.

11 Fraud Awareness

Uncover the behaviours of fraudsters to learn how to reduce the risks of fraud to you, your family and your organisation.

12 Scan for Scam Emails (NZ)

Learn the basics of S.C.A.M. (Sender, Content, Action, Manage) phishing concepts. Employees will understand basic terminology and explore the different approaches scammers use to trick people.

84% learnt something new.

13 — CyberRetail: Removable Media Security

This course explores the ways these devices can be infiltrated, along with the 'traps' we need to avoid to ensure we keep our data from falling into the wrong hands.

14 — CyberEducation: Foreign Interference (NZ Universities)

This course aims to ensure that the students, staff and their research within Aotearoa New Zealand Universities are protected from evolving foreign threats.

15 — CyberUtilities: Critical Infrastructure

This module will teach you about the importance of critical infrastructure and how operational technology helps keep it working properly.

16 — CyberHealth: OT Fundamentals

Learn about what Operational Technology (OT) is, why it is important, explore the different threats and ways to secure the OT environment.

17 — CyberUtilities: IT/OT Fundamentals

This course focuses on securing the IT and OT environments and the importance of implementing operational technology hygiene practices.

18 — CyberEducation: Social Media (for Teens)

This course explains the common risks of social media and the most important tips to stay safe.

NEW COURSES | ROLE-BASED

> **91% learnt something new during this course.**

19 CyberSecureIT: Secure Coding

Secure coding is the practice of building software in a way that ensures it's protected against vulnerabilities. Discover best practice to improve software security.

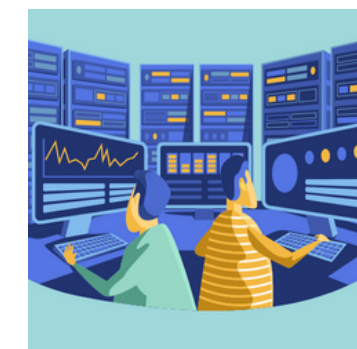> **70% learners are likely to recommend**

20 CyberExecs: Building a Positive Security Culture

This course aims to help leadership shift employees from viewing compliance as a tick-box exercise to fostering a positive security culture.

21 CyberSecureIT: Incident Management

Explain the importance of developing an incident management plan and identify the different roles and responsibilities related to incident management.

NEW COURSES | GOVERNMENT GUIDELINES

22 Essential 8

Learn how to accelerate your Essential 8 maturity level target and reduce the time spent managing security controls and safeguarding your organisation.

23 Countering Foreign Interference for AUS Gov

This course aims to ensure that Aus government employees are protected from any potential or evolving threats by foreign interference.

24 Countering Foreign Interference for NZ Gov

This course aims to ensure that NZ government employees are protected from any potential or evolving threats by foreign interference.

NEW COURSE | UPDATES

WHAT'S NEW...

- Uplift to graphic designs and animations
- Web Content Accessibility Guidelines (WCAG) standards applied
- Updated trends and examples of scams in current landscape (especially to Smishing scams)

1	Intro to Info Security

2	Cloud Security

3	Email Security

4	Wi-Fi

5	Security Incidents

6	Safety Online

7	Personal Information

8	Protecting your Digital Identity

9	Smishing

10	S.C.A.M. 1 Fundamentals

11	S.C.A.M. 2 Identification

12	S.C.A.M. 3 Application