

Cyber Security Introduction

Duration: 1 hour **Prerequisites:** None

Participants: Approx. 15 per session - We advise session headcount to be kept to smaller sizes wherever possible as this allows delegates to participate more fully and ask questions.

Subject	Description
Introduction	An overview of the course.
Strong Passwords	Using strong passwords is key to keeping your environment private and secure. Learn why strong passwords are important and security tips to ensuring compliance.
Social Engineering	What is social engineering and how to spot it.
Cyber Security	Cyber security relates to the protection of computers, networks, and data from malicious attacks.
Phishing/Spear Phishing/Whaling	Phishing and its associates are cybercrimes. The target or targets are contacted via email. Learn how to protect yourself from them.
How Physical and Information Security Complement Each Other	Learn how true security combines cyber security and physical security.
Safer Digital Communications at Work	Learn more about how to be more vigilant about work communication and security.
Malware at Work	Learn more about the different types of malware that can affect your organisation including viruses, spyware, adware, and ransomware.
Mobile Device Security	Mobile device security and the need, in our modern "mobile" world, to protect the data on your devices.
Security for Cloud Services	How security can ensure compliance in the Cloud.
Identifying Personally Identifiable Information	How to make sure data that is meant to remain within your organisation stays that way.
Better Security on the Road	Security when traveling is different than when at work or home. Learn how to stay cyber protected everywhere you go.

Training Requirements: At the Readiness Company we are all about ensuring your customers get the training that they truly need. If the course description above does not fulfil their requirements get in touch with us and we will do our best to tailor it so they are satisfied.