

## Online Security - (1) Online Security in a Connected World

Programme Title:	Online Security	
Module Title:	(1) Online Security in a Connected World	
Content Provider:	The Internet Safety Group's NetSafe® Programme	
		Version: 1

### Goal

The goal of this module is to build the course participants' confidence to use ICT (information and communication technology) safely and responsibly and in particular their confidence to monitor and educate younger users for whom they are accountable.

### Overview

The ISG (The Internet Safety Group) is a non-profit organisation with members representing a wide range of organisations. These include: New Zealand Police, Department of Internal Affairs Censorship Compliance Unit, Customs Service, and the Judiciary, as well as numerous community groups, educators from primary to university level, parents and prominent businesses.

NetSafe™ is the education programme of the ISG (the Internet Safety Group) and fosters safe and responsible use of communication technologies, including the Internet.

People who complete this module will:

- Acknowledge the rapidly changing environment of communication technologies, the constantly evolving risks involved in their use and the need to be up-to-date with strategies to minimise those risks
- Identify a range of choices they have for safer, more responsible use of communication technologies
- Evaluate their own security setup and their responsibility and accountability for other users

### Considerations

**Target audience:** Community adult learners who have previously completed NZQA Unit Standards 18758, 2780, 5941, ICDL module 7, or who have previous experience of web browsing, and in particular parents or caregivers who are accountable for the bill payments and security of mobile phone and computer use of younger users.

The case study examples used in this module are centred on a current New Zealand setting and technologies but may be modified for other international and emerging technologies.

The course is offered as a stand-alone, online course involving five to six hours of unsupervised study, with checkpoints but no formal assessment.

### Content Outline

#### Introduction

- Goals of the course and how to use it
- Description and contact details of the Internet Safety Group's NetSafe® education programme, website and contact centre.

#### The Computer

- Hardware; connecting devices and default security settings
- Software; operating systems, applications, plug-ins and add-ons, risks of freeware
- Data and memory; storage, file sizes, bandwidth
- External storage media; case study of risks of file sharing
- Checkpoint; opportunity to check learning

#### Security Risks

- Malware; descriptions, risks, strategies to minimise risk and case study
- Hackers; criminal activity and case study
- File sharing; peer-to-peer, Instant Messenger services, sexual predators, copyright infringement
- Spam; scams, fraud, viruses and malware
- Surveillance devices; covert surveillance, privacy and publication
- Checkpoint; opportunity to check learning

---

#### Mobile Phones

- Hardware; capabilities, broadcast towers, reception and location data
- NZ handsets; two network technologies (Telecom and Vodaphone), identifier numbers, theft and blacklisting.
- Case study; risks of second hand purchase
- Mobile services; wireless internet access, GPS, tracking, risks and parental involvement
- Checkpoint; opportunity to check learning

#### Connecting

- The Internet; the digital environment and its possibilities and risks
- Case study; personal information on websites
- Administration; domain names, website complaints
- Internet Service Providers; options, Code of Practice
- Connection; minimum protection, choices and Internet Protocol number
- Dial-up; modems, download speed, data transfer
- Broadband; modem, levels of service, account options, security and monitoring
- Wireless; access point, configuration for a secure perimeter
- Checkpoint; opportunity to check learning

#### Security Setup

- Internet Readiness; basics for security
- Operating System; updates
- Firewall; activation and updates
- Anti-Virus; scanning, quarantine, filtering
- Spyware Detection; anti-spyware programs, case study
- Adware; pop-up blocking
- Cookies; setting privacy levels
- Monitoring; traffic reports
- Filtering; offensive content, individual accounts and customised settings
- Checkpoint; opportunity to check learning

#### Security Practices

- Maintenance; updating
- Monitoring; history settings, accountability, privacy, use agreements, education
- Administration; role of administrator, log-ins, locking the computer
- Passwords; steps to maintain a strong password
- Backing Up; security of crucial files
- Encryption; Internet banking, shopping and secure servers
- Checkpoint; opportunity to check learning

---

### Learning Objectives

At the end of the module it is expected learners will have the necessary knowledge, skills and attitudes to confidently do the following:

- Recognise and use the NetSafe® website
- Identify, describe and differentiate a range of communication technologies including computers, mobile phones
- Question, contrast, and discriminate between different provider policies and services
- Recognise, predict, calculate and discuss a range of security risks involved with the use of the Internet and communication technologies
- Appraise, select, set up and operate essential updated security and operating software
- Discuss, explain, value, defend and support safe, responsible use of the Internet and communication technologies

---

### Instructional Strategies

Instructional Strategies used to teach this course include:

- Text, illustrations, animations and video captures where appropriate to teach a procedure
- Hypertext links to the Internet Safety Group's NetSafe® website
- Real examples of relevant case studies or anecdotes which the learner may be able to identify with
- Consistent identifying icons for directing learner's attention to risks and secure practices
- Key words, definitions and information about how current learning relates to previous or later learning with the use of a rollover glossary
- Interactive exercises (multiple-choice, short answer, true or false type questions) with feedback
- 'Check your understanding' quiz at the end of each topic

---

### Certification/Qualifications

There are no qualifications for this module.

---

### Suggested Learning Hours

Estimated time for completion of the 'Online Security in a Connected World' module is five (5) to six (6) hours.