



Australian Government

Department of Education, Employment and Workplace Relations

ICASAS206A Detect and protect from spam and destructive software

Release: 1

ICASAS206A Detect and protect from spam and destructive software

Modification History

Release	Comments
Release 1	This Unit first released with <i>ICA11 Information and Communications Technology Training Package version 1.0</i>

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to reduce the risk of a computer's operation being affected by spam or destructive software.

Application of the Unit

This unit applies to technical support personnel who are required to protect and secure equipment and software in a small or large office environment. Maintaining system integrity through virus security and implementing spam filtering are key components of information and communications technology (ICT) environments.

Licensing/Regulatory Information

No licensing, legislative, regulatory or certification requirements apply to this unit at the time of endorsement but users should confirm requirements with the relevant federal, state or territory authority.

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Element	Performance Criteria
<i>Elements describe the essential outcomes of a unit of competency.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element. Where bold italicised text is used, further information is detailed in the required skills and knowledge section and the range statement. Assessment of performance is to be consistent with the evidence guide.</i>

Elements and Performance Criteria

1. Detect and remove destructive software	1.1 Identify common types of <i>destructive software</i> 1.2 Select and install <i>virus protection</i> compatible with the <i>operating system</i> in use 1.3 Investigate other <i>advanced systems</i> of protection for further options 1.4 Install <i>software updates</i> on a regular basis 1.5 Configure software <i>security settings</i> to prevent destructive software from infecting computer 1.6 Run or schedule to run virus-protection software on a regular basis 1.7 Report detected destructive software to <i>appropriate person</i> and remove the destructive software
2. Identify and take action to stop spam	2.1 Identify common types of <i>spam</i> 2.2 Take <i>appropriate action</i> in regard to spam 2.3 Configure and use a <i>spam filter</i> 2.4 Report spam to <i>appropriate organisation</i>

Required Skills and Knowledge

This section describes the skills and knowledge required for this unit.

Required skills

- communication and literacy skills to present reports
- problem-solving skills to anticipate and respond to a range of known virus and spam types
- technical skills to:
 - install and configure system filtering and security settings
 - install software updates
 - install virus protection
 - operate a computer and software application
 - select virus protection to suit operating system in a limited range of options.

Required knowledge

- spam and virus intrusions and appropriate remedial action
- types of protective applications used against viruses and spam
- operating systems supported by the organisation
- computer hardware
- Spam Act 2003 and associated guidelines.

Evidence Guide

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Overview of assessment	
Critical aspects for assessment and evidence required to demonstrate competency in this unit	Evidence of the ability to: • install virus protection software and updates • schedule virus protection software to run on a regular basis • identify and remove common destructive software • identify common spam types and take appropriate action.
Context of and specific resources for assessment	Assessment must ensure access to: • sites with a representative range of computer hardware, application software and operating systems • current antivirus and anti-spam software • technical records, vendor documentation and enterprise procedures and guidelines • appropriate learning and assessment support when required. Where applicable, physical resources should include equipment modified for people with special needs.
Method of assessment	A range of assessment methods should be used to assess practical skills and knowledge. The following examples are appropriate for this unit: • direct observation of candidate undertaking installation of virus protection and anti-spam software • direct observation of candidate performing virus scan and virus removal • review configuration of virus protection software and creation of operating schedule created • configure and use a spam filter.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, where appropriate. Assessment processes and techniques must be culturally appropriate, and suitable to the communication skill level, language, literacy and numeracy capacity of the candidate and the work being performed. Indigenous people and other people from a non-English speaking background may need additional support. In cases where practical assessment is used it should be combined

	with targeted questioning to assess required knowledge.
--	---

Range Statement

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

<i>Destructive software</i> may include:	• file viruses • keystroke loggers • logic bombs • macro viruses • remote access tools (RATs) • spyware • system sector viruses • trojans • viruses • worms.
<i>Virus protection</i> may include:	• CA Vet Antivirus • freeware • online • open source • proprietary software: • BitDefender • Kaspersky Antivirus • McAfee VirusScan • Panda Antivirus • Symantec Norton Antivirus.
<i>Operating system</i> may include:	• GNUs Not Unix (GNU) • Linux • HP-UX • Mac OS X • Microsoft Windows • Unix-like operating systems: • IBM AIX • Silicon Graphics IRIX • Sun Solaris.
<i>Advanced systems</i> may include:	• hardware firewall • software firewall.
<i>Software updates</i> may	• automatic online updates • security patches

include:	• service packs and service releases • virus definition updates • virus scanning engine updates.
Security settings may include:	• firewall • internet browser • operating system • virus protection.
Appropriate person may include:	• authorised business representative • client • supervisor • system administrator.
Spam may include:	• messages covered by the Spam Act 2003 • unsolicited commercial electronic messaging: • email • instant messaging • mobile phone messaging • social networking • wiki.
Appropriate action may include:	• deleting the spam • blocking the sender by configuring spam filter • unsubscribing from mailing list if company is not reputable.
Spam filter may include:	• email client filters or rules • email server filters • third-party filter programs: • CA Anti-Spam • MailWasher Pro • Norton Internet Security • SpamAssassin.
Appropriate organisation may include:	• relevant government and private media screening organisations, such as: • Australian Communications and Media Authority • Scamwatch company that originated the spam message.

Unit Sector(s)

Systems administration and support