



Australian Government

ICTSAS206 Detect and protect from spam and destructive software

Release: 1

ICTSAS206 Detect and protect from spam and destructive software

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 1.0.

Application

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

It applies to technical support individuals who, while working under a level of supervision, have responsibility to exercise the discretion required to protect and secure equipment and software in a small or large office environment.

No licensing, legislative or certification requirements apply to this unit at the time of publication.

Unit Sector

Systems administration and support

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
<i>Elements describe the essential outcomes.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element.</i>
1. Detect and remove destructive software	1.1 Identify common types of destructive software 1.2 Select and install virus protection compatible with the operating system in use 1.3 Investigate other advanced systems of protection for further options 1.4 Install software updates on a regular basis 1.5 Configure software security settings to prevent destructive software from infecting computer 1.6 Run or schedule to run virus protection software on a regular

ELEMENT	PERFORMANCE CRITERIA
	basis 1.7 Report detected destructive software to appropriate person and remove the destructive software
2. Identify and take action to stop spam	2.1 Identify common types of spam 2.2 Take appropriate action in regard to spam 2.3 Configure and use a spam filter 2.4 Report spam to appropriate person

Foundation Skills

This section describes language, literacy, numeracy and employment skills incorporated in the performance criteria that are required for competent performance.

Skill	Performance Criteria	Description
Reading	1.1-1.5, 2.1-2.3	Researches and interprets information to identify misleading information and compare technical specifications, and identify solutions to new and emerging issues to maintain system
Writing	1.7, 2.4	Uses simple vocabulary to report information in a familiar sequential manner to the appropriate personnel
Oral Communication	1.7	Presents factual information in a clear manner, using specific and appropriate language
Interact with others	1.7	Identifies and takes steps to follow accepted communication practices and protocols
Get the work done	1.1-1.7, 2.1-2.4	- Plans and implements routine tasks, aiming to achieve them efficiently - Initiates standard diagnostic procedures when responding to familiar and unfamiliar problems within immediate context, and seeks input from others when problems remain unresolved - Understands the purposes, specific functions and key features of common digital systems and tools, and operates them effectively to complete routine tasks

Unit Mapping Information

Code and title current version	Code and title previous version	Comments	Equivalence status
ICTSAS206 Detect and protect from spam and destructive software	ICASAS206A Detect and protect from spam and destructive software	Updated to meet Standards for Training Packages	Equivalent unit

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>

Assessment Requirements for ICTSAS206 Detect and protect from spam and destructive software

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 1.0.

Performance Evidence

Evidence of the ability to:

- install virus protection software and updates
- schedule virus protection software to run on a regular basis
- remove common destructive software
- identify common spam types and take appropriate action.

Note: If a specific volume or frequency is not stated, then evidence must be provided at least once.

Knowledge Evidence

To complete the unit requirements safely and effectively, the individual must:

- describe spam and virus intrusions and identify appropriate remedial actions
- identify the types of protective applications used against viruses and spam
- identify the operating systems supported by the organisation
- identify the common components of computer hardware that may be affected by spam.

Assessment Conditions

Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the systems administration and support field of work and include 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, enterprise procedures and guidelines.

Assessors must satisfy NVR/AQTF assessor requirements.

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>