Australian Government
Department of Education, Employment and Workplace Relations

ICAS2243B Detect and protect from spam and destructive software

Release: 1

ISC INDUSTRY SKILLS COUNCILS
Creating Australia's Future

ICAS2243B Detect and protect from spam and destructive software

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to reduce the risk of a computer's operation being affected by spam or destructive software. The following units are linked and form an appropriate cluster: • ICAU2005B Operate computer hardware • ICAU2006B Operate computing packages • ICAU2231B Use a computer operating system No licensing, legislative, regulatory or certification requirements apply to this unit at the time of publication.

Application of the Unit

Application of the unit	

Licensing/Regulatory Information

Refer to Unit Descriptor

Pre-Requisites

Prerequisite units		

Employability Skills Information

Employability skills	This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Elements describe the essential outcomes of a unit of competency.	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.

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
1. Detect and remove destructive software	1.1. Define and identify common types of ***destructive software*** 1.2. Select and install ***virus protection*** compatible with the ***operating system*** in use 1.3. Describe other ***advanced systems*** of protection, in order to understand 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 and/or schedule to run ***virus protection*** software on a regular 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. Define and 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 organisation***

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Decision making in a limited range of options
- Problem solving of known problems in routine procedures
- Plain English literacy and communication skills in relation to the presentation of information
- Basic skills in computer operation and software application operation
- Ability to install and/or activate system filtering and security settings

Required knowledge

- Basic knowledge of identification of spam and virus intrusions and appropriate remedial action
- Broad general knowledge of operating systems supported by the organisation
- Broad general knowledge of computer hardware

REQUIRED SKILLS AND KNOWLEDGE

- Basic knowledge types protective applications used against viruses and spam
- Spam Act 2003 and associated guidelines

Evidence Guide

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 following is essential: • Assessment must confirm the ability to identify, isolate and protect a system from destructive software by installing virus protection and software updates and to identify and take counter-action against SPAM. To demonstrate this unit of Competency the learner will require access to: • the organisation's applications needs • appropriate software • computer hardware
Context of and specific resources for assessment	The spread of junk email or spam over the internet has the potential to threaten the viability and efficiency of electronic messaging. Together with the circulation of destructive software in the form of viruses and the like, spam damages consumer confidence, obstructs legitimate business activities and imposes costs on users. This competency is one of a suite of foundation skills necessary for all users of email and internet services. The breadth, depth and complexity of knowledge and skills in this competency would prepare a person to perform in a range of varied activities or knowledge applications where there is a clearly defined range of contexts in which the choice of actions required is usually clear. There would generally be limited complexity in the range of operations to be applied. Assessment must ensure: • Performance of a prescribed range of functions involving known routines and procedures and some

EVIDENCE GUIDE	
	accountability for the quality of outcomes would be characteristic. • Applications may include some complex or non-routine activities involving individual responsibility or autonomy and/or collaboration with others as part of a group or team.
Method of assessment	The purpose of this unit is to define the standard of performance to be achieved in the workplace. In undertaking training and assessment activities related to this unit, consideration should be given to the implementation of appropriate diversity and accessibility practices in order to accommodate people who may have special needs. Additional guidance on these and related matters is provided in ICA05 Section 1. • Competency in this unit should be assessed using summative assessment to ensure consistency of performance in a range of contexts. This unit can be assessed either in the workplace or in a simulated environment. However, simulated activities must closely reflect the workplace to enable full demonstration of competency. • Assessment will usually include observation of real or simulated work processes and procedures and/or performance in a project context as well as questioning on underpinning knowledge and skills. The questioning of team members, supervisors, subordinates, peers and clients where appropriate may provide valuable input to the assessment process. The interdependence of units for assessment purposes may vary with the particular project or scenario.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, for example: • ICAU2005B Operate computer hardware • ICAU2006B Operate computing packages • ICAU2231B Use a computer operating system

EVIDENCE GUIDE	
	An individual demonstrating this competency would be able to: • demonstrate basic operational knowledge in a moderate range of areas • apply a defined range of skills • apply known solutions to a limited range of predictable problems • perform a range of tasks where choice between a limited range of options is required • assess and record information from varied sources • take limited responsibility for own outputs in work and learning • Maintain knowledge of industry products and services

Range Statement

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.	
Appropriate action may include but is not limited to:	• Delete the spam • Block the sender by configuring spam filter. • Unsubscribe from mailing list, if company is reputable
Appropriate organisation may include but is not limited:	• Company that originated the spam message. • Australian Communications Authority (www.aca.gov.au) • Australian Broadcasting Authority (www.aba.gov.au/internet) • Scamwatch (www.scamwatch.gov.au)
Appropriate person may include:	• supervisor • teacher • authorised business representative • client

RANGE STATEMENT	
Operating System may include but is not limited to:	• Linux 7.0 or above • Windows 2000 or above • Apple OS X or above
Virus protection	• There are various antivirus software applications available. Some include: McAfee, Panda AntiVirus, Protector Plus Antivirus, Symantec's Norton Antivirus, Command Antivirus, Vet. AMIvirus
Destructive Software may include but ins not limited to:	• Viruses • File viruses • System sector viruses • Macro viruses • Worms • Trojans • Logic bombs • Spyware
Software Updates may include but ins not limited to:	• Service packs and service releases • Security patches • Automatic online updates • Virus scanning engine updates • Virus definition updates
Spam may include:	• unsolicited commercial electronic messaging, where electronic messaging covers emails, instant messaging, SMS and other mobile phone messaging, but does not cover normal voice-to-voice communication by telephone. • A formal definition is included in the Spam Act 2003.
Spam filter may include but is not limited to:	• Email client filters or rules • Email server filters • Third party filter programs such as: • MailWasher Pro • Spamassassin • Norton Internet Security
Security settings may include but is not limited to:	• Internet browser security settings • Virus protection security settings • Firewall security settings • Operating system security settings
Advanced systems may include but is not limited to:	• Hardware firewall • Software firewall

Unit Sector(s)

Unit sector	Support

Co-requisite units

Co-requisite units		

Competency field

Competency field	