



Australian Government

BSBXCS302 Identify and report online security threats

Release: 1

BSBXCS302 Identify and report online security threats

Modification History

Release	Comments
Release 1	This version first released with BSB Business Services Training Package 6.0.

Application

This unit describes the skills and knowledge required to identify and report online security threats to limit potential impact of cyber security breaches.

It applies to those working in a broad range of industries and job roles under some supervision and guidance who encounter and report online threats during the course of their work.

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

Unit Sector

Digital Competence – Cyber Security

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. Identify online security threats	1.1 Review internal policies, procedures and plans relating potential online security breaches 1.2 Identify features of common types of potentially fraudulent communications 1.3 Implement techniques to verify suspicious requests for information
2. Respond to an online security breach	2.1 Block and report potential security breaches on computer and mobile device according to organisational policies and procedures 2.2 Respond to actual security breach or cyber security incident according to organisational response plan 2.3 Report security breach or cyber security incident according to legislative requirements and organisational policies and

ELEMENT	PERFORMANCE CRITERIA
	procedures
3. Support post- breach review	3.1 Provide information to required personnel to assist in documenting potential and actual breaches 3.2 Support post-incident review and identifying lessons learnt 3.3 Contribute updates to cyber security incident response plan as required and within scope of own role

Foundation Skills

This section describes those language, literacy, numeracy and employment skills that are essential to performance but not explicit in the performance criteria.

Skill	Description
Learning	Modifies behaviour following exposure to new information
Oral communication	Asks open and closed probing questions and actively listens to ensure that concepts regarding cyber security are well understood
Reading	Recognises and interprets information from relevant sources to determine organisational expectations relating to cyber security
Writing	Uses clear, specific and industry-related terminology relating to cyber security for breach and incident reports
Technology	Uses appropriate technology platforms to share information within the organisation relating to potential online security threats

Unit Mapping Information

No equivalent unit. New unit.

Links

Companion Volume Implementation Guide is found on VETNet: -

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

Assessment Requirements for BSBXCS302 Identify and report online security threats

Modification History

Release	Comments
Release 1	This version first released with BSB Business Services Training Package 6.0.

Performance Evidence

The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to:

- identify and report three different online security threats in a work area.

Knowledge Evidence

The candidate must be able to demonstrate knowledge to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including knowledge of:

- legislative requirements relating to identifying and reporting online security threats, including:
 - data protection
 - implications of Notifiable Data Breach legislation on an organisation and other associated Australian privacy laws
 - established international legislation
- organisational policies and procedures relating to online information security breaches, including:
 - blocking and reporting potential security breaches
 - escalation routes for cyber security issues
- common types of online scams and security risks, including phishing scams
- common techniques of phishing and spear phishing used by attackers, including:
 - spam email and SMS text
 - social engineering, including telephone calls, social media and website requests for information
- basic principles of cyber security
- indicators of insecure connection to websites, in particular where data is being collected
- Australian government sources of information on current online security threats
- common online security threats to which individuals might be exposed to, including physical threats

- common procedures for:
 - mitigating online security threats
 - following organisational cyber security incident response plan
 - responding to cyber security breaches.

Assessment Conditions

Skills must be assessed in a workplace or simulated environment where conditions are typical of a work environment requiring cyber secure practices, processes and procedures.

Access is required to:

- information and data sources relating to cyber security
- device with active internet connection
- internet browser
- industry standards and organisational procedures required to demonstrate the performance evidence.

Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

Links

Companion Volume Implementation Guide is found on VETNet: -

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