



Australian Government

BSBXCS301 Protect own personal online profile from cyber security threats

Release: 1

BSBXCS301 Protect own personal online profile from cyber 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 protect own personal online profile from cyber security threats, and to limit the potential impact of online security breaches.

It applies to those working in a broad range of industries and job roles under some supervision and guidance, who protect their own online profile so that it is cyber secure.

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 existing and potential security threats to own personal online profile	1.1 Determine all current online accounts and profiles 1.2 Identify common threats to security of online profiles 1.3 Identify industry-specific risk factors that raise risk levels to own personal profile
2. Audit own personal online profile for identified security threats	2.1 Review all online accounts, associated applications and browsers at risk of identified threats according to organisational policies and procedures 2.2 Review public online profiles that can be linked to own personal identity 2.3 Check billing and account records carefully to detect early indicators of potential theft

ELEMENT	PERFORMANCE CRITERIA
	2.4 Report identified suspicious cyber activity according to cyber security legislative requirements and organisational policies and procedures
3. Address identified existing and potential security threats to own personal online profile	3.1 Secure personal online profile and remove potential security risks 3.2 Confirm that software used on own desktop/laptop and mobile devices is current and sufficient 3.3 Remove potentially sensitive personal and company information according to organisational policies and procedures 3.4 Create strong passwords across personal and work accounts 3.5 Turn on two factor authentication across all accounts where available 3.6 Adjust privacy/security settings on internet browser, web applications and applicable online accounts 3.7 Delete all unused online accounts/applications according to organisational policies and procedures

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
Reading	• Recognises and interprets information from relevant sources to determine organisational expectations relating to cyber security
Technology	• Uses appropriate technology platforms to assist with protecting online profile from cyber security threats
Problem solving	• Uses problem solving skills to understand the nature of potential threat to personal profile or device and to undertake required action

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 BSBXCS301 Protect own personal online profile from cyber 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:

- conduct one audit of own personal online profile and identify existing and potential cyber security threats
- identify and address three potential cyber security risks to own personal online profile.

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 reporting cyber security threats
- organisational policies and procedures relating to online profiles, including escalation routes for cyber security issues
- basic principles of cyber security, including:
 - importance of data confidentiality, integrity and availability
 - common cyber security terms
 - common cyber security threats that individuals might be exposed to online
 - secure internet browsing
- risk factors relating to own personal online profile, including:
 - password management practices:
 - strength of created passwords
 - number of passwords used for multiple accounts
 - frequency of change to passwords
 - own work role within organisation
 - regular tasks in own work that raise personal risk level, including internet browsing
 - potential targets for cyber attack in own direct professional network
 - protocols for handling personally identifiable information
 - physical safety of devices

- industry-specific risk factors and their risk to online profiles
- common strategies, tools and techniques for improving security of own personal online profile, including for:
 - password protection
 - secure password management and account replicating and splitting
 - fundamentals of two-factor authentication
 - billing and account privacy settings
 - software patching
 - connecting to public Wi-Fi via virtual private networks (VPNs)
- common methods and practices for:
 - responding to cyber security issues, including reporting protocols
 - secure internet browsing, including banking and email
- common cyber security threats that individuals and data might be exposed to, including:
 - phishing
 - social engineering
 - social media
 - malware
 - physical threats, including data loss due to working insecurely in public spaces.

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>