National Unit Specification

General information

Unit title: Cyber Security (SCQF level 3)

Unit code: J6WN 43

Superclass: CB

Publication date: January 2023

Source: Scottish Qualifications Authority

Version: 01

Unit purpose

The purpose of this unit is to introduce learners to the key concepts of cyber security. This unit will equip learners with the basic knowledge and skills for working in the cyber security industry.

No previous knowledge or experience of cyber security is assumed; however, it is assumed that learners will be familiar with computing devices. Learners should possess basic problem solving and numeracy skills; however, these will be further developed during the unit.

Learners will be introduced to the basics of device security, networking and personal data security. These topics will enable the learners to better understand how to recognise, react and recover from cyber incidents they experience on their personal devices.

On completion of this unit, learners will have gained a basic understanding of how the internet and World Wide Web influences their daily lives. The learners will also be equipped with the relevant knowledge and skills to recognise cyber threats to their personal devices and accounts, and know the best way to react and recover from a cyber-incident they may experience when using the internet and World Wide Web to consume, create and communicate.

Learners may wish to progress to the National Progression Award (NPA) in Cyber Security at level 4.

National Unit Specification: General information (continued)

Unit title: Cyber Security (SCQF level 3)

Outcomes

On successful completion of the unit the learner will be able to:

1. Secure a device.
2. Identify the basics of networking.
3. Secure personal data.

Credit points and level

1 National Unit credit at Scottish Credit and Qualifications Framework (SCQF) level 3:
(6 SCQF credit points at SCQF level 3).

Recommended entry to the unit

Entry is at the discretion of the centre. No previous knowledge or experience of cyber security or computers is required.

Core Skills

Opportunities to develop aspects of Core Skills are highlighted in the support notes for this unit specification.

There is no automatic certification of Core Skills or Core Skill components in this unit.

Context for delivery

If this unit is delivered as part of a group award, it is recommended that it should be taught and assessed within the subject area of the group award to which it contributes.

This is an entry level unit. This unit is likely to be the learner's first exposure to formal cyber security.

The target cohort is school and college learners, particularly school learners.

Equality and inclusion

This unit specification has been designed to ensure that there are no unnecessary barriers to learning or assessment. The individual needs of learners should be taken into account when planning learning experiences, selecting assessment methods or considering alternative evidence.

Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**.

National Unit Specification: Statement of standards

Unit title: Cyber Security (SCQF level 3)

Acceptable performance in this unit will be the satisfactory achievement of the standards set out in this part of the unit specification. All sections of the statement of standards are mandatory and cannot be altered without reference to SQA.

Outcome 1

Secure a device.

Performance criteria

(a) Identify the hardware used to store data, locally and remotely.
(b) Recognise the risk to a device when it connects to the internet.
(c) State how to react when devices experience a malware attack.
(d) Describe how to restore a device when recovering from a malware attack.
(e) State why software updates are important.
(f) Identify the operating system used on a device.
(g) State a vulnerability in software and explain why updates are needed.
(h) State the name of a command line operating system.
(i) Write commands for a command line operating system.

Outcome 2

Identify the basics of networking.

Performance criteria

(a) Identify the differences between the internet and World Wide Web.
(b) Identify the different parts of a URL.
(c) Link a protocol and service to its related ports.
(d) Identify an IP address on a device.
(e) Identify the devices connected to a network.
(f) State basic information about a VPN and how it secures your network.
(g) Identify the parts of a data packet.

Outcome 3

Secure personal data.

Performance criteria

(a) Enable two factor Authentication (2FA) on an online account.
(b) State why a password or passcode are needed to access online accounts.
(c) Identify the benefits of enabling two factor Authentication (2FA) on online accounts.
(d) State data an online account will gather when you consume content and identify how to limit the data collected.
(e) State basic information on what internet cookies are, and how they are used to track what a person is consuming.
(f) Identify a BOT on social media platforms.
(g) Explain why encryption is used.

National Unit Specification: Statement of standards (continued)

Unit title: Cyber Security (SCQF level 3)

Evidence requirements for this unit

Evidence is required to demonstrate that learners have achieved all outcomes and performance criteria. The evidence for this unit may be written, oral, or a mix of both. Evidence may be stored in a range of media, including audio and video. Assessors should use their professional judgement, subject knowledge, experience, and understanding of their learners, to determine the most appropriate ways to generate evidence.

This unit has been written in a logical way to enable the assessment to be carried out outcome by outcome. To generate evidence, learners must use a range of security features on a device or online account.

Learner must provide knowledge and product evidence.

Outcomes 1 to 3 — the knowledge evidence relates to explicit and implicit knowledge contained within all outcomes. Minimal evidence, required to infer competence, is acceptable.

Outcome 1 performance criterion (h) — naming an operating system must include a command line operating system.

Outcome 1 performance criterion (i) — learners must use at least three commands for a command line operating system.

Outcome 2 performance criteria (b) — when identifying the different parts of a URL this must include the protocol and domain extension.

Outcome 2 performance criterion (c) — learners must have the knowledge to link a minimal of four ports to their service and protocol.

Outcome 2 performance criterion (e) — the evidence must comprise of a diagram of a network including a minimum of 5 devices and a router.

Outcome 2 performance criterion (g) — when learners are required to identify the parts of a data packet, they are only required to have knowledge of the header and payload of a data packet.

Outcome 3 performance criterion (b) — learners are required to produce evidence that they are competent at creating strong passwords using latest guidance form the National Cyber Security Center. (NCSC).

Outcome 3 performance criterion (d) — when stating pieces of data an online account will gather, learners are required to identify two pieces of observed data not personal data.

National Unit Specification: Statement of standards (continued)

Unit title: Cyber Security (SCQF level 3)

Outcome 3 performance criterion (g) — when learners are explaining why encryption is used by apps, they are required have basic understanding Public Key Encryption is used when you see the padlock and https in your web browser address bar. End to End Encryption (E2EE) is a more secure than Public Key Encryption as your data is encrypted on your phone or computer. It is important that when leaners are asked to identify a BOT on social media, they have the knowledge to identify both good and bad BOTs.

Sampling is permissible when testing is used. The sampling frame must always include command line interface commands, data packet header, IP address, End to End Encryption (E2EE) and how to react and recover if your device is infected with malware.

The evidence for practical competences may be produced on any appropriate medium (text, audio or video or a combination of these). It is permissible to record successful demonstration of practical competences using a checklist (signed by the assessor).

Given the level of this unit, the amount of evidence and corresponding time spent on assessment should be minimised but sufficient to satisfy the requirements set out within this document.

The evidence may be produced over an extended period of time in loosely controlled conditions. Authentication is required when the evidence is produced in lightly controlled conditions.

National Unit Support Notes

Unit title: Cyber Security (SCQF level 3)

Unit support notes are offered as guidance and are not mandatory.

While the exact time allocated to this unit is at the discretion of the centre, the notional design length is 40 hours.

Guidance on the content and context for this unit

The purpose of this unit is to introduce learners to the basics of cyber security. There is no previous knowledge or experience required, although a familiarity with computer hardware and software is assumed. Any appropriate hardware and software can be used during this unit, although it is anticipated that most learners will use the internet and a web browser.

Given the level of this unit, a minimalist approach should be taken to the performance criteria. the focus of the unit is on practical competencies, the unit also seeks to provide basic knowledge and understanding of some key principals of cyber security.

Outcome 1

This outcome ensures the learners are aware that their common digital devices, such as, laptops, smartphones, and tablets have the ability to store data and connect to the internet, which make their devices vulnerable to cyber-attacks.

Performance criterion (b) states learners should be able to recognise the risk to a device when it connects to the internet. This could be done by matching names of common malware to descriptions of them. Performance criterion (d) states learners should be able to describe how to restore a device when recovering from a malware attack. This could be naming the steps to get data from cloud storage to a new device for example when learners purchase a new smartphone, they must get all the images and contacts from their cloud to the new device. Performance criterion (i) states learners should be able to state basic commands for a command line operating system. This could be done by matching common commands such as “dir” or “cd” to descriptions of them.

Outcome 2

This outcome provides the basic understanding of networking, which ensures the learners see the Internet and the World Wide Web as different. It is important that learners have the ability to distinguish between the internet, World Wide Web and other online services such as email. This can be achieved through the basic networking concepts such as IP addressing and linking to a URL domain name.

National Unit Support Notes (continued)

Unit title: Cyber Security (SCQF level 3)

Performance criterion (c) states learners should be able to link a protocol and service to its related ports. This could be achieved by matching names of common ports to descriptions of the service, for example, port 80 = http is the default network port used to send and receive unencrypted web pages. Performance Criterion (d) states learners should be able to identify an IP address on a device. This can be done by learners showing the assessor any IP address of any device for example, a smartphone. Performance criterion (g) states learners should be able to identify the parts of a data packet. Learners are not required to understand anything further than the header contains the sender's IP address, the destination IP address and what number they are in the sequence of packets.

Outcome 3

This outcome ensures the learners must be aware of steps they can take to secure their online accounts such as email and social media.

Performance criterion (e) states learners should be able to state basic information on what internet cookies are and how they are used to track what a person is consuming. Learners are not required to understand anything further than tracking cookies: these files contain a history of your actions across different websites. Performance criterion (g) states learners should be able to explain why encryption is used. Learners are not required to understand anything further than messages are encrypted before they leave the phone or computer and are only decrypted once they reach the intended receiver's phone or computer.

Guidance on approaches to delivery of this unit

A practical hands-on approach to learning should be adopted to engage learners and exemplify key concepts. However, all practical activities should be underpinned with appropriate knowledge before learners commence these activities.

An important aspect of this unit is that learners develop an appropriate technical vocabulary. Terminology and underpinning knowledge should be introduced in a practical context. The actual distribution of time between outcomes is at the discretion of the centre. However, one possible approach is to distribute the available time as follows:

Outcome 1: 13 hours.
Outcome 2: 14 hours.
Outcome 3: 13 hours.

Guidance on approaches to assessment of this unit

Evidence can be generated using different types of assessment. The following are suggestions only. There may be other methods that would be more suitable to learners.

Evidence can be generated using open-book conditions and using the outcome-by-outcome approach to assessment. In this method questions are used to gather evidence that the learner has achieved the knowledge element for each of the three outcomes or a check list can be used to ensure the learner has achieved the performance criteria.

National Unit Support Notes (continued)

Unit title: Cyber Security (SCQF level 3)

The following are suggestions only. There may be other methods that would be more suitable to learners and the type of learner assessment activities will vary depending on the resources available.

Centres are reminded that prior verification of centre-devised assessments would help to ensure that the national standard is being met. Where learners experience a range of assessment methods, this helps them to develop different skills that should be transferable to work or further and higher education.

A traditional approach to assessment might involve the use of a test (for knowledge evidence) and a practical exercise (for product evidence). The test could take the form of a selected response test, comprising 25 questions, with an appropriate pass mark. This test should be taken under open-book conditions. This question can be taken from the three booklets produced by Education Scotland to support the delivery of this unit The practical exercise would require learners to demonstrate the use of the ping command. Command line interface and enabling Two-factor authentication (2fa) on any account.

An alternative approach to assessment could involve the use of a portfolio, which would contain knowledge and product evidence. If this approach is taken, evidence for all performance criteria would be required.

The evidence may be produced over an extended period of time in loosely controlled conditions. Authentication is required when the evidence is produced in lightly controlled conditions. Assessors must ensure that all the performance criteria for these outcomes are covered by learners' own evidence.

Opportunities for e-assessment

E-assessment may be appropriate for some assessments in this unit. By e-assessment we mean assessment which is supported by Information and Communication Technology (ICT), such as e-testing or the use of e-portfolios or social software. Centres which wish to use e-assessment must ensure that the national standard is applied to all learner evidence and that conditions of assessment as specified in the evidence requirements are met, regardless of the mode of gathering evidence. The most up-to-date guidance on the use of e-assessment to support SQA's qualifications is available at **www.sqa.org.uk/e-assessment**.

Opportunities for developing Core and other essential skills

The unit provides an opportunity to develop Core Skills in Communication, Information and Communication Technology (ICT), Problem Solving and Working with Others.

The unit covers the basics of device security, networking and personal data security. These topics will enable the learner to better understand how to recognise, react and recover from cyber incidents they experience on their personal devices.

History of changes to unit

Version	Description of change	Date

Unit template: June 2017

General information for learners

Unit title: Cyber Security (SCQF level 3)

This section will help you decide whether this is the unit for you by explaining what the unit is about, what you should know or be able to do before you start, what you will need to do during the unit and opportunities for further learning and employment.

This section will help you decide whether this is the unit for you by explaining what the unit is about, what you should know or be able to do before you start, what you will need to do during the unit and opportunities for further learning and employment.

This unit provide learners with a basic understanding of how the internet works.

In outcome 1 you will gain a good understanding of how to recognise, react and recover from the risks your personal device faces when it connects to the internet.

In outcome 2 you will acquire knowledge on the basics of networking such as IP address and data packets work.

In outcome 3 you will identify how data is gathered while you're using the World Wide Web and internet.

The unit covers the following knowledge and skills:

Knowledge	**Skills**
♦ Data storage local and remote. ♦ Risks to devices connected to the internet. ♦ operating system. ♦ software vulnerability. ♦ Difference between Internet and the World Wide Web. ♦ Uniform Resource Locator (URL). ♦ Internet Protocol (IP) addresses. ♦ Domain Name Servers. ♦ Data packets. ♦ A Virtual Private Network. ♦ Virtual Private Network (VPN. ♦ Cookies used by web sites. ♦ Encryption.	♦ What to do if your devices experience a malware attack. ♦ what you should and shouldn’t do to keep your device safe. ♦ How to update software. ♦ Command line operating system. ♦ Ports, Protocols and Services. ♦ Draw home or school network. ♦ Create a strong password. ♦ activate Two-factor authentication (2fa). ♦ Identify a BOT.

You can be assessed in a variety of ways, which may include a short test of your knowledge and a series of practical exercises or using the portfolio approach to assessment using the resources created by Education Scotland.

Learners may wish to progress to the National Progression Award in Cyber Security at level 4.