# National Unit specification

## General information

## Unit title: Cyber Security Fundamentals (SCQF level 4)

## Unit code: H9T5 44

**Superclass:** CC

**Publication date:** October 2015

**Source:** Scottish Qualifications Authority

**Version:** 01

## Unit purpose

The purpose of this Unit is to introduce learners to the fundamental concepts of, and basic skills in, cyber security so that they are able to adhere to **cyber hygiene**, in a personal capacity, and maintain **cyber resilience** in a vocational capacity. The Unit is aimed at the **beginner**, with no previous knowledge or experience of online safety or data security. It is suitable for all learners.

The Unit introduces a range of basic knowledge and skills relating to cyber security. The learner will gain a basic understanding of the importance of online safety; common threats to individuals, businesses and nations; and preventative methods that can be used to reduce the risk of cyber-attacks. Learners will gain practical experience of protecting personal digital devices, such as a smartphone or personal computer. The role of social engineering in cyber-attacks and the implications of cyber threats for personal privacy are explored.

On completion of this Unit, learners may progress to the National Progression Award in Cyber Security at SCQF level 4 or related qualifications.

## Outcomes

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

1 State common cyber security threats to individuals, businesses and nations.
2 Describe routine defensive measures to minimise the risks posed by these threats.
3 Secure a digital device for personal use.

## National Unit specification: General info

**Unit title:** Cyber Security Fundamentals (SCQF level 4)

## Credit points and level

1 National Unit credit at SCQF level 4: (6 SCQF credit points at SCQF level 4)

## Recommended entry to the Unit

No previous knowledge of computers or the Internet 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.

The Assessment Support Pack (ASP) for this Unit provides assessment and marking guidelines that exemplify the national standard for achievement. It is a valid, reliable and practicable assessment. Centres wishing to develop their own assessments should refer to the ASP to ensure a comparable standard. A list of existing ASPs is available to download from SQA's website **(http://www.sqa.org.uk/sqa/46233.2769.html)**.

## 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 Fundamentals (SCQF level 4)

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

State common cyber security threats to individuals, businesses and nations.

### Performance Criteria

(a) State the growth of digital technologies, digital networks and digital data.
(b) State the scale of, and reasons for, the growth of cybercrime.
(c) State the potential motivations of malicious hackers.
(d) State common vulnerabilities in digital devices and digital networks including social engineering techniques.
(e) State how these vulnerabilities can be used to attack individuals, businesses and nations.
(f) State the potential risks to personal privacy posed by these vulnerabilities.
(g) Use terminology correctly in the context of cyber security threats.

## Outcome 2

Describe routine defensive measures to minimise the risks posed by these threats.

### Performance Criteria

(a) Describe the security measures that can be taken to reduce vulnerabilities in terms of actions, devices, procedures or techniques.
(b) Describe personal behaviours that minimise the risk of a successful attack.
(c) Describe the ways in which attacks can be detected.
(d) Describe the ways in which individuals and organisations can respond to attacks.
(e) Describe contemporary legislation relating to the protection of data, computer systems and personal privacy.
(f) Use terminology correctly in the context of cyber security defence.

## Outcome 3

Secure a digital device for personal use.

### Performance Criteria

(a) Identify the hardware and software security features in personal digital devices.
(b) Identify the types of vulnerabilities in personal digital devices.
(c) Identify defensive measures to minimise the risk of an attack on personal digital devices.
(d) Configure the security features in personal digital devices.
(e) Test the security of personal digital devices.

## National Unit specification: Statement of standards (cont)

## Unit title: Cyber Security Fundamentals (SCQF level 4)

### Evidence Requirements for this Unit

Assessors should use their professional judgement, subject knowledge, experience, and understanding of their learners to determine the most appropriate ways to generate evidence and the conditions and contexts in which they are used.

Evidence is required to demonstrate that learners have achieved all Outcomes and Performance Criteria. Sampling may be used in certain circumstances (see below) where the sample is sufficiently random and robust to clearly infer competence in the complete domain.

The evidence for all Outcomes in this Unit may be written, oral or a combination of these. Evidence may be captured, stored and presented in a range of media (including audio and video) and formats (analogue and digital). Particular consideration should be given to digital formats and the use of multimedia.

Given the level of this Unit, the amount of evidence, and corresponding time spent on assessment, should be minimised but sufficient to satisfy the Performance Criteria.

Whenever possible, evidence should be a naturally occurring by-product of teaching and learning. However, it must be produced by the learner. Authentication must be used where this is uncertain.

Evidence is required for two types of competence: evidence of cognitive competence (knowledge and understanding) and evidence of practical competence (practical abilities).

The evidence of **cognitive competence** will relate to **Outcome 1 (all Performance Criteria), Outcome 2 (all Performance Criteria) and Outcome 3 (Performance Criteria (a), (b) and (c))**. Evidence may be sampled across this knowledge domain so long as the sample is unknown, and unpredictable, to the learner and large enough to infer competence across the whole domain. Where sampling is used to assess the learner's knowledge and understanding, an appropriate pass mark should be set. The evidence must demonstrate that the candidate has a grasp of cyber security terminology (Outcome 1, PC (g) and Outcome 2, PC (f)) irrespective of the sampling frame.

The evidence of **practical competence** will relate to **Outcome 3 (Performance Criteria (d) and (e))** and may take any appropriate form. Candidates must secure **at least one** personal digital device against the most common vulnerabilities. The security measures should be routine but sufficient to defend the personal device from these common attacks.

Evidence of practical competence may be produced over an extended period of time; but where it is generated without supervision some means of authentication must be carried out. The *Guide to Assessment* provides advice on methods of authentication.

The Guidelines on Approaches to Assessment (see the Support Notes section of this specification) provide specific examples of instruments of assessment.

## National Unit Support Notes

## Unit title: Cyber Security Fundamentals (SCQF level 4)

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 equip learners with a **basic** understanding of the cyber security landscape and gain **elementary** skills in protecting against common security threats.

This is a **general purpose** Unit, designed for the **non-specialist**. It is intended for a wide range of learners who require to know the **fundamentals** of Internet safety and cyber security. At this level (SCQF Level 4), treatment of each topic should be straight-forward and non-complex. It is **not** the intention to create technical experts, although learners are required to develop their vocabulary of technical terminology and develop good behaviours and routines.

The presentation of material should seek to strike a balance between raising awareness of cyber threats and encouraging the use of digital technology. It is not the intention of this Unit to deter learners from engaging with technology and networks.

The Unit has three Outcomes. Outcomes 1 and 2 relate to cyber-attacks and cyber defence respectively. Outcome 3 relates to applying this knowledge to protect a personal device such as a smartphone or laptop computer.

**Outcome 1**

This Outcome relates to cyber security threats. These should be related to threats to individuals, threats to businesses, and threats to nations.

Learners may be unaware of the exponential growth of digital data (**performance criterion a**) and the scale of cyber-crime (**performance criterion b**), and how these are linked. It is recommended that case studies are used to illustrate the growth of cyber-crime. It should be pointed out to learners that the frequency and scale of cyber-crime is under-reported, and the reasons for this explained.

The motivations of malicious hackers should be explained (**performance criterion c**). These will include personal (including revenge attacks), financial, ethical and military motivations (ethical motivations may be malicious if they involve the imposition of ethics on a third party). The growth, and significance, of cyber warfare may have to be explained.

## National Unit Support Notes (cont)

## Unit title: Cyber Security Fundamentals (SCQF level 4)

Common vulnerabilities (**performance criterion d**) include: brute force, backdoors, denial-of-service attacks, direct-access attacks, eavesdropping, spoofing, tampering, privilege escalation, social engineering attacks, and trojans. Special consideration should be given to social engineering attacks since these are subtler than technical vulnerabilities and harder to defend against.

These vulnerabilities should be linked with attacks on individuals, businesses and nations (**performance criterion e**). For example, brute force and behavioral (social engineering) attacks are more common (and more likely to succeed) against individuals than governments.

The importance of personal privacy should be discussed and the potential costs of breaches of privacy explained (**performance criterion f**). Case studies could be used to illustrate these points. Breaches of privacy can used to blackmail victims for financial, political or military objectives.

Common terminology relating to cyber-attacks should be introduced during this Outcome (**performance criterion g**).

**Outcome 2**

This Outcome relates to cyber security defences. It involves looking at ways of protecting systems from the vulnerabilities stated in Outcome 1. It should be made clear to learners that no system can be guaranteed to be 100% secure irrespective of the defensive measures taken. Computer security is about risk management.

The counter measures should be described in terms of actions, devices, procedures and techniques (**performance criterion a**). Learners should appreciate that security can be implemented in hardware software, processes and behaviours. The focus should be on common methods of security such as password selection, two factor authentication and encryption. This is linked to personal behaviours that reduce the likelihood of a successful attack (**performance criterion b**). The use of social engineering to compromise computer systems will have to be carefully introduced, and counter measures explained.

The detection of (**performance criterion c**) and response to (**performance criterion d**) cyber-attacks should be described. The difficulties in responding to a cyber-attack should be explained (which include their global nature and lack of technical knowledge in many victims/target organisations).

The legislation relating to cyber security includes legislation relating to data protection, computer security and personal privacy (**performance criterion e**). There is an opportunity to discuss any perceived gaps in contemporary legislation and the tension between personal privacy and national security.

Common terminology relating to cyber defence should be introduced during this Outcome (**performance criterion f**).

## National Unit Support Notes (cont)

## Unit title: Cyber Security Fundamentals (SCQF level 4)

**Outcome 3**

This Outcome applies the learner's knowledge, gained as part of Outcomes 1 and 2, to the defence of a personal digital device such as a smartphone, tablet or personal computer. It should be emphasised that an increasing number of devices are being made 'smart', increasing the risk of cyber-attack on devices other than recognisable computer systems (such as cars and domestic devices). The Internet of Things (IoT) will significantly expand this threat into a huge range of devices.

Learners are required to appreciate the routine security features commonly found in typical digital devices (**performance criterion a**). In the context of a smartphone, this would include hardware features (such as fingerprint scanning and facial recognition) and software features (such as lock screens and handset encryption). It would be worthwhile to distinguish between the security features provided by the operating system and those provided by third parties.

The specific vulnerabilities in each type of digital device should be explored (**performance criterion b**). For example, device theft (and the resulting data leakage) and network spoofing (creating rogue network access points imitating wi-fi or GSM networks) are more common in smartphones than laptops.

Being aware of the specific vulnerabilities in each type of device will help learners appreciate the most important defensive measures that they should take for each type of device (**performance criterion c**).

Learners are required to secure (**performance criterion d)** and test the security (**performance criterion e**) of a personal digital device. In the case of a smartphone this would involve lock screen configuration, sim lock, encryption, device administration, limitations on app installation and physical security.

## Guidance on approaches to delivery of this Unit

The Unit may be delivered in a variety of ways. It is suggested that the Outcomes are taught in the order which they appear as this builds up a body of knowledge on the subject. All Outcomes lend themselves to group, paired or individual work.

While the time spent on each Outcome is at the discretion of each teacher, an approximate guide to the distribution of time across Outcomes is:

Outcome 1: 15 hours
Outcome 2: 15 hours
Outcome 3: 10 hours.

The use of case studies is recommended to illustrate a number of key learning objectives. Lessons can be learned (and Outcomes contextualised) by using recent breaches of data security to explore their vulnerabilities, the reasons for the attack, the reasons for its success, and its consequences.

## National Unit Support Notes (cont)

**Unit title:** Cyber Security Fundamentals (SCQF level 4)

## 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.

Centres are reminded that prior verification of centre-devised assessments would help to ensure that the national standard is being met.

A traditional approach to assessment would involve the use of a test for Outcome 1 and Outcome 2, and a practical activity for Outcome 3. The test would combine the knowledge involved in Outcome 1 and Outcome 2, and could take the form of a selected response test involving multiple choice questions. An appropriate pass mark would be set. For example, the test could sample from the knowledge in Outcome 1 and Outcome 2 by posing 40 multiple choice questions (with four options) with a pass mark of 25 (guessing alone should produce, on average, 10 correct responses requiring an additional 15 correct responses to set a 'true' 50% pass mark). The duration could be 60 minutes.

The practical evidence would comprise an observation checklist to confirm that the candidate has configured and tested the security on at least one personal digital device. The device should be protected from the most common threats. For example, in the case of a smartphone this would include theft of device, unauthorised access and network spoofing.

A more contemporary approach to assessment would be the creation and maintenance of a web log, which would record candidate activity throughout the Unit. This would record, on a daily or weekly basis, what candidates learn and what they do. However, their posts would have to satisfy the relevant Performance Criteria. Practical activities could also be recorded *via* the blog. When practical activity is recorded on a blog (narratively), authentication could involve a photograph or video of candidate activity (this could be included as part of their post).

Another approach would involve the creation and maintenance of an e-portfolio. The e-portfolio would include all of the identifications and descriptions necessary to satisfy the criteria relating to cognitive competencies, together with digital artefacts that provide evidence of their practical abilities. Digital artefacts would include screenshots, digital photographs, audio and video recordings, *etc.* that collectively evidence candidates' skills. Some form of authentication would be required. This could be a simple statement of originality, signed by the candidate and the assessor.

## 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**.

## National Unit Support Notes (cont)

**Unit title:** Cyber Security Fundamentals (SCQF level 4)

## Opportunities for developing Core and other essential skills

In this Unit, learners will have the opportunity to develop some of the following Core Skills:

- *Communication* (SCQF level 4)
- *Numeracy* (SCQF level 4)
- *Information and Communication Technology (ICT)* (SCQF level 4)
- *Problem Solving* (SCQF level 4)

## History of changes to Unit

| Version | Description of change | Date |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## General information for learners

## Unit title: Cyber Security Fundamentals (SCQF level 4)

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.

You will benefit from this Unit if you want to find out more about cyber-crime and how to protect yourself from it. No previous knowledge or experience of computers is required before you undertake this Unit. You may also find this Unit of benefit if you are considering a career in cyber security or wish to protect your business from cyber-attacks.

This Unit covers the basics of cyber security. You will learn about the main threats to computer and network systems and the best ways to reduce the chances of these threats succeeding. You will learn how to keep yourself safe online by using hardware and software and developing good habits. You will find out about recent examples of computer crime — what happened, why it happened and the impact of the crimes on people's lives.

The cyber threats will relate to individuals, businesses and entire countries. You will learn about threats to you as an individual, threats to businesses, and threats to nations, including cyber warfare.

The Unit also covers the law as it relates to cyber-crime and personal privacy.

You will learn how to protect a personal digital device (such as a smartphone or tablet or laptop computer) from a range of possible attacks.

The assessment is straight-forward and will not take much time. It may consist of a short test and a practical activity.

You can progress to the National Progression Award in Cyber Security at SCQF level 4 on completion of this Unit if you wish to improve your knowledge and skills in this area.