Higher National Unit Specification

General information for centres

Unit title: Internet: Web Technology and Security

Unit code: DX42 35

Unit purpose: Internet security and privacy threats are one of the biggest concerns on the Internet. This Unit develops the candidate's knowledge and understanding of how a user connects to the Internet and communicates with the network, and achieves an appreciation of security concepts and privacy threats.

On completion of the Unit the candidate should be able to:

1 Understand the various technologies associated with the Internet.
2 Identify privacy, intrusion and protection.
3 Understand security threats and protection.
4 Understand digital cryptography/signatures.

Credit points and level: 2 HN Credits at SCQF level 8: (16 SCQF credit points at SCQF level 8*).

**SCQF credit points are used to allocate credit to qualifications in the Scottish Credit and Qualifications Framework (SCQF). Each qualification in the Framework is allocated a number of SCQF credit points at an SCQF level. There are 12 SCQF levels, ranging from Access 1 to Doctorates.*

Recommended prior knowledge and skills: Access to this Unit is at the discretion of the centre.

Core Skills: There are no opportunities to develop Core Skills 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.

Assessment: Outcome 1 will be assessed by a report of approximately 1,200 words which may be based on a project, case study or scenario. This assessment is open-book.

Outcomes 2 and 3 will each be assessed by 20 multiple choice questions testing knowledge and/or skills carried out in closed-book conditions conducted under supervised conditions. Candidates must achieve 60% correct responses in each of the Outcomes.

General information for centres (cont)

Outcome 4 (part 1) will be assessed by five extended response questions to be completed within a specified time. The assessment will be conducted under supervised conditions and completed in one hour. The evidence of this Outcome (part 1) will be collected in the response to a representative set of five questions each approximately completed in 150 words.

Outcome 4 (part 2) will be assessed by a written report of approximately 1,000 words testing the candidate's knowledge of the subject area, this assessment may be based on a project, case study or scenario. This assessment is open-book.

Assessors must assure themselves of the authenticity of each candidate's submission. A candidate is encouraged to use the Internet in any research, etc, however, the evidence produced **must** be the candidate's own written words.

Some of the assessment may be produced using e-assessment. This may take the form of e-testing (for knowledge and understanding and/or e-portfolios (for practical abilities)). There is no requirement to seek prior approval if you wish to use e-assessment for either of these purposes so long as the normal standards for validity and reliability are observed. Please see the following SQA publications for further information on e-assessment: (1) "SQA Guidelines on Online Assessment for Further Education" (March 2003) and (2) "Assessment & Quality Assurance in Open & Learning Distance Learning" (Feb 2001).

If a centre is presenting Outcome 2 and 3 on-line the following assessment methods, where appropriate, may be selected:

- multiple-choice
- drag and drop
- multiple response
- mix and match
- a combination of the above

It is expected that the questions will be of the multi-choice variety. Centres may consider the use of alternative question types, particularly if using Computer Assisted Assessment approaches. However, care should be taken that the questions are valid and at an appropriate level. The use of simple true/false question responses is unlikely to achieve this.

Higher National Unit specification: statement of standards

Unit title: Internet: Web Technology and Security

Unit code: DX42 35

The sections of the Unit stating the Outcomes, knowledge and/or skills, and Evidence Requirements are mandatory.

Where evidence for Outcomes is assessed on a sample basis, the whole of the content listed in the knowledge and/or skills section must be taught and available for assessment. Candidates should not know in advance the items on which they will be assessed and different items should be sampled on each assessment occasion.

Outcome 1

Understand the various technologies associated with the Internet

Knowledge and/or skills

- Network Connections
- Internet Protocols and Switching Techniques

Evidence Requirements

Evidence will be gathered in the form of a report in which the candidate will accurately describe:

- Network Connections: the purposes and basic operation of network connections including, modems, broadband Internet connections, Digital Subscriber Line (DSL), wireless connection, PDAs
- Internet Protocols and Switching Techniques: TCP/IP, HTTP, ARP, ICMP, PPP, SLIP, SMTP, POP3, UUCP and UDP/IP, IP Address, Static Addressing, Dynamic addressing, TCP, FTP, Gateway, Routers, Packets and Network Address Translation

Evidence for the knowledge and/or skills in this Outcome will cover all the knowledge and skills bullet points. The evidence presented for this assessment will be in the form of a report of approximately 1,200 words which will be based on a project, case study or scenario.

The candidate's response can be judged to be satisfactory where the evidence provided is sufficient to meet the requirements as follows:

- all items to be covered
- sample of a minimum of eight items

The questions must change on each assessment occasion.

Assessors must assure themselves of the authenticity of each candidate's submission. A candidate is encouraged to use the Internet in any research, etc., however, the evidence produced must be the candidate's own written words.

Higher National Unit specification: statement of standards (cont)

Unit title: Internet: Web Technology and Security

Assessment guidelines

There may be an opportunity for a candidate to be assessed on-line subject to meeting the prescribed assessment conditions.

Outcome 2

Identify Privacy, Intrusion and Protection

Knowledge and/or skills

- Privacy Intrusion
- UserID Password
- Encryption

Evidence Requirements

Candidates will need evidence to demonstrate their knowledge and/or skills by showing that they can describe:

- Privacy intrusions including: spam, spyware, cookies and pop-up-ads
- User ID and passwords: access control covering authentication, authorisation and audit
- Encryption: symmetric and asymmetric

This Outcome will each be assessed by 20 multiple choice questions testing a representative sample of the knowledge and/or skills carried out in closed-book conditions conducted under supervised conditions.

The questions must change on each assessment occasion.

Candidates are required to answer at least 60% of the questions correctly. Different assessment should be used for reassessment purposes.

Assessment guidelines

Some of the assessment may be produced using e-assessment. This may take the form of e-testing (for knowledge and understanding and/or e-portfolios (for practical abilities)). There is no requirement to seek prior approval if you wish to use e-assessment for either of these purposes so long as the normal standards for validity and reliability are observed. Please see the following SQA publications for further information on e-assessment: (1) *SQA Guidelines on Online Assessment for Further Education* (March 2003) and (2) *Assessment & Quality Assurance in Open & Distance Learning* (Feb 2001).

If the centre is presenting this Outcome on-line the following assessment methods, where appropriate, may be selected:

- multiple-choice
- drag and drop
- multiple response
- mix and match
- a combination of the above

It is expected that the questions will be of the multi-choice variety. Centres may consider the use of alternative question types, particularly if using Computer Assisted Assessment approaches. However, care should be taken that the questions are valid and at an appropriate level. The use of simple true/false question responses is unlikely to achieve this.

Outcome 3

Understand security threats and protection

Knowledge and/or skills

- Browser hijacking
- Identify intentional misuses of a computer
- Identify protection for a computer
- e-mail threats and protection

Evidence Requirements

Candidates will need to demonstrate their knowledge and/or skills by showing that they understand:

- Browser hijacking: which should include spyware, adware, malware and pop-up-ads
- Identify security threats including: instant messaging, sniffers, worms, trojans, hackers/crackers, credit card fraud, wireless network hackers
- Identify protection for a computer including: filters, firewalls, anti-virus software and anti-spyware
- Identify e-mail threats and protection including: phishing, spoofing and viruses

This Outcome will be assessed by 20 multiple choice questions testing knowledge and/or skills carried out in closed-book conditions conducted under supervised conditions.

The questions must change on each assessment occasion.

Candidates are required to answer at least 60% of questions correctly. Different assessments should be used for re-assessment purposes.

Assessment guidelines

Some of the assessment may be produced using e-assessment. This may take the form of e-testing (for knowledge and understanding and/or e-portfolios (for practical abilities)). There is no requirement to seek prior approval if you wish to use e-assessment for either of these purposes so long as the normal standards for validity and reliability are observed. Please see the following SQA publications for further information on e-assessment: (1) *SQA Guidelines on Online Assessment for Further Education* (March 2003) and (2) *Assessment & Quality Assurance in Open & Distance Learning* (Feb 2001).

If a centre is presenting this Outcome on-line the following assessment methods, where appropriate, may be selected:

- multiple-choice
- drag and drop
- multiple response
- mix and match
- a combination of the above

It is expected that the questions will be of the multi-choice variety. Centres may consider the use of alternative question types, particularly if using Computer Assisted Assessment approaches. However, care should be taken that the questions are valid and at an appropriate level. The use of simple true/false question responses is unlikely to achieve this.

Outcome 4

Understand digital cryptography/signatures

Knowledge and/or skills

- Private/public key
- Authentication
- Signature generation
- Common protocols
- Types of attacks, certification

Evidence Requirements

Candidates will need evidence to demonstrate their knowledge and/or skills by showing that they can describe:

- Private/public key (different types) (advantages/disadvantages), RSA/DSA encryption
- Authentication, MD5 128 bit, SHA-1 106 bit, MAC, Data Integrity-Hashing functions
- Signature generation algorithm, verification algorithm
- Common protocols, SSL, TLS, HTTPS
- Types of attacks: know-message, chosen-message, adaptive, man in the middle (MITM)

Higher National Unit specification: statement of standards (cont)

Unit title: Internet: Web Technology and Security

Evidence for the knowledge and/or skills in this Outcome will cover all of the knowledge and skills bullet points. The evidence presented for this assessment will be in two parts.

Part 1 — five extended response questions (covering encryption, security protocols, digital signatures, digital certificates and types of attacks). This assessment is closed-book.

Part 2 — a report of approximately 1,000 words (covering the various technologies used). This assessment is open-book.

The candidate's repose can be judged to be satisfactory where the evidence provided is sufficient to meet the requirements for each item in the above list.

Assessors must assure themselves of the authenticity of each candidate's submission. A candidate is encouraged to use the internet in any research, etc, however, the evidence produced must be the candidate's own written words.

Administrative Information

Unit code: DX42 35

Unit title: Internet: Web Technology and Security

Superclass category: CB

Original date of publication: June 2006

Version: 01

History of Changes:

Version	Description of change	Date

Source: SQA

SQA acknowledges the valuable contribution that Scotland's colleges have made to the development of Higher National qualifications.

Additional copies of this Unit specification can be purchased from the Scottish Qualifications Authority. Please contact the Customer Contact Centre for further details, telephone 0845 279 1000.

Higher National Unit specification: support notes

Unit title: Internet: Web Technology and Security

This part of the Unit specification is offered as guidance. The support notes are not mandatory.

While the exact time allocated to this Unit is at the discretion of the centre, the notional design length is 80 hours.

Guidance on the content and context for this Unit

This Unit is designed to provide the candidate with a broad knowledge of the process of preventing and detecting unauthorised use of a computer.

Outcome 1

This Unit provides the candidate with the understanding of how a computer communicates over the network. This Unit starts off by understand how a computer connects to the Internet. The candidate should be able to understand the different ways this can be achieved.

Bandwidth should be discussed by introducing the technology for enabling high speed information to end users over ordinary copper telephone lines. xDSL making reference to variations of DSL eg ADSL, HDSL, etc. Wireless network connection should be discussed and the standards involved particularly Bluetooth, Digital Enhanced Cordless Telecommunications, IEEE 802.11 and WiFi. (Note, these are the current standards that are available and these should be replaced with new standards as new technology is introduced). Elements of hardware should be introduced although this should be kept to a minimum as the focus should be on the network connection and how this can be achieved through ISPs, etc.

Discussion **must** also include PDAs (personal digital assistants) and how it can communicate with each other and with desktop computers using infra-red signals. While in communication with each other they form a small local network.

A protocol is a specification that allows computers to communicate over the Internet. Internet addressing is required to send data over the Internet. Candidates should understand that IP addresses are typically shown as four numbers separated by decimal points. Candidates should be able to describe the different types of IP addressing. Static IP addressing is when an Internet Service Provider (ISP) permanently assigns one or more IP addresses and Dynamic IP is when the ISP can change the IP address over time. The candidate should be able to describe if there is any disadvantages or benefits of using Dynamic IP addressing.

Candidate should also become familiar with TCP/IP and UDP, routers, gateway and packets Network Address Translation (NAT) provides a way to hide the IP address of a private network candidates should be able to explain how this is achieved.

Understanding about protocols in this Outcome should give your candidate a good understand of how computer communication over the Internet. There is no need to cover all of the protocols listed in the Evidence Requirements, however, a candidate has to cover at least eight of the items listed and they must address both Internet Protocols and Switching Techniques.

Higher National Unit specification: support notes (cont)

Unit title: Internet: Web Technology and Security

Outcome 2

This Outcome deals with privacy intrusion and protection of users on the Internet. Current methods of who to deal with unwanted spam, cookies and pop-up advertisements should be reviewed by the candidate carrying out research (eg the Internet). Items to be discussed should include spamming though junk mail (ie unsolicited, unwanted, irrelevant, or inappropriate messages) and junk newsgroup postings. Spyware, malware and adware software should be explained and discussed in line with current happenings at that time.

UserID and passwords should be described as a common access method of accessing secure sites. The importance of keeping these details secure, and the problems that could be created by revealing this information, should be discussed.

A student should appreciate the method of employing encryption/cryptography cover both data encryption standards and public key encryption of data, e-mail and attachments sent cover the Internet communication medium. Authentication by using digital signatures and certificates as security measures could cover password authentication protocol, authentication header, message authentication code and authentication token.

Outcome 3

This Outcome deals with intentional misuse of the computer and types of protection that is available. A candidate should be able to explain browser hijacking which should include spyware, anti-spyware, adware, malicious software (malware) and virus type programs, popup, popup menu and popup ad. How browser's default starting and search pages are changed by malicious websites and/or software. This most commonly affects users through the download and installation of ActiveX controls and plug-ins on browsers where the options for "download" and "run" are set to "enable" through your Internet settings. Sometimes Internet shortcuts are also added to your favourites folder without your permission.

Under security threats instant messaging should be introduced including current protocols, packet sniffers and wireless snifers, self-replicating viruses, and non-replication viruses.

To complete security threats and protection then filters, firewall, phishing and spoofing should be covered for completeness.

Outcome 4

This Outcome deals with digital signatures and the technology that is available to implement them. A candidate should be able to explain public/private key cryptography, confidentiality, original authentication and data integrity in relation to digital certificates/signatures. Types of system attacks will be explained and their relevance to current system methodologies and design procedures. Common system attacks can be researched. Common security protocols can be researched and candidates' should be aware of the differences and relative advantages between each type chosen. Digital signature algorithms are an important technology in modern computing, candidates' should be aware of different types and overall properties. Finally, signed applets can be discussed and their use in web browsers/certificates, certificate standards and legal authorities can be researched.

Higher National Unit specification: support notes (cont)

Unit title: Internet: Web Technology and Security

Guidance on the delivery and assessment of this Unit

Outcome 1 will be assessed by a report of approximately 1,200 words covering all the knowledge and skills. Evidence will be gathered in the form of an extended response to individual research undertaken covering all points.

Outcome 2 and 3 are assessed by separate closed-book assessments covering all knowledge and skills of each Outcome on a sample basis. Candidates must achieve 60% correct responses in each of the Outcomes. Different assessment should be used for reassessment purposes.

Outcome 4 (part 1) will be assessed by five extended response questions covering each knowledge/skills bullet point. Evidence will be gathered in the form of answers of approximately 150 words per question.

Outcome 4 (part 2) will be assessed by a report of approximately 1,000 words covering all the knowledge and skills. Evidence will be gathered in the form of an extended response to individual research undertaken covering all points.

Some of the Evidence Requirements may be produced using e-assessment. This may take the form of e-testing (for knowledge and understanding) and or e-portfolios (for practical abilities). There is no requirement for you to seek prior approval if you wish to use e-assessments for either of these purposes so long as the normal standards for validity and reliability are observed. Please see the following SQA publication for further information on e-assessment: (i) *SQA Guidelines on Online Assessment for Further Education* (March 2003) and (ii) *Assessment and Quality Assurance on Open and Distance Learning* (Feb 2001).

If a centre is presenting Assessment 2 and 3 on-line the following assessment methods, where appropriate, may be selected:

- multiple-choice
- drag and drop
- multiple response
- mix and match
- a combination of the above

It is expected that the questions will be of the multiple choice variety. Centres may consider the use of alternative questions types, particularly if using Computer Assisted Assessment approaches. However, care should be taken that the questions are valid and at an appropriate level. The use of simple true/false question responses is unlikely to achieve this.

Opportunities for developing Core Skills

There are no opportunities to develop Core Skills in this Unit.

Higher National Unit specification: support notes (cont)

Unit title: Internet: Web Technology and Security

Open learning

If this Unit is delivered by open or distance learning methods, additional planning and resources may be required for candidate support, assessment and quality assurance. A combination of new and traditional authentication tools may have to be devised for assessment and re-assessment purposes. For further information and advice, please see *Assessment and Quality Assurance for Open and Distance Learning* (SQA, February Publication code A1030).

Candidates with disabilities and/or additional support needs

The additional support needs of individual candidates should be taken into account when planning learning experiences, selecting assessment instruments or considering alternative Outcomes for Units. For information on these, please refer to the SQA document *Guidance on Alternative Assessment Arrangements for Candidates with Disabilities and/or Additional Support Needs,* which is available on SQA's website: **www.sqa.org.uk**.

General information for candidates

Unit title: Internet: Web Technology and Security

This Unit is designed to give you an understanding of security and privacy issues on the Internet. The content covers the process of how a user connects to the Internet, communications with the network and issues associated with security concepts and privacy threats.

You will be introduced to network connections and Internet protocols which will include the type of access to the Internet and cover a number of protocols and network addressing.

Next, you will be made familiarise with items relating to privacy, access control, encryption and authentication when accessing web resources.

Outcome 3 covers security threats and protection methods.

The final Outcome covers digital signatures and certificates with each area researched such as authentication, public/private cryptography, generation and verification algorithms, discussion of common protocols and signed applets.

Assessment of this Unit will mainly be through questions that aim to test your knowledge and understanding.

Outcome 1 is by means of a written report and is open-book. You are encouraged to use the Internet in any research, etc., however, the evidence produced must be the candidate's own written words. You assessor must assure themselves of the authenticity of your submission.

For Outcomes 2 and 3 you will be presented with a series of questions which you have to complete under closed-book conditions.

For Outcome 4, part one, will be five extended response questions which will be conducted in supervised conditions in one hour; part two, will be a written report and is open-book. You are encouraged to use the Internet in any research, etc., however, the evidence produced must be the candidate's own written words. You assessor must assure themselves of the authenticity of your submission.