2016 Suite

OCR
Oxford Cambridge and RSA

Cambridge **TECHNICALS LEVEL 2**

Cambridge TECHNICALS 2016

IT

Unit 2

Essentials of cyber security

A/615/1352

Guided learning hours: 30

Version 1 September 2016

ocr.org.uk/it

LEVEL 2

UNIT 2: Essentials of cyber security

A/615/1352

Guided learning hours: 30

Essential resources required for this unit: None required.

This unit is externally assessed by an OCR set and marked examination.

UNIT AIM

With so much data and information being stored on computer systems, the need for security is more important than ever. To lose, or have this information and data manipulated, can cause individuals and organisations loss of time, reputation and, possibly financial loss. It is important that good security procedures are implemented to keep data and information as safe as possible.

This unit has been designed to enable you to gain knowledge and understanding of some of the threats and vulnerabilities that can have an impact on individuals and organisations. You will learn about some of the measures that can be used to protect against a cyber security attack. You will be able to apply your knowledge and understanding of these measures by recommending ways in which a digital system can be best protected.

This unit is designed to give you an understanding of cyber security issues that will prepare you to study this suite of qualifications. It is a mandatory externally assessed unit for all sizes and pathways within the suite.

Learning within this unit will also support the delivery of the Cisco Cyber Security and CompTia Security+ qualifications. The unit also makes reference to the UK National Cyber Security Strategy, Cyber Essentials Scheme, 10 Steps to Cyber Security and Cyber Streetwise.

TEACHING CONTENT

The teaching content in every unit states what has to be taught to ensure that learners are able to access the highest grades.
Anything which follows an i.e. details what must be taught as part of that area of content. Anything which follows an e.g. is illustrative.

For externally assessed units, where the content contains i.e. and e.g. under specific areas of content, the following rules will be adhered to when we set questions for an exam:

- a direct question may be asked about unit content which follows an i.e.
- where unit content is shown as an e.g. a direct question will not be asked about that example.

Learning outcomes The Learner will:	Teaching content Learners must be taught:	Exemplification
1 Know about aspects of cyber security	1.1 The definition of cyber security: Cyber security is the processes, practices and technologies which are designed to protect networks, computers, programs and data/information from attack, damage or unauthorised access. 1.2 The purpose and importance of cyber security: 1. Purpose i.e.: a. to protect information and data b. to keep information and data confidential c. to maintain the integrity of information and data d. to maintain the availability of information and data 2. Importance i.e.: a. the need to protect personal data b. the need to protect an organisations data c. the need to stay safe online	Learners should know about the purpose of cyber security, to protect information and data and why cyber security is important to both individuals and organisations. They should know about differing types of digital system and why it is important to maintain the security of the system and the information held on it.

Learning outcomes The Learner will:	Teaching content Learners must be taught:	Exemplification
	1.3 The targets for cyber security attacks i.e.: 1. individuals 2. data/information 3. equipment 4. organisations	Learners should know about different targets for cyber security attacks.
	1.4 Types of cyber security incidents i.e.: 1. data destruction 2. data manipulation 3. data modification 4. data theft	Learners should know about the types of cyber security incidents which can affect individuals and organisations.
	1.5 1. Types of attacker i.e.: a. cyber criminals b. cyber terrorists c. hackers d. phishers e. scammers 2. Motivations i.e.: a. financial gain b. publicity c. fraud d. espionage	Learners should know about the types of attackers and the motivations behind each type of attacker.
	1.6 The legal implications of cyber security i.e.: 1. The Data Protection Act (1998) 2. The Computer Misuse Act (1990) 3. other relevant legislation	Learners should know the Acts that can be used when managing cyber security incidents. Learners should be aware of the most up-to-date versions of the legislation.

Learning outcomes The Learner will:	Teaching content Learners must be taught:	Exemplification
2 Understand the threats and vulnerabilities that can result in cyber security attacks	2.1 Types of threat i.e.: 1. Denial of Service (DoS) 2. Worm 3. Botnet 4. malware including adware,spyware, clickjacking 5. social engineering including blagging, pharming, phishing, shouldering, hacking, scamming 6. unauthorised access 7. virus 8. fraudulent websites 9. fake/hoax emails 10. identify theft 2.2 How these threats can occur i.e.: 1. accidental a. organisational i.e. downloading files from unauthorised websites b. individual i.e. responding to a fake email/clicking on a hyperlink 2. intentional a. organisational i.e. DoS through flooding it with useless traffic b. individual i.e. hacking into unsecured wireless internet 2.3 The vulnerabilities which can lead to a cyber security attack, i.e.: 1. environmental such as natural disasters, flooding 2. physical such as theft 3. system such as DoS, botnet, malware	Learners should understand the different threats that can impact on any organisation/individual. Social engineering is the term given to the manipulation of people to disclose confidential information. Learners should understand that a cyber security incident may not always begin as a result of a direct attack. An attack may begin as, for example, a result of an individual clicking on a hyperlink in an email. This action will then start the attack. Other cyber security incidents may be intentional, for example, as a result of hacking which may lead to a Denial of Service (DoS). Learners should understand the different types of vulnerability that can lead to a cyber security attack.

Learning outcomes The Learner will:	Teaching content Learners must be taught:	Exemplification
	2.4 The impacts of a cyber security incident i.e.: 1. loss a. financial b. data c. reputation d. intellectual property 2. disruption a. operational b. financial c. commercial 3. safety a. individuals b. equipment c. finances	Learners should understand the possible impacts from a cyber security incident. They should understand how these incidents can affect individuals and organisations.
3 Understand how organisations/individuals can minimise impacts from cyber security incidents	3.1 Logical protection measures i.e.: 1. access rights and permissions 2. anti-virus software 3. authentication 4. encryption 5. firewalls 6. secure backups of data 7. token authentication 8. user name and password 9. emerging measures 10. characteristics i.e.: a. mixture of upper and lower case, numbers and special characters for strong password b. real time updating of virus checking software c. using access credentials and entering a	Learners should understand different types of logical security protection measures and their characteristics and purpose, to secure data and information from a cyber-attack. This should result in an understanding of the requirement for, and effectiveness of, different logical protection measures in a given context.

Learning outcomes The Learner will:	Teaching content Learners must be taught:	Exemplification
	software supplied code to access files d. access rights to files/folders based on user names and passwords 11. purpose i.e.: a. to secure a network from a cyber attack b. to protect data and information c. to protect software 3.2 Physical protection measures i.e.: 1. biometric access devices 2. locks on doors 3. device locks 4. RFID security badges 5. emerging measures 6. characteristics i.e.: a. entry to areas based on swiping a staff badge b. disabling USB ports to ensure no storage media can be used c. locking portable equipment to floors/walls 7. purpose i.e.: a. to protect a network and hardware b. to provide a log of access to buildings/areas c. to protect physical data information 3.3 Organisational policies, procedures and agreements i.e.: 1. Acceptable Use (email and internet) 2. access management 3. clean desk 4. Code of Conduct	Learners should understand different types of physical security protection measures and their characteristics and purpose, to secure data and information from a cyber-attack. This should result in an understanding of the requirement for, and effectiveness of, different physical protection measures in a given context. Learners should be aware of different types of policies, procedures and agreements which can be used by an organisation.

Learning outcomes The Learner will:	Teaching content Learners must be taught:	Exemplification
	5. document and file control 6. password protection 7. social media and blogging 8. physical security 9. risk assessment	This should lead to an understanding of the requirement for, and effectiveness of different policies, procedures and agreements in a given context.

LEARNING OUTCOME (LO) WEIGHTINGS

Each learning outcome in this unit has been given a percentage weighting. This reflects the size and demand of the content you need to cover and its contribution to the overall understanding of this unit. See table below:

LO1	33-38%
LO2	36-40%
LO3	24-29%

ASSESSMENT GUIDANCE

All Learning Outcomes are assessed through externally set written examination papers, worth a maximum of 45 marks and 1 hour in duration.

Learners should study the meaning of cyber security and gain knowledge of its purpose and importance in today's society. They should study the range of issues surrounding cyber security and the measures that can be used by individuals and organisations to protect against a cyber security attack.

Exam papers for this unit will include a mixture of short, medium and long tariff questions within different cyber security contexts. Questions will provide sufficient information to support the knowledge and understanding of the taught content of the unit. During the external assessment, learners will be expected to demonstrate their understanding through questions that require the skills of analysis and explanation in particular contexts.

Some providers for industry qualifications offer quizzes, test and assessment. Reference to these may support knowledge and learning.

www.cisco.com/UK

www.comptia.org

SYNOPTIC ASSESSMENT

It will be possible for learners to make connections between other units over and above the unit containing the key tasks for synoptic assessment, please see section 6 of the centre handbook for more detail. We have indicated in this unit where these links are with an asterisk and provided more detail in the next section.

Links between this unit and other units

This unit and specific LO	Name of other unit and related LO
LO1: Know about aspects of cyber security	Unit 1: Essentials of IT - LO5 Unit 3: Building IT systems – LO2, LO4 Unit 4: Creating programming solutions for business – LO1, LO2, LO3, LO4 Unit 5: Creating business solutions – LO2, LO3, LO4 Unit 6: Participating in a project- LO2 Unit 7: Pitching a product – LO2 Unit 8: Using emerging digital technologies – LO1 Unit 9: Supporting IT functions – LO2, LO3, LO4 Unit 10: IT software installation and upgrade – LO1 Unit 11: IT hardware installation and upgrade – LO1
This unit and specific LO	**Name of other unit and related LO**
	Unit 12: Creating a computer network – LO2, LO3, LO4 Unit 13: Creating websites – LO1, LO2, LO3, LO4 Unit 14: Creating mobile applications for business – LO1, LO2, LO3 Unit 15: Games creation – LO1, LO2 Unit 16: Using social media channels for business – LO1, LO2 Unit 17: Using data analysis software – LO1, LO2 Unit 18: Creating visual business products – LO1, LO2
LO2: Understand the threats and vulnerabilities that can result in cyber security attacks	Unit 1: Essentials of IT - LO5 Unit 3: Building IT systems – LO2, LO4 Unit 4: Creating programming solutions for business – LO1, LO2, LO3, LO4 Unit 5: Creating business solutions – LO2, LO3, LO4 Unit 6: Participating in a project - LO2 Unit 7: Pitching a product – LO2 Unit 8: Using emerging digital technologies – LO1 Unit 9: Supporting IT functions – LO2, LO3, LO4 Unit 10 IT software installation and upgrade – LO1

	Unit 11: IT hardware installation and upgrade – LO1 Unit 12: Creating a computer network – LO2, LO3, LO4 Unit 13: Creating websites – LO1, LO2, LO3, LO4 Unit 14: Creating mobile applications for business – LO1, LO2, LO3 Unit 15: Games creation – LO1, LO2 Unit 16: Using social media channels for business – LO1, LO2 Unit 17: Using data analysis software – LO1, LO2 Unit 18: Creating visual business products – LO1, LO2
LO3: Understand how organisations/individuals can minimise impacts from cyber security incidents	Unit 1: Essentials of IT - LO5 Unit 3: Building IT systems – LO2, LO4 Unit 4: Creating programming solutions for business – LO1, LO2, LO3, LO4 Unit 5: Creating business solutions – LO2, LO3, LO4 Unit 6: Participating in a project - LO2 Unit 7: Pitching a product – LO2 Unit 8: Using emerging digital technologies – LO1 Unit 9: Supporting IT functions – LO2, LO3, LO4 Unit 10 IT software installation and upgrade – LO1, LO3 Unit 11: IT hardware installation and upgrade – LO1, LO3 Unit 12: Creating a computer network – LO2, LO3, LO4 Unit 13: Creating websites – LO1, LO2, LO3, LO4
This unit and specific LO	**Name of other unit and related LO**
	Unit 14: Creating mobile applications for business – LO1, LO2, LO3 Unit 15: Games creation – LO1, LO2 Unit 16: Using social media channels for business – LO1, LO2 Unit 17: Using data analysis software – LO1, LO2 Unit 18: Creating visual business products – LO1, LO2

MEANINGFUL EMPLOYER INVOLVEMENT - a requirement for Technical Certificate qualifications

These qualifications have been designed to be recognised as Technical certificates in performance tables in England. It is a requirement of these qualifications for centres to secure for every learner employer involvement through delivery and/or assessment of these qualifications.

The minimum amount of employer involvement must relate to at least one or more of the elements of the mandatory content. This unit is a mandatory unit in the Certificate and Diploma pathways.

Eligible activities and suggestions/ideas that may help you in securing meaningful employer involvement for this unit are given in the table below.

Please refer to the *Qualification Handbook* for further information including a list of activities that are not considered to meet this requirement.

Meaningful employer engagement	Suggestion/ideas for centres when delivering this unit
1. Learners undertake structured work-experience or work-placements that develop skills and knowledge relevant to the qualification.	An Industry Practitioner/STEMNET could be used to present a guest talk on the logical and physical measures they take to prevent a cyber security attack on their organisation (LO3)
2. Learners undertake project(s), exercises(s) and/or assessments/examination(s) set with input from industry practitioner(s).	
3. Learners take one or more units delivered or co-delivered by an industry practitioner(s). This could take the form of master classes or guest lectures.	
4. Industry practitioners operating as 'expert witnesses' that contribute to the assessment of a learner's work or practice, operating within a specified assessment framework. This may be a specific project(s), exercise(s) or examination(s), or all assessments for a qualification.	

You can find further information on employer involvement in the delivery of qualifications in the following documents:

- Employer involvement in the delivery and assessment of vocational qualifications
- DfE work experience guidance

To find out more
ocr.org.uk/it
or call our Customer Contact Centre on **02476 851509**

Alternatively, you can email us on **vocational.qualifications@ocr.org.uk**

OCR
Oxford Cambridge and RSA

OCR is part of Cambridge Assessment, a department of the University of Cambridge.