

Answers to Student's Book

Exam-style questions and sample answers have been written by the authors. References to assessment and/or assessment preparation are the publisher's interpretation of the syllabus requirements and may not fully reflect the approach of Cambridge Assessment International Education. Cambridge International recommends that teachers consider using a range of teaching and learning resources in preparing learners for assessment, based on their own professional judgement of their students' needs.

Cambridge Assessment International Education bears no responsibility for the example answers to questions taken from its past question papers which are contained in this publication.

The questions, example answers, marks awarded and/or comments that appear in this digital material were written by the author(s). In examination, the way marks would be awarded to answers like these may be different.

5 The internet and its uses

Answers to activities

5.1

1 a urlexample

b .co

c sample_page

d http

2 a Session cookie:

- temporary cookie
- ceases to exist once browser is closed or website session terminated
- doesn't actually collect any information from user's computer

Persistent cookie:

- stored on hard drive of user's computer ...
 - ... until expiry date reached or user deletes cookie
 - remains in operation on user's computer even when browser closed or website session terminated
- b
- allows a website to remember a user's email address and invoice details so these don't have to be typed in each time a user visits a website, which allows a faster log in
 - serves as a memory, enabling a website to recognise users every time they visit the website
 - saves user's items in a virtual shopping basket
 - tracks internet habits and user's website history/favourites (bookmarks)/recommendations made
 - stores customer payment details (in secure format)
 - stores user preferences
 - allows progress in online games/quizzes to be stored

- allows social networking sites to recognise certain preferences and browsing history
- allows different languages to be used on web pages automatically/personalised web pages stored
- indicates if customer is new or returning

3

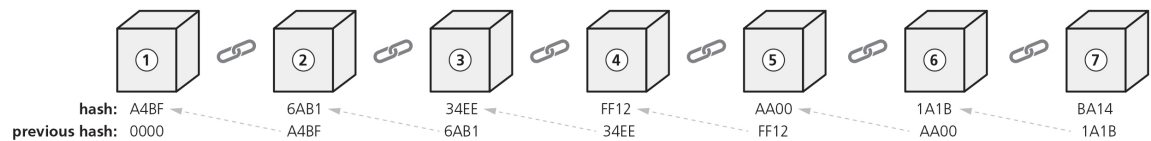
Feature	Internet	World Wide Web
It is possible to send and receive emails	✓	
Makes use of http protocols		✓
Uses URLs to specify the locations of websites and web pages		✓
Resources can be accessed by using web browsers		✓
Makes use of TCP and IP	✓	

4

- they record data about the user ...
- ... such as browsing activity, purchases and preferences ...
- ... IP addresses and geographical location
- they store marketing data which allows adverts to target user

5.2

1 a



- b If block 4 is hacked and any data is changed, then the hash value for the block will change; this will result in the chain being broken since block 5 can no longer point to block 4.

2

- cryptocurrency uses cryptography to track transactions
- cryptocurrency is decentralised unlike digital currencies which are centralised
- traditional digital currencies are regulated by central banks and governments
- unlike normal digital currencies, cryptocurrency transactions are publicly available and can be tracked/money monitored
- cryptocurrency uses blockchaining

5.3

1

a	b	c
Three from:		
brute force attacks	to crack passwords	make passwords difficult to crack and change them often
data interception	tapping into networks to obtain information	use private lines/networks and encrypt all data
denial of service attack	'... which cause it to crash	use a malware checker, firewalls and email filters
hacking	illegal access to a computer system	firewalls and passwords (including biometrics)
malware (worms, viruses, spyware, ...)	deletion or altering of data	use up-to-date anti-malware software
phishing	legitimate-looking emails which contain links to fake websites	don't open links in emails, use up-to-date browsers, look out for https, check if url looks legitimate
pharming	code on HDD/SSD or server which redirects browser to fake website without user's knowledge	use anti-virus software to detect website tampering, check spelling of websites
social engineering	cybercriminal creates social situation that can lead a victim to dropping their guard using: instant messaging, scareware, phishing, baiting or phone calls	be aware of scam text messages, phone calls, memory sticks left lying around on purpose, and so on

- 2
- worm: type of stand-alone virus that can replicate itself with the intention of spreading to other computers/networks; often uses networks to search out computers with weak security
 - ransomware: programs that encrypt data on a user's computer; a decryption key is sent back to the user once they pay a sum of money (ransom); they are often sent via a Trojan horse or by social engineering
 - Trojan horse: malicious programs often disguised as legitimate-looking software; they replace all or part of the legitimate software with the intent of carrying out some harm to the user's computer system

- 3 a**
- i** a date of birth – relatively easy to find or guess
 - ii** too close to name of a pet – easy to crack
 - iii** uses his own name in the password – makes it relatively easy to guess
- b** ensure at least eight characters are used, made up of upper-case and lower-case letters, numbers and other keyboard characters; passwords should be changed on a regular basis
- c** if the computer can be accessed by other people, then it is not a good idea to store passwords on the computer itself since these could be found by another user

5.4

- 1 a** 25-May-2000 – weak password because it is just a date
- b** Pas5word – one of the ten most used passwords!
- c** ChapTer@06 – strong password with letters, numbers and other characters
- d** AbC*N55! – strong password with letters, numbers and other characters
- e** 12345X – weak password since it is easy to guess/crack
- 2 a** make use of levels of access; for example, level 1: passenger information, level 2: airport staff, level 3: senior staff only – use passwords and user IDs
- b** make use of:
- strong passwords and user IDs
 - firewalls
 - scan for malware at all times
 - don't allow plug-in devices at information desks
 - don't allow internet access from information desks

5.5

- 1 a**
- as soon as motion detector recognises a person, a camera automatically photographs the face of the person
 - software scans face for key features and creates an electronic image/file
 - the file is compared to the database containing face scans of authorised people
 - if key features match database data then entry is allowed ...
 - ... otherwise entry is denied
- b** finger/thumb print, voice recognition using a microphone
- 2**
- | | |
|---|---|
| <p>Benefits:</p> <ul style="list-style-type: none"> • more secure system since only certain people can be recognised as authorised drivers • safer since driver doesn't need to look at screens/dials to select options or look at key data • relatively inexpensive technology | <p>Drawbacks:</p> <ul style="list-style-type: none"> • a person's voice can be recorded to overcome the security system • low accuracy; doesn't understand verbal commands • change of voice (e.g. due to a cold) can make recognition 'hit and miss' • sometimes there is a need to remember certain commands to make system work |
|---|---|

5.6

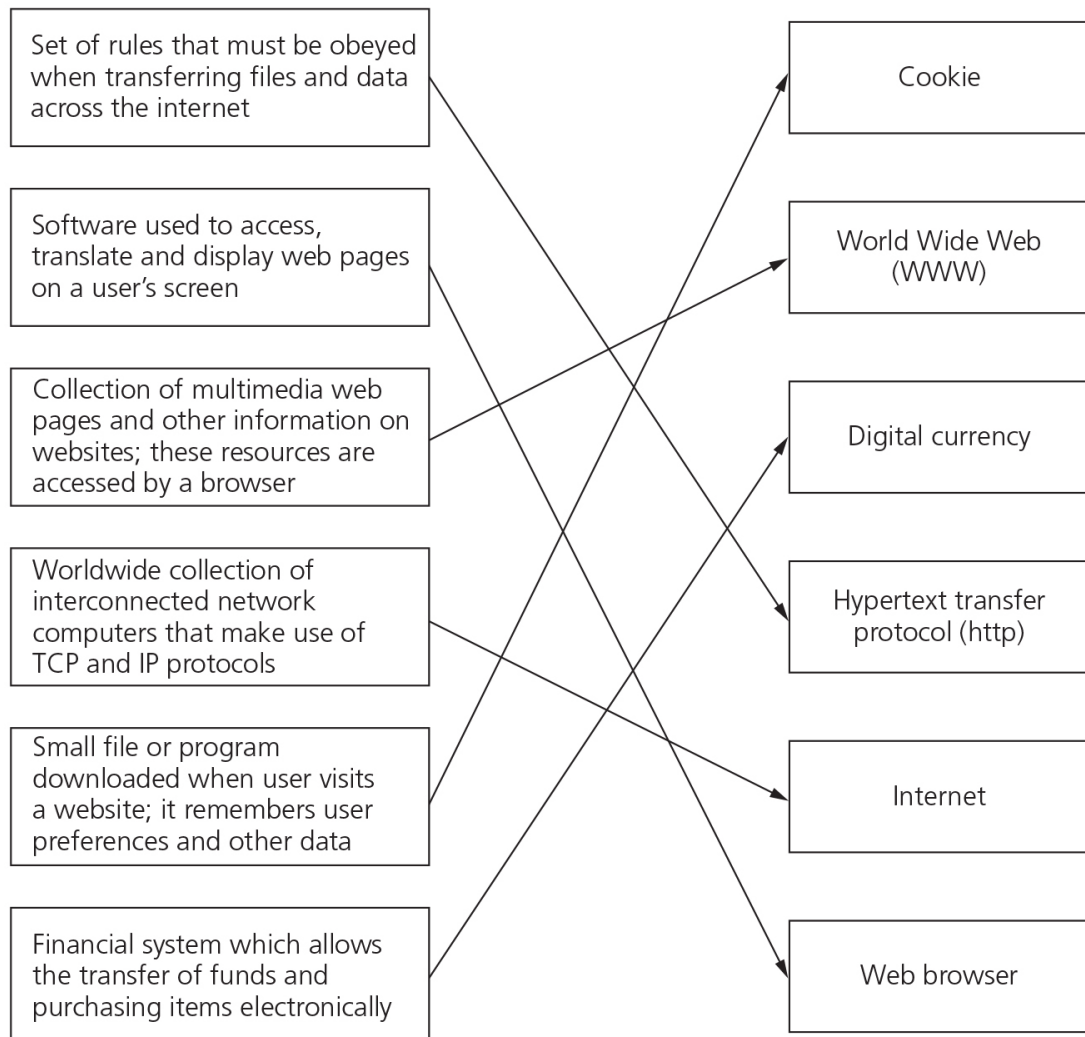
- 1
 - a two-step verification
 - b proxy server
 - c privacy settings
 - d SSL
 - e firewall
 - f DNS
 - g biometrics
 - h authentication
 - i social engineering
 - j pharming
- 2 A browser requests an SSL/TLS digital certificate from the website it is trying to access. This is sent from the web server to the user's browser, containing a public key which can be used to authenticate the website. Once the digital certificate is authenticated, the browser lets the web server know, and secure communication can begin.
- 3
 - a Three from:
 - Are there spelling or grammar errors?
 - Does the email FROM address look like it is real?
 - Is the domain name in the email address spelt correctly, or does it exactly match the real company?
 - Is the email addressed to you?
 - Is there a clickable link? If so, what address does the link point to when you hover over it? (DO NOT CLICK THE LINK!) It may not match the expected website.
 - If it claims to be from a real company, log into your account with the company without using the link.
 - b Three from:
 - poor spelling and grammar
 - not addressed to the user
 - WW and Co does not look like a real company
 - the email address which this is from does not look like a real or reputable company
 - there is no further information in the email, such as details about the company itself
 - reputable companies would not expect a customer to click on a link in an email to pay an account
 - does not look professional

Answers to exam-style questions

- 1 a i** A cookie is a small file stored on a user's computer; they are sent by a website to a browser when a user visits the site.
- ii** Session cookies are stored in a temporary memory on the computer; they don't collect any information from the user's computer and don't identify the user; they cease to exist when the browser is closed or the user terminates the session with the website. Persistent cookies are stored on the hard drive of the user's computer; they remain stored until an expiry date is reached or the user deletes the cookie; they remain in operation on the user's computer even when the browser is closed or the website session has been terminated; they remove the need to type in login details every time a website is visited.
- iii** Three from:
- allows a website to remember a user's email address and invoice details so these don't have to be typed in each time a user visits a website, which allows a faster log in
 - serves as a memory, enabling a website to recognise users every time they visit the website
 - saves users items in a virtual shopping basket
 - tracks internet habits and user's website history/favourites (bookmarks)/recommendations made
 - stores user preferences
 - allows progress in online games/quizzes to be stored
 - allows social networking sites to recognise certain preferences and browsing history
 - allows different languages to be used on web pages automatically/personalised web pages stored
 - indicates if customer is new or returning
- 2 a •** Spyware is software that gathers information by monitoring activity on a user's computer. It can gather information by finding information such as bank account details and passwords stored on the computer or within web browser cookies. Spyware called keyloggers can record what a user types and which websites they visit. The gathered information is then sent back to the person who created or sent the software, which can be used for fraudulent purposes.

- b** Two step verification – extra security that means that even if passwords are stolen criminals cannot gain access to the bank account. It requires some biometric identification – this would limit access to specified employees only.
- c**
 - checks for any unusual network traffic and blocks access to the local network
 - can be used to only allow specified external connections, so that all traffic is blocked apart from these specified sites
 - any known undesirable sites can be added to a list of blocked network sites
- d**
 - passwords/biometrics
 - levels of access
 - proxy servers
 - physical security methods – e.g. PCS in locked rooms, etc.

3



4 a Order: C, E, A, B, D

- b
- student places finger on scanner
 - map of fingerprints taken and converted to digital image
 - data sent to a computer
 - fingerprint map compared to those stored
 - if recognised, the database is updated to show student present (including time and date of entry)
 - on leaving, the same process is carried out and the database is again updated to show the date/time student left the school premises

5 a Four from:

- instant messaging – links embedded in messages to fake websites
 - scareware – pop-up message claiming, for example, user's computer is infected with a virus and user downloads the fake virus checker
 - emails/phishing – apparently genuine emails sent out which contain links to fake websites
 - baiting – cybercriminal leaves malware-infected memory stick so that it can be easily 'found'; once inserted into a computer, the malware is transferred
 - phone calls – so-called IT professional calls a user on their mobile phone claiming their device has been compromised and they are advised to download software which lets the cybercriminal take over their device
- b
- Stage 1 – victim is identified and necessary information is gathered
 - Stage 2 – victim is targeted by the chosen method
 - Stage 3 – attack on victim takes place and information is gathered or disruption to their system done
 - Stage 4 – when cybercriminal has achieved their goal, all traces of the attack are removed
- c
- i digital currency exists purely in a digital format; there is no physical money (fiat currency); digital currency involves electronic transfer of funds
- ii if a hacker accessed a block and changed anything (for example, an amount of money) ...
- ... the hash value of the block would change
 - this means that all blocks beyond the hacked block would now be invalid because the chain would be broken
 - use of 'proof-of-work' is necessary before a block can be added to the chain ...
 - ... thus preventing a hacker quickly creating a new block to complete the chain

6 a Used for layout of content – this structure is defined by HTML tags, e.g. for each heading and paragraph text.

b browser

Internet Protocol address (IP address)

web server

Hypertext Markup Language (HTML)

7 a SSL is a security protocol:

- it encrypts any data that is sent
- it uses/sends digital certificates ...
- ... which are sent to the user's browser ...
- ... that contains the gallery's public key ...
- ... that can be used to authenticate the gallery
- once the digital certificate is authenticated, the transaction can begin

b

Statement	True (✓)	False (✓)
Firewalls are only available as hardware devices		✓
Firewalls allow a user to set rules for network traffic	✓	
Firewalls will automatically stop all malicious traffic		✓
Firewalls only examine traffic entering a network		✓
Firewalls encrypt all data that is transmitted around a network		✓
Firewalls can be used to block access to certain websites	✓	