Chapter 6 Student Book Answers

What you should already know

1 a) Hacking – is unauthorised access to a computer system without the user's knowledge or consent.

b)

- Hacking is illegal if it aims to cause harm (For example, delete files, transfer money illegally, etc.).
- 'Ethical hacking' is an expert who attempts to penetrate a computer system/network on behalf of the owner(s) of the system to try and determine the security vulnerability that an illegal hacker could exploit.

2

Pros	Cons
• convenient since there is no need to tap in a PIN	• not yet universally available
• user is protected against fraudulent transactions	• only available to users with contactless credit/debit cards
• uses *Near Field Communications (NFC)* which uses encryption thus protecting user against illegal acts	• since there is no PIN to type in, lost cards could still be used until the owner realises the loss
• quicker transactions leads to shorter queues at check-outs	• limit set by the bank is fairly small and therefore only useful for small purchases
• retailers no longer have access to user's credit/debit card details	• studies have shown that customers are more likely to spend money when using contactless payment

3

- Hacking – the act of stealing personal or private data without the owner's knowledge or consent.
- Cracking – is where someone edits/changes the source code of a program or they create a program (known as a ***patch***) that can trick the software in to thinking a certain process has occurred
  - for example, a patch could trick software into thinking that a security key has been successfully entered giving illegal access
  - this is known as finding the 'back door' to the software and is used for malicious use or for breaking of software copyright
  - whilst cracking is always essentially illegal, it is generally thought to be less harmful than hacking and also requires more skill to carry out since there is a need to understand program coding methods.

4 a **Pop ups**

- a window that opens without the user selecting it form a menu
- used by websites to display adverts
- can come from malware in which case it is evidence that a computer has become infected
- can generate 'scareware' such as the selling of fake antivrus programs by claiming that a user's computer has a virus and won't remove it until a fee is paid.

b **Cookies**

- small files which are stored on a user’s computer
- sent to a computer when the user visits a website
- allow the website to know a user’s preferences and can make suggestions based on a user’s previous searches
- each time the user visits the website, they will be recognised and the user’s information will be retrieved from a database making it much faster and easier to access the website (e.g. baskets, user names, and so on).

c i) **session cookies**

- used when buying online, for example
- keep a user’s items in a ‘shopping basket’
- cease to exist on a user’s computer when the web browser is closed or the website session is terminated.

ii) **permanent cookies**

- these cookies remember user login details (such as passwords)
- remain in operation on the user’s computer even after the web browser is closed or the website session is terminated
- advantage is they remove the need to type in personal details every time a certain website is visited
- many countries have introduced laws to protect users and these cookies are supposed to become deactivated after 6 months of inactivity.

iii) **third party cookies**

- these cookies are created by a ‘third party’ to carry out market research into a user’s buying habits and surfing habits
- the user can delete or block such cookies by configuring their web browser
- the disadvantage of blocking such cookies is that the website will no longer recognise a user’s preferences.

5 It is possible to corrupt a memory stick if the correct withdrawal procedures are not followed.

Activity 6A

1 a, b, c three examples have been chosen … other answers are possible:

Phishing (risk to the security of stored data)

- With phishing, the creator sends out legitimate-looking emails to target users …
- … as soon as the recipient clicks on a link in the email or attachment …
- … they are sent to a fake website or they are fooled into giving personal data in response to the email.
- The email often appears to come from a trusted source such as a bank or well-known service provider.
- The key aspect is that the recipient has to carry out a task (e.g. click on a link) before the phishing scam can cause any harm.
- The creator of the email can gain personal data such as bank account data or credit card numbers from the user which can lead to fraud or identity theft.

There are numerous ways to help prevent phishing attacks:

- Users need to be aware of new phishing scams.
- It is important not to click on any emails links unless totally certain that it is safe to do so …
- fake emails can often be identified by "Dear Customer ……" or "Dear email person@gmail.com ………" and so on.
- It is important to run anti-phishing toolbars on web browsers.
- Always look out for https or the green padlock symbol in the address bar.
- Make regular checks of online accounts are also advisable as well as maintaining passwords on a regular basis.
- Ensure an up-to-date browser is running on the computer device (which contains all of the latest security upgrades) …
- … and run a good firewall in the background at all times; a combination of a desktop firewall (usually software) and a network firewall (usually hardware) considerably reduces the risk of hacking, pharming and phishing on network computers.
- Be very wary of pop-ups and use the web browser to block them …
- … if pop-ups get through your defences, don't click on 'cancel' since this can ultimately lead to phishing or pharming sites down.

Pharming (risk to the security of stored data)

- Pharming is malicious code installed on a user's computer or on a web server …
- … the code will re-direct the user to a fake website without their knowledge …
- … redirection from a legitimate website to the fake website can be done using DNS cache poisoning.
- When a user enters a web address (URL) into a browser, the computer is sent the IP address of the website …
- … if the IP address has been modified somehow (for example, through pharming) the user's computer will be redirected to the fake website.
- The creator of the malicious code can gain personal data such as credit/debit card details from users when they visit the fake website.
- Usually the website appears to be that of a well-known and trusted company and can lead to fraud or identity theft.

It is possible to mitigate the risk of pharming:

- Using antivrus software can detect unauthorised alterations to a website address and warn the user of the potential risks …
- … however, if the DNS server itself has been infected) it is much more difficult to mitigate the risk
- Many modern web browsers can alert users to pharming and phishing attacks
- It is very important to check the spelling of websites to ensure the web address used is correct

Viruses

- A virus is a program/program code that can replicate/copy itself with the intention of deleting or corrupting files …
- … or cause the computer to malfunction

- They need an active host program on the ta.rget computer or an operating system that has already been infected before they can run.
- Running antivirus software in the background on a computer will constantly check for virus attacks.

All antivirus software have the following common features:

- They check software or files before they are run or loaded on a computer.
- Antivirus software compares a possible virus against a database of known viruses.
- They carry out heuristic checking.
- Any possible files or programs which are infected are put into quarantine which …
- … allows the virus to be automatically deleted or …
- … allows the user to make the decision about deletion.
- Antivirus software needs to be kept up to date since new viruses are constantly being discovered.
- Full system checks need to be carried out once a week, for example, since some viruses lie dormant and would only be picked up by this full system scan.

2 Worms – this is a type of stand-alone virus that can replicate itself with the intention of spreading to other computers; often uses networks to search out computers with weak security which are prone to such attacks.

Logic bombs – these are code embedded in a program on a computer; when certain conditions are met (For example, Friday 13th) they are automatically activated to carry out tasks such as deleting files or start sending data to a hacker.

Trojan horses – these are malicious programs often disguised as legitimate 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 first password is his date of birth

second password contains name of his pet dog

third password contains his name

b strong passwords should

- contain upper case letters
- contain lower case letters
- contain numerical characters
- contain other keyboard characters
- contain at least 8 characters in length
- not contain easy to guess words or numbers
- be changed on a regular basis but not in sequence e.g. if existing password is AXtuLr0045 then the next one should not be AXtuLr0046 etc.

c

- If the device John is using can be accessed by other people, it isn't safe to store the password on the device.
- If it is saved on the shared device, the password is accessible to hackers etc.

d John should be suspicious because

- the link may not be to a genuine website

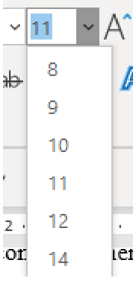
- by supplying details, the user may be inadvertently giving away personal details to a third party
- it is very likely to be a phishing scam.

6.2 What you should already know

1 to ensure data is reasonable and meets certain input criteria before it can be used

2 proofreading checks that a document reads correctly and is factually correct (it doesn't necessarily check against the original document)

3 can use drop down boxes:



Activity 6B

1 error at intersection of ***bit 6*** and ***byte 4***:

(bit 6 has even parity and byte 4 has even parity)

2 a Name: character check, presence check

Date of birth: range check, character check, presence check, format check

Tel No: character check, presence check, length check, format check (0……)

Title/Sex: consistency check

b Validation checks – if the input data matches a set of rules/meets a given criteria.

Verification checks – checks to make sure that the input data matches the original data by double data entry and/or visual check.

- Both methods needed since original data may not be correct.
- For example 1, year of birth 1840 rather than 1940; a verification check would not pick this up since the input data would match the original data and only a validation check would show this data to be in error.
- For example 2, data of birth input as 11/04/2004 when it should be 04/11/2004 would not be picked up by validation checks (matches format, character check. length checks) but it would be picked up by a verification check since it didn't match the original data.

3 a

- Verification could use double data entry when the data is entered twice by the same person/different operators; the computer compares both sets of input.
- Alternatively, as data is input the user checks the entries against the original to check for mis-matches.

b Code NXXXXXNN – length check e.g. A516412KK would fail the check (it would also be equally possible to do character checks on each field or carry out a format check to ensure it matches NXXXXXNN or carry out a uniqueness check since each product should have a unique code).

Number in stock – range field e.g. 125 would fail the check (it would also be equally possible to do a character check to ensure only numeric values input or a length check to ensure number of digits didn't exceed 3 but this wouldn't be enough on its own since it could still exceed 100 and pass the check).

Unit cost – range check e.g. (assuming max price of an item is \$1000.00) –\$450 would fail the test because it is negative or \$1500.00 would also fail because it is > \$1000.00 (it would also be equally possible to do a character check to ensure only numerical values are input).

Telephone number – length check e.g. 012345678901112 would fail the check (it would also be equally possible to do a character check since all characters entered must be numerical or it would be possible to do a format check since the telephone number must fit the format 0XXXXXXXXXX; NOTE: a range check would not work here since the telephone number begins with a zero).

Note: in all cases a presence check could be acceptable if the data is being input to an online form where all fields require an entry

Extension Activity 6A

Levels of access controlled by use of different passwords

Extension Activity 6B

a weak – could be a birthday which would be relatively easy to guess

b fairly weak – this is a very common password to use

c strong – mix of numbers, upper and lower case letters, use of other characters

d strong – mix of numbers, upper and lower case letters, use of other characters

e weak – easy to guess the number sequence of 1 2 3 4 5

Extension Activity 6D

1 ISBN-13:

take first 12 digits

multiply each in turn (left to right) by 1, 3, 1, 3, …… 1, 3

add all 12 totals and carry out modulo-10 division

subtract remainder from 10 to give check digit

example: 9 7 8 0 3 4 0 9 8 3 8 2
×1 ×3 ×1 ×3 ×1 ×3 ×1 ×3 ×1 ×3 ×1 ×3
= 9 + 21 + 8 + 0 + 3 + 12 + 0 + 27 + 8 + 9 + 8 + 6
= 111 ÷ 10 = 11 remainder 1

check digit = 10 − 1 = ***9***

2 **a** modulo-11

2 1 3 1 1 1 0 0 0 4 2 8
×13 ×12 ×11 ×10 ×9 ×8 ×7 ×6 ×5 ×4 ×3 ×2
= 26 + 12 + 33 + 10 + 9 + 8 + 0 + 0 + 0 + 16 + 6 + 16
= 136 ÷ 11 = 12 remainder 4
check digit = 11 − 4 = *7*

ISBN-13
2 1 3 1 1 1 0 0 0 4 2 8
×1 ×3 ×1 ×3 ×1 ×3 ×1 ×3 ×1 ×3 ×1 ×3
= 2 + 3 + 3 + 3 + 1 + 3 + 0 + 0 + 0 + 12 + 2 + 24
= 53 ÷ 10 = 5 remainder 3
check digit = 10 − 3 = *7*

b modulo-11

9 0 9 8 1 2 1 2 3 5 4 4

×13 ×12 ×11 ×10 ×9 ×8 ×7 ×6 ×5 ×4 ×3 ×2

= 117 + 0 + 99 + 80 + 9 + 16 + 7 + 12 + 15 + 20 + 12 + 8

= 395 ÷ 11 = 35 remainder 10

check digit = 11 − 10 = ***1***

ISBN-13

9 0 9 8 1 2 1 2 3 5 4 4

×1 ×3 ×1 ×3 ×1 ×3 ×1 ×3 ×1 ×3 ×1 ×3

= 9 + 0 + 9 + 24 + 1 + 6 + 1 + 6 + 3 + 15 + 4 + 12

= 90 ÷ 10 = 9 remainder 0

check digit = 10 − 0 = ***X***

Extension Activity 6E

1 1

2 0

3 1

4 1

5 0

Extension Activity 6F

1 **a** ✓

b ✗

c ✗

d ✓

e ✗

2 No it isn't possible

End of chapter questions

1 **a** any description of the following: use of passwords/user ids, use of a firewall, use of antivrus or anti-spyware software, use of secure/private lines, and so on.

b 1 5 6 3 4 1 2

×7 ×6 ×5 ×4 ×3 ×2 ×1

= 7 + 30 + 30 + 12 + 12 + 2 + 2

= 95 ÷ 11

= 8 remainder 7

check digit = 11 − 7 = ***4***

c student ID: length check, character check or format check

2 **a**

- A virus is a program/program code that can replicate/copy itself with the intention of deleting or corrupting files …
- … or cause the computer to malfunction.

- They need an active host program on the target computer or an operating system that has already been infected before they can run.
- Running antivirus software in the background on a computer will constantly check for virus attacks.
- All antivirus software have the following common features:
  - They check software or files before they are run or loaded on a computer.
  - Antivirus software compares a possible virus against a database of known viruses.
  - They carry out heuristic checking.
  - Any possible files or programs which are infected are put into quarantine which …
  - … allows the virus to be automatically deleted or …
  - … allows the user to make the decision about deletion.
  - Antivirus software needs to be kept up to date since new viruses are constantly being discovered.
  - Full system checks need to be carried out once a week, for example, since some viruses lie dormant and would only be picked up by this full system scan .

b

- A firewall can be either software or hardware.
- It sits between the user's computer and an external network …
- … and filters information in and out of the computer.
- This allows the user to decide to allow communication with an external source …
- … and it also warns a user that an external source is trying to access their computer.
- Firewalls are the primary defence to any computer system to help protect it from hacking, malware, phishing and pharming.
- The main tasks carried out by a firewall include:
  - Examine the 'traffic' between user's computer (or internal network) and a public network.
  - Check whether incoming or outgoing data meets a given set of criteria …
  - … if the data fails the criteria, the firewall will block the 'traffic' and give the user a warning that there may be a security issue.
  - The firewall can be used to log all incoming and outgoing 'traffic' to allow later interrogation by the user.
  - Criteria can be set so that the firewall prevents access to certain undesirable sites …
  - … the firewall can keep a list of all undesirable IP addresses.
  - It is possible for firewalls to ***help prevent*** viruses or hackers entering the user's computer.
- The firewall can be a hardware interface which is located somewhere between the computer and the internet connection.
- It is often referred to in this case as a gateway …
- … alternatively the firewall can be software installed on a computer and …
- … in some cases this is part of the operating system.

3 At the intersection of bit 6 and byte 5 – the bit in this position is incorrect.

(bit 6 is even parity; byte 5 is even parity)

corrected byte: 1 1 1 0 1 ***0*** 1 0