# Answers

**Task 1**

(a) List, with an example of each, ways in which the **integrity of data** may be compromised.

* Program error, e.g. which changes data incorrectly
* Accidentally deleting a file
* Dishonest employee who deliberately alters facts or figures
* Errors in backup procedure resulting in backups not being correctly carried out, or older version of file being used instead of current version
* Data not being validated/verified on entry resulting in input being incorrect
* (This question is not looking for answers to do with accidental damage, viruses, other types of malware, which would come under the heading of security)

(b) Look up the following website and make a list of the seven greatest causes of   
data loss:

<http://www.databackuponlinestorage.com/7_Causes_of_Data_Loss>

What is the greatest cause of data loss?

How many of the events described have happened to you?

**This site lists the following causes of data loss:**

1. Deleting files accidentally
2. Viruses and damaging malware
3. Mechanical damage to hard drive
4. Power failures
5. Theft of computer
6. Spilling coffee
7. Fire, accidents and explosions

Task 2

The following are five types of malware:

* Virus
* Worm
* Trojan horse
* Ransomware
* Spyware

Choose **two** of these types of malware, research them and then describe below how   
they work.

**Virus** – malicious code is attached to or embedded in a program or file. When the file is opened or the program run, the malicious code is also executed. The virus can cause damage to the computer system and replicate to other computer systems.

**Worm** – a worm will use security holes in operating systems or software to gain access to a system. Having gained access, it will then be able to replicate to other computer systems. The worm is likely to slow down the computer especially if it is involved in a botnet or denial of service attack.

**Trojan horse** – a Trojan will consist of a program that someone wants (such as cracked software) that also has malicious code inside it. When the program is installed or run, the malicious code will also run. Advertising pop-ups may now appear, the system may not perform correctly, and files may be altered or deleted.

**Ransomware** – This software will first encrypt a user’s hard disk. It will then request payment (usually in bitcoin) from the user in order to decrypt the drive. The encryption is usually so strong that there is no other way for the users to get access to their data without paying. If backups exist, the data can be restored to a point before the ransomware infected the system.

**Spyware** – This type of software is often delivered by a Trojan. The software may contain a key logger which logs key presses. It may also take screenshots of the system or other data stored on the system. The information gathered can be sent to a remote computer.

**Task 3**

The term hacker can refer to black hat, grey hat and white hat hackers.

(a) Which of these is usually referred to in news reports of company systems being compromised or misused?

Black hat (hacker)

(b) What is another name, more commonly used by the media, for a white hat hacker?

Computer security expert / consultant / penetration tester

(c) Research a famous computer hacker and note the following:

* What was their name or groups name?
* When did they operate?
* What attacks or misuse were they responsible for?
* What was their motivation?

Task 4

Look at the following four emails.

(a) Which of them are genuine?

Only the first of the emails is genuine.

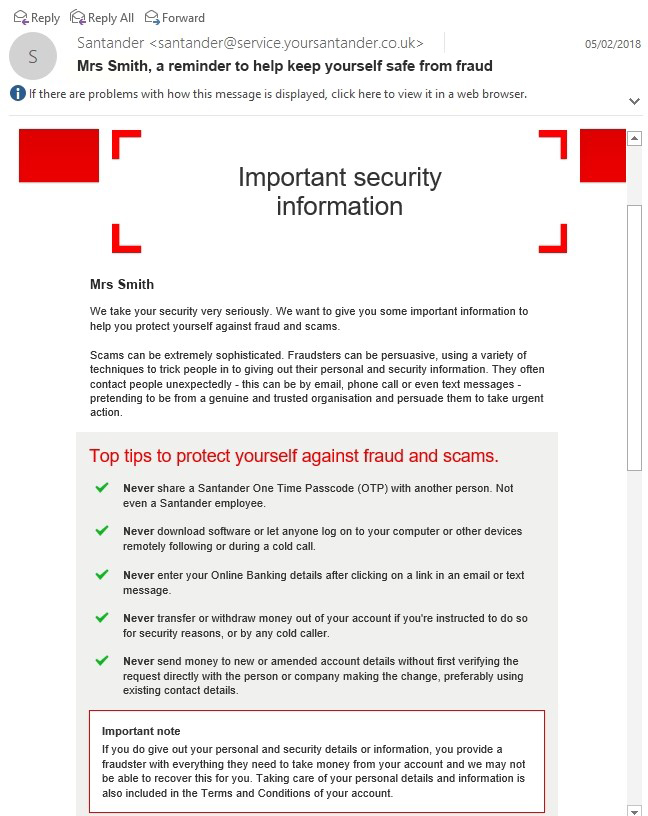
(b) How can you tell?

See each of the emails below that are not genuine.

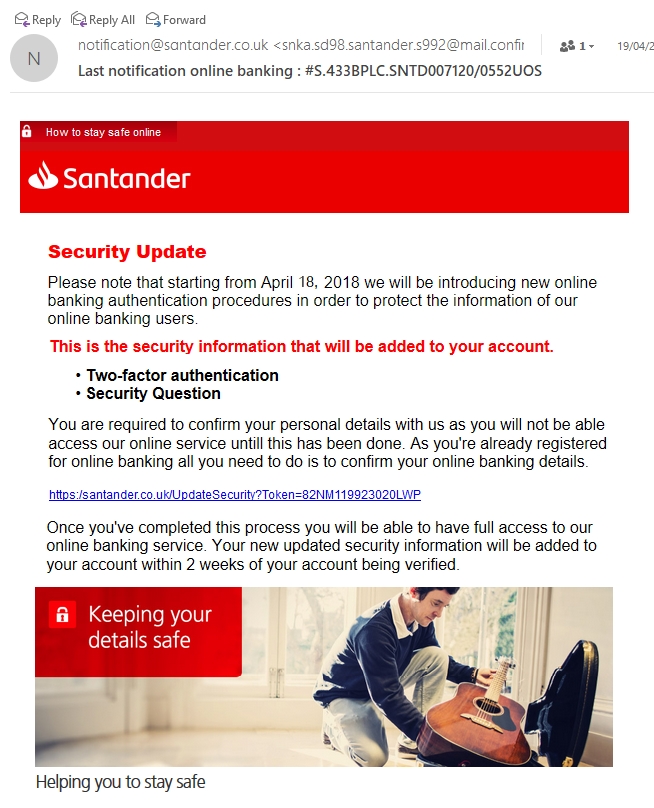
(c) What will you do in each case?

You should report each of the others as a “phishing scam” and then delete it.

**Email 1**

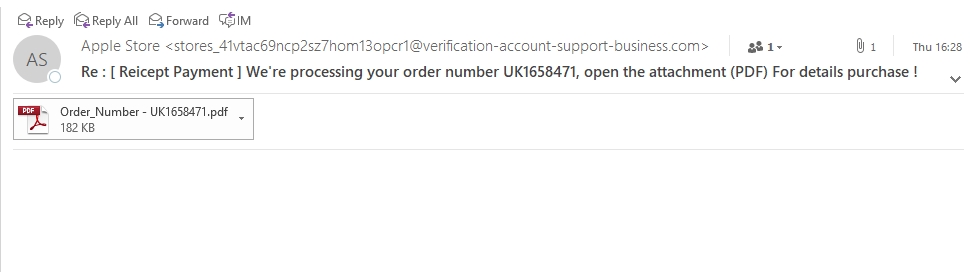
This email is genuine

**Email 2**

This one looks genuine at a casual glance, but nothing is personalised, it comes from an odd-looking email address and it asks the recipient to click on a link. It is a phishing scam.

**Email 3**

Students should ask themselves, “Have I even ordered from Apple Store lately?”. The email includes spelling mistakes (*Reicept*), it comes from a phoney business address, it is not personalised, and it is inviting you to open the attachment.

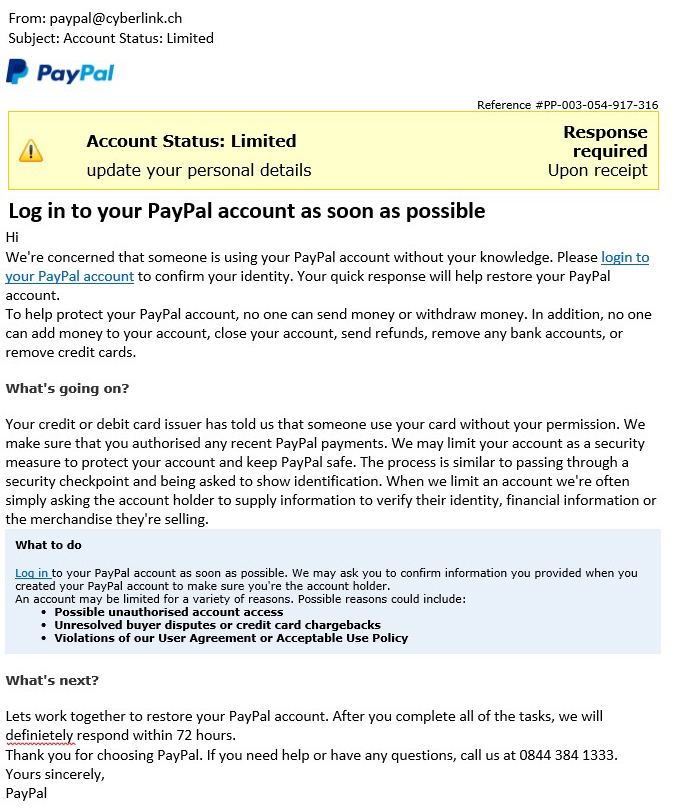


**Email 4**

This email hasa spelling mistake …”definietely” near the end – a frequent sign of a phishing email.

The sender’s email does not look like a genuine company email.

The email is not personalised.

 There is a suggestion that something bad might happen if you don’t follow the instructions.

**Task 5**

List the ways you can reduce the risk of being a victim of phishing.

**Tip:** Look at the webpage <http://www.banksafeonline.org.uk/node/9>

**This site gives the following advice:**

*Be wary of emails that:*

* *Are unsolicited and supposedly come from a reputable organisation, such as a bank or credit card company.*
* *Do not use your proper name, but instead have a vague greeting such as “Dear customer” or “Dear Sir/Madam”.*
* *Request your personal information such as username, password or bank details.*
* *Have addresses which do not match the actual website of the organisation.*

*Remember:*

* *Do not open or forward emails which you suspect might be spam.*
* *Never visit a website from a link in an email and then enter your personal details, as the email could be from a fraudulent source.*
* *Be cautious about any unexpected changes to your bank’s website which involve you being asked for more information than you normally provide.*
* *Check the website address - the login page on your bank’s website address should start with “https”.*

There are many other sites giving information on this topic. Look up “Threats to data security”.