# Homework 3 Internet security

1. Two writers are sharing draft sections of a book they are collaborating on together electronically. They are concerned other people may intercept these communications and leak the material.

Explain why encryption might be appropriate. [2]

Since they are sharing files across the internet, it can be intercepted when being sent across the internet. Encryption makes it so that the data is unintelligible unless you have a key to decrypt (decode what the data says). If it is intercepted, the hacker or thief cannot understand and use the data because they don’t have a key to determine what the data actually is.

1. Network security can be enhanced by the use of a firewall and a proxy server.
   1. Define what is meant by a firewall. [1]  
        
      A network security device that manages the opening and closing of ports in order to prevent unauthorised / unrecognised / malicious data from entering, and important / vital information and data from leaving to go to an unknown location.
   2. Explain how content filtering within a proxy server can provide network security. [2]

The proxy server can check where the data is coming from, and make inspections on the data such as who sent it as well. If the data is of a certain criteria, e.g a suspicious software that is being sent from an unknown user from an unknown location, it is most likely harmful and therefore discarded and prevented from being redirected to the user’s computer which is linked to the proxy server.

1. Malicious software introduced to a network can cause damage to operating systems and data loss.
   1. Explain the differences between a Trojan, a virus and a worm. [2]

A trojan is a software or application that disguises itself to be useful or innocent, but actually is a malicious piece of software that will run itself once the user buys into it (downloads it for example and runs it)

A virus is a kind of malware that is a code that runs and spreads itself to other devices connect to the infected computer once the user executes it.

A worm is a standalone malware that is a computer program that spreads itself to other computers, unlike a virus it is just a program by itself, viruses might be embedded in another software or hidden.

* 1. Describe **three** precautions that users can take to minimise the risk of   
     introducing malicious software onto a single computer. [3]

Not pressing on suspicious links / downloading random advertisements and unofficial software

Getting antimalware softwares like antiviruses

Using proxy servers when browsing or sending things so that people dont know who you are and send malicious software to you.

[Total 10 Marks]