Activities: Solutions

*Written module activity, Page 101*

1. Malware

2. Social engineering refers to techniques to convince people to give out information or provide access to their computers.

   Phishing attacks are normally done via e-mail and they attempt to con the user into giving out personal and confidential details such as PIN numbers and passwords, etc. by posing as a legitimate organisation, such as a bank.

3. Adware

4. A bot (or ‘robot’) refers to a computer that has been compromised (or infected) and which can be controlled remotely when it is on and connected to the Internet. It is sometimes called a ‘zombie’ and the computer’s resources (such as computing power) can be ‘illegally used’ as part of a group of infected computers to flood a server with requests for information. The attack is successful if the server becomes so overwhelmed that normal users cannot access the system.

5. It is a program that is written to disrupt the normal functioning of a computer without the owner’s knowledge or consent.

6. A computer worm is able to distribute itself over a network, normally via e-mail, without the user even running an infected program.

7. Spyware is software that tries to monitor and track the way you use your computer. It then sends this information to third parties without your consent or knowledge. A keylogger is software that records your keystrokes as you type and can even possibly record the movements of your mouse and take screenshots of what is displayed on your screen in an attempt to find your usernames and passwords, etc.

   When using public computers you cannot be sure that those computers do NOT contain spyware.

8. Pharming refers to when a computer is ‘hacked’ so that when the user types in a ‘valid’ URL (or web address) in their browser (such as that of their Internet banking site) they are taken to another website, which is often a replica.

9. You receive electronic junk mail containing many unwanted and sometimes embarrassing adverts via e-mail.

10. It is the forgery of an e-mail header so that the source of the e-mail appears to be from a different sender or origin.

11. A Trojan is a destructive program disguised as a useful application.
12. A card skimmer is a device that reads and stores the data on the magnetic strip of a bank card or credit card. It allows criminals to write this data to a new, duplicate card that they can use.

13. Any three of the following reasons are correct:
   - Most computer crime happens in the 'virtual world'.
   - It is difficult to track, trace and identify computer crime.
   - It is also very difficult for most people to fully understand computer crime and to protect themselves against it.
   - Police lack the resources to combat it.
   - It can occur across international borders, etc.

14. It is important to password-protect wireless networks because then no one can illegally access your data and files and they also cannot access your Internet or steal bandwidth.

15. An identity thief collects data that can be used to help them pretend that they are someone else in cyberspace.

   Any suitable example (such as setting up a fake Facebook account by using someone else’s details) can be given.

16. They do so in order to prevent data theft (such as the theft of trade secrets, design secrets and financial information) by copying the data onto a portable storage device.

17. SharePoint and Chrome

18. Anti-virus software uses virus ‘definitions’ to detect the signs or specific traces that a specific virus leaves. Anti-virus software therefore needs to be updated regularly to update the list of virus ‘definitions’ to include ‘new’ viruses.

19. A firewall is software or hardware that acts as a barrier between your computer and the Internet. It checks which programs are trying to access your computer via the Internet and it also checks which programs are trying to access the Internet from your computer. It can then be set to allow or block the program(s).

   A firewall will therefore not prevent viruses which can be unknowingly downloaded by the user from the Internet and it will also not prevent viruses that are spread by the use of infected portable media such as flash drives, etc.

20. Anti-spyware software detects spyware by using ‘definitions’, so the anti-spyware software needs to be updated so that newer forms of spyware can be detected. In addition, anti-spyware programs also maintain a database of websites known to spread spyware.

21. Any four of the following measures are correct:
   - Be careful when installing free software from the Internet.
   - Have good password policies.
   - Install anti-virus and anti-spyware software and keep the software updated.
   - Don’t give out personal information.
   - Don’t click on links in pop-ups.
• Don’t open attachments or programs unless you are sure of what they are.
• Don’t be gullible – if something sounds too good to be true, it probably is.