Task A

1. In the table below, look at the different threats to data you’ve covered over the past few weeks. Identify and justify a strategy to prevent this from happening.

Try and provide a different answer to help each one where possible. You may need to re-visit topics from the past to help you such as: operating systems and utility programs.

|  |  |  |
| --- | --- | --- |
| **Threat** | **Recommended prevention strategy** | **Justification of chosen strategy.** |
| Phishing | * Never click on emails for unknown senders. * Hover the link provided to check to see if it’s genuine. In most cases, it doesn’t match up the URL of the company it’s come from. * Double check email address/sender name. * Contact the website of the company this email has claimed to have come from for further verification. * Report the email to anti-phishing agencies. * Block the sender * Avoid entering any personal information. | Any suitable justification to the recommended strategy. |
| Shouldering | * Be aware of who is standing or sitting around and behind you * Spend more for a screen filter or protector to obscure the visibility of the display * Never give your password or any vital information to anyone * Locate a quiet spot away from the crowd * As much as possible, never open personal accounts in public * Tilt your device, block their view, sit out of their view |  |
| Trojan horse virus | * Never download or install software from a source you don’t trust completely. * Never open an attachment, click a link, or run a program sent to you in an email from someone you don’t know. * Update your operating system’s software as soon as the updates are available. * Look out for sites that have security certificates – their URL should start with https:// rather than http:// - the “s” stands for “secure” and there should be a padlock icon in the address bar too. * Avoid clicking pop-ups and banners. * Use of strong passwords. * Install a firewall * Regularly backup your data. |  |
| Worm virus | * Install some good anti-malware software. * Avoid opening suspicious emails, a place where worms can appear. * Ensure your operating system is up to date. |  |
| Brute force attack | * Use an advanced username and strong password. * Remove any unused accounts with high-level permissions. * Limit the number of attempts to login/lock account after a number of unsuccessful attempts. * Use of CAPTCHA for repeated login attempts. * Use of encryption. * Use two-factor authentication. |  |
| Packet sniffers | * Encryption * The use of VPN * Avoid using public networks, especially if it’s to use websites where a login is required. |  |

1. Organisations could backup data in case of a cyber-attack.

Identify the most appropriate backup method that could be used in this situation.

|  |
| --- |
| Incremental backup could be performed to ensure that data modified since the previous backup is up-to-date.  GFS backup could be a good method to use because it allows data to be stored on site and off site. |

1. Physical security is just as important as digital security.

In the table below, describe each prevention method and explain how this keeps the data secure. The first one has been done for you.

|  |  |  |
| --- | --- | --- |
| **Prevention Method** | **Description** | **How does this keep help to keep data secure?** |
| Chains and locks | This can be used to fix a computer to a desk. | This stops users from taking the computer or other pieces of hardware. |
| Lock screens | This could be pressing CTRL + ALT + DEL to lock the screen. | Stops other users accessing files, folders and other important data |
| People need to be authorised to enter. | May need to sign up when they enter the building. | This helps to authenticate the person and prevent unauthorised access. |
| Swipe cards | A card which has a magnetic strip that the user swipes through a machine. The card will have the user’s details stored. | This will allow authorised users to entered locked rooms. |
| Fit blinds | To cover the windows | This is people can’t see in and spot valuable equipment. |
| CCTV | Cameras to be installed inside and outside. | This can be used to monitor activity. |
| Burglar alarm | These could be fitted in each room at points where entry is restricted. | Can stay in operation when nobody is on site. |
| Security keypads | Users required to enter a PIN code to access. | This unique number should only be known by authorised users. |
| Biometrics | This could face, iris or fingerprint recognition. | Using the characteristics of that person to uniquely identify them.. |