Task A

1. What is a trojan virus?

|  |
| --- |
| A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. |

1. How does a trojan virus work?

|  |
| --- |
| * A user falls victim to a phishing or other social engineering attack by opening an infected email attachment or clicking on a link to a malicious website. * A user sees a pop-up for a fake antivirus program that claims your computer is infected and invites you to run a program to clean it up. This is known as “scareware”. In reality, users are downloading a Trojan onto their device. * A user visits a malicious website and experiences a drive-by download pretending to be helpful software. * A user downloads a program whose publisher is unknown from an untrustworthy website. * Attackers install a Trojan through exploiting a software vulnerability or through unauthorised access. * Hackers create a fake Wi-Fi hotspot network that looks like one a user is trying to connect to. When the user connects to this network, they can be redirected to fake websites containing browser exploits that redirect any file they try to download. |

1. What impact could a trojan virus have on a user?

|  |
| --- |
| * Poor device performance – for example, running slowly or frequently crashing (including the infamous “blue screen of death”) * The desktop has changed – for example, the screen resolution has altered, or the colour appears different * The taskbar has changed – or perhaps disappeared altogether * Unrecognised programs appear in your task manager – you didn’t install them * An increase in pop-ups – not just ads but browser pop-ups offering products or antivirus scans which, when clicked on, download malware onto your device * Being redirected to unfamiliar websites when browsing online * An uptick in spam emails |

1. What measures can users put in place to protect themselves from a trojan 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. |

Task B

1. What is a computer virus?

|  |
| --- |
| A type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. |

1. How does a computer virus work?

|  |
| --- |
| Once a virus has successfully attached to a program, file, or document, the virus will remain idle until circumstances cause the computer or device to execute its code. In order for a virus to infect your computer, you have to run the infected program, which in turn causes the virus code to be executed. |

1. What impact could a computer virus have on a user?

|  |
| --- |
| * Frequent pop-up windows. * Changes to your homepage. * Mass emails being sent from your email account. * Frequent crashes. A virus can inflict major damage on your hard drive. This may cause your device to freeze or crash. It may also prevent your device from coming back on. * Unusually slow computer performance. A sudden change of processing speed could signal that your computer has a virus. * Unknown programs that start up when you turn on your computer. * Unusual activities like password changes. This could prevent you from logging into your computer. |

1. What measures can users put in place to protect themselves from a computer virus?

|  |
| --- |
| * Install anti-malware software * Avoid clicking on any pop-up advertisements. * Always scan your email attachments before opening them. * Always scan the files that you download using file sharing programs. |

Task C

1. What is a computer worm?

|  |
| --- |
| A type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage. |

1. How does a computer worm work?

|  |
| --- |
| Computer worms could arrive as attachments in spam emails or instant messages. Once opened, these files could provide a link to a malicious website or automatically download the computer worm. Once it’s installed, the worm silently goes to work and infects the machine without the user’s knowledge. |

1. What impact could a computer worm have on a user?

|  |
| --- |
| * Modify and delete files * Add additional malicious software onto a computer. * Increased usage of system resources because it makes copies of itself over and over. (e.g. increased use of hard drive and/or bandwidth) * Steal data by installing a back door so hackers can gain control of a computer and its system settings. |

1. What measures can users put in place to protect themselves from a computer worm’?

|  |
| --- |
| * Install some good anti-malware software. * Avoid opening suspicious emails, a place where worms can appear. * Ensure your operating system is up to date. |