Task A

1. What is a bot?

|  |
| --- |
| A software program that performs automated, repetitive, pre-defined tasks. Bots typically imitate or replace human user behaviour. |

1. How does a bot work?

|  |
| --- |
| Good bots carry out useful tasks, however, bad bots – also known as malware bots – carry risk and can be used for hacking, spamming, spying, interrupting, and compromising websites of all sizes. |

1. What impact could a bot have on a user?

|  |
| --- |
| * Steal financial and personal information. * Criminals may use botnets to create DoS and DDoS attacks that flood a legitimate service or network with a crushing volume of traffic. * To extort money from victims * Cybercriminals may also lease their botnets to other criminals who want to send spam, scams, phishing, steal identities, and attack legitimate websites and networks. * Your computer keeps crashing without an identifiable reason. * Applications that previously worked seamlessly now work in fits and starts. * Programs which previously loaded quickly are now slow to start. * The computer takes a long time to shut down or does not shut down properly. * Your internet access slows to a crawl. * The browser features components you didn’t download. * Windows Task Manager shows programs with cryptic names or descriptions. * Settings have changed, and there is no way to reverse them. * Pop-up windows and advertisements appear even when you are not using a web browser. * The fan goes into overdrive when the device is idle. * Friends and family report receiving email messages from you, but you did not send them. * You cannot download operating system updates. |

1. What measures can users put in place to protect themselves from bots?

|  |
| --- |
| * Install anti-malware software * Ensure all your software is up to date * Use a strong password * Only click on links you trust and avoid untrustworthy websites and ads * Install a firewall * Use a bot manager - can be used to allow the use of some bots and block the use of others that might cause harm to a system |

1. Many organisations use bots. In the table below, identify some advantages and disadvantages to using computer/internet bots.

|  |  |
| --- | --- |
| Advantages | Disadvantages |
| Faster than humans at repetitive tasks  They save time for customers and clients.  They reduce labour costs for organisations.  They are available 24/7  Organizations can reach large numbers of people via messenger apps.  They are customisable.  They are multi-purpose.  They can offer an improved user experience. | Bots cannot be set to perform some exact tasks, and they risk misunderstanding users – and causing frustration in the process.  Humans are still necessary to manage the bots as well as to step in if one misinterprets another human  Bots can be programmed to be malicious.  Bots can be used for spam. |

Task B

1. What is a rootkit?

|  |
| --- |
| A type of malware designed to give hackers access to and control over a target device. |

1. How does a rootkit work?

|  |
| --- |
| Rootkits can sometimes appear as a single piece of software but are often made up of a collection of tools that allow hackers administrator-level control over the target device. This could be done via a phishing/social engineering attack, weakness in software (if it hasn’t been updated) or through files. |

1. What impact could a rootkit have on a user?

|  |
| --- |
| * Blue screen * Unusual web browser behaviour or web pages don’t function properly. * Slow device performance * Windows system settings change without permission/knowledge. |

1. What measures can users put in place to protect themselves from rootkits?

|  |
| --- |
| * Install good anti-malware software. * Keep software up-to-date. * Match out for suspicious emails that may look like a phishing attack. * Download files from trustworthy sources. |

Task C

1. Back in 2017, the NHS were a victim of a ransomware attack.



Use the internet to do some research that will help you answer the following questions.

1. How was this ransomware attack on the NHS executed?

|  |
| --- |
| The ransomware was labelled ‘Wannacry’ and the origins of this attack occurred when emails were sent to staff who were tricked into opening attachment which release malware onto the system. Once computer’s became affect, the files become locked and encrypted and the only way they were able to access this is through a payment. |

1. What impact did this attack have on the NHS and it’s patients?

|  |
| --- |
| It resulted in the cancellation of thousands of operations and appointments which impacted emergency patients.  Staff were forced to revert to pen and paper and use their own mobile phones after the attack affected key systems, including telephones. |