|  |  |
| --- | --- |
| 1a | Designed to gain unauthorised access to a computer system (1)   * In order to disrupt it’s functioning or collect information (1) |
| 1b | • Software that was installed from an untrustworthy source, for example, screensavers, etc.  • Existing anti-malware software is out of date  • Out of date system software/application software  • Out of date browser  • Out of date firewall  • Infected removable drives  • Exploitation of a software vulnerability  • Various social engineering techniques, e.g. phishing  • Scareware  • Infected email attachment  • Infected link  • Spam email  • A hacked website  • Fake website  • Popup software  • Illegal file sharing  • Distributed denial of service  • Adware   * • Rootkits |
| 1c | 1 mark for naming threat, 1 for description, 1 for prevention. Max 3 per threat  e.g.   Virus / trojan / worm   Piece of software/code/a program that replicates itself // causes damage e.g. editing/deleting files   Running anti-virus/anti-malware software // don’t download from unknown sources // don’t click on unknown links   Spyware / keylogger   Piece of software/code/a program that records actions/key presses and sends this data to a third party for analysis   Running anti-spyware/anti-malware software/firewall  Other examples accepted. |