|  |  |
| --- | --- |
| 1a | * Staff respond to fake email * Staff respond to fake link * Staff respond to fake website * Staff respond to spam * Staff respond to popup software fake instant messages * Staff respond to social media messages, ‘likes’, etc. |
| 1b | * Acquisition of user names and passwords * Acquisition of financial details/credit card details * Identity theft * Data theft * Staff disclose personal/confidential data * Financial data theft |
| 1c | 1 mark for name, 1 mark for brief description   * Blagging (1)….inventing a new scenario to gain sensitive information (1) * Shouldering (1)…..looking over someones shoulder to gain sensitive information (1) * Dumpster diving (1)…… the act of an unwanted party going through the trash at a company whether it be inside or outside the building.(1) * Disgruntled employee (1)…… deleting data on purpose.(1) * Scareware (1)…. programs designed to trick a user into buying and downloading dangerous software (1)   Do not accept other types of phishing as the question states other social engineering techniques. |
| 1d | * Attachment of an exe file – could be a virus * Not personalised – dear customer * Pressurising language – your account has been restricted. * Other reasonable examples can be accepted. |