|  |  |  |
| --- | --- | --- |
| **D** | **Threats to data** | |
| **Physical** | | The device storing the data could be stolen or lost |
| **System** | | Data could be *lost*, *manipulated*, *modified* or *stolen* through hacking attempts |
| **Environmental** | | Natural disasters, such as earthquakes or floods. These could affect the data systems, backups and power supplies |

|  |  |  |
| --- | --- | --- |
| **C** | **Types of social engineering** | |
| **Social Engineering** | | Manipulating people so they give up confidential information |
| **Phishing** | | Directing a user to a malicious website from a bogus email where they will, eg, enter their bank details |
| **Pretexting** | | Pretending to confirm someone’s identity in order to get the information they provide |
| **Baiting** | | Users can get free goods (eg downloads) in return for their confidential details |
| **Quid pro quo** | | Users can get free services (eg IT assistance) in return for their confidential details |
| **Tailgating/ Piggybacking** | | Gaining entry to a room or building by following someone else in who holds the door open |
| **Shoulder surfing** | | Getting access to confidential information by watching someone enter it (eg at a cash machine) |

|  |  |  |
| --- | --- | --- |
| **B** | **Types of malware** | |
| **Adware** | | Software which displays advertising |
| **Bot** | | A computer program which operates by itself |
| **Botnet** | | A large collection of bots, working together |
| **Ransomware** | | Malware which disrupts the use of a system until a ransom has been paid |
| **Rootkit** | | Modifies operating system to avoid detection |
| **Spyware** | | Gathers and reports data from the host |
| **Trojan** | | Poses as legitimate software and must be installed by the user. Does not self-replicate |
| **Virus** | | Hidden in an executable and self-replicates |
| **Worm** | | Malware which self-replicates but does not require an executable file |

|  |  |  |
| --- | --- | --- |
| **A** | **Types of attack** | |
| **Hacking** | | Accessing someone else's data without consent |
| **White hat** | | Hacking but with consent. Generally this is to test for weaknesses and is legal |
| **Grey hat** | | Hacking without consent, and without intent to do damage. |
| **Black hat** | | Hacking with malicious intent |
| **Denial of Service (DoS)** | | An attack which aims to stop a server working by using up all its bandwidth |
| **Pharming** | | Directing a user to a malicious website by an attack on the DNS server |
| **Phishing** | | Directing a user to a malicious website from a bogus email |

|  |  |  |
| --- | --- | --- |
| **A** | **Types of attack** | |
| **Hacking** | | Accessing someone else's data without consent |
| **White hat** | | Hacking but with consent. Generally this is to test for weaknesses and is legal |
| **Grey hat** | | Hacking without consent, and without intent to do damage. |
| **Black hat** | | Hacking with malicious intent |
| **Distributed Denial of Service (DDoS)** | | An attack which aims to stop a server working by using up all its bandwidth. Requests are sent to the server by several different clients at once, sometimes by using a botnet |
| **Pharming** | | Redirecting a user to a malicious website when they follow a link from a legitimate one |

Information Technology: Data Threats

Name: