Name:

Networks: Security

|  |  |  |
| --- | --- | --- |
| **D** | **LECE** | |
| **Lawful interception** | | Checking data as it is transferred between networks by a legitimate entity, typically for purposes of cyber security |

|  |  |  |
| --- | --- | --- |
| **B** | **Preventative Measures** | |
| **Authentication** | | A process for checking the identity of the user |
| **Encryption** | | The process of making data unintelligible except to the intended recipient |
| **Key** | | The method of decrypting an encrypted message |
| **Public / private key** | | An asymmetric encryption technique where the encryption key is public and different to the decryption key |
| **Firewall** | | Software and/or hardware which controls traffic between nodes |
| **Network forensics** | | Investigation to find the cause of cyber crime |
| **Packet-filter firewall** | | Firewall which inspects each packet and drops non-qualifying packets |
| **Penetration testing** | | Testing a system by mimicking different forms of attack |
| **Update** | | The latest version of a software, including fixes of vulnerabilities |
| **User access level** | | The amount of the network that a user has access to |
| **Wifi Protected Access (WPA)** | | Encryption of wireless signals |

|  |  |  |
| --- | --- | --- |
| **A** | **Security policies** | |
| **Acceptable use** | | Policy about what a user might reasonably use IT equipment for |
| **Email** | | Policy about what can be sent over email |
| **Incident response plan** | | Policy about what to do if there is a security failure |
| **Internet** | | Policy about what data is allowed in and out |
| **Password** | | Policy about how often passwords should change and what complexity they must be |
| **Remote access** | | Policy about how to access the network from off-site |
| **Web** | | Policy about what sites can be visited |
| **Wireless** | | Policy about how access points are managed |

|  |  |  |
| --- | --- | --- |
| **C** | **Malware** | |
| **Adware** | | Software which displays advertising |
| **Key logger** | | Spyware which stores every keystroke in a file |
| **Ransomware** | | Malware which disrupts the use of a system until a ransom has been paid |
| **Rootkit** | | Modifies operating system to avoid detection |
| **Scareware** | | Creates alarm and causes the user to follow a malicious link in their panic |
| **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 |