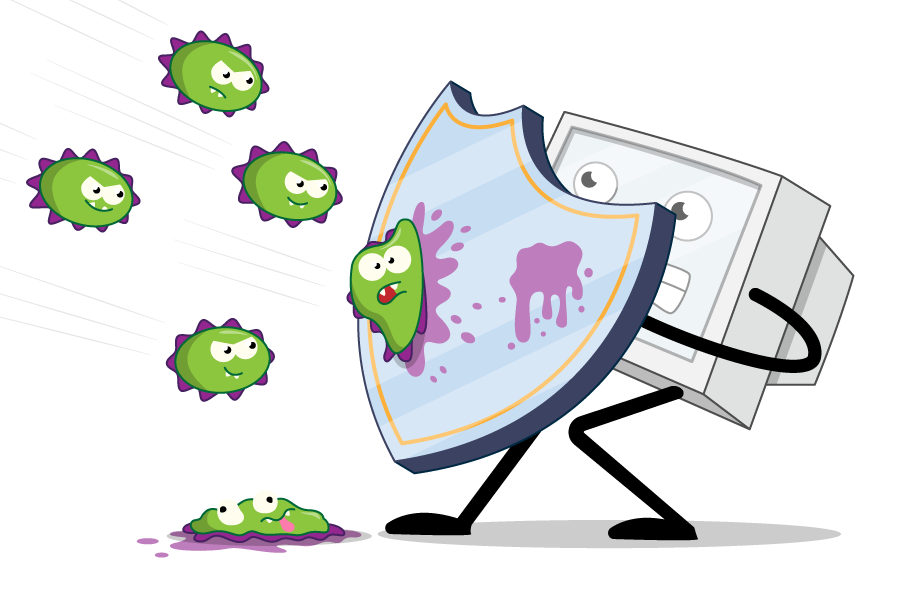
Cybersecurity definitions booklet

# You will build up the definitions in this booklet over the coming weeks. At the end of the unit, your understanding and recollection of the definitions will be assessed.

**Definitions from Lesson 1 – The cost of cybercrime**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Cybersecurity |  |
| Network security |  |
| Hackers | Individuals who will violate computer security for malicious or financial reasons; AKA crackers. |
| Planting the flag | Individuals who may seek financial reward for finding vulnerability but are more interested in finding vulnerabilities than gaining for themselves. |
| Ethical hackers | Individuals whose activities are designed to test and enhance computer security; AKA ethical hackers. |
| Hacktivists | Individuals who use technology to announce a social, ideological, religious, or political message. |

**Definitions from Lesson 2**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Social engineering | The psychological manipulation of people into performing actions or divulging confidential information. |
| Keylogging |  |
| Tailgating |  |
| Pharming |  |
| Phishing |  |
| Digital devices |  |
| Eavesdropping |  |
| Shoulder surfing |  |
| Pretexting | Attackers focus on creating a good pretext, or a fabricated scenario, that they can use to try and steal their victims’ personal information. This type of attack commonly takes the form of a scammer who pretends that they need certain bits of information from their target in order to confirm their identity. |
| Baiting | Similarly to phishing attacks, the scammer promises items or goods to entice their victims. |
| Quid pro quo | These attacks promise a benefit in exchange for information, usually a service. |

**Definitions from Lesson 3**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Malware |  |
| Trojan | A malicious computer program that tricks users into willingly running it is called a ‘Trojan horse’ or simply a ‘Trojan’. They can be delivered via internet downloads, infected USBs, or email attachments. |
| Zombie |  |
| Data breach/data interception |  |
| Brute force attack |  |
| DoS | A denial of service attack (DoS attack) is a cyberattack in which a criminal makes a network resource unavailable to its intended users by flooding the targeted machine or website with lots of requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. |
| DDoS | In a distributed denial of service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This makes it impossible to stop the attack simply by blocking a single source. |
| SQL injection | SQL injection occurs when malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). |
| Virus |  |
| Worm |  |
| Ransomware | This type of Trojan can modify data on a computer or device so that it doesn’t run correctly or so that users can no longer use specific data. The criminal will only restore the computer’s performance, or unblock data, after the victim has paid them the ransom money they demand. |
| Spyware | Programs that can spy on how a user makes use of their computer or device, for example by tracking the data entered via a keyboard, taking screenshots, or getting a list of running applications. |
| Adware | Software that contains advertisements embedded in the application. It is not always a bad thing and is considered a legitimate alternative offered to consumers who do not wish to pay for software. |
| Exploit | Code that takes advantage of a security vulnerability in an operating system, application, or any other software code, including application plug-ins or software libraries. |

**Definitions from Lesson 4**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Encryption |  |
| Caesar cipher | The cipher works by giving a number value to a key. Each plain text letter is replaced by a new letter: the one found at the original letter's position in the alphabet, plus or minus the value of the key. |
| Encryption key | An encryption key is a piece of information, usually random characters, used by a software algorithm to encrypt data or a message into a form that is unreadable (encryption) and allow the data or message to be made readable again (decryption). |
| Asymmetric encryption |  |
| Input sanitisation | Including code that removes any SQL commands from the input data, preventing a hacker from gaining control of a database. |
| Code reviews | Plans to review and test code in an attempt to discover vulnerabilities in programs before cybercriminals find them. |
| Modular testing | Testing that checks individual subprograms, subroutines, classes, or procedures in a program. |

**Definitions from Lesson 5**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Firewall |  |
| Antivirus software | Software that is designed to detect and block attacks from malware. Some operating systems have their own inbuilt antivirus software. |
| Network policy |  |
| Archiving policy |  |
| Acceptable use policy | States how the network may be used, including what is and is not acceptable, e.g. online shopping or gambling. |
| Backup policy | A backup is a copy of data or files. A backup policy is a written statement that specifies how backups will be organised in an organisation, including frequency, by whom, using what media, and how the files are labelled. |
| Disaster recovery policy |  |
| MAC address | A unique identifier that is used as a network address in communications within a network. |
| MAC address filtering | This limits the devices that can access a network, either including or excluding specific devices by using their unique MAC address. |
| MAC address white list | MAC addresses permitted to access a network. |
| MAC address black list | MAC addresses banned from a network. |

**Definitions from Lesson 6**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Penetration testing  (Pen test) |  |
| Network forensics | The monitoring and analysis of computer network traffic for information gathering and intrusion detection. |
| Physical security |  |
| White box pen test | Testing in which the tester has full knowledge, more like a malicious insider. |
| Grey box pen test |  |
| Black box pen test | Testing in which the tester has no knowledge, more like an external hacker. |

This resource is licensed under the Open Government Licence, version 3. For more information on this licence, see [ncce.io/ogl](http://ncce.io/ogl).