Social engineering techniques 1

GCSE

P P

The table below provides definitions for common social engineering techniques. Drag and drop the words into the spaces provided to match the technique to the definition.

Technique	Definition
	An attack in which the victim receives a message disguised to look like it has come from a reputable source (for example, a bank), in order to trick them into giving up personal information.
	An attack in which the perpetrator invents a scenario in order to convince the victim to give them personal information or money.
	Deceiving users by sending them to a fake website that the user believes is the real one, with the intention of tricking them to submit personal data.

Items:

Blagging Shouldering Pharming Phishing

Cookies definition

GCSE

P P

Complete the paragraph that describes cookies using the words provided. Choose the most appropriate word for a marked spot and drag it into position.

A cookie is a [ ] file that contains a relatively [ ] amount of data. The file is stored on [ ]. It is exchanged between your computer and the [ ] when you browse a website. The data in the file is used to [ ] activity and to [ ] content.

Items:

small | track | web server | text | binary | large | personalise | your computer

Types of malicious software 2

GCSE

P P

Using the statements provided, **match** the form of attack to the correct description by dragging the items into the table.

Form of attack	Description
	Replicates and is designed to infect as many systems as possible. Does not require a host program.
	Appears to be a legitimate file, but actually performs malicious actions.
	Replicates and attaches to other programs or files to spread over computer systems.

Items:

Trojan Virus Worm

Types of malicious software 5

A Level

P P

Malware refers to **malicious software**, and describes programs designed to cause damage to computer systems, corrupt or change files, steal data, or cause disruption to services. There are several types, including viruses, worms, and trojans.

Select the **two** true statements about malware.

- [ ] Trojans look like legitimate software, such as free games, emojis, or utility programs, but they contain malware that installs itself at the same time.
- [ ] A virus can only be caught by clicking on a malicious link or attachment.
- [ ] Antivirus software can only remove viruses, not worms or trojans.
- [ ] Worms can spread autonomously, for example, by emailing themselves to everyone in your address book.
- [ ] A worm cannot install a back door to enable remote control of a computer.

Malware protection 1

A Level

C C

Select **four** options that describe appropriate measures to minimise malware risks.

- [ ] Only open emails without attached files
- [ ] Receive and share files only with users on a local area network
- [ ] Choose secure passwords
- [ ] Use of firewall
- [ ] Use defragmentation software often
- [ ] Perform regular computer scans
- [ ] Maintain and update anti-virus software
- [ ] Use biometric authentication to log in to your computer

MAC addresses 1

A Level

C C

A MAC address is a unique identifier given to a network interface card. MAC address filtering is a technique that is sometimes used to help secure a network. However, this approach to network security has limitations.

Which one of the following statements is **false**?

- MAC addresses can be obtained by intercepting network packets.
- A computer can have multiple MAC addresses.
- MAC addresses can be spoofed.
- MAC addresses are irrelevant if a computer has an IP address.

Limiting devices on a network

A Level

P P

A company wants to control which devices can use their private network. They would like to make sure that only devices **owned by their employees** are able to connect to the WiFi inside their offices.

Which of the following device characteristics should the company use to identify the devices that they will allow to connect to the network?

- IP Address
- Device model number
- MAC address
- Device name

Password rules

A Level

P P

A website uses the following rules to determine if a password can be used. The password must be:

At least 8 characters long AND contain at least 3 out of the following 4 character types:

- A lowercase letter
- An uppercase letter
- A number
- A symbol

OR

At least 16 characters long

Which **four** passwords can be used on this site?

- [ ] pAsw0rd
- [ ] horsebatterycomputerstaple
- [ ] fRiEnDenter
- [ ] aA1,aA1,
- [ ] @1234/221B+24601!
- [ ] saveEarth89

Memory vulnerabilities

A Level

C C

Quality of code is essential to avoiding vulnerabilities that can be exploited by malware. One code quality issue is a type of memory fault, where a data structure is not large enough for certain values of data to be passed into it. Malware can exploit this by making data spill out of the field and into nearby memory, overwriting program instructions.

What is the name for this type of error?

- Fault
- Buffer underflow
- Stack flow
- Excessive overflow
- Buffer overflow

SQL injection

A Level

C C

Many websites ask users to fill in and submit information. Examples include places to type usernames, passwords, or credit card details. Often these forms are linked to a database that can record the data. A SQL injection occurs when hackers type malicious commands using SQL code into the input boxes, with the intent to gain unauthorised access to the database's contents.

Read the options below and select an example of a SQL injection.

- **Option D**

```
SELECT * FROM Users WHERE Name ="noName" AND Pass =""
```

- **Option C**

```
SELECT * FROM Users WHERE Name ="Username" AND Pass ="myPassword"
```

- **Option A**

```
SELECT * FROM Users WHERE Name ="" or ""="" AND Pass ="" or ""=""
```

- **Option B**

```
SELECT * FROM Users WHERE Name ="John Doe" AND Pass ="myPass"
```