# GCSE Computer Science
# Topic 1.6 System Security (2)

**Users** (people who use computers) are often described as the ***weak point*** in terms of security.
Some network attacks target people.
***This form of attack is called social engineering.***

**SOCIAL ENGINEERING** is a way of gathering sensitive information or illegal access to networks by influencing / manipulating / tricking people.

**PHISHING** is a social engineering technique which involves sending emails or text messages (SMs) claiming or appearing to be from a bank/ e-commerce site asking for personal details.

**SHOULDERING** is a social engineering technique which involves finding passwords and pins by *watching people* enter them. This could happen in a busy office or at a distance using binoculars or recording equipment.

**BLAGGING** is a social engineering technique which involves a criminal inventing a scenario to persuade a victim to give out information.

Organisations should have **acceptable use policies** which employees must read, sign and abide by.

It should include some of the following terms/ conditions:

- Users must not use their own devices as they may contain malware (e.g. USB drives).
- Users should not download files from the internet (as they may contain malware).
- Users must have strong passwords which should be changed frequently to prevent brute force attacks.
- Users should not leave themselves logged on.

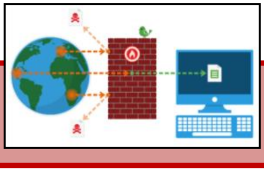
**PEN TESTING**: testing a computer system to find weaknesses that a hacker could exploit.
Testers take the role of hackers to gain unauthorised access.
Assess the security awareness of users and tests the effectiveness of network policies.

**ANTI-MALWARE** software is designed to detect and block attacks from malware. Anti-malware software scans computers and quarantines any malware found.

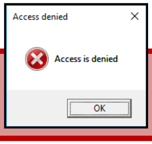
Norton by Symantec McAfee Proven Security AVG Anti-Virus

A **firewall** monitors connections to and from your computer. If it detects a suspicious connection the firewall closes the connection.

Most operating systems include a firewall and it should be turned on by default.



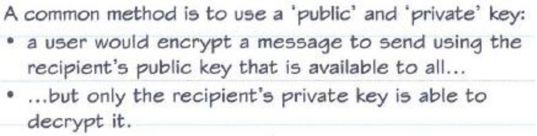
**USER ACCESS LEVELS:** controls which parts of the network different users or groups of network users can access /edit.


Access denied ✕

Access is denied

OK

**ENCRYPTION**: encoding data into an unreadable format so that unauthorised users cannot read it. Can only decoded with a decryption key. Essential for sending data securely.


A common method is to use a 'public' and 'private' key:

- a user would encrypt a message to send using the recipient's public key that is available to all…
- …but only the recipient's private key is able to decrypt it.

**Employee training /education on how to spot social engineering attempts and how to protect themselves / the network is the most effective way to prevent social engineering.**

**Every company should have a network policy that the ICT technicians should enforce.**

A GOOD NETWORK POLICY:

- ❑Use passwords.
- ❑Enforce user access levels.
- ❑Encrypt sensitive data.
- ❑Regularly test the network to find & fix weaknesses.
- ❑Install anti-malware & firewall software.

PASSWORDS are like UNDERWEAR

1. Change them regularly
2. Don't leave them on your desk
3. Don't loan them to anyone

**NETWORK FORENSICS:** Monitoring, recording and analysis of network activity

- Who has logged on
- How many unsuccessful attempts have been made
- What users have done
- What has been deleted.

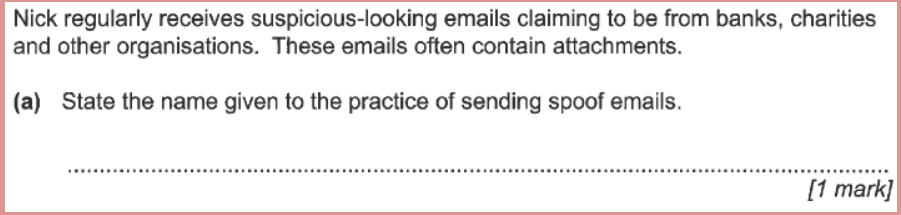
Network forensics can be used as legal evidence if illegal activity is detected.

*** To conduct network forensics a company must have a system of capturing data packings as they enter a network.**

# GCSE Computer Science - Topic 1.6 System Security (2)

## What I need to know:

| |
|---|
| Define social engineering. |
| State the 3 common methods of social engineering. |
| Describe the social engineering technique phishing. |
| Describe the social engineering technique shouldering. |
| Describe the social engineering technique blagging. |
| Describe how best to prevent against social engineering. |
| Describe an ‘acceptable use policy’. |
| Explain some of the terms and conditions that should be included in an acceptable use policy/why they are beneficial to network security. |
| Describe how to create a strong password. |
| Explain pen-testing and how it can help protect a network. |
| Describe network forensics and explain how it can help protect a network. |
| Describe the function of antimalware software. |
| Describe the function of a firewall. |
| Describe how user access levels can help protect a network. |
| Explain how encryption can help secure the data on a network. |
| State the five elements required for a good network policy. |
| Explain how the different elements of a good network policy help protect the security of a network. |

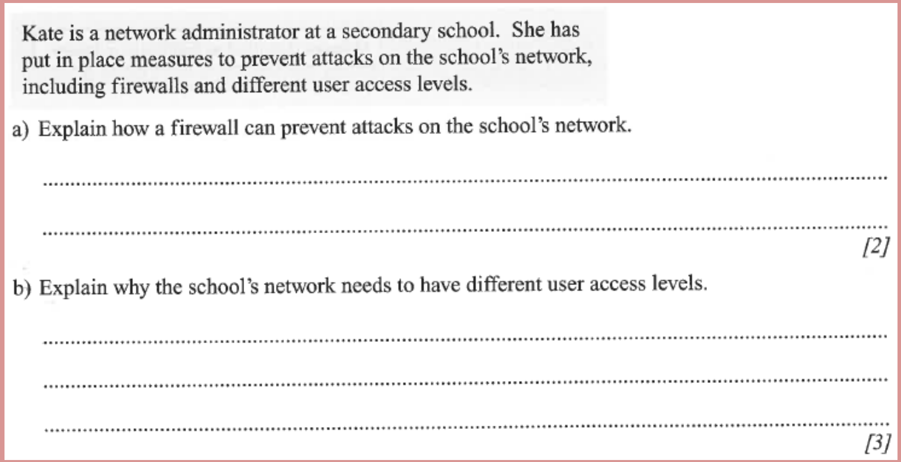


Nick regularly receives suspicious-looking emails claiming to be from banks, charities and other organisations. These emails often contain attachments.

**(a)** State the name given to the practice of sending spoof emails.

.......................................................................................................

*[1 mark]*



Kate is a network administrator at a secondary school. She has put in place measures to prevent attacks on the school’s network, including firewalls and different user access levels.

a) Explain how a firewall can prevent attacks on the school’s network.

.......................................................................................................

.......................................................................................................

*[2]*

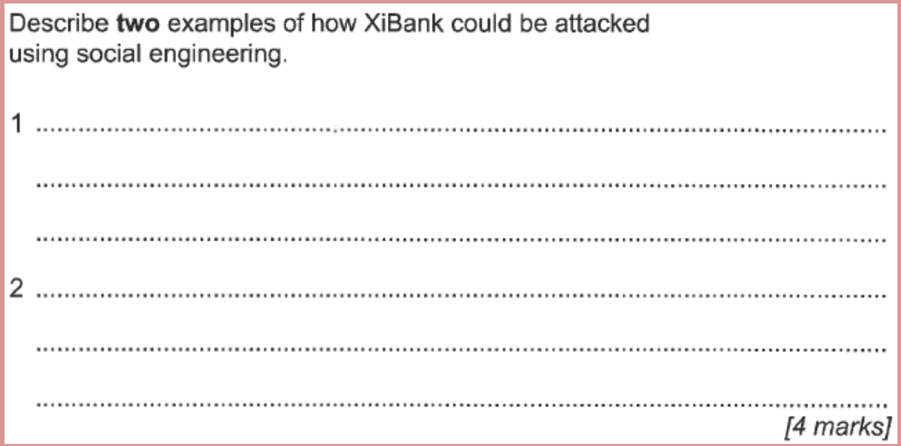
b) Explain why the school’s network needs to have different user access levels.

.......................................................................................................

.......................................................................................................

.......................................................................................................

*[3]*



Describe **two** examples of how XiBank could be attacked using social engineering.

1 .......................................................................................................

.......................................................................................................

.......................................................................................................

2 .......................................................................................................

.......................................................................................................

.......................................................................................................

*[4 marks]*