Network Security

Physical security

When thinking about securing an IT system it's easy to overlook how important it is to keep it physically safe. Locked doors can be as important as firewalls. It is much, much easier to hack a system if you have physical access to the hardware, and easier still if you steal the hardware that contains the data you wish to access.

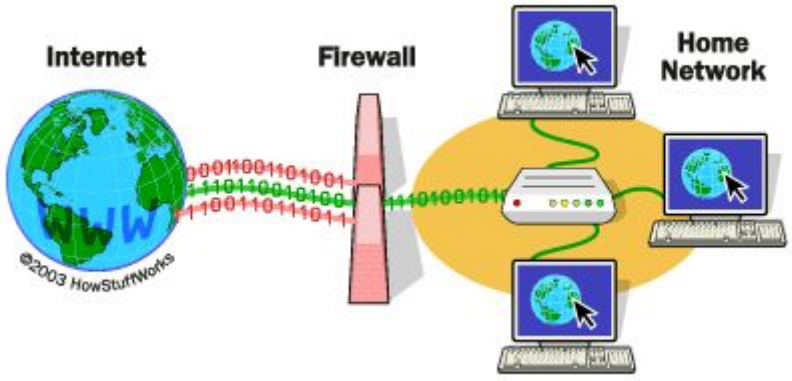
Therefore, computer rooms, and particularly server rooms, should be kept physically safe. Methods include:

- Keep the doors to computer/server rooms locked at all times
- Use swipe cards containing users details for entry to the building/computer rooms
- Install closed circuit television to monitor the building
- Install burglar alarms
- Fit RFID chips (radio frequency identification) to all key equipment - these can be set so an alarm sounds when they leave a specific location.
- Use chains and locks to attach smaller equipment to desks
- Use keyboard locks that shut down keyboards when a user moves away from their desk

Question 1 - In what way does a swipe card give better security than simply having a lock and key system to access rooms or buildings?

Firewalls

A firewall may be a program, or a separate piece of hardware running software, that is designed to protect an internal network from a WAN, such as the internet. It sits on the connection between the network and the WAN and monitors all network traffic in and out. It will block unknown or unauthorized traffic onto the network.



Individual desktop computers usually have software firewalls, but a larger network will often have a device sitting on the internet connection that controls incoming and outgoing traffic for the whole network. If, say, a trojan sneaks onto your computer, it may well attempt to 'connect out' to a hackers computer to allow them to control your computer. A firewall would recognise it as an unknown program and block it's connection. This is why it's important that users don't blindly click on 'allow' when a firewall pops up asking if a program can have access to the internet.

Question 2 - What is a trojan?

Reasons for Network Security

Any computer connected to the internet is vulnerable to attack. In an experiment 15 years ago, a computer running unpatched Windows XP was connected to the internet without a firewall, and it was hacked within 30 seconds. This is because there are programs running online constantly searching for vulnerable computers to break into and install software on.

Computers are, on average, much more secure today. Operating systems have security software built in, the routers we use introduce another layer of protection, and security vulnerabilities in operating systems get patched automatically (if we don't prevent them). However, there are still a large number of programs and individuals seeking to attack us, so it's vital we keep all of this security in place.

What does having good network security do?

- It ensures only authorised users can access the network and its resources
- It ensures that users can only access data relevant to them (so your network might contain the home addresses of all staff, but that doesn't mean you should personally be able to see it unless it's part of your job)
- It prevents misuse - either deliberate or accidental - from employees or users. E.g. stopping them from deleting useful data, installing unauthorised software, taking data away
- It prevents damage to hardware.

Question 3 - Not all damage to systems is malicious, sometimes it's accidental. Give two examples of how users might accidentally damage data or hardware, and suggest a security measure that could be used to prevent it.

Why is this important?

Privacy - the data may be about individuals, and it's important to keep that private (indeed, we may be legally obliged to do so under the DPA)
Financial - the data may be valuable, e.g. a list of clients we do business with, a list of who owes us money.

Business success - good data is vital for running a business successfully, so having it damaged or stolen could cause serious issues.

Authentication

To authenticate is to check whether something is truly what it appears to be. Authentication in computer science usually refers to the way we check that a user is who they say they are, which normally means through a username and password.
Password policy is important. Good passwords should be:

- Long - at least 8 characters
- Contain a combination of numbers, letters and special characters
- Not contain dictionary words
- Not be strongly associated with the user
- Unique - users should not use passwords from other systems or sites
- Should never be written down, emailed, texted, etc.

Question 4 Why is a long password necessary? What benefit do we get from including numbers and special characters in a password?

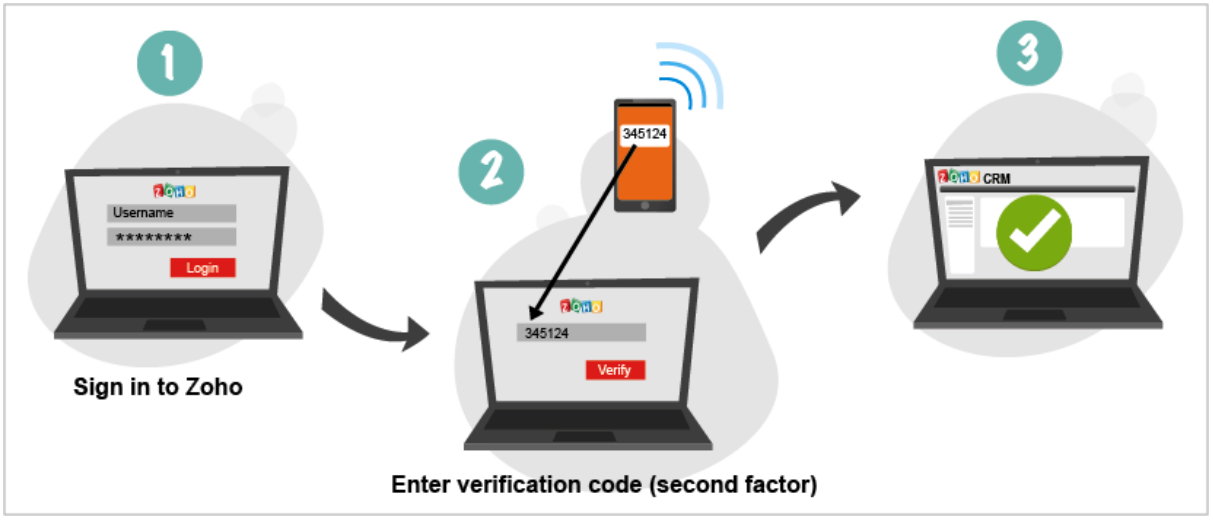
Question 5 Why is it important not to reuse passwords between different sites and systems?

Good password policy used to be to change passwords regularly, but as passwords have become more complex this has become counterproductive. The best solution to passwords is generally to use a password manager, like 1Password or LastPass.

Other forms of authentication include **Biometric**, which involves measuring a part of the body to check on identity (most commonly fingerprints or facial recognition).

Question 6 What is a potential issue with the use of biometric security, particularly if it gets cracked?

Two factor authentication is now commonly used on some systems. This means that in addition to supplying a username and password a user must provide some other information - usually a short code that is texted to their phone, or generated by a special piece of hardware. This means that even if their password is compromised it is difficult for a hacker to access their account.



Question 7 Describe how two factor authentication improves security on a system.

Question 8 “The user is frequently the weakest part of the security of any IT system.” What does this quote refer to? What hacking techniques seek to exploit the ‘weakest part of an IT system’?

Access Control

As discussed elsewhere in this course, access controls can be set on networked systems so that different users have different levels of access. This means that one user might be able to see data that another user cannot access, but perhaps they are not able to edit it whilst a manager could. Common levels of access granted to different files or folders include: no access, read only, read/write and read/write/delete.

Question 9 Imagine a large shop with multiple employees. Describe how access levels might control what data different employees can see and edit, using the examples of a low level shop floor employee, the store manager, and the business owner.