**Task 3 – Protecting IT Systems from security threats**

**Unit 7 - IT Security Systems and Encryption**

**Mohammed Mahin Ibnay Mamun**

**Methods of protection**

**CCTV:**

**Do you think it is an invasion of privacy?**

I believe that having CCTV within an organization is an invasion of privacy since it captures employees and staff. However, if the staff are unaware or refuse permission then it would be against the human rights act (1998).

I also do not consider it to be an invasion of privacy since CCTV cameras are used to catch out criminals and theft. If no harm is being done to the organization, then the CCTV cameras should remain unchecked. For privacy reasons.

The use of CCTV cameras should only be used in the radius of the organisation no further. It should not be used in any changing rooms or toilets.

**Is there too much CCTV?**

A reasonable amount of CCTV equipment should be deployed throughout a company's radius (both inside and outside) without being excessive or too limited. There is one surveillance camera for every 14 individuals, according to CCTV statistics in the UK.

The average amount of CCTV for a home is 2 – 6 cameras. On the other hand, businesses vary their amount of CCTV from 16 – 64. This depends on; the size of the building, whether the business has a car park, if there is more than one entrance/ exit, floors/ rooms, and others.

**How are the images recorded by CCTV systems used?**

An analog camera's video is captured and stored digitally in a DVR (digital video recorder) at the desired resolution and frames per second. After the capture has taken place, Video footage can either be stored on the cloud or local storage, such as a hard drive or microSD card. The image/video can then be used further for example at a court case.

**Is there a possibility that these images could be abused?**

There is a chance of this happening if a hacker takes over your CCTV system. The hacker would have access to your surveillance system and could take pictures or create recordings. Then, the hacker may use the information to blackmail you.

Another example could be: in this case if a burglar broke into your house or shop, and whether they stole anything or not, if your CCTV can pick up images of the burglar then you can use this information in the court or for a police investigation.

**Backing Up Data:**

Backups are copies of computer data made and stored elsewhere with the intention of restoring the original in the event of data loss. Since security cannot be guaranteed, the security of your system depends on well-regulated backups.

Malware infections may cause data to be deleted from an IT system or damaged. In these cases, it is possible to recover the system from backup files.

You must regularly backup your important data preferably weekly to protect against inevitable data loss situations caused by unforeseen events like system crashes.

**Selection of data for backup and storage of backup media:**

**Incremental Backups:**

Incremental backups are security copies that contain only files that have been modified since the last full backup. By using incremental backups, all the data first must be backed up in a full backup first. Therefore, each backup contains less data and is more efficient.

The advantage of incremental backups is that they are quick and not as time-consuming as a full backup. However, the downside is that the incremental backup is processed for each restore operation, which could cause the restore job to take a long time.

**Differential Backups:**

Data backups performed differentially include the entire change history of the files that have been created, updated, or otherwise altered since the last full backup, rather than copying all the data every time. It is this method to perform a full back up at the start, followed by successive backups that reflect any changes. This could also be done with a weekend full backup followed by daily differential backups.

This has several advantages:

* It is faster to back up than to make a full backup.
* Compared to incremental backups, restore is faster.
* Compared to full backup, the storage needs are lower

**IT Disaster recovery plans**

Companies need to consider how they would continue to operate in case of a catastrophe such as a fire, flood, or other disaster. The only use of data backups in these cases is if there is no IT system on which the applications are to be run.

It refers to the process of a company regaining access and functionality of its IT framework after a natural disaster, a cyber-attack, an outbreak of COVID-19 could lead to business disruption.

**Three main types of plans:**

**Hot Site:**

When disaster strikes, a hot site can be defined as a backup site that stores the data in real time and is quickly available. It includes staff to monitor and manage the equipment. Hot sites are fully functional data centres with software, hardware, and customer data.

As an example, if a company's data centre becomes unusable, all data-processing operations can be moved to a hot site.

**Cold Site:**

It is a temporary office that is used as a backup site in the event of a disruption of operations at the primary site. Cold sites are offices but lack the necessary equipment to resume operations immediately.

As part of setting up the company's systems, servers and other equipment would need to be purchased, along with backups of the application data and the system configuration.

**Warm Site:**

An organization's warm site is used in case its primary data centre goes down to recover its technology infrastructure. Warm site contains a fully equipped data centre but no customer information.

**Policies and procedures**

Employees are not directly protected from security threats by organisational policies and procedures; instead, they are made aware of these risks and shown what methods of unsafe behaviour they should avoid.

**In terms of acceptable IT use, organisations should include the following:**

* This document should outline how passwords should be protected, such as not writing them down or allowing anyone else to see them.
* Guidelines for email use should cover how to treat emails from unknown sources with care, including how to handle attachments and web links.
* The disciplinary procedure document should describe the disciplinary consequences for deliberately breaking any of the organization's IT policies.
* There should be guidelines for browsing the internet, including how to avoid inappropriate websites that contain malware and how to avoid downloading files that are infected with malware.
* As members of staff, you may be required to lock desk drawers and file cabinets, secure unattended computers, wear ID badges, challenge strangers, etc.

**Security audits:**

An information security audit is an investigation of the level of information security within an organization. The diverse types of audits and objectives for information security audits can be found within the broader scope of information security audits.

**Security baselines:**

The IT security policy of an organization may, for example, specify that anti-malware software and firewalls must be installed before a system can function properly. Security baselines are often used in organisations to define a secure starting point.

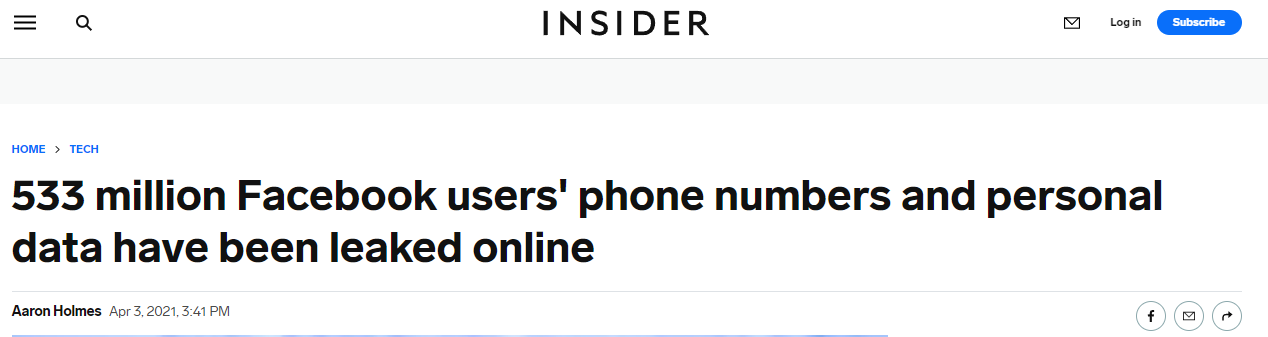
**Avoiding impedance of business operations:**

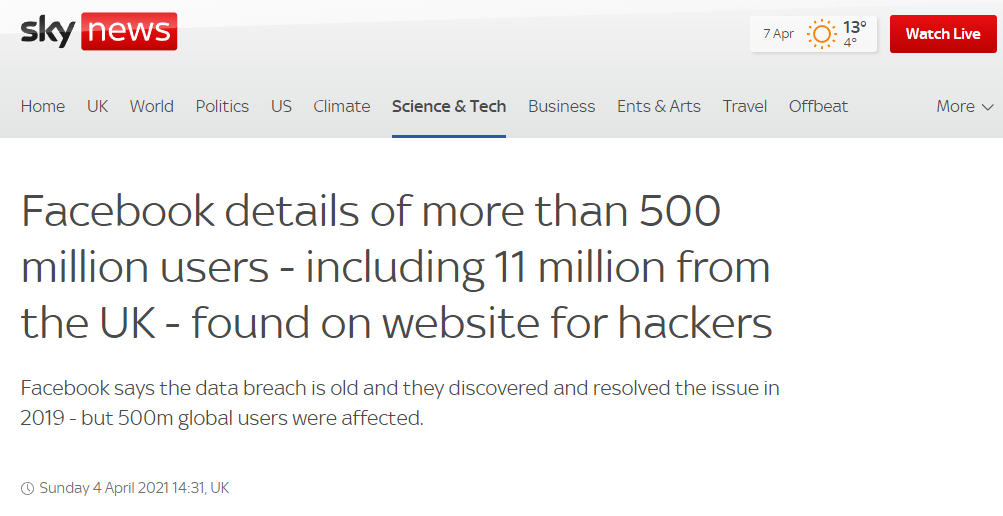
It is crucial to maintain a balance between security and usability when it comes to security policies and baselines: that is, rules implemented for the sake of security should not obstruct businesses in performing their regular business operations.

An example would be Traffic coming into and leaving the network: security system rules that block legitimate incoming or outgoing traffic can frustrate users and increase the number of IT support calls.

**Case study: Search for a case study**

Headlines across the internet are informing us about the data breach which took place not too long ago on a very common software called Facebook. This could have happened due to weak password policies.





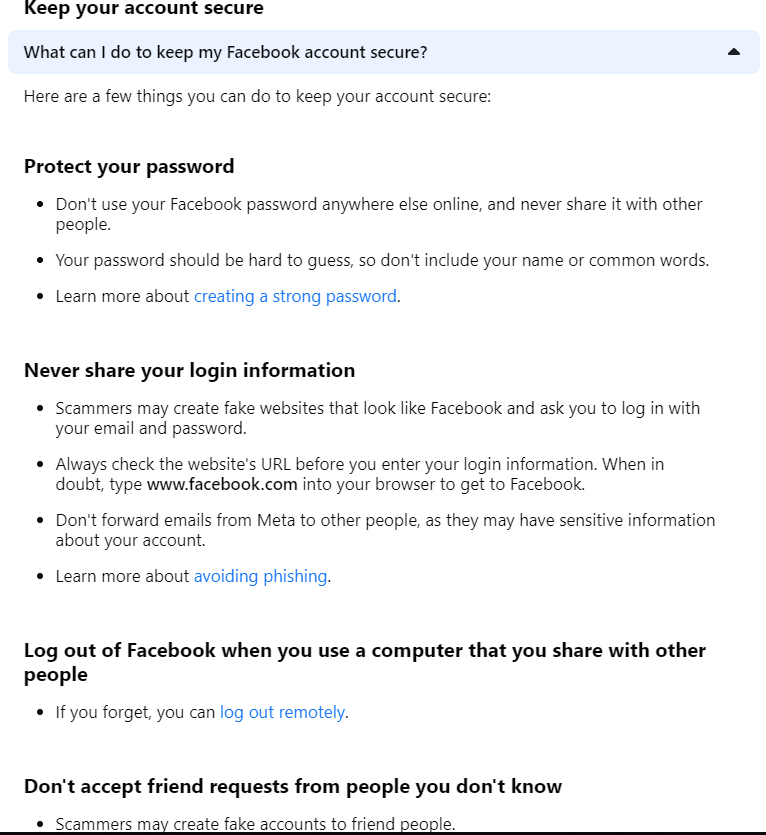
Facebook has many policies: terms & service, data policies and community standards. This breach was affected by the user's data policies. Before you successfully create your Facebook account, you are demanded to read the Facebook data policy and accept. If you choose not to, therefor Facebook will not give you an account.

Facebook warns you that they are collecting this information from you:

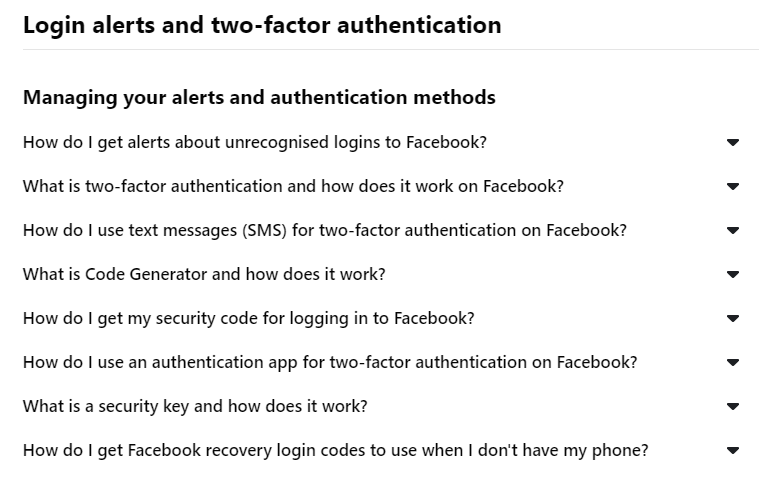
* Connections & networks
* Your usage
* Transaction details
* Device information
* Device operations
* Device signals
* Data from device setting (GPS, location, camera)
* Cookie data

Therefore, if Facebook gets hacked, the criminals will have access over all this information which puts you at huge risk.

However, in the past cases, the data breaches took place and ended up leaking users phone numbers and personal data. The reason the criminals were not able to take over every user was because those users who were safe had a more secure account.

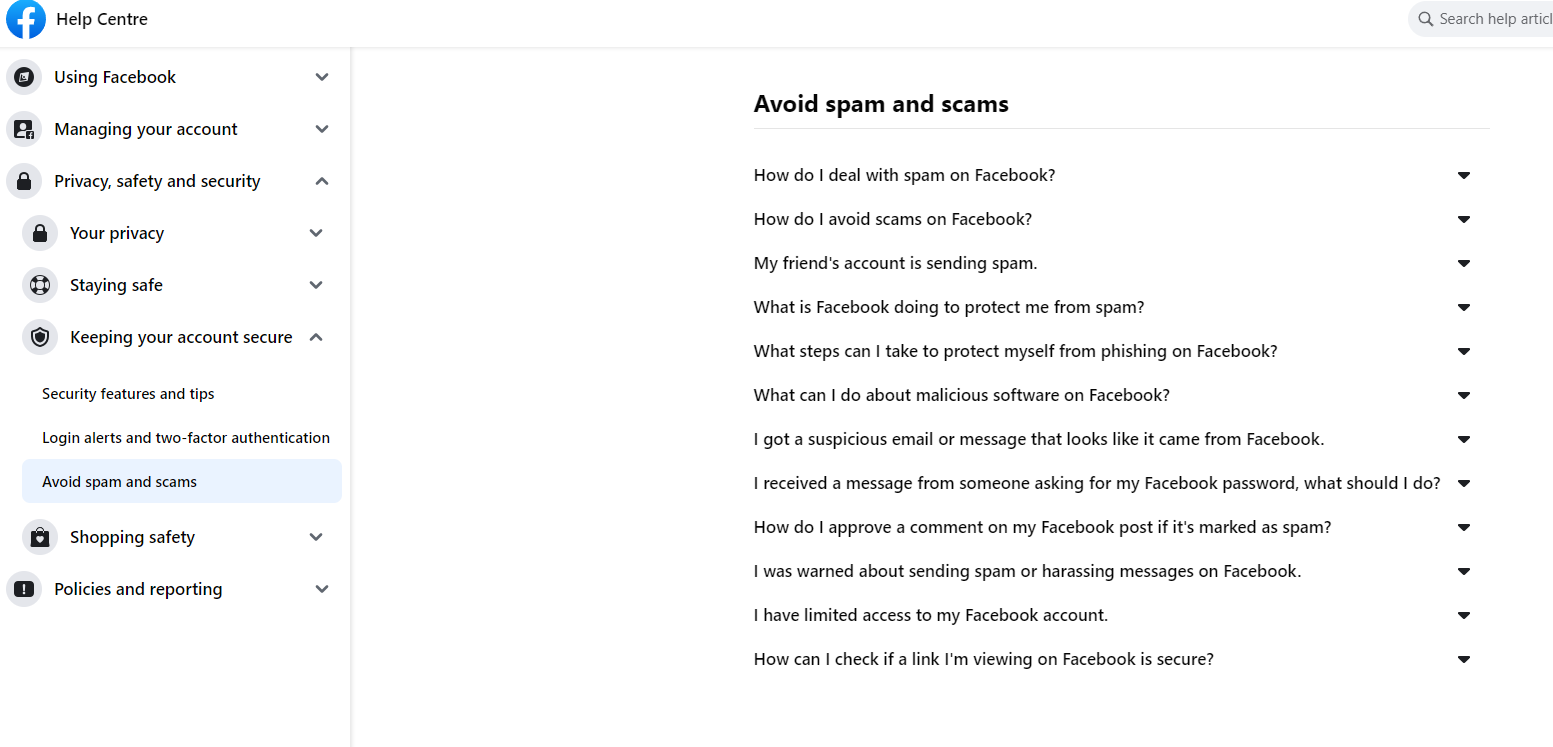


The image above is found in the help centre in Facebook. This section of the help centre allows you to keep your account more secure and protected from others.



There is also section on how to make your account more secure if you do not know how to.

The way they were able to access the data was through fraud emails.



**Software-based protection**

An organisation's IT system should have a variety of software- and hardware-based protection methods enabled. Likewise, an individual's system is likely to have fewer options, but still need some protection, such as:

* Antivirus
* Firewalls
* Domain management
* User authentication
* Access controls

**Antivirus:**

Anti-virus and anti-malware software is available, including free anti-virus software and paid for anti-virus products, which can protect IT systems from malware that may be uploaded from the internet or external storage devices.

**Virus signature:**

Signatures of viruses are lists of code strings found in specific viruses. Since new viruses are created all the time, antivirus software downloads signature updates from developers on a regular basis. An anti-virus software program uses this signature list to determine if any viruses are present on a system and in its memory.

**Heuristics:**

It avoids the day-zero attack vulnerability, though it may create more false positives than using virus signatures. Heuristic methods do not remove the day-zero attack vulnerability, but they do spot the types of behaviour that viruses commonly display.

**Firewalls:**

Firewalls prevent unauthorized data from entering or leaving a network. They can be implemented as software running on a workstation or server. As the name implies, network firewalls provide protection for a whole network by creating a barrier between a LAN and the Internet.

**Packet Filtering:**

An administrator can set rules to reject packets that do not conform to the rules that are applied at the lower layers of the TCP/IP protocol. Packets that do not conform to these rules are rejected.

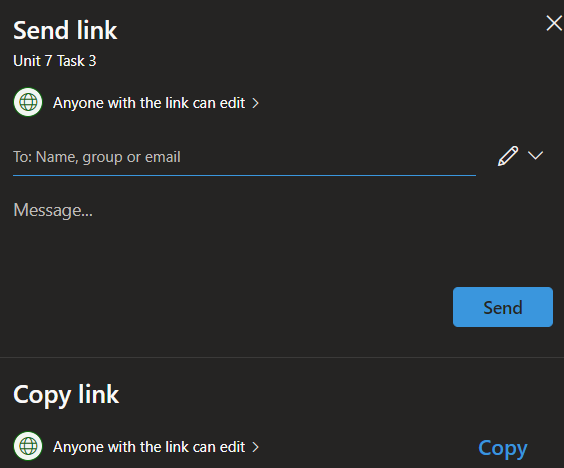
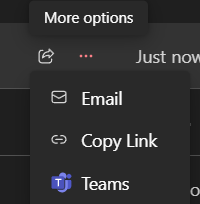
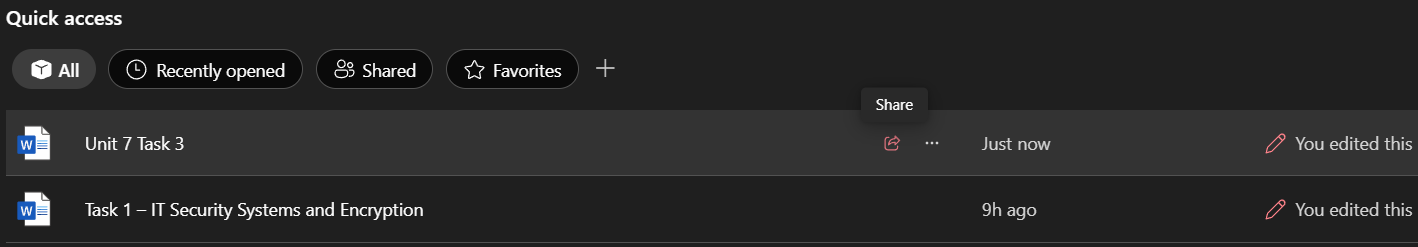
**Application Layer Filtering:**

Rather than filtering connections at the port level, as does a packet filter, application layer filtering inspects data higher up in the TCP/IP stack. Filtering prevents data from passing through that does not comply with the application rules.

**Kerberos:**

In an untrusted network, such as the internet, Kerberos enables trusted hosts to authenticate one another. The client-server application uses secret-key cryptography and a third party to verify user identities and authenticate client-server applications.

**Example of file/folder sharing**



As you can see in the images I have provided above, you can see 3 screenshots. The first image which I have screenshotted show how to share a document. To share on OneDrive, you need to select the share icon.

The second screenshot shows the options which you can select once you click the share button. For this example, I chose the first option which was email.

The final screenshot shows the page which appears when you select email option on the share icon. At this page, you must type in a valid email address to send to your recipient. You can then upload a link which can be sent off. You also have the option to send folders with multiple files.