D1 Threats to data, information and systems

Implication of Threats

A business' data, information and systems are extremely important to any organisation. They're also extremely important to individuals who keep a lot of personal information on their computer systems that could cause great harm if lost or stolen.

Unfortunately, when using IT systems there are many things that can cause harm to your data, information and systems. These are often malicious users trying to steal data and purposely cause harm, but can also happen completely accidentally.

	Explanation	The Impact on Individuals & Organisations
Malware	Malicious software is a computer program that is designed to harm or gain unauthorised access to a computer system. We most commonly are aware of viruses, and often use the term virus interchangeably with malware. However, viruses are just one type of malware. The key characteristics that define the different types of malware are: Viruses, Worms, Trojans and Spyware.	Malware can be used to corrupt or delete data being stored on IT systems. This could cause a lot of inconvenience to an organisation as they will need to spend time recovering the data from backups. The impact on individuals could be just as harmful. For example, personal photos that have real emotion value could be lost forever causing a lot of distress. Malware, especially spyware, could also be used to gather personal data, such as bank details, in order to steal money from individuals or to commit identity fraud.
Hackers	A hacker is someone who gains unauthorised access to a computer system. This can be performed in many ways, and not all are extremely technical. For example, guessing someone's password and using it to gain access to their computer system without their permission is hacking. Hackers also use programs that will automatically go through a list of common passwords until it breaks into the computer system by eventually guessing the correct password. This is known as a "brute force attack". This type of attack is why we're encouraged to use complex passwords.	The unauthorised access to an organisation's or individual's data can be used to steal financial information in order to steal money from them. Personal information taken from individuals, or via records stolen from hacking a business, could also be used for identity fraud. Hackers could also use any private and confidential data for blackmail purposes. Due to hacking causing a big impact on an organisations reputation, a hack could be used to blackmail the business by revealing the hack to the public.
Phishing	This is where emails are sent purporting to be a reputable company but in fact have been sent by a malicious user for the purpose of gaining personal or financial information. The email will appear to be from the reputable business and will usually contain a link that appears to be for their website. However, when clicked on it will take the user to another website that is designed to look like the business' but is not. This website will contain a form to be filled out with personal data and when submitted will go to the malicious user.	The goal of phishing is usually to obtain personal and financial information. This is therefore commonly used for stealing money from an individuals or an organisations bank account. Individuals can also be impacted by identity fraud, where personal data is stolen and used to sign up for loans for example. The data stolen from organisations through a phishing email could be used to then perform a hack on the organisation. For example, a user may reveal their login details.
Accidental Damage	Not all damage to an IT system is malicious. Through human error, we can lose data and damage our IT systems. Some examples of this include: • Dropping laptops, tablets, smartphones, etc. • Spilling liquids on IT systems. • Misplacing external storage devices, laptops, tablets & smartphones. • Accidentally deleting or overwriting files or folders. All of these are done with no malicious intent but can have catastrophic consequences to the business as you could lose a massive amount of data. This is a major reason why businesses will perform regular backups to their data.	Individuals may lose data, such as photos, with emotional value. Organisations may lose important business data such as sales records. This is extremely expensive to recover from for both individuals and businesses. You may need to pay a specialist to try and recover the data or will need to recapture and re-enter data from its source. Finally, you will need to replace any lost or damaged devices which will be costly too, especially to individuals.

Implication of Threats

A business' data, information and systems are extremely important to any organisation. They're also extremely important to individuals who keep a lot of personal information on their computer systems that could cause great harm if lost or stolen.

Unfortunately, when using IT systems there are many things that can cause harm to your data, information and systems. These are often malicious users trying to steal data and purposely cause harm, but can also happen completely accidentally.

	Explanation	The Impact on Individuals & Organisations
Malware		
Hackers		
Phishing		
Accidental Damage		