Malware

Viruses
- A program designed to disrupt or damage a computer system.
- May cause the system to stop functioning or loose data.

Worms
- A computer program which makes copies of itself.
- Works by itself rather than attaching to another program.
- Sends out the copies to try and infect other systems.
- Once installed will damage the system or attempt to steal data.

Trojans
- Malicious software hidden in what seems to be a normal program.
- Free games or music often contain trojans.
- Once installed will damage the system or attempt to steal data.

Ransomware
- Encrypts data and demands money to unlock it.
- Leaves systems unusable causing huge organisational impact.

Key Loggers
- Records all keystrokes and activity.
- Capture usernames, passwords, and any other data typed.

Principals of the Data Protection Act 2018

1. Fair, lawful and transparent processing.
   a. Data must only be used for the purposes which it was collected.
   b. The rights of the data subject must be considered.
2. Purpose Limitation.
   a. Data must only be collected for specified defined purposes.
   b. There is an exception for public interest and research
3. Data minimisation
   a. Only the data needed must be held, no more
   b. Must be accurate and relevant.
4. Accuracy
   a. Data must be accurate and kept up to date.
5. Data Retention periods
   a. Data must not be kept for longer than needed.
   b. It may be stored for longer in the case of research but must be anonymised.
6. Data Security
   a. Data must be kept secure against unlawful processing or loss.
7. Accountability
   a. Must be able to prove that data protection methods are sufficient.
   b. Must have appropriate organisational processes.

Hacking

Unpatched or Outdated Software
- Software patches contain fixes for bugs and security flaws.
- Software should include features to automatically apply patches.
- Programmers may stop updating software, leaving it unsupported.
- Hackers take advantage of bugs to gain access to systems.
- Hackers look at patches to see what bugs are fixed and try to exploit them.

Out-Of-Date Anti-Malware
- Anti-malware requires definitions to be kept up to date to be effective.
- Hackers can target systems with outdated anti-malware.

Social Engineering
- Targets people rather than systems.
- Attempt to manipulate people into handing over data.
- Strong policies and user training can help.
- Phishing tries to get people to hand over data using messages which look like they have come from a trusted party.
- Blagging uses a fake story to try and get a person to hand over money or information.
- Shoulder surfing is watching someone enter their password.

Environmental Issues

Energy Consumption
- Computer systems consume huge amounts of energy.
- Computers are becoming more efficient so use less energy.
- We are using computers more than before, meaning higher energy use.

Manufacture
- Building uses up natural resources, which are limited in supply.
- A computer requires 10 x its weight in fossil fuels to make.

Replacement Cycle
- How long is a device designed to be used before it breaks or becomes too old to be used?
- Organisations may set a 3, 5 or 10 year replacement cycle.

Disposal
- Computers contain harmful and so must be disposed of carefully.
- Often sent to countries with lower disposal standards.
- People there will go through waste to find metals they can sell on.
- This exposes them to dangerous chemicals.

Issues with AI, Machine Learning and Robotics

These fields are growing and changing rapidly, bringing up new ethical and legal issues. Often, there is not yet a right or wrong answer, but it is important to consider these issues nevertheless.

Accountability
- All choices have consequences, sometimes significant in legal, financial or safety terms.
- Who is responsible? The person operating the system, the person who produced it, or the system itself.

Legal Liability
- Actions taken by systems may have legal consequences.
- Who should be accountable in these cases? The system owner, the manufacture or the system itself?

Safety
- Ensuring that systems do not cause harm.
- Fail safe processes mean the system will default to a safe state.
- How should a system act in cases where some harm is unavoidable?

Algorithmic Bias
- The design of an algorithm may favour certain groups.
- Should a robot choose to save a young person over an older person?
- Should a self driving car swerve into one person to avoid hitting four?
- Are these things ethical?

Topic 5 – Issues and Impacts

Protecting Systems and Data

Anti-Malware
- Scans for, removes, and protects against malicious software.
- Includes anti-virus, anti-phishing, and anti-spyware.
- Can be set to scan manually, at a certain time, or when files are accessed.
- Will attempt to stop malware before it can be installed.
- Scans files against a list of malware (called definitions).
- These definitions must be kept up to date.
- Cannot protect against new malware until definitions are updated.
- Organisations should run this software on their systems and networks.

Encryption
- Changes data so it can't be read by anyone other than the intended recipient.
- Encrypted with an encryption algorithm and decrypted with a decryption algorithm.
- An encryption key is a string of characters used to encrypt data.
- Encrypting data before transmission helps security, as the message cannot be read without the key.
- Data can also be encrypted when stored meaning if the device is stolen the data cannot be read.
- Organisations may be required to use encryption by policies, laws, or contracts.

Acceptable Use Policy (AUP)
- Rules for how systems and networks may be used.
- Users should read and agree before using the system.
- Discourages users from actions which may damage the system.
- Allows the organisation to discipline those who use systems inappropriately.
- Provides clear guidance to users on what they can and cannot do.

Backup and Recovery Procedures
- The process used for backing and restoring.
- Backups allow organisations to recover data which may have been lost or damaged.
- Allows people to have all the information to hand when dealing with an incident.
- It is important that recovery is tested.
- Backups will contain sensitive data, so it is important that they are kept secure.

Ethical and Legal Issues with Personal Data

- Many areas are constantly being debated with people having different views.
- Computer systems hold large amounts of personal data.
- Organisations also collect data such as history of our Internet activity.
- Smart devices collect data such as our voice, video and activity.
- Governments want access to this data to prevent crime. Is this right?
- Should organisations be allowed to collect this much data, and how do they use it?

Ownership
- Who owns data supplied to a company or organisation?
- UK law makes clear that you are the data owner, whilst those who hold the data are data stewards.
- Data Stewards have obligations under law to keep data secure, up to date, and delete it when they no longer need it.
- Right to erasure, allowing us to tell companies to delete data we don't want them to hold.
- There are exceptions to this, such as the Police for crime prevention.

Consent
- Data protection laws require positive consent for data collection.
- Data cannot be collected automatically without consent.
- It is insufficient to use opt out processes, requiring people to tick a box saying they do not want their data to be used.
- Consent must be easy to understand and obvious.

Misuse
- Data can be misused by hackers, phishing scams or viruses.
- Systems should have processes in place to prevent this.

Data Protection
- Data protection law lays out legal rights and responsibilities for data.
- Gives rights to those who own data, and places responsibilities on those who use it.
- UK law is very robust.
- The Data Protection Act 2018 is the UK implementation of the EU GDPR (General Data Protection Regulations)
- Before this, the Data Protection act already provided protection, but it has now been updated to be even more robust.

Using Intellectual Property to Protect Computer Systems

Copyright
- Protection for works such as music, books or software.
- Automatic when work is created and does not need to be registered.
- Does not last forever and will expire.
- Illegal to share or copy without the owner's permission.
- Prevents others from selling copies of the work.

Patents
- Allows someone to register ownership of an invention or process.
- Can apply to different parts of a device or system such as the interface.
- Protects the idea and prohibits people from copying it.

Trademarks
- Protection for a logo, name or phrase.
- Must be registered.
- Allows companies to protect what makes their brand distinctive.
- Provides protection for software names and logos and prevents someone from attempting to sell their own version.
- Also prevents people using names which are too similar and designed to confuse.

Licencing
- Defines how software may be used.
- Prevents people from using the software in a way the owner would not want.
- Proprietary licenses are expensive and must be purchased from a company but are often more secure and include software support and updates.
- Open source licenses are free and available to anybody, but can be less secure and harder to find support for when something goes wrong.