DIGITAL WORLD
@TOYNBEE

9.1 Cyber Security

This unit takes you on a journey of discovery of techniques that cybercriminals use to steal data, disrupt systems, and infiltrate networks.

DATA PROTECTION ACT 2018

ALL ORGANISATIONS USING AND STORING DATA MUST **ABIDE** BY THE FOLLOWING **PRINCIPLES** →

- Used fairly, openly, and in accordance with the law
- Used for a specific and stated reason
- Used only in a way that is necessary and sufficient for the purpose for which it was collected
- Accurate and up-to-date
- Only kept for as long as it is needed
- Protected against loss, damage, and unauthorised access

AS A **DATA SUBJECT** YOU HAVE THE RIGHT TO FIND OUT WHAT INFORMATION THE GOVERNMENT AND OTHER ORGANISATIONS STORE ABOUT YOU. ←

- Find out how your data is being used (by an organisation)
- Access the data that an organisation has about you
- Update your data
- Have your data deleted
- Stop an organisation from processing your data
- Transfer your data to a different organisation

The Computer Misuse Act (1990)

The Computer Misuse Act (1990) and its amendments were created so that unauthorized access to computers and crimes committed using a computer could be prosecuted. The act is based on three principles and makes the following actions illegal:

PRINCIPLES	LEGAL ACTIONS
Unauthorised access to digital/computer material. This means a person asking a computer to perform any function with the intent of accessing anything on the computer for which they do not have permission, and for which they know they do not have permission.	Punishable by up to two years in prison and a £5,000 fine.
Unauthorised access to digital/computer material with intent to commit or facilitate the commission of further offences. This means a person gaining access to a computer without permission in order to commit another crime or to enable someone else to commit a crime.	Punishable by up to five years in prison and an unlimited fine determined by the damage caused and the severity of the crime.
Unauthorised acts with intent to impair, or with recklessness as to impairing, the operation of a computer. This means a person intentionally impairing the operation of any computer or program, or intentionally preventing access to any data or program on any computer. This includes creating or supplying materials that could be used to carry out this offence.	Punishable by a prison sentence of up to ten years and an unlimited fine, but if the act puts life at risk or endangers national security, the sentence may be extended to life imprisonment.

SOCIAL ENGINEERING

Social engineering is a set of methods used by cybercriminals to deceive individuals into handing over information that they can use for fraudulent purposes.

How might a hacker use the data you submitted?

- Name of first pet
- Favorite colour
- Mother's maiden name
- Favorite band or artist
- Date of birth
- Name / Email address

Shouldering (also known as **shoulder surfing**) is an attack designed to steal a victim's password or other sensitive data. It involves the attacker watching the victim while they provide sensitive information, for example, over their shoulder. This type of attack might be familiar; it is often used to find out someone's PIN at a cash machine.

PHISHING ATTACK

A **phishing attack** is an attack in which the victim receives an email disguised to look as if it has come from a reputable source, in order to trick them into giving up valuable data. The email usually provides a link to another website where the information can be inputted.

Phishing: Key indicators of a phishing email

- Unexpected email with a request for information
- Message content contains spelling errors
- Suspicious hyperlinks in email
  - Text that is hyperlinked to a web address that contains spelling errors and/or lots of random numbers and letters
  - Text that is hyperlinked to a domain name that you don't recognise and/or isn't connected to the email sender
- Generic emails that don't address you by name or contain any personal information that you would expect the sender to know

BLAGGING

Blagging (also known as **pretexting**) is an attack in which the perpetrator invents a scenario in order to convince the victim to give them data or money.

Hacking *in the context of cyber security* is: **Gaining unauthorised access to or control of a computer system**

Why might people want to hack?

- To steal data
- To disrupt services
- For financial gain
- For political reasons (espionage and activism)
- For fun (planting the flag)
- For ethical reasons

BLAGGING

Denial of service attack (DoS) This is a cyberattack in which the criminal makes a network resource unavailable to its intended users. This is done by **flooding** the targeted machine or website with lots of **requests** in an attempt to overload the system.

Distributed denial of service attack (DDoS)
This uses the same concept as a DoS attack, but this time it is **multiple computers** making the attacks at the same time.
It is a lot harder to:

- Stop the attack by simply blocking a single source
- Identify who is responsible, as lots of machines are making requests, many of them because they are infected by malware

Brute force attack This is a form of attack that makes multiple attempts to discover something (such as a password).

MALWARE

Typical actions of malware include deleting or modifying files.

Spyware—secretly monitors user actions, e.g. key presses, and sends information to the hacker. Some spyware can even use your webcam without your knowledge.

Viruses—spreads through normal programs and might slow down your device or change your applications and documents.

Worms— spread from device to device and copy themselves hundreds of times. A worm might copy itself onto your email account and then send a copy to all of your email contacts!

Trojan horse— pretends it will be a useful and safe program, when actually it will try to attack your device.

Adware—displays adverts while it is running; some can serve as spyware, gathering information

BOTS

Internet bots
Bots are automated programs that perform tasks repeatedly.
Bots are a crucial part of the internet's infrastructure and perform useful tasks such as:

- Finding new websites for search engines to index
- Providing customer service online (chatbots)
- Monitoring the prices of items to find the best deal (shopbots)

PROTECTION

Firewalls A firewall checks incoming and outgoing network traffic. It scans the data to make sure it doesn't contain anything malicious and that it follows the rules set by the network.

Anti-malware Anti-malware is software that scans any file that is able to execute code. The anti-malware will have a list of definitions of sequences of code that they are aware are malicious. If the code in your files matches the definitions, the files are quarantined.

Auto-updates Auto-updates refers to software that automatically checks for available updates for the software you have on your computer. Once it finds an update, the software can be set either to alert the user or to install it automatically. This software is often included with an operating system.

User permissions Users on a network can be put into groups, with each group having a unique set of privileges, such as: Which network drives they have access to, Their read/write permissions, Which printers they are able to use, What software they can use, Which websites they are allowed to access