Overview

KEY VOCABULARY
LOOK COVER, WRITE AND CHECK!

Advanced fee fraud	An email scam; the promise of a large sum of money in return of a small advance fee.
Copyright	The law that protects creative works, such as films or music, from being copied.
Cybercrime	Also known as computer crime – a criminal act committed using an internet connected device.
Data harvesting	Gathering data about others using information online, such as GPS data. Often done illegally or with the view to commit illegal acts, such as commit identity fraud.
GDPR	General data protection regulations, formally known as the data protection Act. The rules about who can hold information on you and what this information can be.
Hacking	Accessing information not owned without permission of the owner.
Logic bomb	A type of malware; A program that tells the computer to perform an operation at a certain time, such as wipe all the data.
Malware	Malicious software; a program that has been downloaded, without the device owners consent.
Phishing	An email scam; tricks the user into handing over security information, such as bank account log-in details.
Plagiarism	Copying someone else's work and presenting it as you own.
Ransomware	A type of malware; denies access to the data/operating system/network until a ransom is paid, essentially holds the user to ransom.
Shoulder surfing	Spying on a person (usually over their shoulder) when they are logging in to gain passwords or other security information for that person's accounts.
Trojan	An email scam; distracts the user with something, such as a funny video while embedding malware on the device.
Virus generating	An email scam; an email that may appear to come from a genuine contact asking for money, it may contain a link, can allow a similar email to be sent from your email account to all of your contacts.

Key Learning that will take place in this unit:

- Understand what is meant by 'Cybercrime', the types of cyber crime and how to avoid becoming a victim.
- Learn the different types of email scams, how to recognise them and how to protect yourself from being a victim,
- Learn the different types of malware, how to protect your device from becoming infected and how to recognise the signs your device may have been infected,
- Understand what is contained in the Computer Misuse Act 1990 and why it is important,
- Learn what hackers do, how and why they may do it,
- Understand how to keep yourself safe from harm working with and working on devices, such as computers, including ensuring that your data is appropriately stored.

Software and resources that will be used:

- Schoology

Passwords:

The most commonly used passwords are 'password' or 'Password1'.
Always include at least 1 uppercase letter, 1 lowercase letter, 1 number AND a special character:

*pa$$WorD_2070

Don't include personal information

Make it at least 8 characters long

Weak passwords are one of the most common weaknesses exploited by hackers!

Cybercrime:

Cybercrime, sometimes called computer crime, is a crime committed using the internet and any internet enabled device including smartphones

Cyber crime fact file

- Cyber crime makes more money for criminals than drug trafficking
- Around the world someone's identity is stolen online every 2 seconds
- It takes just 4 minutes from connecting to the internet for an unprotected device to become infected.

Hackers:

A hacker is (as defined in the Computer Misuse Act, 1990) someone who looks at or modifies another users' data without permission.

Why do hackers hack?:

- For money
- For information
- For political reasons
- For revenge
- For the thrill of the challenge
- To cause chaos and mischief

Email scams

Phishing

Tricks you into handing over sensitive details, such as security log-in details.

Appears to be from a genuine company, such as PayPal, eBay or Amazon.

Virus-generated

Opening it can generate a similar email to be sent to all your email contacts. Can contain a forged link, can contain a please for cash.

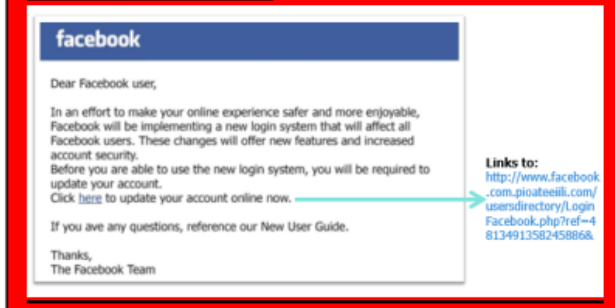
Advanced fee fraud

Usually accompanied by a long, emotional plea, promises a large sum of money in return for a small advanced fee.

Trojan horse/ malware

Offers you something tempting to look at – like a funny video – and installs malware on your device

Example phishing email:



Phishers will send out thousands of emails, there is on average a 5% response rate.

Following the link will take you to a fake website where your log-in details will be recorded – it could allow access to all your other accounts if you use the same password.

Example Trojan horse email:

Will install malware that may record your keystrokes, provide access to your files or send spam to all your contacts

Malware:

Malware means Malicious software. Malware can be accidentally downloaded, usually as a virus via a vulnerability in the network or intentionally added by a hacker.

Ransomware:

Denies access to the network or computers until a ransom is paid.

Famously the NHS was victim to a ransomware attack in 2017.

Logic bombs:

Used by disgruntled employees or blackmailers – executes a destructive sequence, set to detonate at a certain time.

Other common types of malware:

Browser, also called spyware – hijacks browser functions, File infector – Infects a particular file and may overwite or alter that file, Macro virus – can be embedded in templates and will spread to other computers if the file is shared.

Avoid becoming a victim of malware or email scams:

Malware

- Avoid clicking on everything, e.g. offers that seem too good to be true (on both websites and email)
- Don't visit illegal sites, such as those that let you download copyright material
- Make sure your browser is configured to always ask before running files and downloading automatically
- Keep your browser software up-to-date
- Install up-to-date antivirus and anti-spyware software

Email scams

- Use a SPAM filter to prevent common scams ever reaching your inbox
- Be suspicious! If you aren't completely certain it's genuine, NEVER click any links or download attachments.

Data protection:

Knows your rights about your information. Certain companies and organisations are permitted to hold data on you but:

- The data must be accurate and up to date
- You have a right to see what data is held about you
- The data must be protected from unauthorised access

AND

- It can only be kept for as long it is relevant (the company can't keep your details forever)

Copyright and plagarism:

Copyright © protects the rights of an author/creator of creative work. It means that someone else's work cannot be copied without permission.

Plagarism is using someone else's creative work as if it is yours.

Copyrighted material online can be music, films or pictures. Sharing or downloading these illegally (without paying the owner of the copyright) is a copyright infringement. However, there are many sites, like amazon music or iTunes, where downloading music is legal because the owner has been paid.

But what is the problem with downloading music?

It is estimated that the illegal downloading of films, TV programmes and music could mean the loss of 30,000 British jobs

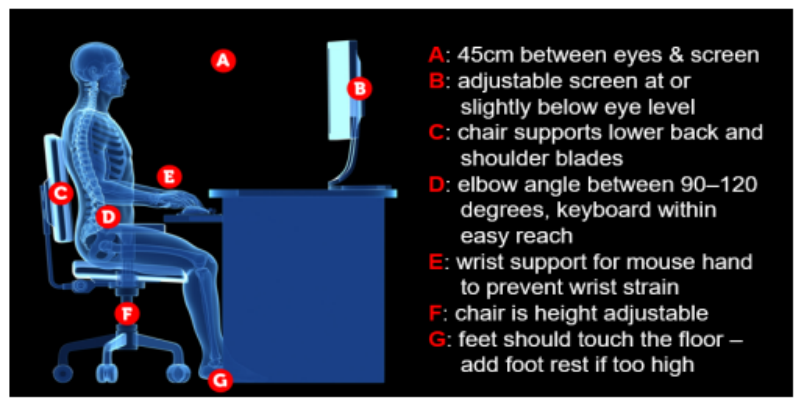
At home:

Check your security and privacy settings, are they secure? What can a stranger see on your social media? Could they recreate/copy your identity?

Check - Is your home work station damaging you back?

Health & Safety:

Are you sitting comfortably? Take a break every 15 minutes, even if it just looking off into the distance.



Useful links:

BBC Bitesize: Cybercrime
https://www.bbc.co.uk/bitesize/guides/zycm97h/revision/7

BBC Bitesize: Hacking
https://www.bbc.co.uk/bitesize/guides/zbgg4qt/revision/8

BBC Bitesize: Viruses and malware
https://www.bbc.co.uk/bitesize/topics/zd92fg8/articles/zcmbgk7

Safety online:

Keeping your identity safe

If criminals can access your information, they can steal your identity… but where can they get this information from? Social media!

Before you post, think who can see it and what information does this tell me about me?

Even a photo can disclose your location, even if there is nothing obvious, they are all embedded with location information that is shared if you don't turn it off.

If you wouldn't tell them in real life why tell them online?

Test yourself?

1. Write the definition of 'GDPR'
2. What are the 4 most commonly used email scams?
3. What does 'malware' mean?
4. Give two examples of malware
5. What is a hacker?
6. What is a common weakness hackers exploit?
7. How do you protect yourself from becoming a victim of cybercrime?
8. How do you protect your data online?