FACTFILE:

GCSE DIGITAL TECHNOLOGY

Unit 1

CYBERSPACE, NETWORK SECURITY AND DATA TRANSFER

Rewarding Learning

Introduction

Learning Outcomes

Students should be able to:

- Define the term cybercrime and give examples of threats to cybersecurity, including:
  - Hacking
  - Pornography
  - Cyber stalking
  - Data theft
  - Denial of service
  - Digital forgery
  - Cyber defamation
  - Spamming
  - Phishing
- Define the term malware and describe the following forms of malware: virus, Trojan horse, worm, key logger and spyware.

Contents

- Cybercrime
- Threats to cybersecurity
- Malware

Cybercrime

Cybercrime is any illegal activity that involves the use of a computer or other device that is connected to a network, for example a mobile phone. There are various criminal acts that are carried out using the internet. These include acts which are carried out in order to profit from the victim (for example, data theft or phishing) or as an act of malicious intent (such as cyber stalking or cyber defamation).

Global growth of internet access has provided those wishing to carry out illegal activities with increased opportunities to commit crimes. Criminals no longer need to be physically present to commit a crime and the convenience and anonymity of the internet makes crimes easier to carry out. Cybercrime may be committed an individual, a group, or co-ordinated by criminal organisations. Policing cybercrime comes with challenges, as the criminal may be in a different country than the victim, with different laws in each.

Hacking

Hacking is the act of attempting to gain unauthorised access to a computer system. This illegal access to a system is usually associated with malicious activity and can include the further use of the computer system to commit other crimes. Common techniques include the use of worms or scripts, remotely accessing a device on the network through an unauthorised remote connection, or using a denial of service attack. A hacker may also gain access to a network by using specific software, for example, a keylogger program may be used to record the sequence of every key press that a user completes on their keyboard. The hacker can then use software to discover a legitimate user's username and password.

Pornography

Pornography is the representation of sexual activity. It is present on the internet in the form of videos and images. Some of the material stored and shared in electronic form shows illegal acts. If an individual is found in possession or there is evidence that they have accessed illegal material, they can be prosecuted.

Cyber stalking

Cyber stalking is the use of a network or other electronic communications to harass or scare someone. A cyber stalker may be a stranger or someone who the victim knows. Like real world stalking, cyber stalking typically involves monitoring the target over a period of time and gathering information about their activities online. It can include impersonating someone, making threats and in some cases, can progress to physical stalking in the real world.

Data theft

Data theft is the act of stealing data from an unknowing victim or organisation with the intent of obtaining confidential information. Security precautions within a business often address the risk of outsiders gaining access to sensitive data by protecting their network, for example, with firewalls but it is more difficult to ensure that all authorised users act in the best interests of the company. An individual might commit data theft to profit from the data they have stolen or they may wish to make data available to others for moral or ethical reasons. In the second case, this is often referred to as whistleblowing and there are websites that specialise in sharing stolen data for that purpose, for example Wikileaks.

Denial of service (DoS)

Denial of service is a web server's inability to service clients' requests for web pages. This means that if a user tries to access the web page, the web server is unable to send the page to the user. This loss of functionality occurs when the web server is sent large numbers of requests for pages almost simultaneously and cannot cope with the demand. This might happen when many people are trying to access a page, for example when tickets are released for a popular concert, but it can also happen as the result of a deliberate attack. Hackers might target a website for a variety of reasons including to make a political statement, trolling (seeking to upset or annoy someone for entertainment) or for blackmail purposes. One method that hackers use for this is called a distributed denial of service (DDoS). In a DDoS attack the requests for the target website are sent by computers which have been infected with a virus. The attackers allow the virus to spread for a period of time and then use the virus to hijack infected computers to send the requests to the target website.

Digital forgery

Digital forgery is a criminal act involving the creation of a copy of a document or image with the intent to profit from it. Criminals could reproduce or alter a document in a manner which is misleading or a misrepresentation of the original. This could be in the form of altering a video or image to implicate someone in a crime.

Cyber defamation

Defamation is the communication of false information that damages a person's or business's reputation. Cyber defamation is the use of the internet to share that false information. This type of activity could be small scale, for example a user sharing false information or images on social media about someone they know, or it could be large scale, for example a news outlet publishing an article which has not been thoroughly fact checked.

Spamming

Spam is an email or other electronic message that is sent to a person who has not requested it. Many email providers filter spam messages into junk folders for their users. Spammers are people who bulk send unsolicited messages to large numbers of internet users. Sending spam is sometimes the first step in a phishing campaign, in the hopes that a recipient will respond to a bogus email.

Phishing

Phishing is the practice of persuading individuals to disclose private information, such as bank account details or passwords, by sending an email pretending to be from an official body and requesting 'reconfirmation' of data that the organisation should already have. Despite this type of crime being around for a long time, it is still effective because some of the emails sent by criminals can be very convincing, including elements such as the company logo or a working phone number.

Malware

Malware is the general name for malicious software that users may inadvertently download onto their computers. These security threats include viruses, Trojan horses, key loggers and spyware.

Virus

A virus is a program designed to copy itself between and within computers, to make a computer system unreliable. The code of the virus may include commands to damage the computer system by corrupting or deleting user files, or to fill up the memory, thus causing the computer to run slowly. Sometimes the user will be aware that there is something wrong, because the virus is causing the computer to display unwanted messages or pop-ups. If this is not the case, a computer may be infected by a virus for some time without the user being aware. While the user is unaware the computer may be used to further infect other computers. The copying process takes place automatically and sometimes is triggered by an event or can be scheduled to happen on a specified date.

Trojan horse

A Trojan horse is a program that performs a normal process in the computer while also performing another, possibly harmful, process at the same time. Trojan programs are hidden in other programs and are disguised to look like something the user would want to open. Hackers may create Trojan horse programs to copy data from secure files or can allow the hacker access to a system without a username and password.

Worm

A worm is a type of virus. Worms are programs that spread themselves via network connections to other systems. It is a stand-alone program so it does not require a host program or file for it to replicate.
It will cause systems to slow down because the computer's processing power will have been hijacked to replicate the worm.

Key logger

A key logger is a type of spyware which will record every keystroke that a user carries out, and sends it secretly across the internet. This is a security risk when buying products or services online, so many websites require a user to select characters or photos that are randomly generated and displayed on screen.

Spyware

Spyware is the name given to software which seeks to secretly monitor the user's actions on the computer and send them over the internet. This can include key logger software (described above), adware software (which will monitor online shopping for other targeted marketing purposes), or browser hijacking software (which will take control of the browser and show unsolicited advertisements). The spyware may record personal details, such as credit card information, passwords, or online purchase history. Information gathered in this way can be used to commit fraud or blackmail.

Bibliography

http://www.bbc.co.uk/webwise/guides/about-spyware

https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals

http://www.bbc.co.uk/news/av/technology-35731734/technology-explained-what-is-a-ddos-attack

BCS Glossary of Computing and ICT, 13th Edition, BCS Academy Glossary Working Party