FACTFILE: GCSE DIGITAL TECHNOLOGY

Unit 1

CYBERSPACE, NETWORK SECURITY AND DATA TRANSFER

cea 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; and
  - Phishing;

- Define the term malware and describe the following forms of malware:
  - Virus;
  - Trojan horse;
  - Worm;
  - Key logger; and
  - Spyware;

- Explain how networks and data can be protected using encryption, passwords, levels of access, backup and firewalls;
- Describe the role of a protocol in data transfer; and
- Describe the purpose of the following protocols:
  - File Transfer Protocol (FTP);
  - HyperText Transfer Protocol (HTTP); and
  - HyperText Transfer Protocol Secure (HTTPS).

Contents in Cyberspace, Network Security and Data Transfer

- Cybercrime and Cybersecurity
- Malware
- Networks and Data Protection
- Data Transfer
- Transfer Protocols

Cybercrime

Criminal activity has taken advantage of the opportunities offered by technology and the internet. The largest growth is in the e-commerce and online banking industry. Criminals try to steal personal information so they can profit from the data available to them.

Cybersecurity

Cybersecurity is the collection of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access. It includes both physical security and cybersecurity.

Physical security involves ensuring levels of access are adhered to, rooms and computer stations are locked when not in use and equipment is properly labelled so that it can be returned to its rightful owner should it get stolen.

Cybersecurity can include ensuring levels of access are adhered to and that all computers have software that will prevent infection and transferring of virus's, stop hackers gaining access to sensitive equipment and ensure that only secure websites are being accessed.

Common Cyber Threats

Hacking

This is an attempt to gain access to a computer system or private network without the owners' permission. It is unauthorised access to or control of a computer system for some illegal purpose.

Pornography

Pornography is material such as books, images, magazines or videos that show sexual or erotic behaviour. Cyberpronography is a criminal offence as it is classed as causing harm to people. Cyberpronography has become a serious problem due to being easily distributed over the internet.

Cyber stalking

This is online stalking. It is the use of technology to harass someone. It can include the following characteristics: false accusations, threats, identity theft, destruction of personal data, exploitation (sexual or otherwise). It can be in the form of email, instant messaging, phone calls, and social media.

Data theft

This is the act of stealing data held on a computer with the intent of gaining confidential information. This type of criminal activity is an increasing problem for both individuals and businesses.

Denial of service

This is usually a cyber-attack that stops a computer user from gaining access to their network. It is unauthorised and usually is done with malicious intent.

Digital forgery

This involves falsely altering digital content such as pictures and documents. It is becoming increasingly more common within the digital age and can include the illegal reproduction of electronic signatures to assume the identity of another victim of identity theft.

Cyber defamation

This is publishing offensive or untrue material against another person with the help of computers and the internet. It is not a specific criminal offense but is classed as slander against another person and is more usually done via social media.

Spamming

Sending multiple unwanted emails or text messages to someone, these are usually sent from companies for marketing purposes.

Phishing

This is a malicious way of obtaining sensitive information such as usernames, passwords and credit card details. Often this is done via email by disguising it as a trustworthy source.

Malware

Short for malicious software, it is specifically designed to gain access to or damage a computer without the user's permission or knowledge. Much of today's malware is created for profit through forced advertising (adware), stealing sensitive information (spyware), spreading email or spam or child pornography (zombie computers) or to extort money (ransomware). There are many different types of malware:

Virus

A virus is a malicious piece of software that when executed can spread from computer to computer. It can reproduce itself providing it is attached to a file or document. A virus will lie dormant until the digital device has executed its code.

Trojan horse

A Trojan Horse virus is any malicious program used by cyber-thieves/hackers to try to gain access to users' systems. Computer users are tricked into loading and executing the virus onto their system. This allows the criminal to spy on them, steal their data and gain access to their system.

Worm

A WORM is a program that replicates itself over and over again using up memory space and spreading itself to other computers. Infections spread very quickly because the subsequent copy of a network worm can also self-replicate.

Key logger

A key logger is a type of surveillance technology used to monitor and record all keys that are pressed on a keyboard. The aim is to enable the criminal to work out user passwords by looking at the keys pressed most frequently and the order they are pressed in.

Spyware

Spyware is software that allows the user to gain information about another person's computer activity. They can be used for legal purposes but the majority of spyware is malicious. Its aim is to capture passwords, bank details and credit card details.

Networks and Data Protection

Encryption

This is the most effective way to achieve data security. It is the process of changing data into a secret code. To decode the data you must have a secret key or passcode. Encrypted text is called *cipher* text.

Passwords

A password is a string of characters that only a user should know to allow them access to a computer system. A strong password should consist of upper and lower case letters, numbers and characters. The stronger the password the harder it is for a criminal to guess. Passwords are usually used alongside a username. Most organisations have their systems set to encourage users to change their passwords. They will set a time limit so that the password expires after a set period of time.

Levels of Access

Within organisations different levels of access ensure the network is secure. At the top level a manager can install software, give users passwords and usernames. At the bottom level users may be able to use the software and files in their own area.

Backup

Backing up files and computer data is another way to ensure user files are secure. This is usually done when the network is not being used for example at night. It involves copying and archiving all data so that it can be used to restore the original data if it gets corrupted.

Firewalls

A firewall is a security system that monitors and controls the incoming and outgoing traffic on a network. If the software detects a piece of code that is not legitimate or from a trusted source then the firewall will stop the traffic getting into the network.

Data Transfer

Data transfer is the transmitting of data from point to point using a digital signal. Data and files can be easily transferred using the internet. They can be emailed, sent via instant message, downloaded from a website or accessed over a private network. Files can be can be stored on a web server and accessed by any computer using an internet connection, this also allows for collaborative working.

Transferring files over the internet is not the most secure way to share data; therefore transfer protocols must be used to ensure that the transferring data cannot be corrupted in any way.

A protocol is simply an agreed method of doing something. Protocols manage the speed of transmission, size of the message and error checking. Protocols decide how two computers will send and receive messages. Data packets travel between the computers from one router to the next. This is known as packet switching.

File Transfer Protocol (FTP)

FTP is built for transferring both single and bulk files. It is an agreed standard way of moving files from one computer to another. One server will have an FTP server application that is consistently listening for transfer requests. The computer will have an FTP client that sets up the connection to the server. The user will have a username and password to access the server. Once the connection is set up files can either be downloaded or uploaded.

Hypertext Transfer Protocol (HTTP)

HTTP is the protocol used by the World Wide Web. It defines how messages are formatted and transmitted. It decides what actions Web servers and browsers should respond to. It is the set of rules used for transferring text, graphics, images, sound, video and multimedia files on the World Wide Web. As soon as a web browser opens the user is using HTTP as all webpages begin with HTTP. HTTP runs on top of the TCP/IP protocols (Transmission Control Protocol/Internet Protocol).

Hypertext Transfer Protocol Secure (HTTPS)

HTTPS is HTTP with a Secure Socket Layer. A secure socket layer is a standard security technology for establishing an encrypted link between a computer and a server (usually a web server). Having a secure socket layer means that users can safely use the internet without their data or files being corrupted or stolen, for example hen using online banking.

Websites

http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime

http://whatis.techtarget.com/definition/cybersecurity

https://cybercrime.org.za/data-theft/

https://www.collinsdictionary.com/dictionary/english/spamming

http://searchwindevelopment.techtarget.com/definition/HTTP

http://www.bbc.co.uk/education/guides/zp9jpv4/revision/5