KNOWLEDGE ORGANISER

LO2—Understand the issues surrounding cyber security

Money Laundering—The process by which criminals hide the origin if the proceeds of their crime, by transferring money through different bank accounts and countries to make it look as if it comes from a legal source

Data Mining—the process of using special software to look at large amounts of computer data in order to find out useful information, for example what types of product a company's customers buy

Cyber enabled crime—which can only be committed by using a computer, computer network or other form of Information Communication Technology (ICT). They are primarily acts directed against computers or network resources and are typically offences under the Computer Misuse Act (CMA).

Cyber Dependent crime— are offences that can only be committed using a computer, computer networks or other form of information communications technology (ICT). These acts include the spread of viruses or other malware, hacking and distributed denial of service (DDoS) attacks.

Vulnerabilities – are flaws or issues that results in weaknesses in the secu- rity of a system. They can be intentional, accidental or a natural phenome- non.

- **System attacks** e.g. denial of service, botnet, malware, social engineering
- **Physical threats** e.g. theft
- **Environmental** e.g. floods, natural disasters)

Accidental e.g. responding to hoax email, dropping an item, uploading Mal- ware, deleting data or software.

Intentional e.g. attacks from hackers, social engineering and theft

Organised crime e.g. cyber dependent and cyber enabled crime, stealing identities, blackmailing.

State sponsored e.g. spying, espionage,

7 Main types of Malware

computer viruses—is simply a malicious computer program that can copy itself and infect a computer. The term "virus" is also commonly used to refer to other types of malware.

worms—is a self-replicating malware computer program. It uses a computer network to send copies of itself to other computers on the network, often without permission.

Trojan horses - is a program that appears harmless but hides malicious functions.

Ransomware—a type of malicious software designed to block access to a computer system until a sum of money is paid.

Spyware—is software that collects and transmits user specific behaviour and information, with or without per- mission.

Adware— software that automatically displays or downloads advertising material such as banners or pop-ups when a user is online.

Scareware—malicious computer programs designed to trick a user into buying and downloading unnecessary
and potentially dangerous software, such as fake antivirus protection.

Ethical hacking— is when a hacker is allowed to attempt to breach the security systems of an organisation with their permission with the intention of helping the organisation improve their current security systems by high- lighting and fixing the flaws, ethical hacking can also take the form of hacking into terrorist or threatening governments databases to see if they have ill intentions for innocent people at which point can be stopped before anyone is hurt.

Hacktivism - is the rebellious use of computers, computer networks and the internet to promote a political agenda. When a hacker uses their abili- ties to fulfil a political motivation, for example when Anonymous a internationally known hacktivist group) shut down ISIS radicalization twitter profiles because they are against the terrorists beliefs not because they stand to gain any profits.

Legal

Regulation of Investigatory Powers Act 2000—Makes it an offence to intentionally and without lawful authority to incept any communication which is transmitted on a public or private communication system.

Communications Act 2003—makes it a criminal offence to transmit text messages or emails via a public communications network which are: grossly offensive, indecent, obscene or menacing

The Computer misuse Act 2000—makes the following an offence: unauthorised access to computer materials, unauthorised access with intent to commit a further offence or unauthorised modification of material. 2 important points about the Computer Misuse Act: the individual must know that they are not authorised to access or modify the system and it is not necessary to actually carry out a further offence, merely to intend to do so is the offence.

Cookie—a small text file sent from a web server that is stored on the user's computer to track and store information about the user's web activities.

Targets for cyber security threats

People – Social Engineering/ Spam / phishing/ & malware attacks

Organisational – Internal / External Hacking, Denial of Service, Theft of data, data misuse inc: deleting, editing and black mail

Equipment – Mobile devices – Loss / Theft, Unsecure location

Information – Theft, publishing, altering / destroying information.

KNOWLEDGE ORGANISER

Hacktivist – Individuals and groups which use computers and computer systems to promote their own views on a particular issue such as human rights, animal rights or ethics. They hack into computer systems and cause disruption such as DDoS, steal or destroy information and put individuals, organisations and countries at risk.

Cyber Criminal – Anyone who commits a cyber-crime by breaking national or international law. They may use the computer in different ways to carry out the crime- as a tool e.g. commit fraud, send spam – to aim crime at a particular copter or system e.g. looking up information they are not allowed to read, installing Trojan horse, spreading Malware, stealing data, altering data

Insider – Insider threats are often disgruntled employees or ex-employees who believe that the business, institution, or agency has "done them wrong" and feel justified in gaining re-venge. An insider threat could be: the introduction of viruses, worms, or Trojan horses; the theft of information or corporate secrets; the theft of money; the corruption or deletion of data; the altering of data to produce inconvenience or false criminal evidence; and the theft of the identities of specific individuals in the enterprise.

Script Kiddie - is an unskilled individual who uses scripts or programs developed by others to attack computer systems and networks and deface websites. The term, 'Script kiddies' does not relate to the actual age of the participant, but to anyone who lacks the ability to write their own sophisticated programs.

Scammers – try to cheat you by offering goods or opportunities to make some quick money. Scams often come via emails and are activated once clicked on. E.G. 'click here to try the free trial of XXX' to register pay £1 that will be refunded. The link will not work and you will not be refunded.

Vulnerability Broker – Several companies make money by either finding program bugs themselves or buying them from researchers of hackers to sell the information on – not to the company who created the program.

Phishers— Gain access to your personal details (passwords, bank account numbers, NI) normally an email is sent from your e.g. bank or Paypal asking you to click the link and log in. The link takes you to a webpage that looks like 'Paypal' but is fake. If data is entered then it will provide access to the phishers.

Cyber Terrorists— the use of computer systems to cause fear or intimidation in society through destruction of or damage to people, property and systems.

Operational

Ways in which the systems can be protected from cyber security threats include the use of **encryption**— turning data and infor-mation into a format which can only be read by someone with the key. There are 2 main types of encryption:

Symmetric key—where the encryption and decryption codes are the same

Asymmetric or public key—where the encryption key is available to anyone to use and encrypt data but only the per- son who receives the message receives the decryption key.

Surveillance of networks and computer systems is another way in which cyber threats can be identified /prevented. Traffic on the network is monitored if irregularities are found an alert is issued.

Email Monitoring

Surveillance is on-going collection, collation, and analysis of data about an individual or group.

The law on employee email surveillance is covered by Data Protection Act 1998 and Regulation of Investigatory Pow- ers Act 2000. Employers must take reasonable steps to let staff know that monitoring is happening, what is being monitored and why it is necessary.

An employer can legally monitor your use of the phone, internet , e-mail or fax in the workplace if:

- The monitoring relates to the business
- The equipment being monitored is provided partly or wholly for work
- The employer has made all reasonable efforts to inform you that your communications will be monitored.

Cyber criminals concentrate their efforts around taking advantage of poor email security management to access credit card information, social security numbers and a myriad of other records containing sensitive data

Extra reading: www.eweek.com/security/sony-hackers-used-apple-id-phishing-scheme-researchers-claim-at-rsa.html

Professional bodies — such as the British Computer Society BCS have codes of ethics or codes of conduct which IT professionals agree t abide by when they join.

Know it

1. Give 3 examples of system vulnerabilities.
2. what is the difference between a hacker and a hacktivist?
3. Identify 4 reasons why computer systems are attacked
4. give 3 examples of threats to mobile devices.
5. name 3 pieces of legislation which are relevant to computers and networks.