Types of Cyber Crime

SCAREWARE – this is malicious software which is designed to trick a user into believing their computer is infected with a virus, or is in danger of becoming infected. It then suggests the security software they need to buy and download to remove it, or protect against it. This 'protection', is either useless or, in the worst case, actually dangerous – infecting the computer with its own viruses. They may then have to pay the cyber criminals to remove these viruses and any damage they've caused.

FISCAL FRAUD – this is where official online channels (such as online self-assessment forms) are targeted. Cyber criminals can hamper processes, such as tax collection or make fraudulent claims for benefits.

THEFT FROM BUSINESS – this is online theft from a business, usually by fraudulently obtaining access to company accounts. An 'insider' may be involved.

EXTORTION – this happens when a website, email server or computer system is subjected to, or threatened with, repeated denial of service or other attacks by malicious hackers (for example by using malware to flood a company server with erroneous internet traffic) or by altering company website links to cause damage to a brand (for example, by redirecting links for a retailer website to an online pornography website). The idea is to cripple a company's ability to operate and then demand payments to restore their service.

CUSTOMER DATA LOSS – this is where cyber criminals steal sensitive customer data from a company (such as financial, medical or criminal records). They may want to sell it, or use it themselves for blackmail.

INDUSTRIAL ESPIONAGE – this is computer-based 'spying' for commercial purposes, such as accessing confidential information to gain a competitive or strategic advantage, or to gain insider knowledge for financial gain (for example - to influence the buying or selling of shares). It includes stealing information (by copying it) from unattended computers in offices; people taking jobs to get into a company and then gaining unauthorised access into that company's computers; and information being stolen from laptops taken outside the workplace.

DDOS ATTACK – DISTRUBUTED DENIAL OF SERVICE (DDoS) ATTACK – this is a way of sabotaging systems. It's where computer systems are used to orchestrate a flood of requests on the target system, causing it to shut down and deny service to other users. It can be used in economic or industrial espionage.

IP THEFT – INTELLECTUAL PROPERTY THEFT – this includes stealing ideas, inventions, designs, product specifications, trade secrets, proprietary products and parts, films, music and software. The main purpose is often to erode a rival company's competitive advantage, so cyber criminals are often paid by rival organisations to steal this type of information.

MONEY LAUNDERING – Cyber criminals use online means to launder the proceeds of criminal acts (for example through complex, internet-enabled transfers between global or offshore bank accounts). This is usually associated with organised criminal networks that have a wide or international reach.