

## CYBERSECURITY

**Cybersecurity** looking at common attacks and methods to protect ourselves and our networks against these attacks.

**Data:** raw facts and figures

**Information:** data that has been processed and has context

### Data Protection Act 2018:

All organisations and people using and storing personal data must abide by the DPA principles . It states how data should be stored/accessed and what rights a data subject has for the protection of their data.

**Computer Misuse Act 1990:**It is an offence to

have unauthorised access to computer material

have unauthorised access with intent to commit or facilitate the commission of further offences

commit unauthorised acts with intent to impair, or with recklessness as to impairing, the operation of a computer.

**Hacking** in the context of cyber security is gaining **unauthorised** access to or control of a computer system .

### Unethical versus ethical hacking

Penetration testers (pen testers) are people who are paid to legally hack into computer systems with the sole purpose of helping a company identify weaknesses in their system.

<b>adware</b>	advertises for products a user may be interested in, based on internet history
<b>authentication</b>	verifying the identity of a user or process
<b>auto update</b>	updating software to remove vulnerabilities automatically
<b>biometrics</b>	'password' created from the user fingerprint, iris, retina, facial, voice
<b>blagging</b>	inventing a scenario to obtaining personal information
<b>CAPTCHA</b>	Completely Automated Public Turing Test To Tell Computers and Humans Apart
<b>DoS/DDoS</b>	Denial of Service attack/Distributed Denial of Service
<b>encryption</b>	mathematically converts data into a form that is unreadable without a key
<b>firewall</b>	checks incoming and outgoing network traffic for threats
<b>hacking</b>	gaining <b>unauthorised</b> access to or control of a computer system'
<b>malware</b>	a variety of forms of hostile or intrusive software
<b>penetration testing</b>	testing a network/program for vulnerabilities
<b>pharming</b>	redirecting web traffic to fake websites designed to gain personal information
<b>phishing</b>	messages designed to steal personal details/money/identity
<b>ransomware</b>	virus which locks a computer and encrypts files until a "ransom" is paid
<b>script kiddies</b>	hackers with no technical hacking knowledge using downloaded software
<b>shouldering</b>	directly observing someone enter personal details e.g. PIN number, password.
<b>social engineering</b>	manipulating people so they give up personal/confidential information
<b>spyware</b>	gathers information about a person or organisation without their knowledge
<b>trojans</b>	masquerades as having a legitimate purpose but actually has malicious intent
<b>viruses</b>	self-replicating software attached to another program/file
<b>worms</b>	Replicate and spread through the network