COMPUTING 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

It is the law

GDPR:
All organisations and people using and storing personal data must abide by the GDPR 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
1.have unauthorised access to computer material
2.have unauthorised access with intent to commit or facilitate the commission of further offences
3.commit unauthorised acts with intent to impair, or with recklessness as to impairing, the operation of a computer.

Key words

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

Network and System **security measures** include:

Auto updates

Anti-malware

passwords

Penetration testing

User permissions

firewall

biometrics

User authentication

encryption

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.