Year 9 | Topic 3 | **Computer Science** | Cyber Security

Operation of a DDoS attack

Attacker Computers
Malicious Traffic
Internet
Target Server
Real Users
Clean Traffic
Out of Resources
SERVICE OFFLINE
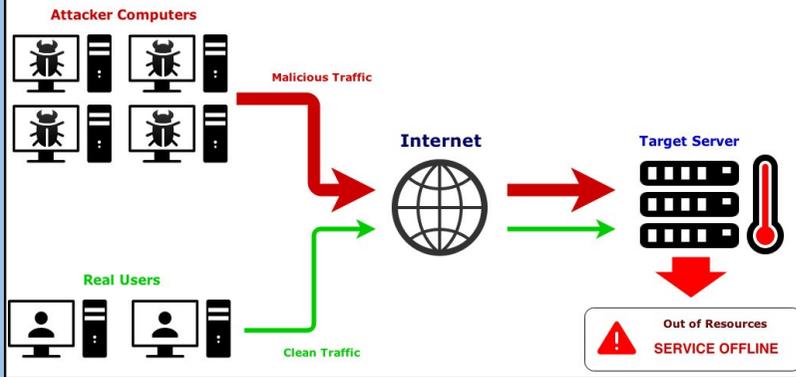
Social Engineering Explained

Also known as human hacking, social engineering is the manipulation of someone to divulge confidential information that can be used for fraudulent purposes.

1 — The social engineer gathers information about their victims.

2 — The social engineer poses as a legitimate person and builds trust with their victims.

3 — The social engineer gathers information about their victims.

4 — The social engineer poses as a legitimate person and builds trust with their victims.

How Encryption Works

May the Force be with you.
Unencrypted Plaintext Message

t8qyN6v3o4 hBsI6AMd6b /nkfh3P4uE5 yLWymGznC 9JU=
Encrypted Ciphertext

May the Force be with you.
Decrypted Plaintext Message

Encryption Key — Decryption Key

Internet — Firewall — Home Network
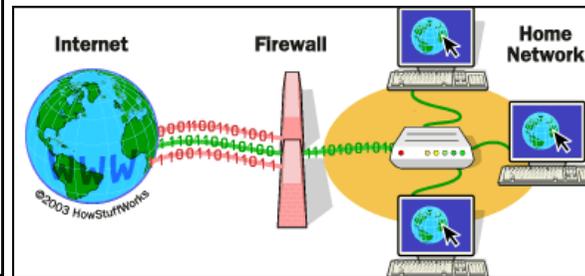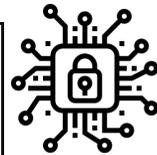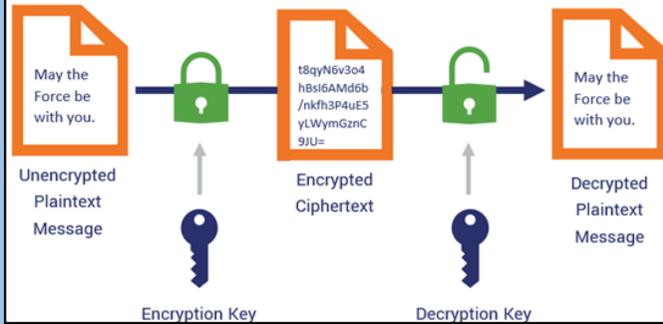
Types of Malware

RANSOMWARE — Blackmails you

SPYWARE — Steals your data

ADWARE — Spams you with ads

WORMS — Spread across computers

TROJANS — Sneak malware onto your PC

BOTNETS — Turn your PC into a zombie

PASSWORD — MULTIFACTOR AUTHENTICATION

LOGGED IN
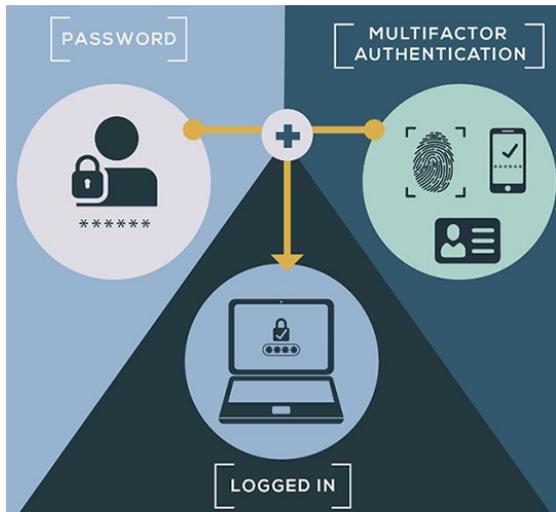
Term	Definition
Cyber Security	Defending computers, servers, devices and systems from malicious attacks.
Data	data is information that has been translated into a form that is efficient for movement or processing
Information	Data that has meaning, not just a number or a letter.
Online	Using a device which is connected to a network—e.g the internet, 3G, wifi hotspot, etc.
Privacy	A users control over their personal information.
Hacking	Gaining unauthorised access to data in a computer.
Data Protection Act	Legislation passed by parliament that governs the protection of personal data in the UK.
Computer Mis-use Act	Defines and criminalises a number of offences involving the use of a computer, e.g. unauthorised access to computer systems.
DoS/ DDoS Denial of Service / Distributed Denial of Service	An attack designed to render online services inaccessible. One type of this attack involves many computers simultaneously flooding a target with network traffic.
Brute Force Attack	Repeatedly entering a password/ pin code to gain access
Malware	Software designed to cause harm or damage to a computer. This includes viruses, adware, spyware, etc.
Network	A group of interconnected computers/devices.
Policy	provide *rules* and guidelines on what network users can and cannot do.
Social Engineering	the act of exploiting human weaknesses to gain access to personal information and protected systems. Social engineering relies on manipulating individuals - such as blagging, phishing and shoulder surfing
Penetration testing	Systems are tested for vulnerabilities to reveal any weaknesses in the system which can be fixed.
Firewall	An application that prevents unauthorised connections to and from the Internet.
User authentication	Checking the user is who they are—log on details, CAPTCHA and biometrics
Encryption	Files that are encrypted have been altered using a secret code and are unreadable to unauthorised parties.

Impacts