GCSE Computer Science Knowledge Organiser
SLR 1.4 Network Security:
Malware

Key Terminology	BCS Definition
Malware	"A broad term that covers all software written to facilitate loss of data, encryption of data, fraud and identity theft."
Anti-malware software	"Protects against many types of malware including viruses, worms, trojans, rootkits, spyware, key loggers, ransomware and adware."
Firewall	"Network software or hardware designed to prevent external users from gaining unauthorised access to a computer system."

What is Malware:

Software written to infect computers and commit crimes – for example:

- Fraud
- Identify theft

Malware often exploits vulnerabilities in operating system software.

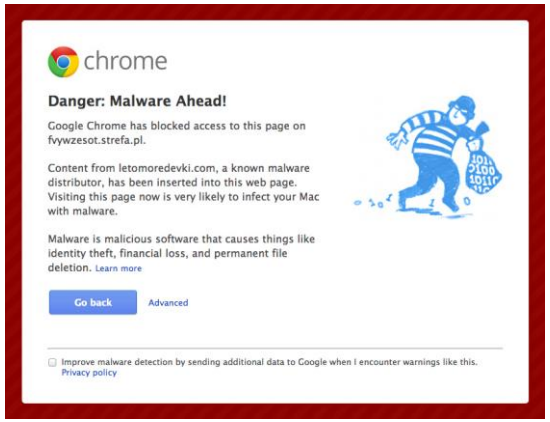
The term malware covers:

- Viruses
- Trojans
- Worms
- Ransomware
- Spyware
- Adware

How to Prevent

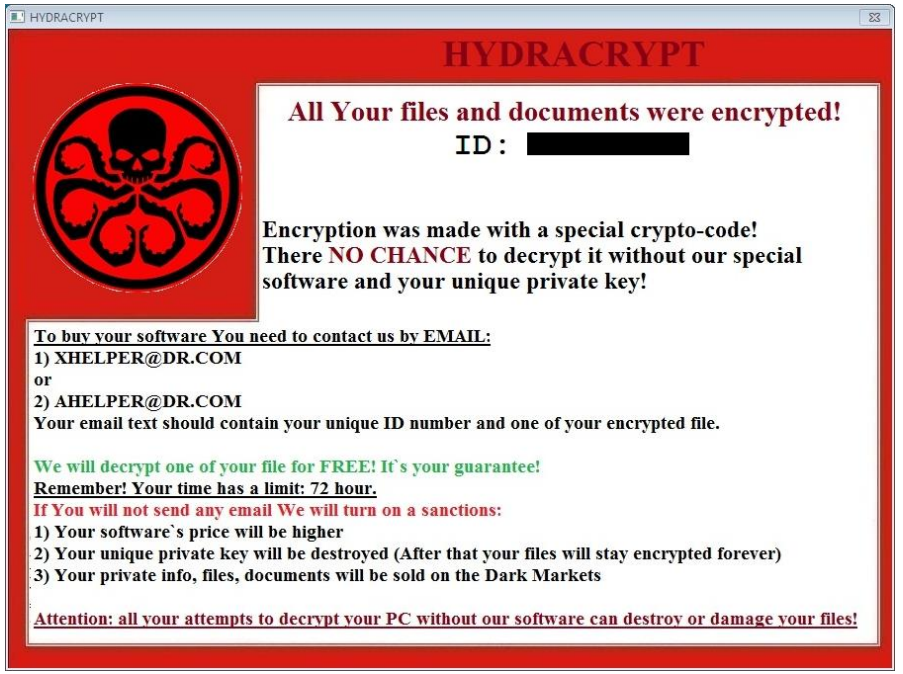
Strong security software:

- Firewall
- Spam filter
- Antivirus
- Anti-spyware
- Enabling OS and security software updates.
- Staff training around email attachments and downloads.
- Regular data backups.



Threats to the network:

- Deleting, corrupting or encrypting files.
- Causing computers to crash, reboot or slow down.
- Reducing internet connection speeds.
- Logging keyboard inputs and sending them to hackers.



GCSE Computer Science Knowledge Organiser
SLR 1.4 Network Security:
Phishing

Key Terminology	BCS Definition
Phishing	**"Sending emails purporting to be from reputable companies to entice people into revealing personal information."**

What is Phishing:

An online fraud technique designed to trick computer users into giving away personal information such as:

- Usernames
- Passwords
- Credit/debit card details

Perpetrators disguise themselves by imitating a trusted company or institution via email or a fake website.

Threats to the network:

Obtaining an individual's financial details to:

- Withdraw money.
- Make fraudulent purchases.
- Open new bank or credit card accounts.
- Cash illegitimate cheques.

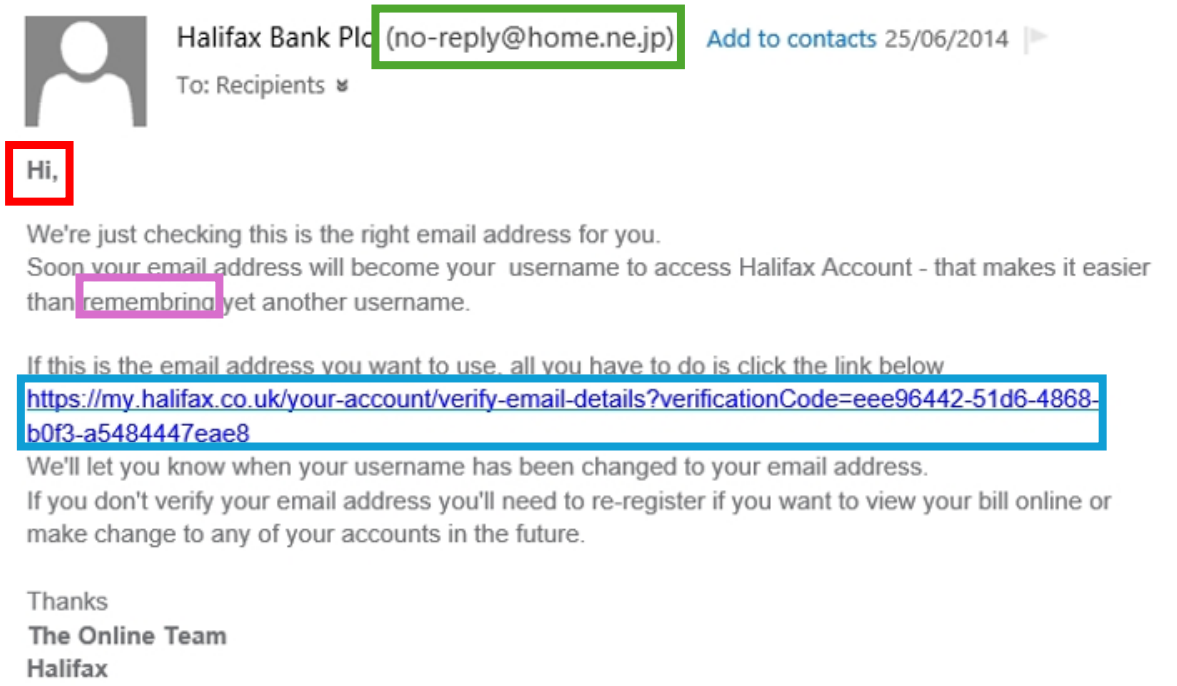
Gaining access to high-value corporate data – financial services may blacklist the company, damaging its reputation.

How to prevent:

Strong security software.

Staff training around:

- Spotting fake emails and websites.
- Not disclosing personal or corporate information.
- Disabling browser pop-ups.



How to spot a Phishing email

Greeting: The phishers don't know your name – just your email address, so the greeting is not personalised

Forged link: The link looks genuine, but it may not link to the website given. Roll your mouse over it to check

The sender's address is often a variation on a genuine address

Request for personal information: Genuine organisations never do this

Sense of urgency: Criminals try to persuade you that something bad will happen if you don't act fast

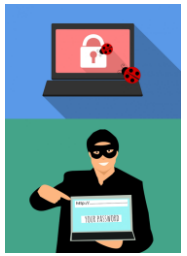
Poor spelling and grammar

GCSE Computer Science Knowledge Organiser
SLR 1.4 Network Security:
Brute Force Attack & DDOS

Key Terminology	BCS Definition
Brute-Force Attack	"A trial-and-error method of attempting to guess passwords. Automated software is used to generate a large number of guesses."
Denial-of-service attack	"Flooding a server with so much traffic that it cannot process legitimate requests."
Firewall	"Network software or hardware designed to prevent external users from gaining unauthorised access to a computer system."

Brute Force Attack

What is a Brute-Force-Attack:
A trial-and-error method used via a computer program to decode encrypted data like passwords and other personal information.
It uses exhaustive effort in an attempt to steal sensitive data.

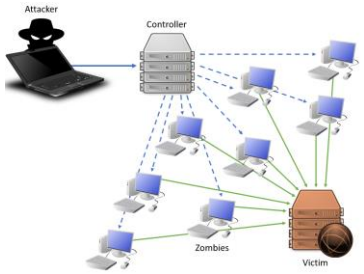


Threats to the network:
- Generating repeated password attempts to gaining unauthorised access to a system.
- Theft and/or disclosure of corporate data.

How to prevent a Brute Force Attack:
- Network lockout policy – accounts lock after a certain number of failed login attempts.
- Progressive delays.
- Staff training around effective passwords with symbols, letters, numbers and mixed case.
- Challenge response – e.g., reCAPTCHA.

Denial of Service Attack
(AKA - DOS or DDOS):

What is a Denial of Service Attack:
Flooding a server with useless traffic, causing it to become overloaded and unavailable.
Many DoS attacks exploit limitations in the TCP/IP stack



Threats to the network:
- Loss of access for customers.
- Lost revenue.
- Reduced productivity.
- Reputational damage.

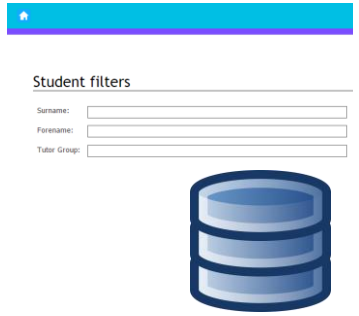
How to prevent a DDOS attack:
- Strong firewall.
- Packet filters.
- Web server configuration.
- Auditing, logging and monitoring systems.

GCSE Computer Science Knowledge Organiser
SLR 1.4 Network Security:
SQL Injection & Data Interception and Theft

SQL Injection

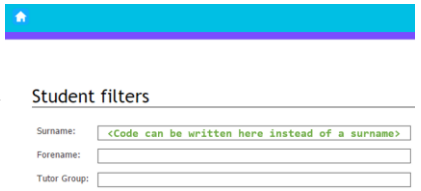
What is SQL Injection:

- A code injection technique used to attack data-driven applications.
- SQL injection makes use of vulnerabilities in poorly coded database applications.
- Code can be entered into text boxes and is then executed by the server.



Threats to the network:

- Outputting the contents of a database to reveal private data.
- Amending or deleting data.
- Adding new rogue records.



How to prevent SQL Injection

- Input box validation.
- Parameter queries.
- Setting database permissions.
- Penetration testing.

Data Interception and Theft

What is Data Interception and Theft:

Monitoring data streams to and from a target to gather sensitive information.
Attackers may use a technique known as network sniffing – monitoring traffic on a network to pick out:

- Unencrypted passwords
- Configuration information

Threats to the network:

- Compromising usernames and passwords to gain unauthorised access to a system.
- Theft and/or disclosure of corporate data.

How to prevent Data Interception and Theft :

- Encryption.
- Virtual networks.
- Staff training around passwords, locking computers, logging off and portable media.
- Investigating network vulnerabilities.

Key Terminology	BCS Definition
Data interception and theft	"Stealing computer-based information."
SQL injection	"A hacking technique used to view or change data in a database by inserting SQL code into a form instead of data."
Penetration testing	"Designed to test the security of a system and identify vulnerabilities."
Password	**"A secret word or phrase used to gain access to a computer, program, interface or system."**
Physical security	"Any form of physical security intended to protect data and systems – e.g., alarms, locks, security patrols, etc."
User access level	"The degree of system access that a specific type of user is allowed. On a network, most users will have restricted access, whereas a system administrator or network technician will be allowed much greater access with fewer restrictions."