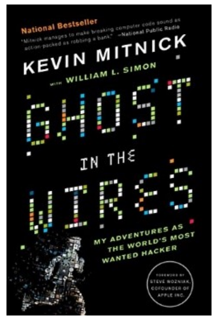
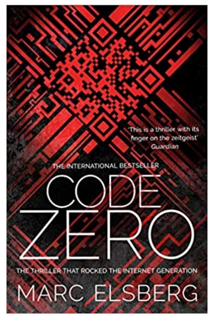
Cyber Security Knowledge Organiser

Topic Summary: The different types of Malware (focus on Virus, Trojans and worms), the different types of hacker (Black, Grey, White) and what each does, how to spot suspicious emails, how to recognise social engineering techniques (Blagging, shoulder-ing, etc) and how to prevent them in a business

Fancy reading more?
Try these great books that explore this topic more widely!
\>>>>>>>>>>>>>>>>>





Want to know more?

Scan the QR code to visit the curriculum over-view for Year 8 Computing, including topic sum-maries, key words, and other ways to learn more about this particular topic.

SCAN ME

Cybersecurity

Cybersecurity is concerned with the protection of computer systems, computer networks and data. Its purpose is to:

to protect computers and networks from cyberattacks
to prevent unauthorised access to computers
to protect computers against damage caused by malicious software
to prevent data from being stolen
to protect against the disruption of services running on the computer

Cyber Security Threats

Malware is software that has been purposely developed to damage, dis-rupt or take control of computer systems.

Social engineering techniques manipulate people into giving away confi-dential and personal information.

Weak passwords are easy to guess. Passwords that use words are easy to crack using an algorithm that systematically goes through all the words in a dictionary until the word matches the password.

Default passwords Upon registration for an online account, users may be given a default password that they do not change. Often these passwords are sent out unencrypted via email so pose a major security vulnerability.

Removable media such as a USB pen drive can be a vector for trans-mitting malware.

Unpatched/outdated software Software needs regular updates to fix se-curity vulnerabilities in computer systems. Software that remains un-patched is vulnerable to attack.

.

Cyber Security Threats

Computer viruses replicate themselves and can transfer from one com-puter to another. They are activated by a user often as email attachments and attachment to other files and programs.

Trojan gains access to a computer by pretending to be legitimate soft-ware. The trojan allows unauthorised backdoor access to a computer without the user being aware.

Cyber Security Threats – Social Engineering

Blagging (Pretexting) Fraudsters make up a scenario to con victims into revealing something they would not ordinarily do. They may have found out some personal information about you from social media sites, to pre-tend they already know you.

How to prevent
Use biometric measures because these cannot be divulged.
Ensure you have your privacy settings on any social media to maximum so that fraudsters cannot find information about you such as your date of birth, where you live etc.

Phishing Normally an email or text messaging scam where victims are conned into believing that they are being contacted by their bank for in-stance and can give sensitive personal details such as bank account pass-words.

How to prevent
Awareness and vigilance. Be particularly aware of unsolicited texts, emails and phone calls. Do not give personal confidential information away. Official organisations such as banks will never ask for this information.
Apply email filtering to prevent dubious emails getting through.

Topic Links:

This topic helps expand upon the knowledge learnt in Year 7's E-safety lessons and Networks lessons. This will also form the basis of the GCSE Year 9 knowledge on cybersecurity.

Key Words:
Malware
Trojan
Virus
Social Engineering
Networks
Phishing
Advanced Fee
Anti-virus
Anti-malware
Computer Misuse Act
Data Protection Act
Ransomware
Adware
Spyware
Identity Theft
Personal Data
Copyright
Plagiarism
Repetitive Strain Injury (RSI)
Health & Safety
E-waste