AQA Computer Science GCSE
3.6.2 Cyber Security Threats

Flashcards

Name three cyber security threats.

Name three cyber security threats.

Any three from: Malicious code (malware), social engineering, pharming, weak and default passwords, misconfigured access rights, removable media, unpatched and/or outdated software.

What is malware?

What is malware?

An umbrella term used to refer to a variety of forms of hostile or intrusive software.

Name three forms of malware.

Name three forms of malware.

Computer viruses, trojans and spyware.

What is a computer virus?

What is a computer virus?

A type of malware that attaches itself to a legitimate program or file and spreads when the infected file is opened.

What is a trojan?

What is a trojan?

A malicious program that disguises itself as legitimate software.

What is spyware?

What is spyware?

A type of malware that secretly gathers information about a user's activity, such as keystrokes, and sends this information to the attacker.

State two methods to protect against malware.

State two methods to protect against malware.

Install reliable antivirus and anti-malware software. Avoid downloading files or software from unknown or untrusted sources.

What is social engineering?

What is social engineering?

An umbrella term used for a range of techniques that are used to manipulate people into giving away confidential information.

State three forms of social engineering.

State three forms of social engineering.

Blagging, phishing and shouldering.

What is blagging?

What is blagging?

Using an invented scenario to increase the chance a victim will divulge information or perform actions that would ordinarily be unlikely.

What is phishing?

What is phishing?

Sending victims a communication that looks genuine, containing a link to fraudulently obtain their personal information.

What is shouldering?

What is shouldering?

Observing a person's private information over their shoulder.

How can users protect against blagging and phishing?

How can users protect against blagging and phishing?

Exercise caution around unexpected phone calls, emails, or messages, and check the source carefully; verify the sender's information.

How can users protect against shouldering?

How can users protect against shouldering?

Cover the keypad when entering PINs or passwords, and check first that you aren't being watched.

What is pharming?

What is pharming?

A cyber attack intended to redirect a website's traffic to a fake website, e.g. through mistyped web addresses.

Explain the risk posed when users select weak or default passwords.

Explain the risk posed when users select weak or default passwords.

Weak passwords can be easily cracked through brute force methods and default passwords allow hackers to gain access to a system without any effort.

What are misconfigured access rights?

What are misconfigured access rights?

When users are given permission to access more files or systems than they need as part of their role.

Explain the risk posed by misconfigured access rights.

Explain the risk posed by misconfigured access rights.

Staff may be allowed to access areas they are not supposed to, and network admins might not know that secure areas have been breached as no-one has “broken in”.

Explain the risk posed by removable media.

Explain the risk posed by removable media.

They can spread malware or be used to steal data if plugged into a system.

What is unpatched or outdated software?

What is unpatched or outdated software?

Software that hasn't been updated with security fixes, making it vulnerable to known attacks.

What is penetration testing?

What is penetration testing?

Attempting to gain access to resources without knowledge of usernames, passwords and other normal means of access.

Why is penetration testing used?

Why is penetration testing used?

To test the effectiveness of security measures, and find any vulnerabilities / weaknesses that a hacker could exploit, before real attacks happen

What do white-box penetration tests simulate?

What do white-box penetration tests simulate?

An attack from a malicious insider.

In white-box penetration tests, what knowledge does the tester have of the system?

In white-box penetration tests, what knowledge does the tester have of the system?

Knowledge of and possibly basic credentials for the target system.

What do black-box penetration tests simulate?

What do black-box penetration tests simulate?

An external attack.

In black-box penetration tests, what knowledge does the tester have of the system?

In black-box penetration tests, what knowledge does the tester have of the system?

No knowledge of any credentials for the target system.