3.6 Cyber security

3.6.1 Fundamentals of cyber security

Content	Additional information	Chk
Be able to define the term **cyber security** and be able to describe the main purposes of cyber security.	Students should know that cyber security consists of the processes, practices and technologies designed to protect networks, computers, programs and data from attack, damage or unauthorised access.	

3.6.2 Cyber security threats

Content	Additional information	Chk
Understand and be able to explain the following cyber security threats: • social engineering techniques • malicious code (malware) • pharming • weak and default passwords • misconfigured access rights • removable media • unpatched and/or outdated software.	Pharming is a cyber attack intended to redirect a website's traffic to a fake website.	
Explain what **penetration testing** is and what it is used for.	Penetration testing is the process of attempting to gain access to resources without knowledge of usernames, passwords and other normal means of access. Students should understand that the aim of a **white-box penetration test** is to simulate a malicious insider who has knowledge of and possibly basic credentials for the target system. Students should understand that the aim of a **black-box penetration test** is to simulate an external hacking or cyber warfare attack where the attacker has no knowledge of or any credentials for the target system.	

3.6.2.1 Social engineering

Content	Additional information	Chk
Define the term s**ocial engineering**. Describe what social engineering is and how it can be protected against.	Students should know that social engineering is the art of manipulating people so they give up confidential information.	
Explain the following forms of social engineering: • blagging (pretexting) • phishing • shouldering (or shoulder surfing).	Blagging is the act of creating and using an invented scenario to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances. Phishing is a technique of fraudulently obtaining private information, often using email or SMS. Shouldering is observing a person's private information over their shoulder eg cashpoint machine PIN numbers.	

3.6.2.2 Malicious code

Content	Additional information	Chk
Define the term '**malware**'. Describe what malware is and how it can be protected against. Describe the following forms of malware: • computer virus • trojan • spyware.	Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software.	

3.6.3 Methods to detect and prevent cyber security threats

Content	Additional information	Chk
Understand and be able to explain the following security measures: • biometric measures (particularly for mobile devices) • password systems • CAPTCHA (or similar) • using email confirmations to confirm a user's identity • automatic software updates.		