THIRD TERM
WEEKLY LESSON NOTES – B8
WEEK 4

Week Ending: 21-07-2023	**DAY:**	**Subject:** Computing	
Duration: 60mins		**Strand:** Communication Networks	
Class: B8	**Class Size:**	**Sub Strand:** Information Security	
Content Standard: B8.3.3.1. Recognize data threats and security protections	**Indicator:** B8.3.3.1.2 Map the protection methods to each of the four identified data threats (Authorisation, Authentications, Encryption and Decryption)		**Lesson:** 1 of 2
Performance Indicator: Learners can map the protection methods to each of the four identified data threats		**Core Competencies:** CC8.2: CP6.1	
Reference: Computing Curriculum Pg. 34			

Activities For Learning & Assessment	**Resources**	**Progression**
Starter (5mins) Ask learners if they have ever heard of or encountered situations where data or personal information was compromised. Explain that information security is a crucial aspect of computing and is essential for protecting data from unauthorized access or misuse. ***Main (35mins)*** Introduce the four main threats in information security: authorization, authentication, encryption, and decryption. Define each threat briefly and explain their significance in safeguarding data. Focus on authorization as the first threat and explain its role in controlling access to data and resources. Discuss various methods of authorization, such as user accounts, permissions, access controls, and role-based access control (RBAC). Engage learners in a discussion about real-life scenarios where authorization is important, such as accessing bank accounts, social media profiles, or school records. Move on to the second threat, authentication, which involves verifying the identity of users or systems. Explain the concept of usernames, passwords, biometrics (e.g., fingerprints, facial recognition), and two-factor authentication (2FA). Discuss the importance of strong passwords and the risks associated with weak or shared passwords.	Pictures and videos	Mapping the protection methods to each of the four identified data threats

Introduce encryption as a method of protecting data by converting it into a secure and unreadable format. Explain the difference between encryption and decryption, where encryption converts plain text into ciphertext, and decryption converts ciphertext back to plain text. Discuss commonly used encryption techniques, such as symmetric key encryption (e.g., AES) and asymmetric key encryption (e.g., RSA). Provide examples of situations where encryption is used, such as online banking, secure messaging apps, and e-commerce transactions. Divide learners into small groups and provide them with handouts or worksheets related to information security. Learners in their groups discuss and identify examples of authorization, authentication, encryption, and decryption in everyday computing scenarios. Encourage group discussions and collaboration to reinforce their understanding of the concepts. <u>Assessment</u> 1. What are the four main threats in information security? 2. Explain what authorization means in the context of information security. 3. Give an example of a situation where authorization is important. 4. What is authentication and why is it important in protecting data? 5. Name two methods of authentication mentioned in the lesson. 6. What is the purpose of encryption in information security? 7. Explain the difference between encryption and decryption. ***Reflection** (10mins)* Use peer discussion and effective questioning to find out from learners what they have learnt during the lesson. Take feedback from learners and summarize the lesson.		

Homework/Project Work/Community Engagement Suggestions
• Provide an example of a situation where encryption is commonly used. • Describe symmetric key encryption and asymmetric key encryption. • How does two-factor authentication enhance security?
Cross-Curriculum Links/Cross-Cutting Issues
None
Potential Misconceptions/Student Learning Difficulties
None

Week Ending: 21-07-2023	**DAY:**	**Subject:** Computing	
Duration: 60mins		**Strand:** Communication Networks	
Class: B8	**Class Size:**	**Sub Strand:** Information Security	
Content Standard: B8.3.3.1. Recognize data threats and security protections	**Indicator:** B8.3.3.1.2 Map the protection methods to each of the four identified data threats (Authorisation, Authentications, Encryption and Decryption)		**Lesson:** 1 of 2
Performance Indicator: Learners can map the protection methods to each of the four identified data threats		**Core Competencies:** CC8.2: CP6.1	
Reference: Computing Curriculum Pg. 34			

Activities For Learning & Assessment	**Resources**	**Progression**
Starter (5mins) Ask learners if they have ever heard of or encountered situations where data or personal information was compromised. Explain that information security is a crucial aspect of computing and is essential for protecting data from unauthorized access or misuse. ***Main (35mins)*** Introduce the concept of threats to data security and explain that these are potential risks or vulnerabilities that can lead to data breaches. Discuss common threats, such as unauthorized access, malware, social engineering, and physical theft or loss of devices. Focus on unauthorized access as a threat and explain its impact on data security. Move on to malware as a threat and explain its potential dangers, including viruses, worms, trojans, and ransomware. Discuss methods of preventing malware infections, such as • installing and regularly updating antivirus software, • avoiding suspicious downloads or email attachments, and • Practicing safe browsing habits. Introduce social engineering as a threat and explain how it involves manipulating individuals to gain unauthorized access to sensitive information. *Social engineering refers to the manipulation and exploitation of human behavior to deceive individuals into divulging sensitive information or performing actions that may compromise the security of computer systems, networks, or data.* Discuss common social engineering techniques, such as phishing emails, impersonation, and pretexting.	Pictures and videos	Mapping the protection methods to each of the four identified data threats

Teach learners to be cautious of unsolicited requests for personal information and to verify the authenticity of requests before sharing any sensitive data. Discuss physical theft or loss of devices as a threat to data security. Explain the importance of securing devices through physical measures, such as locking them, encrypting data, and using remote wipe or tracking features. Encourage learners to report any lost or stolen devices immediately to minimize the risk of data compromise. Divide learners into small groups and provide them with handouts or worksheets related to data security. Have groups discuss and identify examples of each threat and brainstorm preventive measures for each one. <u>Assessment</u> 1. What is data security, and why is it important? 2. Name two common threats to data security. 3. Explain what unauthorized access means and how it can be prevented. 4. What is malware, and how can its impact be minimized? 5. Describe one method of preventing malware infections. ***Reflection** (10mins)* Use peer discussion and effective questioning to find out from learners what they have learnt during the lesson. Take feedback from learners and summarize the lesson.		

Homework/Project Work/Community Engagement Suggestions
• What is social engineering, and why is it a threat to data security? • Give an example of a social engineering technique. • How can individuals protect themselves from social engineering attacks? • Why is physical theft or loss of devices a threat to data security? • Name two measures that can be taken to secure devices from physical theft or loss.
Cross-Curriculum Links/Cross-Cutting Issues
None
Potential Misconceptions/Student Learning Difficulties
None