THIRD TERM

WEEKLY LESSON NOTES – B9

WEEK 2

Week Ending:	**DAY:**	**Subject:** Computing
Duration: **6**0mins		**Strand:** Communication Networks
Class: B9	**Class Size:**	**Sub Strand:** Information Security

Content Standard: B9.3.3.1. Recognize data threats and the means of protection	**Indicator:** B9.3.3.1.2 Explain ten (10) information hacking techniques on the Internet environment.	**Lesson:** 1 of 2

Performance Indicator: Learners can identify the hacking techniques used on the internet environment	**Core Competencies:** CC8.2: CP6.1

New words	Information, Hacking, Phishing, Keyloggers, Denial, Service

Reference: Computing Curriculum Pg. 51

Activities For Learning & Assessment	**Resources**	**Progression**
Starter (5mins) Begin by asking learners if they have heard about hacking and what they think it means. Share performance indicators and introduce the lesson. ***Main (35mins)*** Introduce the lesson by explaining that today they will learn about hacking techniques used in the internet environment. Define hacking as the unauthorized access, modification, or disruption of computer systems or networks. Introduce and discuss common hacking techniques: ● Phishing: Trickery to obtain sensitive information like passwords or credit card details. ● Keyloggers: Software that records keystrokes to steal login credentials. ● Denial of Service (DoS) Attack: Flooding a system to make it unavailable to users. ● Eavesdropping: Intercepting and listening to communications without authorization.	Pictures and charts	Identifying the hacking techniques used on the internet environment

Provide examples of each hacking technique and discuss their potential effects on individuals and organizations. Assessment 1. Define phishing and provide an example. 2. Explain what keyloggers are used for. 3. Describe a Denial of Service (DoS) attack and its impact. 4. Discuss why eavesdropping is considered a hacking technique. ***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		
●		
Cross-Curriculum Links/Cross-Cutting Issues		
None		
Potential Misconceptions/Student Learning Difficulties		
None		

Week Ending:	**DAY:**	**Subject:** Computing
Duration: 60mins		**Strand:** Communication Networks
Class: B9	**Class Size:**	**Sub Strand:** Information Security

Content Standard: B9.3.3.1. Recognise data threats and the means of protection	**Indicator:** B9.3.3.1.2 Explain ten (10) information hacking techniques on the Internet environment.	**Lesson:** 1 of 2

Performance Indicator: Learners can explain ten (10) information hacking techniques	**Core Competencies:** CC8.2: CP6.1
New words	Information, Hacking, Phishing, Keyloggers, Denial, Service
Reference: Computing Curriculum Pg. 51	

Activities For Learning & Assessment	**Resources**	**Progression**
Starter (5mins) Begin by asking learners if they have heard about hacking and what they think it means. Share performance indicators and introduce the lesson. ***Main (35mins)*** Introduce the lesson by explaining that today they will learn about information hacking techniques used in the internet environment. Define information hacking as unauthorized access or manipulation of digital data for malicious purposes. Present and discuss ten information hacking techniques in simple words: ● Phishing: Deceptive emails or websites to obtain sensitive information. ● Keyloggers: Software that records keystrokes to steal login credentials. ● Denial of Service (DoS) Attack: Flooding a system to make it unavailable. ● Eavesdropping: Intercepting and listening to digital communications. ● Man-in-the-Middle (MitM) Attack: Intercepting and altering data between parties.	Pictures and charts	Explaining ten (10) information hacking techniques

- SQL Injection: Injecting malicious code into a database to access or modify data.
- Social Engineering: Manipulating people to divulge confidential information.
- Ransomware: Malware that encrypts files and demands payment for decryption.
- Trojan Horse: Malware disguised as legitimate software to gain access.
- Distributed Denial of Service (DDoS) Attack: Coordinated attack from multiple sources to overwhelm a system.

Discuss the potential effects of each hacking technique and ways to prevent or mitigate them.

Assessment

1. Define phishing and explain how it works.
2. Describe a Denial of Service (DoS) attack and its effects.
3. What is social engineering, and how can individuals protect themselves from it?
4. Discuss the difference between SQL Injection and Trojan Horse malware.

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

- State and explain the ten (10) information hacking techniques

Cross-Curriculum Links/Cross-Cutting Issues

None

Potential Misconceptions/Student Learning Difficulties

None