THIRD TERM

WEEKLY LESSON NOTES – B8

WEEK 3

Week Ending: 14-07-2023	**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:** B8.3.3.1.1 Describe the nature of four major data threats (Interruption, Interception, Modification, Fabrication)	**Lesson:** 1 of 2
Performance Indicator: Learners can describe the nature of four major data threats		**Core Competencies:** CC8.2: CP6.1
Reference: Computing Curriculum Pg. 34		

Activities For Learning & Assessment	**Resources**	**Progression**
Starter (5mins) Revise with learners to review their understanding in the previous lesson. Share performance indicators and introduce the lesson. ***Main (35mins)*** Brainstorm learners to explain the meaning of data threats. *Threats to data security refer to potential risks and vulnerabilities that can compromise the confidentiality, integrity, and availability of data.* Engage learners to watch a video on threats to data security. Discuss the threats that can prevent information from reaching its destination. • *Network Failures: Network failures can occur due to hardware malfunctions, software glitches, or misconfigurations. These failures can disrupt the transmission of data, causing delays or complete loss of connectivity.* • *Connectivity Issues: Connectivity issues, such as internet outages or disruptions in network infrastructure, can prevent information from reaching its destination. This can happen due to factors like severed cables, power outages, or issues with internet service providers.* • *Routing Problems: Routing problems occur when there are errors or misconfigurations in the routing infrastructure of a network. Incorrect routing information can cause data to be sent on incorrect paths or be lost in transit, preventing it from reaching the intended destination.* • *Packet Loss: Packet loss refers to the failure of network packets to reach their destination. It can happen due to network congestion, hardware issues, or errors in*	Pictures and videos	Describing the nature of data threats

transmission. If a significant number of packets are lost, the information may not reach its destination correctly.

Discuss the threats that can cause data corruption.

- *Hardware Failures: Hardware failures, such as hard drive crashes, memory errors, power surges, or faulty components, can corrupt data stored on the affected devices.*
- *Software Glitches and Bugs: Software glitches, bugs, or programming errors can introduce flaws into applications or systems, leading to data corruption. For instance, a programming error in a data storage or retrieval function can result in data being written or read incorrectly, causing corruption.*
- *Malware and Viruses: Malicious software, such as viruses, worms, or ransomware, can infect systems and cause data corruption. Some malware is specifically designed to modify or encrypt data, rendering it inaccessible or corrupted. Ransomware attacks.*

Assessment
1. What are two common causes of data corruption?
2. How can organizations mitigate the threat of data corruption?
3. How can network failures and connectivity issues affect the transmission of data and prevent it from reaching its intended destination?

***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 the primary goal of a Denial-of-Service (DoS) attack, and how does it impact the delivery of information?

Cross-Curriculum Links/Cross-Cutting Issues

None

Potential Misconceptions/Student Learning Difficulties

None

Week Ending: 14-07-2023	**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:** B8.3.3.1.1 Describe the nature of four major data threats (Interruption, Interception, Modification, Fabrication)	**Lesson:** 1 of 2
Performance Indicator: Learners can describe the nature of four major data threats	**Core Competencies:** CC8.2: CP6.1	
Reference: Computing Curriculum Pg. 34		

Activities For Learning & Assessment	**Resources**	**Progression**
Starter (5mins) Revise with learners to review their understanding in the previous lesson. Share performance indicators and introduce the lesson. ***Main (35mins)*** Describe the nature of the four major data threats. 1. Interruption: Interruption refers to the disruption or denial of access to data and systems. It involves the intentional or unintentional actions that result in the unavailability of data or system resources. Examples include: • Distributed Denial of Service (DDoS) attacks: Overwhelming a system or network with a flood of requests, rendering it inaccessible to legitimate users. • Power outages or hardware failures: These events can disrupt access to data and systems until the issues are resolved. • Natural disasters: Events like earthquakes, floods, or fires can physically damage infrastructure and interrupt data access. The goal of interruption is to render data or systems unusable or inaccessible, causing disruption, financial loss, or reputational damage. 2. Interception: Interception involves unauthorized access to data during transmission. It occurs when an attacker intercepts or eavesdrops on communication channels to capture sensitive information. Examples include: • Man-in-the-Middle (MitM) attacks: An attacker positions themselves between the sender and receiver, intercepting and potentially modifying the communication. • Wi-Fi snooping: Unauthorized individuals intercepting data transmitted over unsecured or public Wi-Fi networks. • Packet sniffing: Capturing and analyzing network traffic to obtain sensitive data, such as passwords or financial information.	Pictures and videos	Describing the nature of data threats

Interception threatens the confidentiality of data by allowing unauthorized individuals to access and exploit sensitive information.

3. Modification:
Modification refers to unauthorized alteration or tampering of data. Attackers aim to modify data to manipulate its integrity, accuracy, or trustworthiness. Examples include:

- Data tampering: Unauthorized modification of data to manipulate records, transactions, or information.
- Man-in-the-Middle attacks: Intercepting and modifying data during transmission.
- Unauthorized changes to critical files, databases, or configurations.

Modification can lead to data corruption, false information, financial loss, or reputational damage, compromising the integrity of data.

4. Fabrication:
Fabrication involves the creation or insertion of false or counterfeit data into a system or network. It refers to the unauthorized addition of data that appears legitimate, but is, in fact, fraudulent. Examples include:

- Falsified records: Creating or adding false information to deceive users or manipulate systems.
- Counterfeit digital certificates: Generating fake digital certificates to impersonate trusted entities.
- Spoofed email addresses or websites: Creating fake email accounts or websites to deceive users and collect sensitive information.

Fabrication can lead to misinformation, identity theft, financial fraud, and compromised trust in systems and data.

Assessment
1. What is the difference between interception and modification as data threats?
2. How does interruption pose a risk to data availability?
3. Provide an example of a real-world scenario where fabrication of data can lead to significant consequences.

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 real-world scenario where fabrication of data can lead to significant consequences

Cross-Curriculum Links/Cross-Cutting Issues

None

Potential Misconceptions/Student Learning Difficulties

None