or 0248043888
https://www.TeachersAvenue.net
https://TrendingGhana.net
https://www.mcgregorinriis.com

BASIC 8

WEEKLY LESSON PLAN – WEEK 3

Strand:	Communication Networks		**Sub-Strand:**	Information Security	
Content Standard:	B8.3.3.1. Recognise data threats and security protections				
Indicator (s)	B8.3.3.1.1 Describe the nature of four major data threats (Interruption, Interception, Modification, Fabrication) B8.3.3.1.2 Map the protection methods to each of the four identified data threats (Authorization, Authentications, Encryption and Decryption)		**Performance Indicator:** Learners can apply measures to prevent data thefts.		
Week Ending	14-07-2023				
Class	B.S.8	**Class Size:**		**Duration:**	
Subject	Computing				
Reference	Computing Curriculum, Basic 7 Computing Textbook, Teachers Resource Pack, Learners Resource Pack.				
Teaching / Learning Resources	Power Point Presentation, Chart, Poster, Video		**Core Competencies:**	• Communication and Collaboration • Digital Literacy	

DAY/DATE	**PHASE 1 : STARTER**	**PHASE 2: MAIN**	**PHASE 3: REFLECTION**
THURSDAY	Discuss the meanings of some keywords and terminologies in the lesson with the Learners.	1. Show Learners a video clip on threats to data security. 2. Discuss with Learners about the meaning of data security and data threats. 3. Assist Learners to identify examples of threats that can prevent information from reaching its destination. 4. Using a Presentation, explain how threats can cause data corruption. **Data Security;** Data security is the process of safeguarding digital information throughout its entire life cycle to protect it from corruption, theft, or unauthorized access. It covers everything—hardware, software, storage devices, and user devices; access and administrative controls; and organizations' policies and procedures. **Data threats ;**	Learners in small groups to discuss and report to the class on the nature of the four major data threats. **Exercise;** 1. Explain the following; i. Data Security ii. Data threats 2. Write 4 examples of threats that can

		Threats could be an intruder network through a port on the firewall, a process accessing data in a way that violates the security policy, a tornado wiping out a facility, or an employee making an unintentional mistake that could expose confidential information or destroy a file's integrity. **Crypter** A type of malware designed with the ability to encrypt, obfuscate, and alter other malware—making it significantly more difficult to be detected by antivirus and security programs. **Cybercrime** Cybercrime is a term that encompasses any criminal activity involving the use of digital technology or communication, such as the internet, computers, or smartphones. In most cases, these crimes are financially driven but attacks may also be politically or personally motivated. Cybercrime can include a wide range of activities, such as fraud, theft, cyberstalking, ransomware, malware distribution, and so many others. Read more about cybercrime. **Cybersquatting** Also referred to as domain squatting, cybersquatting is the practice of registering and using an internet domain name with ill-intent for the purposes of deceiving and/or profiting from unassuming "mistakes" on part of a human web user or computer system. The name is derived from "squatting"—the act of occupying a deserted or uninhabited space without proper permission. **Bitsquatting** A form of cybersquatting—Bitsquatting is the practice of registering slight variations of popular domain names likely to result from a random memory error in a user's computer. (e.g. excmple.com or exaeple.com for example.com) The name is derived from "bit" + "typosquatting". **Example**: **"amczon.com"** or **"aeazon.com"** instead of **"amazon.com"** **Typosquatting**	prevent information from reaching its destination.

		Also referred to as URL hijacking—Typosquatting is form of cybersquatting. It is the practice of registering slight variations of popular domain names that are likely to be mistyped by users when inputting a website address. **Example**: **"goolge.com"**, **"aamzon.com"**, **"wellsfarog.com"**, etc. Also see, Homograph Attack for other types of cybersquatting including spoofing attacks using ASCII and Internationalized Domains Names (IDNs). **Dark Web** The Dark Web refers internet content that exists on 'darknets'—or overlay networks that require specific software and/or non-standard network configurations and communication protocols to access. The Dark Web prioritizes anonymity and encryption to keep communications private. This is purposeful—as the Dark Web is home to a wide range of illicit activities and dealings like illegal marketplaces that sell stolen media and content, hacking tools, drugs, and even child pornography. The Dark Web makes up only a small percentage of the 'Deep Web'. See Deep Web. **Data Breach** Data Breach refers to the intentional or unintentional release of private or confidential information or data. Other terms for data breach include unintentional information disclosure, data leakage, or data spill. Data compromised during a breach may have been viewed, copied, destroyed, extracted, and used or sold for profit. Some common reasons and methods of data breach include: • Theft or loss of digital media or property • Careless disposal of used computer equipment (laptop, hard drives, etc.) • Failure to encrypt data in transit (sent via email, SMS, etc.) • Failure to properly secure/authenticate access to an available internet service	

		• Computer bugs and vulnerabilities (zero-day attacks, etc.) • Ransomware and phishing attacks • Social engineering campaigns Examples of sensitive data may include credit card information, SSNs, usernames/passwords, trade secrets, intellectual property, emails, private customer information such as medical records (personal health information or PHI) or financial documents, and more. **Deep Web** The Deep Web refers to the parts of the internet that are not indexed (not visible) on search engines like Google, Bing, Yahoo, etc. There are a number of legitimate reasons to prevent search engines from indexing content. Much larger than the "Clearnet" (i.e. indexed internet), the Deep Web is made up of content delivery networks (CDNs), servers that support web services, content behind paywalls, email, online banking tools, and much much more. See Dark Web. **Distributed Denial-of-Service (DDoS)** Commonly referred to as DDoS, a distributed denial-of-service attack is the malicious attempt to interrupt network traffic to a target destination, network, or server by overwhelming it with a massive amount of fraudulent traffic from hundreds of thousands (or more) of source locations. Bad actors typically enlist the help of giant botnets of malware-infected routers, IoT devices, and other computers to drive "legitimate" traffic at the target—and thus making it difficult to distinguish the attack from normal traffic. **Domain Generated Algorithm (DGA)** These algorithms are used in a variety of malware types to create a large number of domain names for use in communication with command and control (C&C) servers. In order to achieve autonomous update capabilities, C&C server	

		destinations are often hard-coded into the malware itself—making it easier for law enforcement and cybersecurity forces to find and shut down. DGA's create a large number of potential communication points, and allows malware to reach out to any number of those points—at random—to request updates. Read more about Domain Generated Algorithms. **DNS Spoofing** Also referred to as DNS Cache Poisoning, DNS Spoofing is a of cyber attack (and form of Pharming)—aimed at compromising and manipulating Domain Name System data in a DNS resolver's cache—resulting in a DNS server returning an incorrect result and routing internet traffic to a website or location chosen by the hacker.	
FRIDAY	Review Learners knowledge on the previous lesson.	1. Discuss with Learners about methods of protecting data against the four main threats. 2. Using a Presentation, describe examples of threats to data security. 3. Learners brainstorm to identify methods of preventing each threat. **measures to protect data against the four main threats;** • Back up your data. • Secure your devices and network. • Encrypt important information. • Ensure you use multi-factor authentication (MFA) • Manage passphrases. • Monitor use of computer equipment and systems. • Put policies in place to guide your staff. • Train your staff to be safe online. **Examples of threats to data security;** Physical: i. Theft ii. Tampering iii. Snooping iv. Sabotage v. Vandalism	Through questions and answers, conclude the lesson. **Exercise;** 1. State 4 methods of protecting data against the four main threats. 2. Mention 4 examples of threats to data security

		vi. local device access vii. assault **Environmental:** i. Natural events such as tornadoes ii. power loss iii. Fires iv. floods **Preventing data thefts;** • Keep your software and systems fully up to date. • Ensure Endpoint Protection. • Install a Firewall. • Backup your data. • Control access to your systems. • Wifi Security.	

Name of Teacher: ***School:*** ***District:***