Information Technology (IT)



"If you know the enemy, and know yourself, you need not fear the result of 100 battles. If you know yourself, but not the enemy, for every victory gained, you'll also suffer defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

These ideas come from Chinese General and Philosopher, Sun Tzu.
-The Art of War.

IT Department Orientation:

Cyber Security and Privacy Training

ABOUT THIS MODULE

This module is designed to empower every member of our organization with the knowledge and tools necessary to protect the integrity, confidentiality, and availability of our digital assets, because ultimately, **cybersecurity is everyone's responsibility**.

Led by Franklin K. Coleman (IT Officer), this session serves as a foundational step in our commitment to operational resilience, efficiency and data stewardship.

The Importance of Cybersecurity & Data Protection

- To begin, consider this: **What is the first word that comes to mind when you hear "cybersecurity"?** Whether it's "trust," "defense," or "accountability," your perspective is vital. We must deeply understand **why data protection matters** – not just as an IT policy, but as a core component of our ethical and professional conduct.

Learning Objectives

By the end of this session, participants will be equipped to:

- **Define and Classify Incidents:** Clearly define cybersecurity events and differentiate between various types (phishing, social engineering, malware, etc.).
- **Identification Skills:** Gain the ability to identify both potential threats (suspicious links, unauthorized access attempts) and actual security events as they occur.
- **Build a "If you see something, say something" culture:** Recognize the critical importance of a blame-free reporting culture, where prompt disclosure of mistakes or suspected breaches is encouraged to enable rapid response and organizational learning rather than punishment.
- **Attendance awareness**: Be aware of the nuances associated with ensuring smooth attendance registry and scheduling.

Training Outline

- Cybersecurity
- Types of Attacks
- Your role in this fight
- Data Protection
- Best practices
- Attendance Machine
- Hospital Management System
- CCTV

Introduction

The purpose of this presentation is to increase your awareness of the threats and risk that are part of using any information system and the sensitive information and data contained in information systems.

By information system, we mean computers, mobile devices, networks, databases, and electronic information storage.

Introduction: Cyber Security Defined

- Cyber Security is: "**Protection** of information systems **against unauthorized** access to or **modification** of information, whether in storage, processing or transit, and against the **denial** of service to authorized users, including those measures necessary to detect, document, and counter such threats."

Sensitive Data

- Information is considered **sensitive** if the **loss** of **C**onfidentiality, **I**ntegrity, or **A**vailability could be expected to have a **serious**, **severe**, or **catastrophic** adverse **effect** on organizational operations, organizational assets, or individuals.
- **Types** of sensitive information include:
  - Personnel
  - Financial
  - Payroll
  - Medical
  - Others

Personal vs Sensitive Information

Personal information (or **personal data**) refers to any information that can directly or indirectly identify a person. This type of information is typically considered less sensitive than **sensitive information**, but it is still protected under data protection laws.

Sensitive information refers to personal data that is more private or confidential in nature and, if exposed, could cause significant harm, distress, or discrimination to an individual.

Due to the sensitive nature of this information, data protection laws typically impose stricter rules for collecting, processing, and sharing it.

Personal vs Sensitive Table

Personal information	Sensitive personal information
Name	Race
Address	Religion
Age/Date of birth	Political opinion
Email address	Trade union membership
Photographs	Sexual orientation
IP address	Sex life
Location data	Gender identity
Financial Information e.g. bank account details	Health information
Mobile Number	Biometric data
NHIS Number	Genetic data
Family details	Philosophical beliefs

Personal vs Sensitive Example

Mr. Hoffman, of 433 Honey's Drive Avenue, has been recovering at FOCOS Hospital following a successful hip replacement surgery on Friday, 16th March 2020.

The operation was a complete success, and we are sending our best wishes to his family.

Mr. Hoffman has been a member of Recovery Ghana since his diagnosis in 2019 and has raised several thousand cedis for the association over the past few years, with help from connections made through his membership in the PPP Party.

You can visit him in the 2-Bed Ward at 2:00 PM on Thursdays at FOCOS, or contact his wife, Mabel, at 0244444444 or mabel@stanbicghana.com.

Threats and Vulnerabilities

- **Threats**--any circumstances or events that can potentially harm an information system by destroying it, disclosing the information stored on the system, adversely modifying data, or making the system unavailable

- **Vulnerabilities**--weakness in an information system or its components that could be exploited.

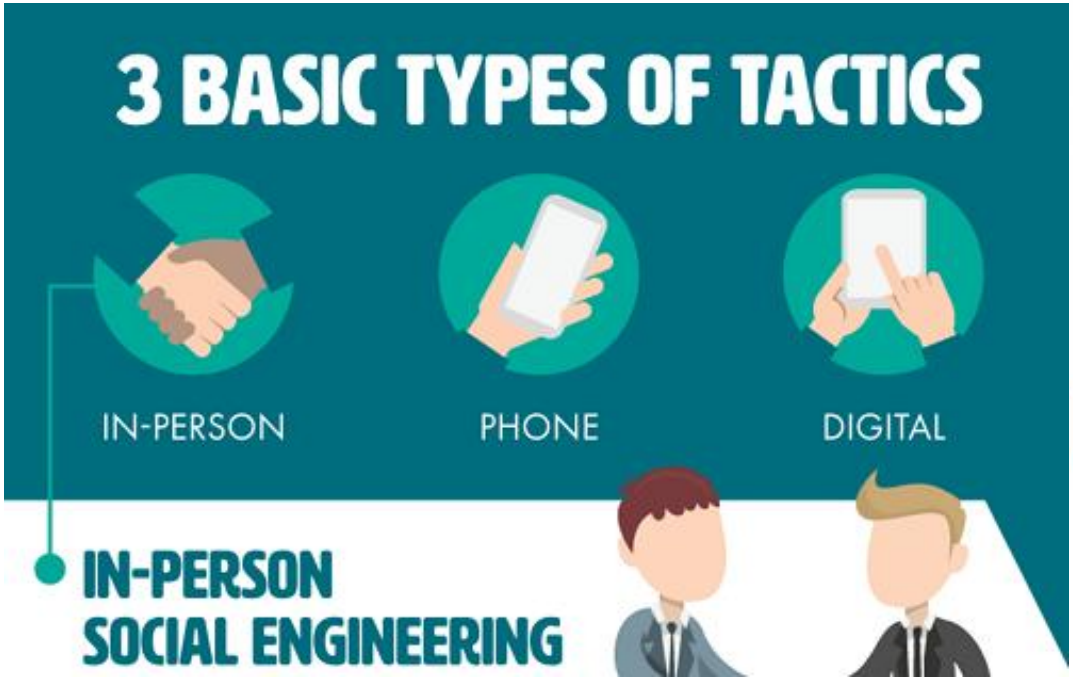
Who and Where is the Enemy?

The enemy could be thousands of miles away, or in the very next cubicle at work, or both!

We often fear the unknown hackers from the outside, but insiders are a much greater threat and can do far greater damage.

They already have some level of access, means, and opportunity.

Attacks - Social Engineering





Social engineering is a collection of techniques intended to trick people into divulging private information. Includes calls emails, web sites, text messages, in-person, etc. Currently the most frequent of cyberattacks globally.

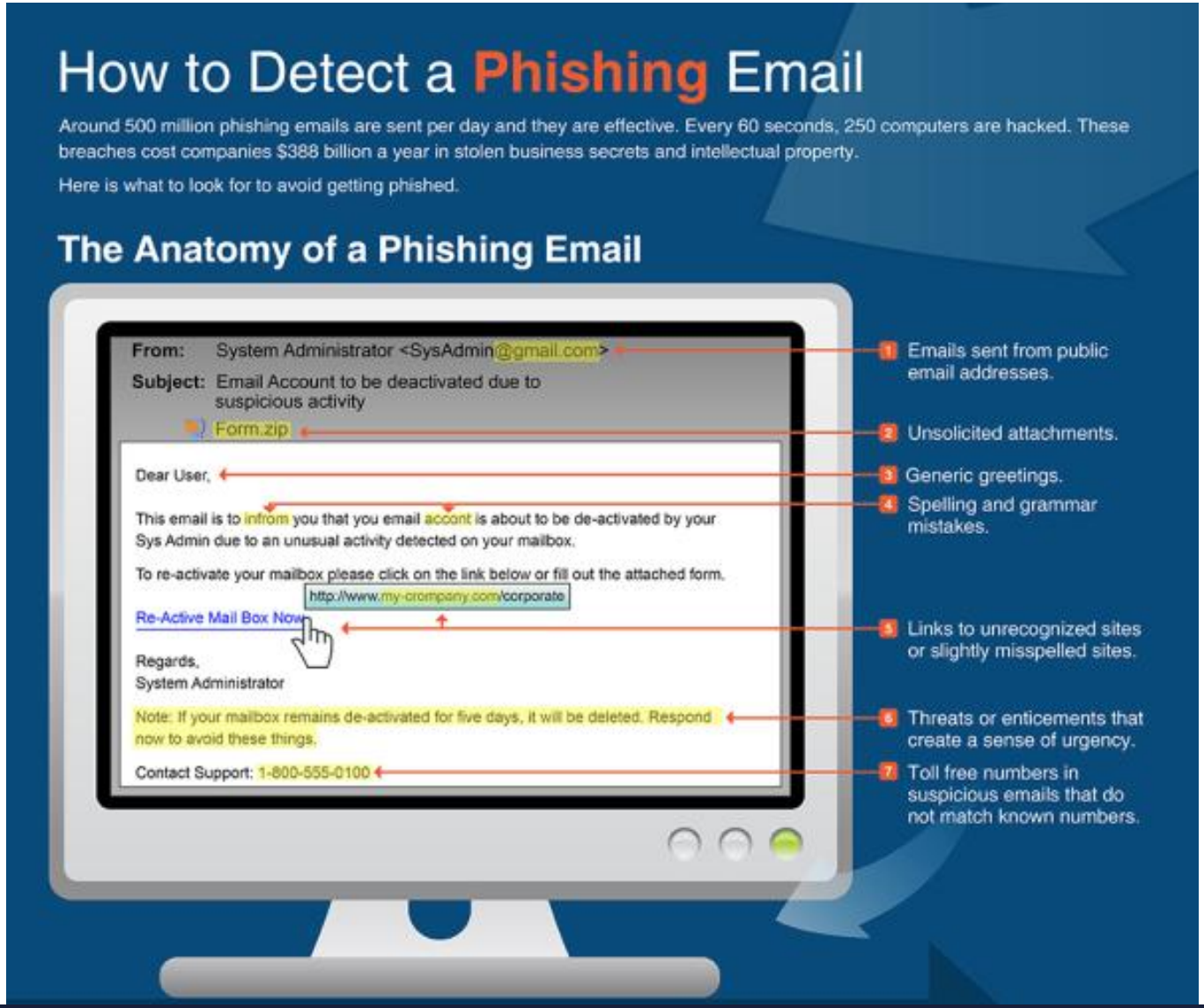
Attacks - Phishing

Phishing - Email attacks are untargeted, mass emails sent to many recipients that are meant to acquire sensitive information (e.g. password, username or bank details). With this information, a hacker can perform a data breach. It's difficult to spot a phishing email because it's disguised as a trustworthy entity that prompts a recipient to visit a malicious website.

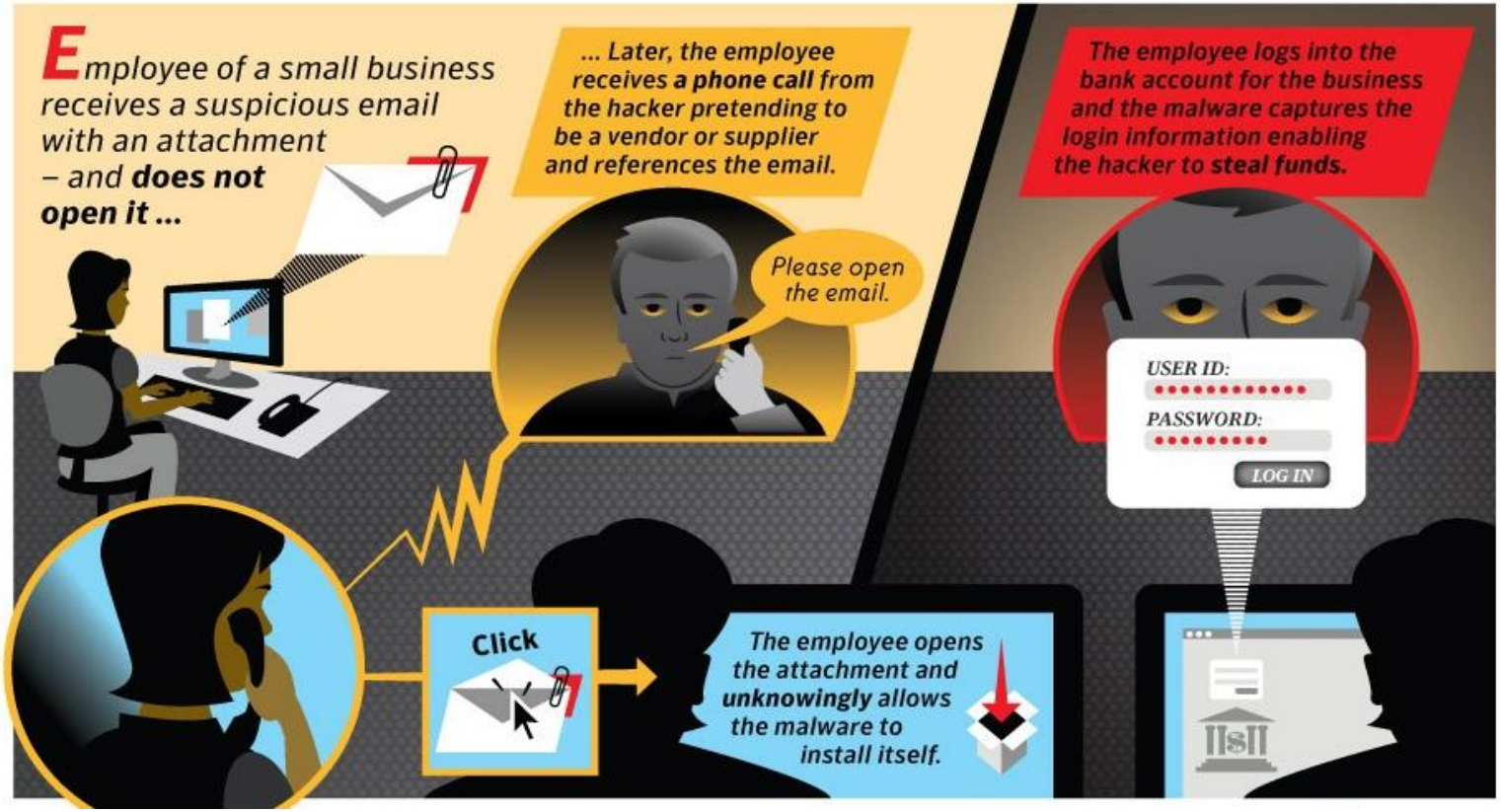
Spear-phishing - Is a more targeted form of cyber attack. An email is designed to look like it's been sent from a person the recipient knows or trusts. Senior management or privileged account owners are often the target of spear-phishing attacks.



Phishing – Email Anatomy

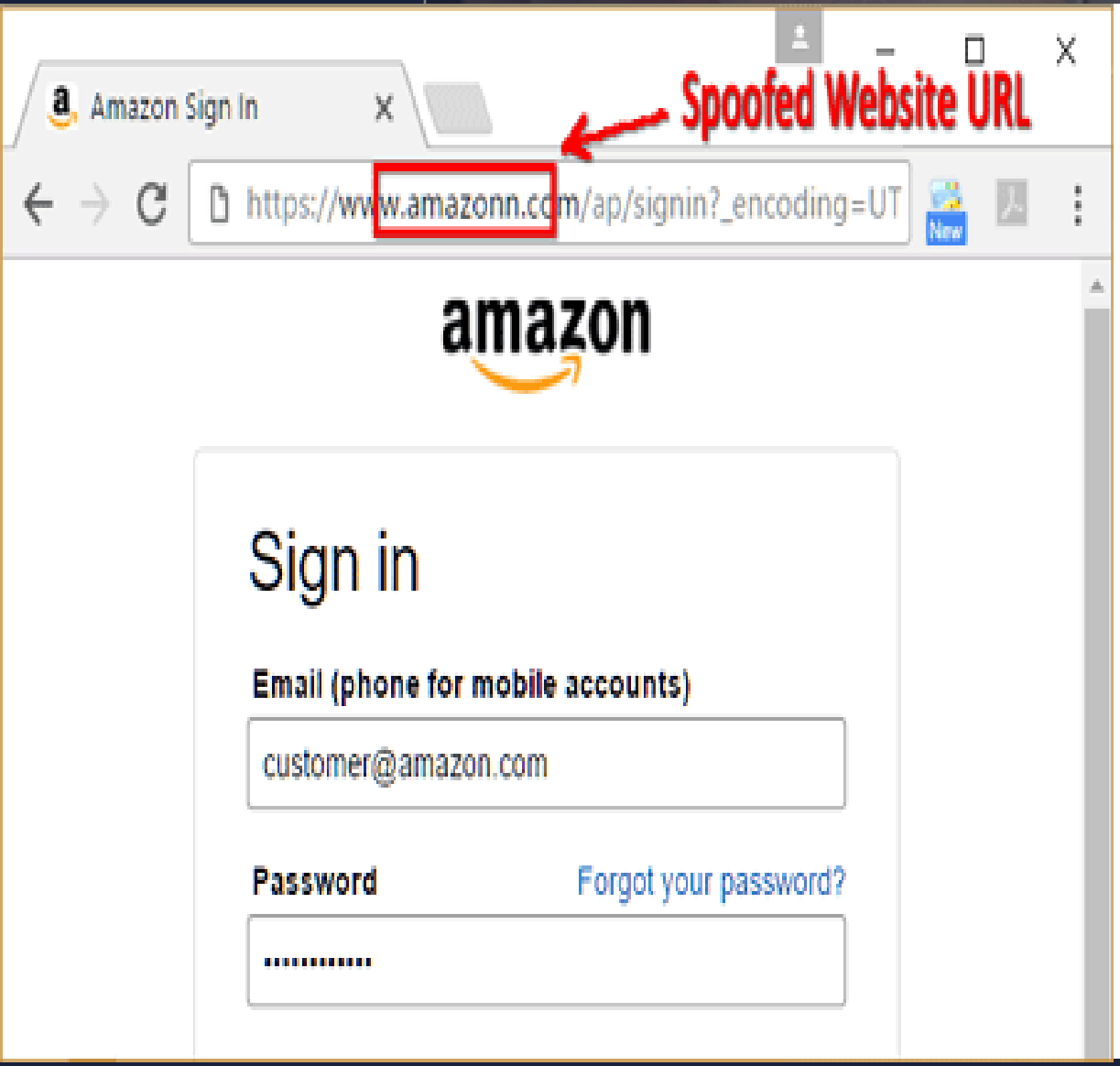


Phishing - Scenario



- An attacker could employ multiple threat methods to attempt to breach a system.
- From sending a phishing email with a suspicious attachment or link, to resorting to social engineering through phone calls, which would finally lead a victim to click on the suspicious link which loads a malware unto their systems or sends them to a spoofed website.

Spoofed Website



- A spoofed website is simply a website that has been designed by an attacker to look like a legitimate website.
- These fake websites are designed to steal the login credentials of unsuspecting victims.
- These credentials will then be used by the attacker to attempt to access the victim's data on the legitimate website.
- These sort of websites can be identified by analyzing their links or URLs.
- Take the image on left for instance the genuine link should have been: https://www.**amazon**.com/ap/signin?_encoding=UT

Malware:

Among the most common cybersecurity threats, malware refers to multiple forms of harmful software executed when a user mistakenly downloads it. Some of the most recent cybersecurity breaches involved malware, including the ransomware attacks WannaCry. Traditional malware such as viruses, Trojans and backdoors also remain persistent.



Insider threats:

An emerging method common in many recent data breaches, internal cybersecurity threats, are orchestrated by your own employees. Insider threats can be unintentional (an employee who falls victim to a phishing attack) or malicious (a disgruntled employee deliberately extracting data). Regardless, a data breach from the inside is especially difficult to detect.



Computer-Based: Baiting

- Attacker leaves a piece of media in a place to be found
- Labels media with something intriguing
- Someone plugs it in to see what is on it
- Malware is immediately installed

- If you come across a piece of media storage that no one claims ownership of, please send it to an IT expert to properly format the device before use.



Your role in Cyber security and privacy



Social Engineering

Do

- Document the situation—verify the caller identity, obtain as much information as possible, if Caller ID is available, write down the caller's telephone number, take detailed notes of the conversation
- Contact your IT Dept.

Don't

- Participate in surveys (Verify)
- Share personal information
- Give out computer systems or network information



Situational Awareness

- To practice good situational awareness, take the following precautions, including but not limited to:
  - Avoid discussing topics related to FOCOS business outside the Hospital premise, whether you are talking face to face or on the phone.
  - Avoid discussing PHI outside FOCOS
  - Don't talk about work outside the office
  - Be discreet when retrieving messages from smart phones or other media



Tips to Help Protect PII/PHI

- Collect only **PII/PHI** that you are authorized to collect, and at the minimum level necessary to accomplish a required purpose
- When not in use, store **Records** in an access-controlled environment
- Use fictional personal data for presentations or training
- Review documents for **PII/PHI** prior to posting on web pages
- Safeguard PII in any format around your work area
- Only disclose **PII/PHI** to authorized viewers

Tips to Help Protect PII/PHI

- Contact IT Department if electronic transmission of **PHI** is needed.
- Use the secure shredding bins to dispose of documents containing **PII/PHI**
- Ensure that CDs containing **PII/PHI** are purged (deleting alone is not enough)
- Work with the IT Dept. to ensure that drives containing **PII/PHI** are wiped before they are disposed of
- Delete/dispose of **PII/PHI** at the end of its retention period.

FOCOS Password Policy

- FOCOS has guidelines pertaining to password use.
  - Passwords must be:
  - Obscured during login and during transmission.
  - Changed after the initial login.
  - Forced by the system to be changed every 90 days.
  - Strong - shall include three of the four characteristics:
    - Numerals
    - Alphabetic characters
    - Upper and lower case letters
    - Special characters
    - Passwords shall be at least eight (8) characters in length.

Data Protection Act, 2012 (Act 843)

Data Protection

Data protection refers to the legal, regulatory, and organizational measures designed to safeguard personal data and ensure privacy for individuals.

In Ghana, data protection is governed by the **Data Protection Act, 2012 (Act 843)**, which provides the legal framework for protecting personal data.

Data Protection Act

- The Data Protection Act, 2012 (Act 843) sets out the **rules and principles governing the collection, use, disclosure and care for your personal data** or **information** by a data controller or processor.

- **The Act** also established the **Data Protection Commission as an independent statutory body to ensure and enforce compliance.**

- **Data Protection Law binds the Republic.** All entities; private, public and NGOs must comply with the requirements of the Act 843.

POWERS OF DPC

- Enforcement of Act
- Cancellation of DPC license
- Investigate complaints
- Carry out random audits (compliance audits)
- Accredit and certify organisations and DPS
- Issue fines and enforcement notices
- Imprisonment of CEO/Director

Data Protection Objectives

- Promote privacy and protect individuals' personal data
- Ensure compliance with the Data Protection Act
- Regulate and oversee data processing activities
- Monitor and investigate data breaches and non-compliance
- Encourage best practices in data protection
- Promote international cooperation in data protection
- Enforce sanctions and penalties for non-compliance

DPC Territorial Scope

- Established in Ghana and the processing takes place in this country.
- Not established in Ghana but uses equipment or a data processor in carrying out business in this country to process the data.
- Processing is in respect of information which originates partly or wholly from this country.
- Other jurisdictional legal requirements e.g. European Union.

Data Subject – The 10 Right

- Right to be informed
- Right to give and withdraw consent
- Right to access his or her personal information
- Right to amend (rectification)
- Right to object
- Prevent processing
- Right to prevent processing of personal data for direct marketing
- Right to compensation
- Right to erasure
- Right to data portability

Data Protection Best Practices

- **Data Minimization**:

  Only collect the personal data you need. Don’t ask for unnecessary details, like social security numbers, unless required.

- **Data Encryption**:

  Use strong encryption to protect personal data, especially when storing or sharing it online.

- **Access Control**:

  Limit who can access personal data. Only allow employees who need the data for their work to see it. Use **multi-factor authentication** (MFA) for added security.

- **Anonymization or Pseudonymization**:

  If possible, make personal data anonymous or pseudonymous (replace identifying details with fake ones) to reduce risk if there's a breach.

Data Protection Best Practices

- **Data Retention**:

  Don’t keep personal data longer than necessary. Regularly review and delete or anonymize old data.

- **Training and Awareness**:

  Train employees on data privacy and security. Make sure they understand their role in protecting personal information.

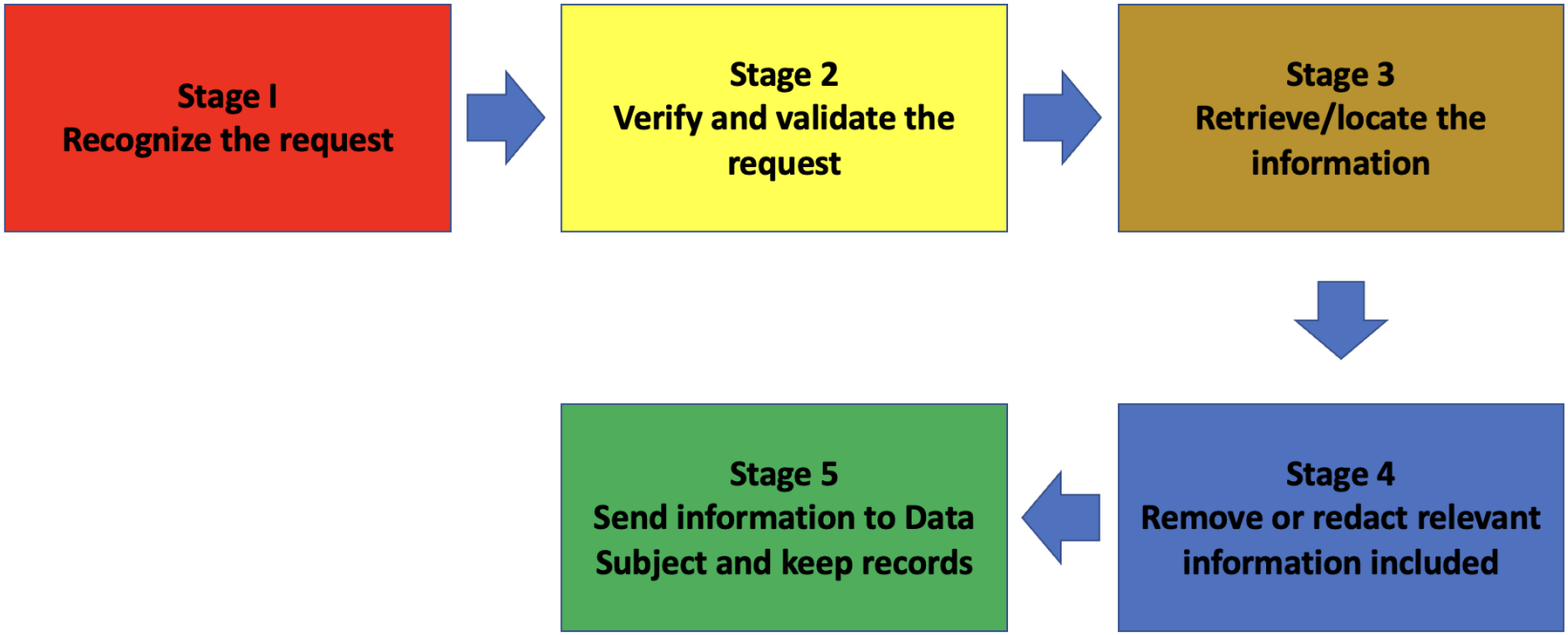
- **Data Subject Rights**:

  Allow individuals to easily access, correct, or delete their personal data.

- **Third-Party Service Providers**:

  If you use third-party services (like cloud storage), ensure they also protect the data properly. Set clear agreements (Data Processing Agreements) with them to outline their responsibilities.

Access Request Stages



How to report Data Breach

1. Report to your Data Protection Supervisor in the organization
2. Data Protection Supervisor to notify DPC of the breach
3. Data Controller to inform Data subjects of data breaches
4. Data Controller to take steps to restore integrity of information system

Note: **The data controller shall delay the notification** to the data subject where the security agencies or the Data Protection Commission inform the data controller that the notification will impede a criminal investigation.

Data Subject can also report to the commission if they notice the organization which holds their personal data is non-compliance with protection laws of the land.

Biometric Attendance & Hospital Management System

Biometric/Face Attendance





Benefits of Biometric Attendance

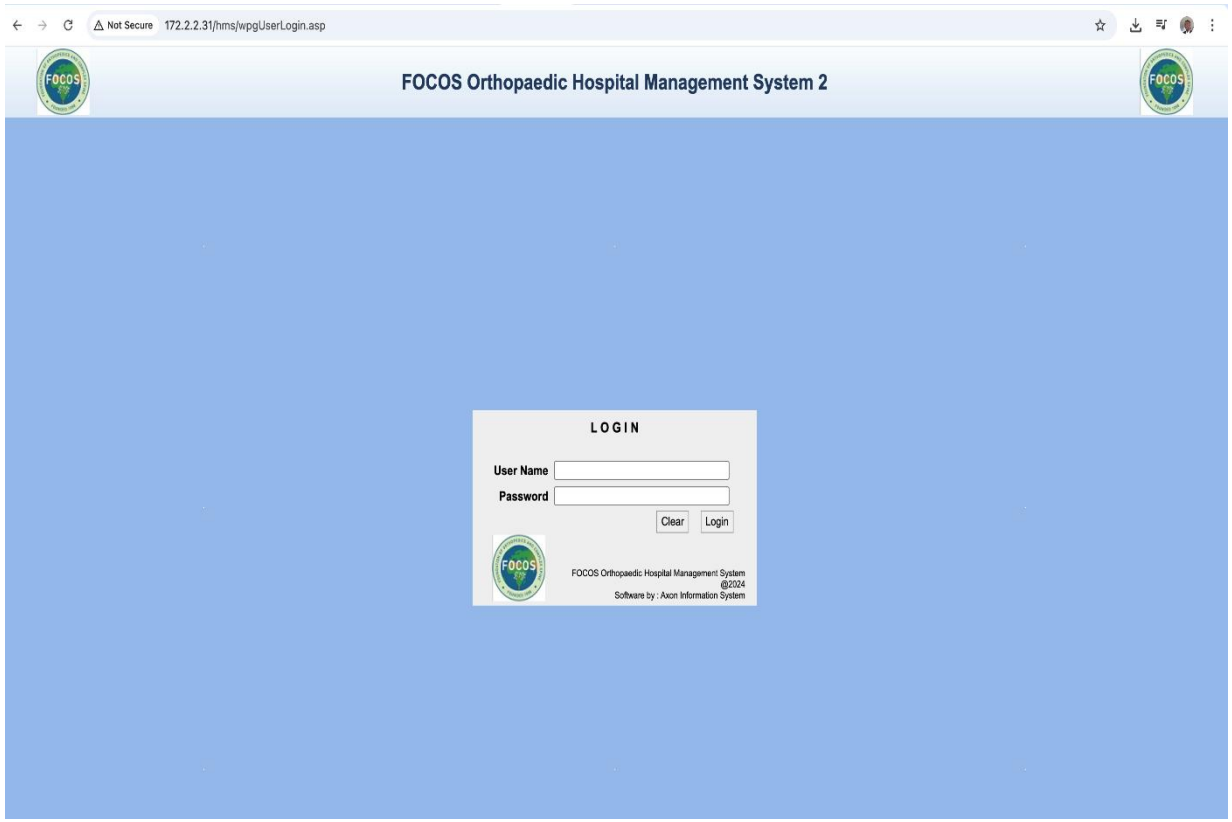
- **Transparency:** Employees can trust that their working hours are logged accurately, which can prevent disputes over salary.
- **Time Savings:** Facial and fingerprint recognition are faster than traditional methods, reducing time spent clocking in and out.
- **Infection Control:** Facial recognition is contactless, reducing the risk of spreading germs and infections, which is crucial in FOCOS.
- **Personalized Access:** Only authorized personnel can clock in and out using their unique biometric data, preventing fraudulent activities like buddy punching.
- **Regulatory Compliance:** Ensures that FOCOS complies with labour laws and regulations regarding working hours and overtime, protecting employee rights.

Example of Attendance Issues

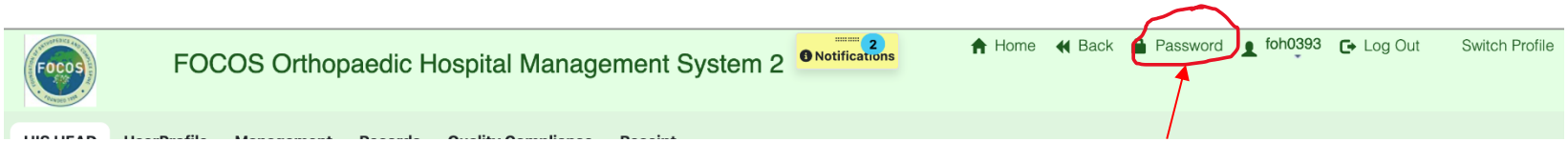
Attendance Report First & Last (8Hour Shift)						
Date	Weekday	First Punch	Last Punch	Total Hours	Worked Hours	
2024-06-03	Monday	08:00	17:00	9	8	
2024-06-04	Tuesday	09:00	18:00	9	7	
2024-06-05	Wednesday	07:00	16:00	9	7	
2024-06-06	Thursday	08:00	20:00	12	8	Overtime not approved
2024-06-07	Friday	08:00	20:00	12	11	Overtime approved

- Staff are advised to remember to clock-in at the beginning of a given shift and clock-out at the end of that shift.
- If said staff is to immediately continue with another shift; the staff should clock-in once again at the beginning of that given shift and endeavor to clock-out at the end of that new shift.
- Night-shift staff are advised to confirm from their supervisors if their shift schedules have been entered into the Attendance Management System.

Hospital Management System

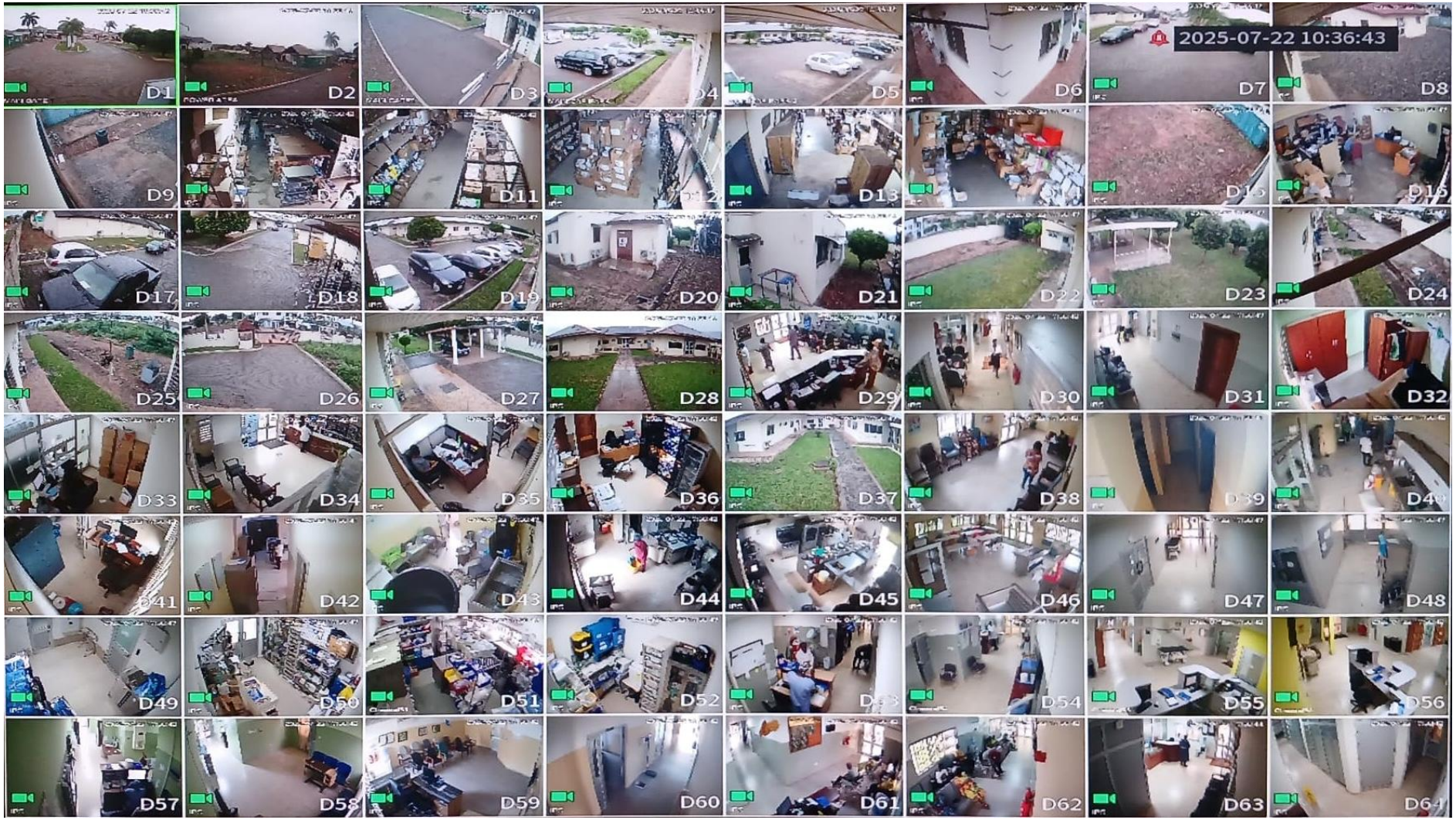


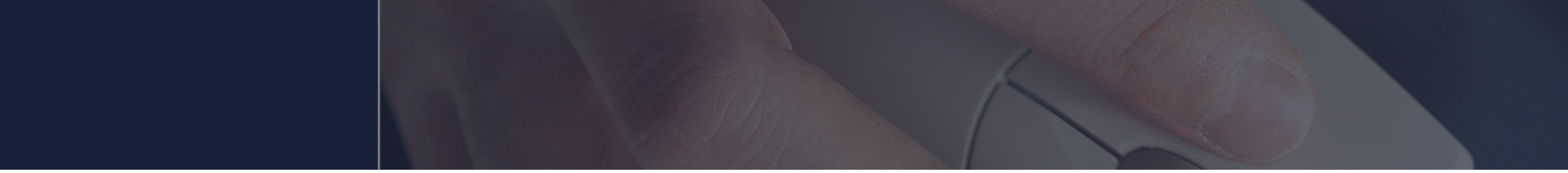
- This is FOCOS Hospital's main system of information management.
- Accessible by all registered and authorized staff.
- Can be accessed on all computers within the facility.
- First-time-users of the system will be given default generic passwords, along with their usernames for initial login.
- After initial login, said user is expected to change their generic passwords to a strong one following FOCOS's password policy.



- To change your password, click on this section and follow the given instructions.

24Hrs CCTV Surveillance





THANK YOU