



# CYBERSECURITY

**Presented By:**

Anna Tew THIAO

Maramé FALL

**Supervised By:**

Mrs DABO



# PLAN

## ▶ INTRODUCTION

I. CYBERSECURITY' S COMPONENTS

II. VULNERABILITY AND PROTECTION  
OF INFORMATION SYSTEMS

III. HACKERS

IV. VIRUSES

## ▶ CONCLUSION



# INTRODUCTION

- ▶ Cybersecurity refers to the practice of protecting computer systems, networks, and data from unauthorized access, use, theft, or damage. With the rapid growth of technology and the internet, cybersecurity has become an essential concern for individuals, businesses, and governments alike.
- ▶ IS, which consists of establishing security strategies that work together to help protect our digital data, also protects the integrity of information technologies such as systems, networks, and computer data against threats, risks, and vulnerabilities.
- ▶ The goal of cybersecurity is to ensure the confidentiality, integrity, and availability of digital information and assets. Cybersecurity threats can come in many forms, including viruses...To prevent cybersecurity threats, cybersecurity professionals use a range of tools and techniques, including firewalls, intrusion detection.

# I. CYBERSECURITY'S COMPONENTS

- The main components of cybersecurity are:





However, we are also note other components namely:

- ❖ Authentication: ensures the identification of an individual, an entity but also the origin of the information or of an operation carried out on it
- ❖ Authorization: Provides control over the type of activities or information a person or entity is authorized to perform or access;
- ❖ Logging: ensures that all access to a system, all access to information as well as any operation carried out on them is logged/listed.

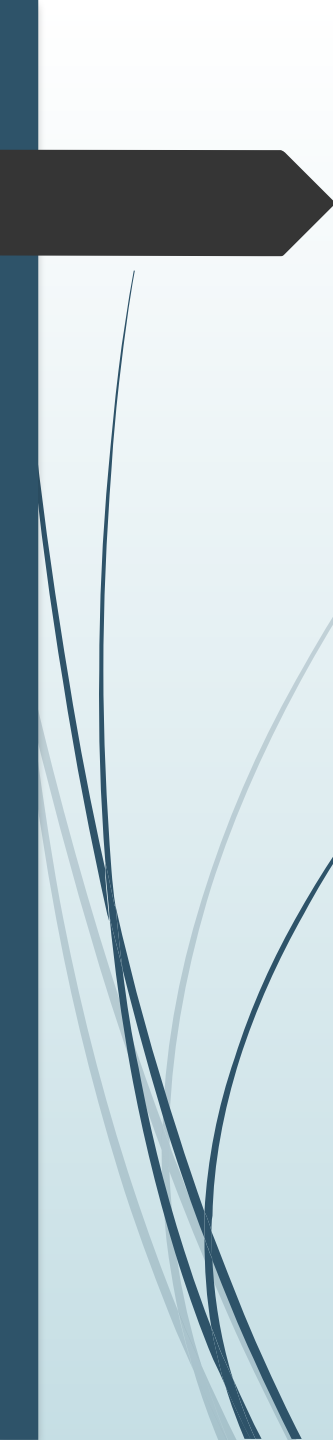


## II, VULNERABILITY AND PROTECTION OF INFORMATION SYSTEMS

### 1. **VULNERABILITY OF INFORMATION SYSTEMS**

The vulnerability of information systems refers to the potential weaknesses or flaws that exist in an organization's technology infrastructure, software, hardware, or processes that can be exploited by attackers to compromise the CIA of data or systems.

- ❖ Information systems can be vulnerable to various types of cyber attacks. These attacks can lead to financial losses, reputational damage, and legal consequences for the organization.

- 
- ❖ Vulnerabilities in information systems can arise from various sources, including coding errors, misconfigurations, outdated software and hardware, human error, and social engineering tactics used by attackers to exploit weaknesses in the organization's security culture.
  - ❖ To mitigate the risk of cyber attacks and protect against vulnerabilities in information systems, organizations should implement a comprehensive cybersecurity strategy that includes software updates , network segmentation, access controls, and employee training on cybersecurity best practices. Regular security audits and testing can help identify and address vulnerabilities before they can be exploited by attackers.



## 2. PROTECTION

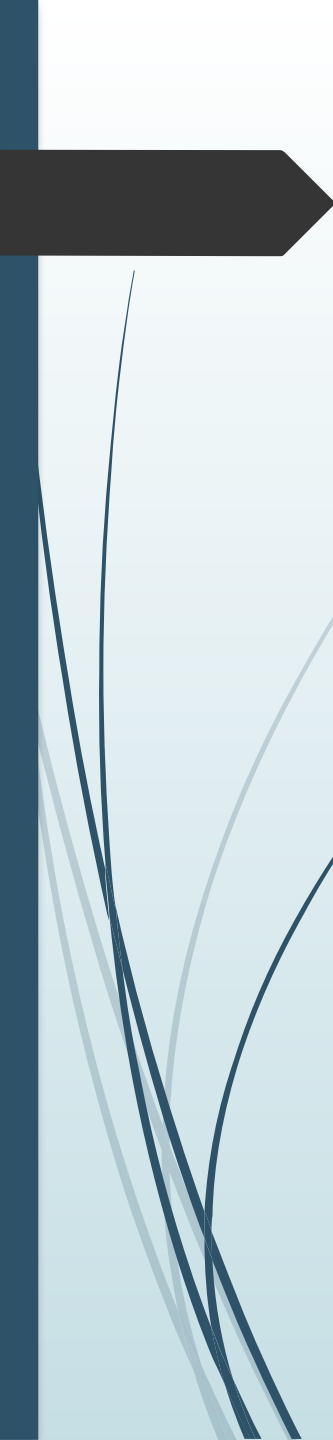
Protection of information systems refers to the process of implementing security measures to safeguard information systems against unauthorized access, use, disclosure, disruption, modification, or destruction.

Effective protection of information systems requires a comprehensive and multi-layered approach that addresses various potential threats and vulnerabilities.

To protect your information system through cybersecurity, here are some recommended measures:

- Use strong passwords and two-factor authentication to secure access to your systems and data.





Keep your software and operating systems up to date with the latest security patches and updates.

Regularly back up your data and store it securely offsite to protect against data loss and ransomware attacks.

Train employees on cybersecurity best practices and implement security policies and procedures to ensure compliance.

Implement firewalls, antivirus software, and intrusion detection/prevention systems to prevent unauthorized access and detect potential threats.



## III . HACKERS

- ▮ 1. The Ethical Hacker has excellent technical skills which they use for the benefit of the community, by discovering security vulnerabilities that they communicate and help resolve.
- ▮ 2. The Cracker simply wants to distinguish themselves from hacker groups with strong negative connotations . The Cracker is the purist of hacking. They are not attracted by profit.
- ▮ 3. The Wannabe (or Lamer) is usually a child or teenager who uses hacking techniques out of curiosity without fully understanding the consequences. There are many hacker toolkits available on the internet that the hacker can download for free to conduct their experiments.



## IV .VIRUSES

- A computer virus is "a malicious software program or piece of code that infects a computer and replicates itself by copying its code to other files or programs. There are different types of computer viruses, the most common ones are:
  - File viruses
  - Boot viruses
  - Macro viruses
  - Network viruses



# CONCLUSION

In conclusion, cybersecurity is a critical and ever-evolving field that plays a crucial role in protecting individuals, businesses, and governments from a wide range of cyber threats. With the increasing reliance on technology and the growth of the digital economy, it is more important than ever to have robust cybersecurity measures in place. By staying vigilant, implementing best practices, and investing in the latest security technologies, we can work towards a safer and more secure digital future for everyone