CHAPTER TWO: CYBERSECURITY

2.1 Concept of Cybersecurity

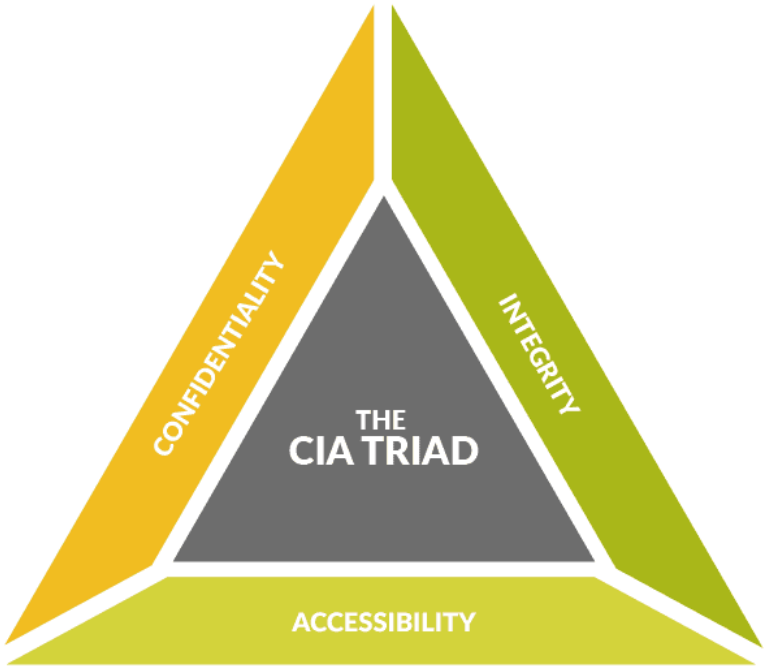
Imagine your school without a fence, doors left open, and no lockers for students. Anyone could walk in, steal property, or interfere with school activities. To prevent this, the school puts **security measures** in place.

Cybersecurity works in the same way—but in the **digital world**.

Cybersecurity is the practice of protecting **internet-connected systems** such as computers, smartphones, tablets, servers, and networks from **unauthorized access, damage, misuse, or theft**. It protects:

- **Hardware** – physical devices like computers and phones
- **Software** – operating systems and applications
- **Data** – personal files, photos, passwords, school records, and financial information

Cybersecurity is not just a single tool. It is a **combination of technologies, rules, and good user habits** that work together to keep digital information safe. Examples include using strong passwords, installing antivirus software, updating systems, and being careful online.



The CIA Triad: Goals of Cybersecurity

Cybersecurity is guided by three main principles, commonly known as the **CIA Triad**:

- **Confidentiality**

  Ensures that information is seen only by authorized people.

  Example: Your private emails, WhatsApp chats, and passwords should not be accessed by hackers or strangers.
- **Integrity**

  Ensures that information remains accurate, complete, and unaltered.

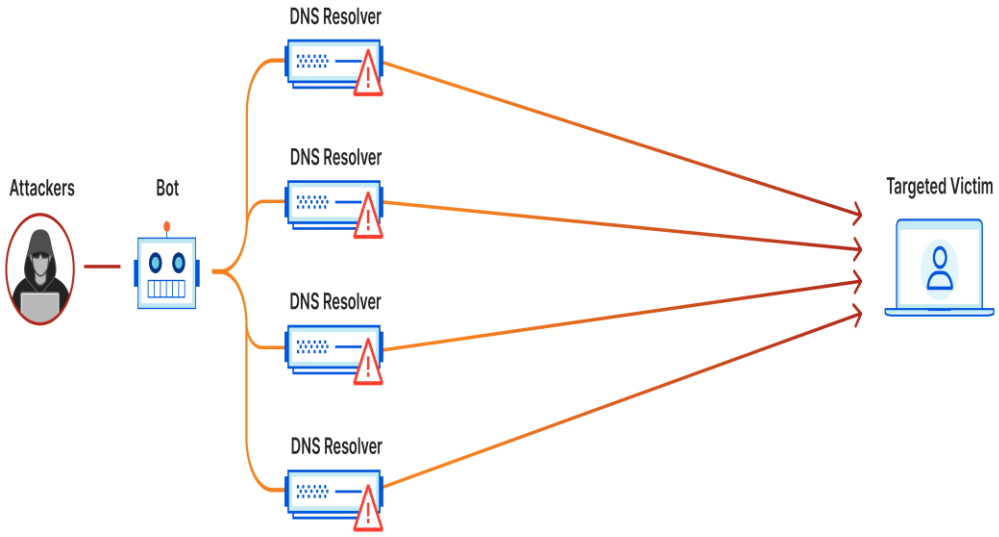
  Example: Exam results stored in a school database should not be changed illegally.
- **Availability**

  Ensures that systems and information are accessible when needed.

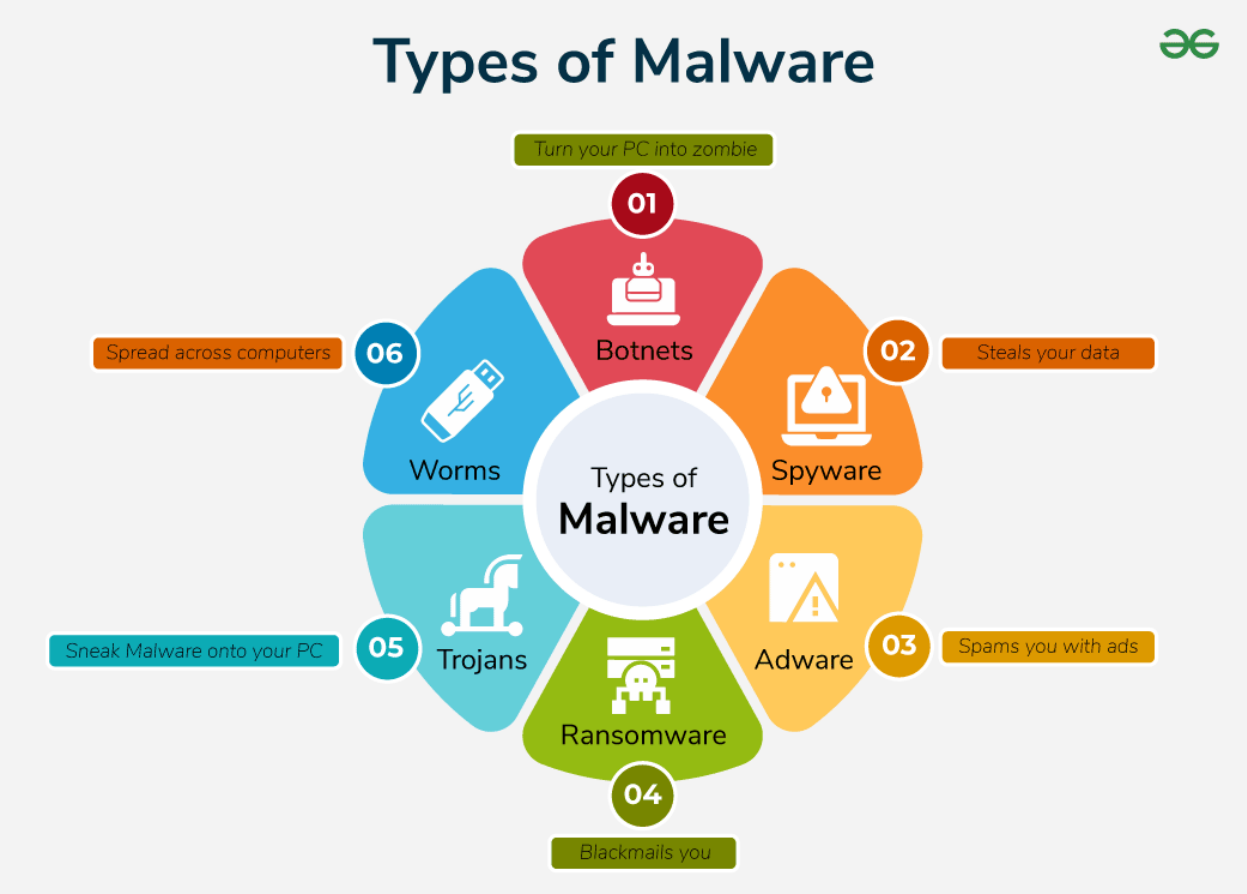
  Example: A school online registration system should be available to students and not disabled by attackers.

Cybersecurity is important for **everyone**, not just governments or big companies. Any person who uses a phone, computer, ATM card, or the Internet must understand and practice basic cybersecurity to stay safe online.

2.2 Cyber Threats and Attacks



A **cyber threat** is a possible danger that can exploit a weakness in a computer system. A **cyber attack** is the actual attempt to break into a system, steal data, or cause damage.



Malware (Malicious Software)

Malware is software intentionally designed to harm devices or gain unauthorized access.

- **Virus:**

  Attaches itself to legitimate files or programs and spreads when the file is opened, often damaging the system.
- **Worm:**

  Self-replicates and spreads across networks without needing a host file, consuming system resources.

- **Trojan Horse:**
  Appears as useful or harmless software (such as a free game or app) but secretly allows attackers access to the system.
- **Ransomware:**
  Encrypts or locks files and demands payment (ransom) to restore access. This can cause serious loss of data.

Phishing

Phishing is a **social engineering attack** where attackers send fake emails, SMS, or messages pretending to be from trusted organizations (banks, schools, mobile companies). The aim is to steal passwords, PINs, or money. These messages often create urgency or fear.

Denial-of-Service (DoS) Attack

A DoS attack overwhelms a website or server with too much traffic, making it unavailable to legitimate users. This affects **availability**, one of the CIA principles.

Man-in-the-Middle (MitM) Attack

Occurs when an attacker secretly intercepts communication between two users, often on **unsecured public Wi-Fi**. The attacker can read or alter the data being exchanged.

Password Attacks

These involve trying to guess or crack passwords using automated tools or common word lists. Weak passwords make such attacks easier.

Google

Gmail

Important: Your Password will expire in 1 day(s) Inbox x

MyUniversity 12:18 PM (50 minutes ago)

to me

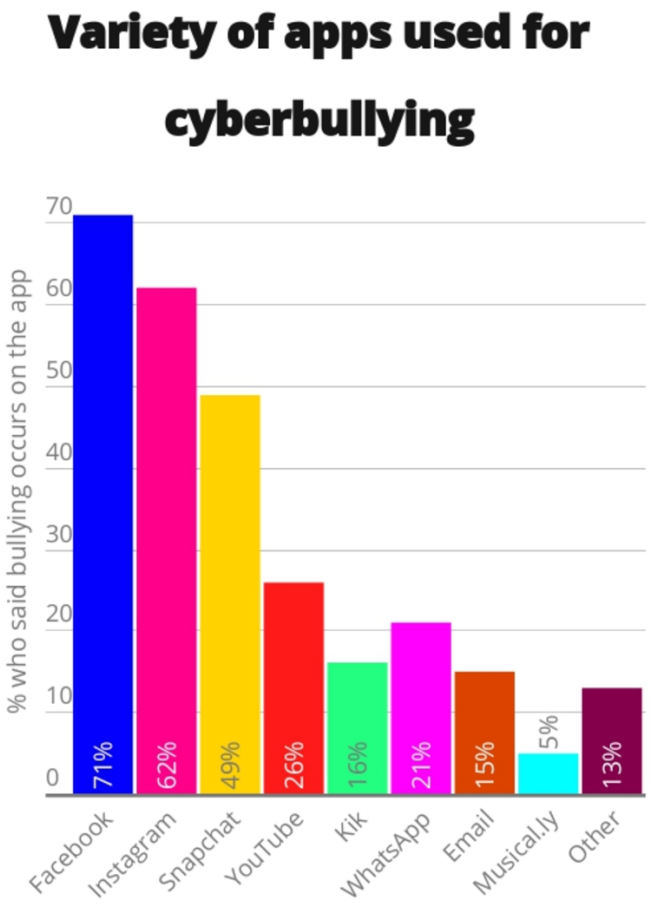
Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

MY UNIVERSITY

Thank you
MyUniversity Network Security Staff

2.3 Cybercrimes



A **cybercrime** is any illegal activity carried out using computers, mobile devices, or the Internet. Cybercrimes are real crimes with serious **legal, financial, and emotional consequences**.

- **Identity Theft:**

  Stealing personal information such as ID numbers or bank details to commit fraud or impersonation.
- **Cyberbullying:**

  Using digital platforms to insult, threaten, embarrass, or harass someone repeatedly. It can cause emotional distress and psychological harm.
- **Online Fraud:**

  Internet-based scams aimed at stealing money, such as fake online shops, fake job offers, or get-rich-quick schemes.
- **Software Piracy:**

  Illegal copying, sharing, or use of copyrighted software without permission. This violates the law and creators' rights.
- **Cyberstalking:**

  Repeated online harassment, monitoring, or threatening behavior that causes fear or distress to the victim.
- **Spreading Hate Speech or Incitement:**

  Using online platforms to promote violence, discrimination, or hatred against individuals or groups. This is unethical and illegal in many countries.

2.4 Ethical Issues and Related Principles

As technology becomes more powerful, **ethical questions** naturally arise about how it should be used. **Cybersecurity ethics** focuses on deciding what is **right or wrong behavior in the digital world**, especially when actions affect other people's data, privacy, and safety.

Privacy vs. Security

One of the biggest ethical debates in cybersecurity is the balance between **privacy** and **security**.

- **Privacy** means a person's online activities, messages, and personal data should not be monitored or accessed without consent.
- **Security** involves monitoring systems and communications to prevent crimes such as terrorism, fraud, or cyberattacks.

The ethical challenge is finding a **fair balance**:
Should governments or companies monitor online communications to catch criminals if it means invading everyone's privacy? Too much surveillance threatens freedom, while too little may allow cybercrime to grow.

Responsible Disclosure

Cybersecurity experts sometimes discover **vulnerabilities** (weaknesses) in software or systems.

- **Ethical behavior** requires responsible disclosure:
  The researcher should **privately inform the company or organization first**, giving them time to fix the problem.
- Publicly announcing the weakness or exploiting it for profit can put millions of users at risk.

Responsible disclosure protects users while still improving system security.

Hacking Ethics

Not all hackers are the same. Their **intentions** determine whether their actions are ethical or unethical:

- **White Hat Hackers:**
  Ethical hackers who are authorized to test systems and identify weaknesses so they can be fixed. They help improve cybersecurity and are often employed by companies.
- **Black Hat Hackers:**
  Criminal hackers who break into systems illegally to steal data, cause damage, or make money. Their actions are unethical and illegal.

- **Grey Hat Hackers:**

  Operate between the two. They may access systems without permission but do not intend to cause harm and may report vulnerabilities. However, accessing systems without permission is still ethically questionable.

Intellectual Property

Intellectual property refers to creations of the mind, such as software, music, movies, books, and digital art.

- Downloading pirated movies, cracked software, or unlicensed applications violates the creator's rights.
- Ethical Internet use requires **respecting ownership**, giving credit, and using legal versions of digital content.

2.5 Practices of Cybersecurity (Personal Cyber Hygiene)

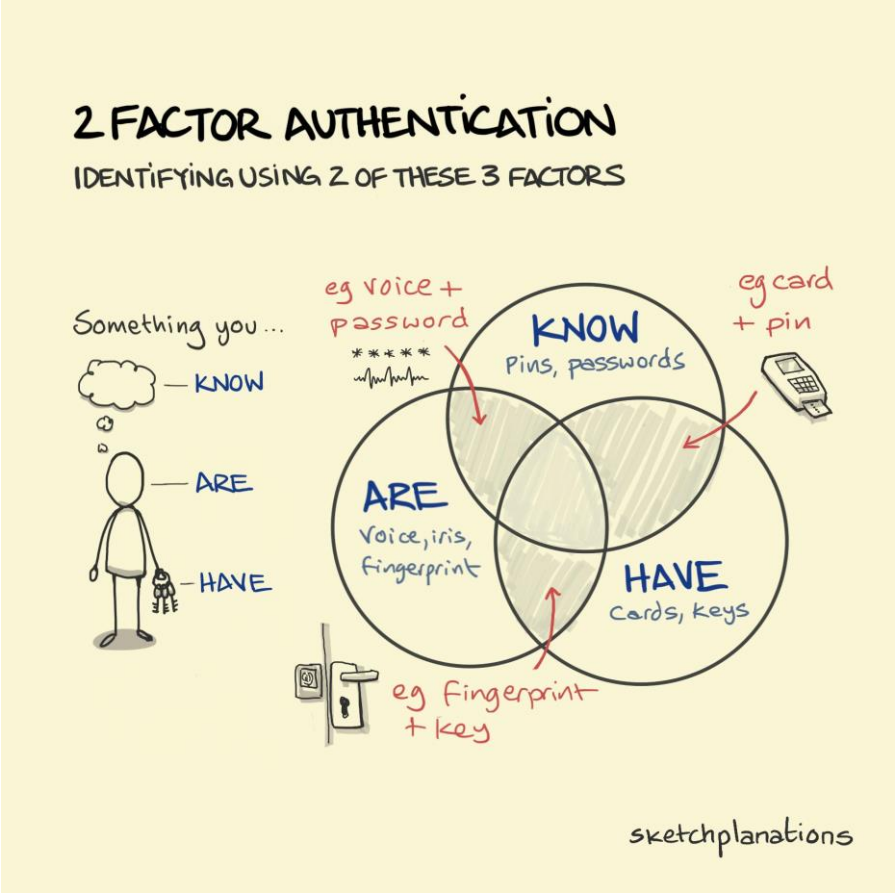
Just as personal hygiene protects your body, **cyber hygiene** protects your digital life. These are **daily habits** that every Internet user should practice to stay safe online.

1. Use Strong, Unique Passwords

A strong password combines **uppercase and lowercase letters, numbers, and symbols**. Avoid using names, birthdays, or simple words.
Each important account should have a **different password**. Password managers can help store and generate strong passwords securely.

2. Enable Two-Factor Authentication (2FA)

2FA adds an extra layer of protection. Even if someone knows your password, they still need a **second verification code** sent to your phone or generated by an app. This greatly reduces the risk of unauthorized access.



3. Keep Software Updated

Software updates are not just for new features—they often fix **security vulnerabilities**. Always update your operating system, browser, antivirus, and apps to stay protected against new threats.

4. Be Skeptical of Links and Attachments

Cybercriminals often use fake links and attachments to spread malware or steal information.
Do not click links or open attachments from unknown or suspicious sources. When in doubt, **verify first**.

5. Use Security Software

Install reputable **antivirus and anti-malware software** and keep it updated. This helps detect and remove malicious programs before they cause harm.

6. Back Up Your Data

Regularly back up important files to an **external hard drive or cloud storage**. If your device is damaged or attacked by ransomware, you can restore your data without losing it or paying criminals.

7. Be Careful on Public Wi-Fi

Public Wi-Fi networks are often unsecured and vulnerable to attacks. Avoid online banking or entering passwords on such networks. When necessary, use a **Virtual Private Network (VPN)** to encrypt your data.

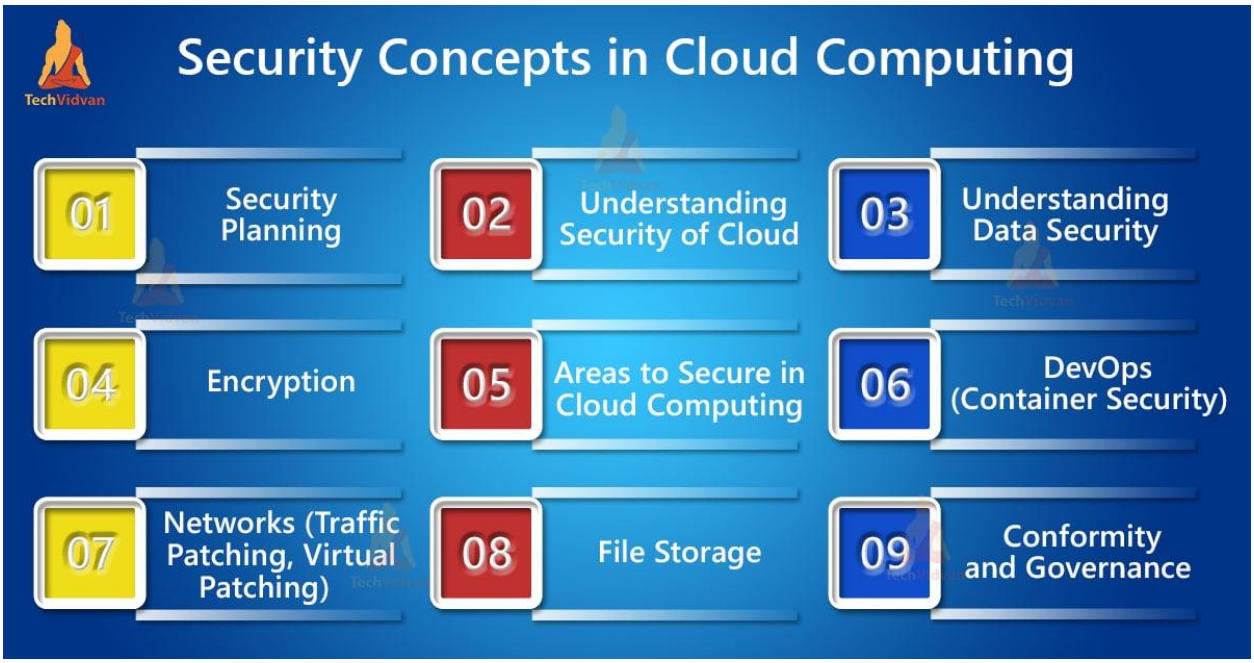
8. Think Before You Share

Information shared online can be misused for scams, identity theft, or social engineering. Always consider **who can see your posts** and how that information could be used.

2.6 Cloud Security

The **cloud** refers to storing data and running applications on remote servers accessed through the Internet, rather than on your personal computer or phone. Common cloud services include **Google Drive, iCloud, Microsoft OneDrive, Dropbox**, and cloud-based apps like Google Docs.

Cloud Security is the protection of **data, applications, and services** stored in these online systems. Because cloud data is stored on servers you do not physically own or control, security becomes a matter of **trust, responsibility, and good user practices**.

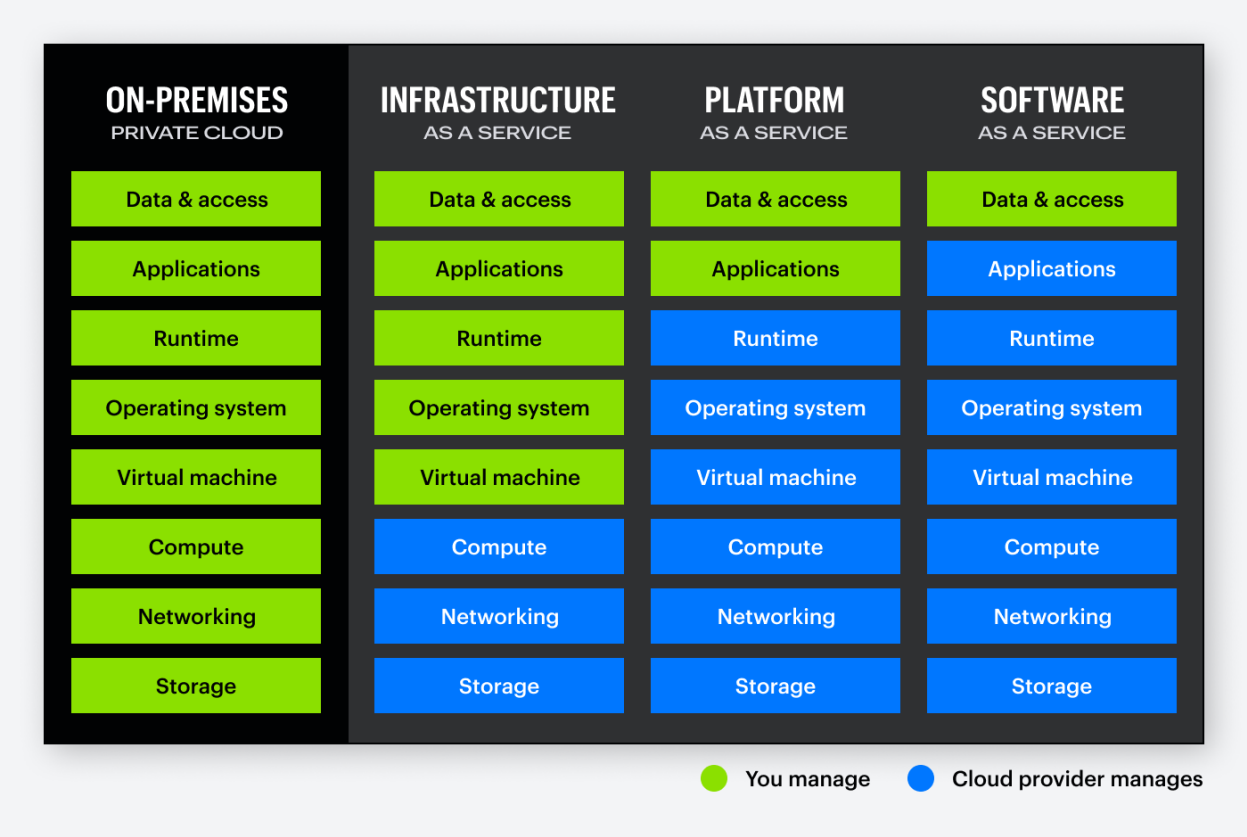


The Shared Responsibility Model

Cloud security is not handled by one party alone. It follows a **Shared Responsibility Model**, meaning both the cloud provider and the user have roles to play:

- **Cloud Provider's Responsibility**
  - Securing physical data centers
  - Protecting servers, storage systems, and network infrastructure
  - Ensuring reliable availability and protection against large-scale attacks
- **User's Responsibility**
  - Protecting account passwords
  - Controlling who can access files and folders
  - Managing privacy and sharing settings
  - Securing the data uploaded to the cloud

Even if the provider has strong security, weak user behavior (such as poor passwords) can still lead to data breaches.



Key Practices for Cloud Security

To keep your cloud data safe, users should follow these best practices:

- **Use strong passwords and enable Two-Factor Authentication (2FA)**
  This prevents unauthorized access even if a password is stolen.
- **Encrypt sensitive files before uploading**
  Encryption converts data into unreadable form, adding extra protection.
- **Manage sharing settings carefully**
  Avoid setting files to “public” unless necessary. Share only with specific people and review access regularly.
- **Understand privacy policies**
  Read and understand how your cloud provider stores, processes, and uses your data.

Cloud security works best when **technology and responsible behavior** are combined.

Chapter Summary

- Cybersecurity protects systems, networks, and data from digital attacks, guided by the **CIA Triad**: Confidentiality, Integrity, and Availability.
- Common cyber threats include **malware**, **phishing**, and **Denial-of-Service attacks**.
- **Cybercrimes** such as identity theft, fraud, and cyberbullying are illegal and harmful.

- Ethical principles guide responsible behavior, including **responsible disclosure**, ethical hacking, and respect for **intellectual property**.
- Personal cybersecurity practices (cyber hygiene) include **strong passwords**, **2FA**, **software updates**, and **regular data backups**.
- **Cloud security** follows a shared responsibility model where both the **provider** and the **user** must take action to protect data.

Revision Exercise 2

Section A: Multiple Choice (Choose the correct answer)

1. What are the three main goals of cybersecurity known as the CIA Triad?
   a) Control, Intelligence, Access
   b) Confidentiality, Integrity, Availability
   c) Coding, Internet, Analysis
   d) Cyber, Information, Attack
2. Which cyber attack involves locking a user's files and demanding payment to unlock them?
   a) Phishing
   b) Virus
   c) Ransomware
   d) Denial-of-Service
3. The illegal copying and distribution of a movie online is an example of:
   a) Cyberbullying
   b) Software Piracy

c) Ethical Hacking

d) Responsible Disclosure

4. What is the primary purpose of Two-Factor Authentication (2FA)?

   a) To make your computer faster

   b) To add an extra layer of security to your login process

   c) To back up your data automatically

   d) To block all emails from strangers

5. In cloud security, who is responsible for securing the physical data centers and servers?

   a) The user

   b) The cloud provider

   c) The government

   d) The Internet Service Provider

Short Answer Questions

1. Define the term **phishing** and give one real-world example of what a phishing message might ask you to do.
2. State **TWO differences** between a *White Hat* hacker and a *Black Hat* hacker.
3. Why is it important to keep your computer's operating system and software updated?
4. List **THREE essential elements** of a strong password.
5. What does the **Shared Responsibility Model** mean in the context of cloud security?

Structured Questions

1. Maria received an email that appeared to be from her bank. It said her account was locked and she must click a link to verify her details.

   a) Identify the type of cyber threat described.

   b) What are **TWO actions** Maria should take instead of clicking the link?

   c) Explain how this threat could lead to a serious cybercrime.

2. Your school wants to improve its cybersecurity awareness.

   a) Recommend **THREE good cyber hygiene practices** that all students should follow.

   b) Explain why **backing up data** is a critical practice, especially against ransomware attacks.

   c) Discuss **one ethical issue** related to a school monitoring students' activity on school-owned computers or networks.