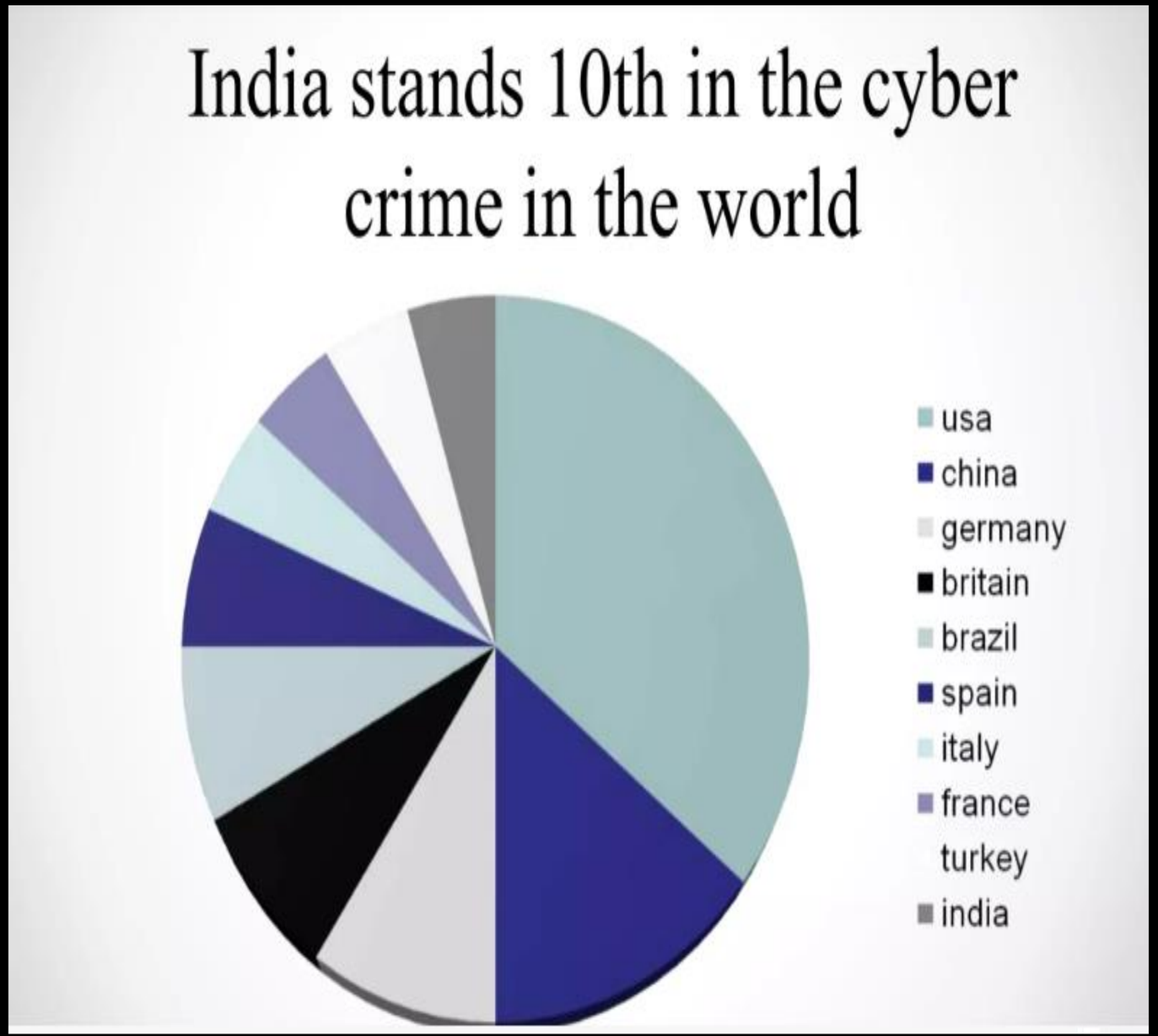
Introduction to cyber Security

Topics covered….

- Introduction to Information Security and its policies:
- CIA Triad-3 pillars of information security architecture,
- CIA components and its importance,
- Cyber security threats and best practices,
- Access controls and its types,
- Discretionary access control,
- Mandatory access control,
- Role based access control,
- Arbitrary based access control ,
- Active Reconnaissance, Types of Reconnaissance,
- Passive Reconnaissance,
- Types of Cyber Attack,
- Vulnerability Assessment and its features,
- Concept and types of Scanning Methodology, Penetration Tests



Introduction

- The term cyber security is used to refer to the security offered through on-line services to protect your online information.

- With an increasing amount of people getting connected to Internet, the security threats that cause massive harm are increasing also.

Cyber Security Template 2

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Meaning of the Word CYBER

- It is a combining form relating to information technology, the Internet, and virtual reality.

Need of cyber security

- Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses.

Major security problems

- Virus
- Hacker
- Malware
- Trojan horses
- Password cracking

Viruses and Worms

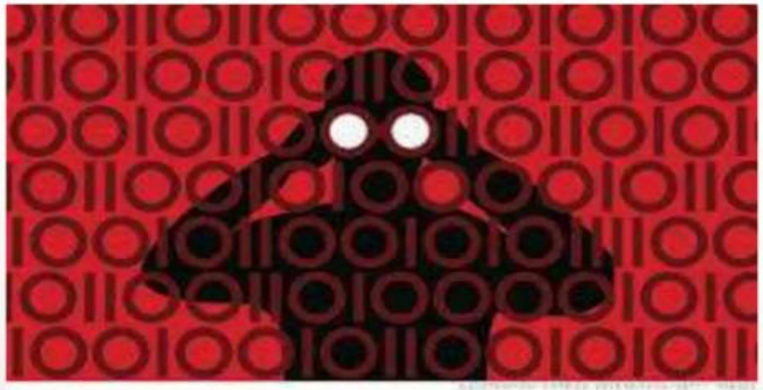
- A Virus is a "program that is loaded onto your computer without your knowledge and runs against your wishes

Solution

- Install a security suite that protects the computer against threats such as viruses and worms.

Hackers

- In common a hacker is a person who breaks into computers, usually by gaining access to administrative controls.



How To prevent hacking

- It may be impossible to prevent computer hacking, however effective security controls including strong passwords, and the use of firewalls can helps.

Malware

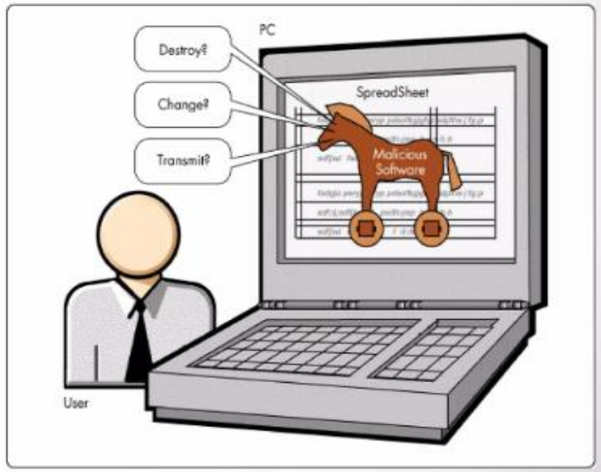
- The word "malware" comes from the term "MALicious softWARE."
- Malware is any software that infects and damages a computer system without the owner's knowledge or permission.

To Stop Malware

- Download an anti-malware program that also helps prevent infections.
- Activate Network Threat Protection, Firewall, Antivirus.

Trojan Horses

- Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system.
- These viruses are the most serious threats to computers



How to Avoid Trojans

- Security suites, such as Avast Internet Security, will prevent you from downloading Trojan Horses.

Password Cracking

- Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.

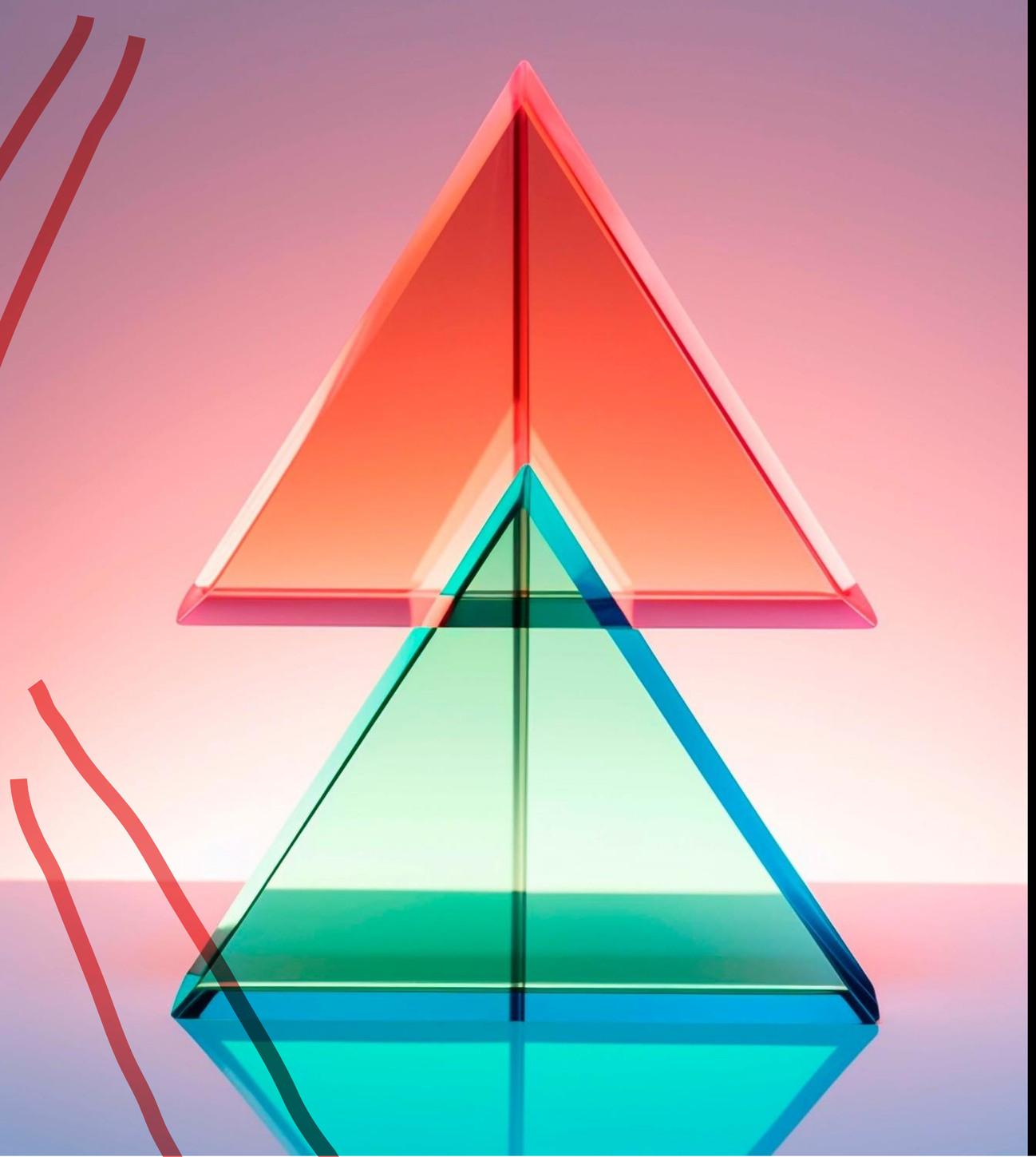
Securing Password

- Use always Strong password.
- Never use same password for two different sites.

Cyber Security Is Everyone's Responsibility

Introduction to Cyber Security

In today's digital world, cyber security is crucial for protecting sensitive information. This presentation will explore the CIA Triad—Confidentiality, Integrity, and Availability—and its vital role information security architecture.



What is the CIA Triad?

The CIA Triad is a foundational model in information security that guides policies for data protect. It consists of three core principles: Confidentiality, Integrity, and Availability, each essential for ensuring a secure environment.

Confidentiality Explained

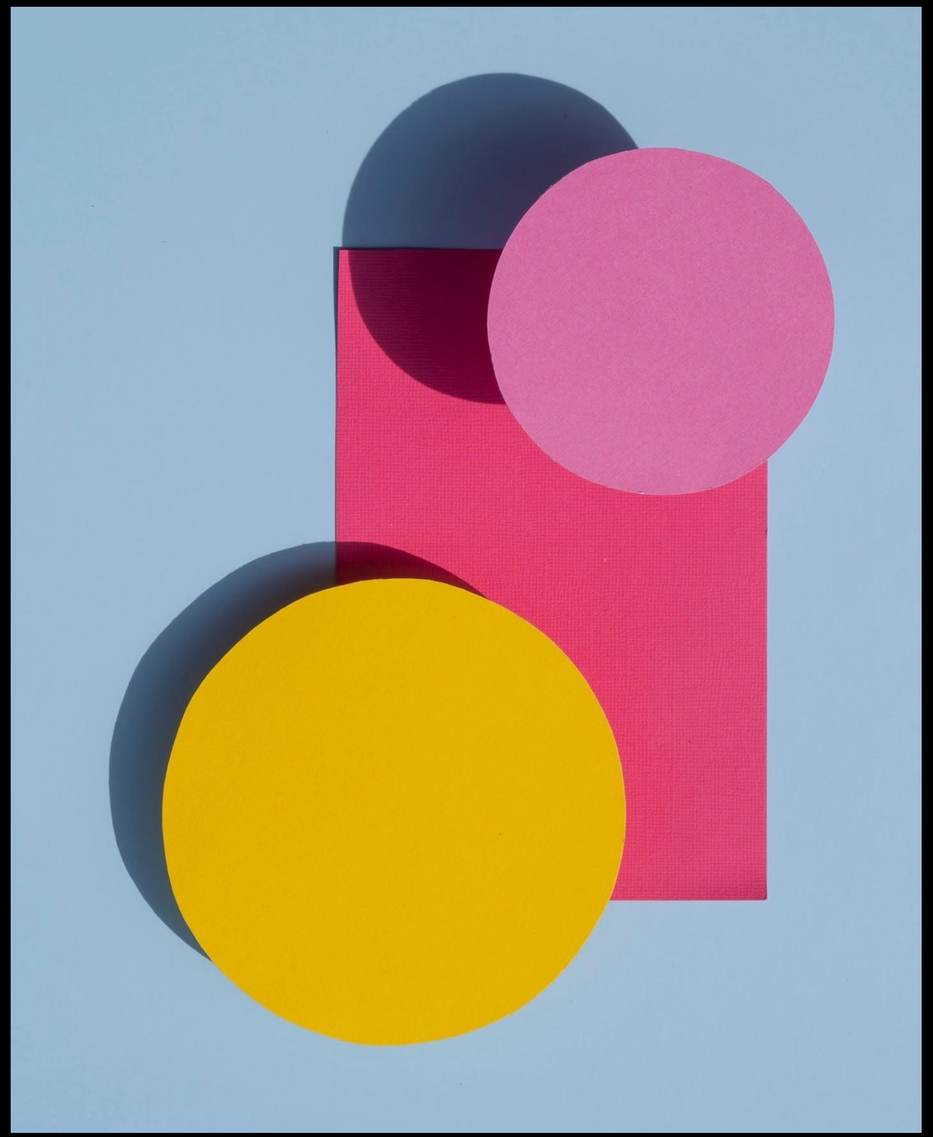
Confidentiality ensures that sensitive information is accessed only by authorized users. It involve measures like encryption, access controls, and authentication to protect data from unauthorized access.

Integrity in Cyber Security

Integrity refers to the accuracy and reliability of data. It ensures that information is not altered or tampered with during storage or transmission, using techniques like hashing and checksums.

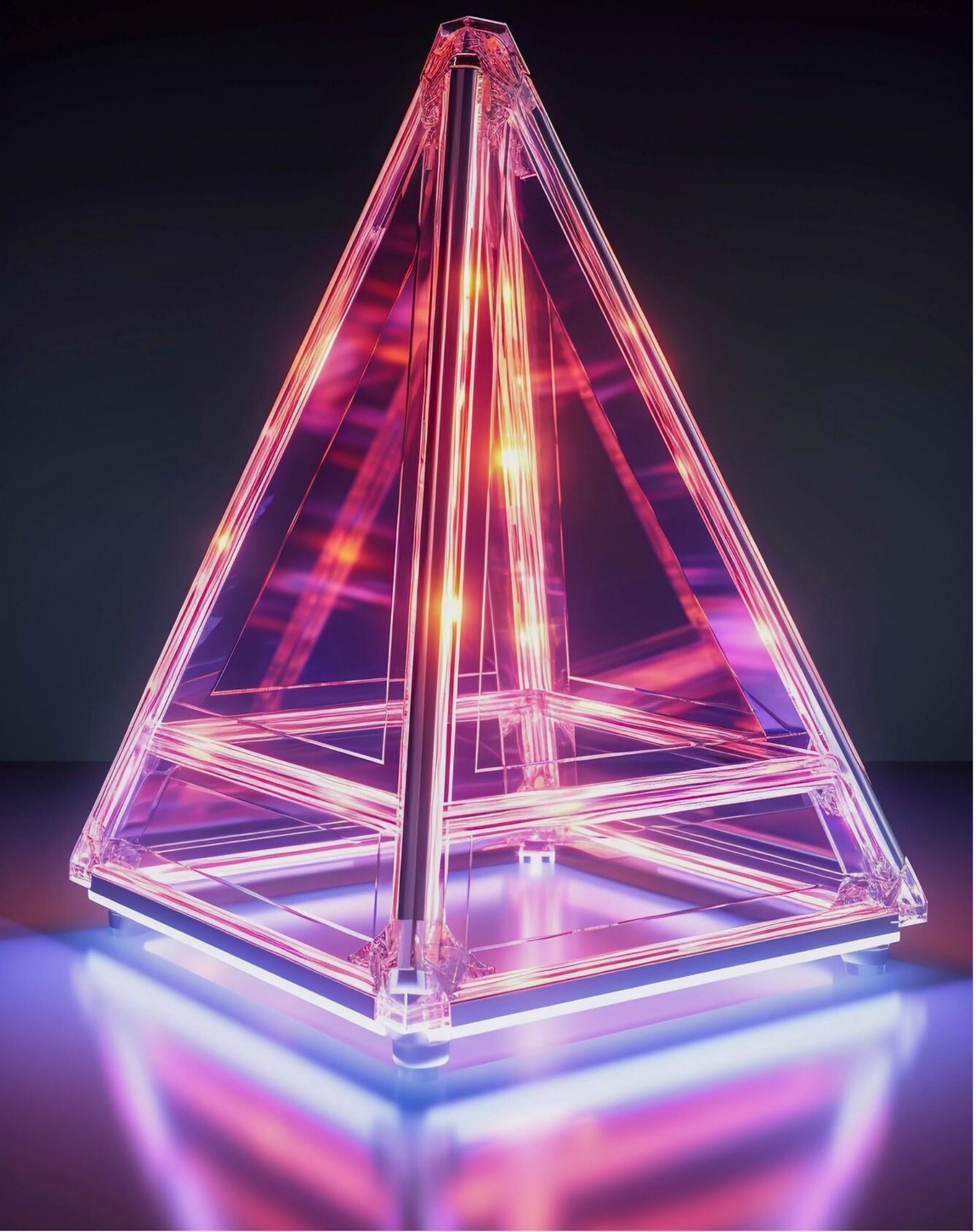
Understanding Availability

Availability ensures that information and resources are accessible when needed. This involves maintaining systems and networks to prevent downtime and using redundancy and backups to protect against failures.



The Interconnection of CIA

The principles of the CIA Triad are interconnected; compromising one can affect the others. For example, if confidentiality is breached, it may lead to a loss of integrity and availability.



Role in Information Security Architecture

The CIA Triad is integral to designing an effective information security architecture. It helps organizations assess risks and implement controls that align with their security objectives and compliance requirements.

Threats to the CIA Triad

Various threats can jeopardize the CIA Triad. These include malware, phishing, and insider attacks. Understanding these threats is essential for developing effective security strategies and defenses.

Best Practices for CIA Implementation

To effectively implement the CIA Triad, organizations should adopt best practices such as regular security audits, employee training, and robust incident response plans to mitigate potential risks.

Case Studies in Cyber Security

Examining real-world case studies highlights the importance of the CIA Triad. Successful organizations prioritize these principles to safeguard their data and maintain customer trust.

Future of Cyber Security

As technology evolves, so do the challenges in cyber security. The CIA Triad will continue to be a guiding framework, adapting to new threats and innovations in information security architecture.

What is Access Control?

Access control refers to the methods and policies that restrict access to resources in a computing environment. It ensures that only authorized users can view or modify data. Understanding its importance is crucial to maintaining a secure system against potential threats.

Types of Access Control

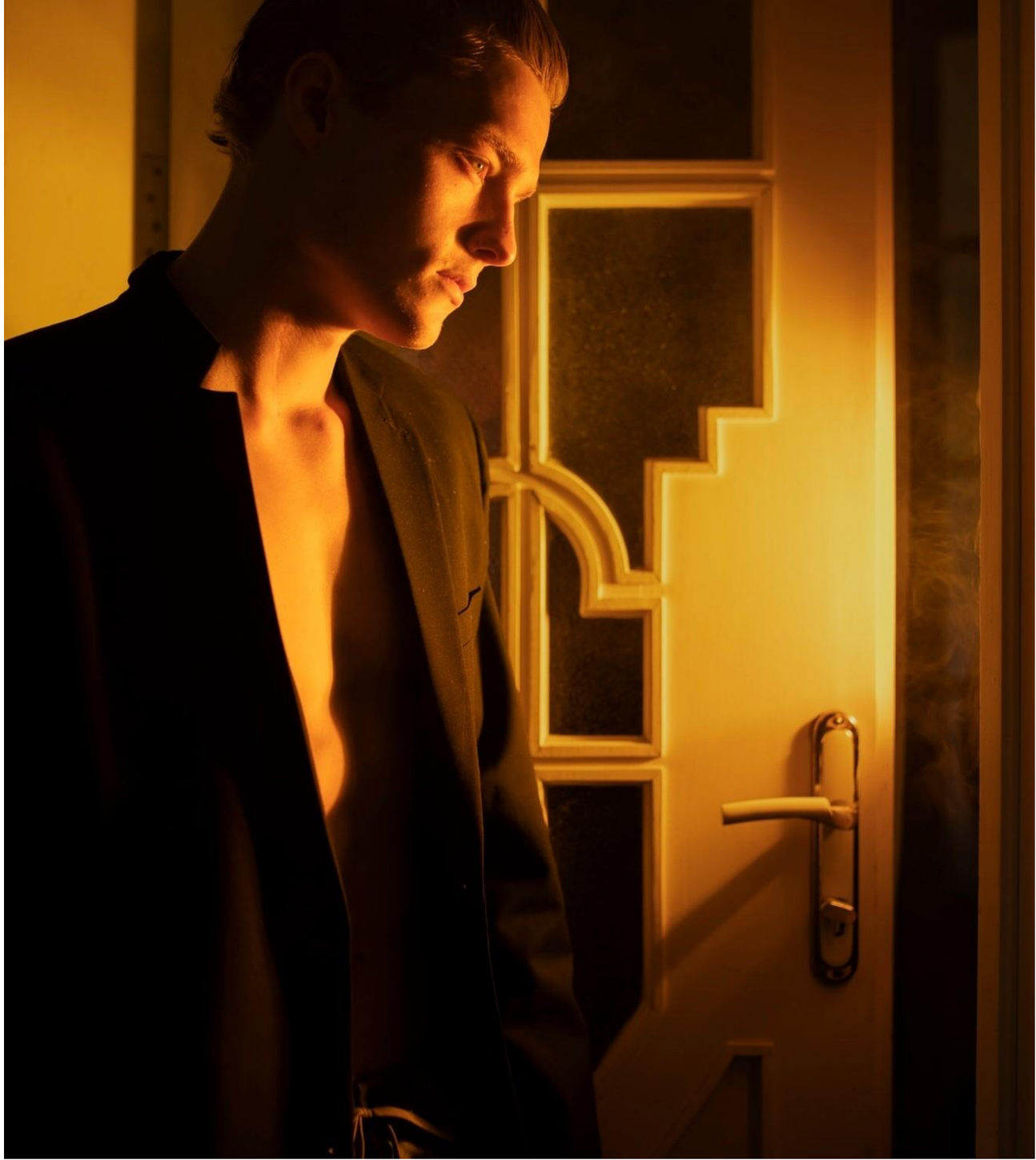
There are several types of access control, including discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC). Each type has its unique features and is suited for different organizational needs and security requirements.

Discretionary Access Control (DAC)

In DAC, owners of resources have the discretion to make decisions about who can access their resources. This flexibility can lead to vulnerabilities if not managed properly, as it relies heavily on users' judgment and compliance with security policies.

Mandatory Access Control (MAC)

MAC enforces strict policies determined by a central authority. Users cannot change access permissions, which enhances security but can reduce flexibility. This approach is often used in environments where data confidentiality is paramount, such as government systems.



Role-Based Access Control (RBAC)

In RBAC, access rights are assigned based on user roles within an organization. This method simplifies management and enhances security by ensuring users only have access to information necessary for their job functions, minimizing the risk of data breaches.

Best Practices for Access Control

Implementing best practices for access control includes regularly reviewing permissions, using multi-factor authentication, and training employees on security awareness. These practices help mitigate risks and strengthen the overall security posture of an organization against cyber threats.

Understanding Reconnaissance

Reconnaissance is the initial phase of cybersecurity assessments. It involves gathering information about a target system to identify potential vulnerabilities. This step is critical as it lays the groundwork for more in-depth testing and analysis.

Types of Reconnaissance

There are two main types of reconnaissance: Active and Passive reconnaissance involves gathering information without direct interaction, while active reconnaissance includes direct engagement with the target system to collect data. Each method has its advantages and risks.

Types of Cyber Attacks:

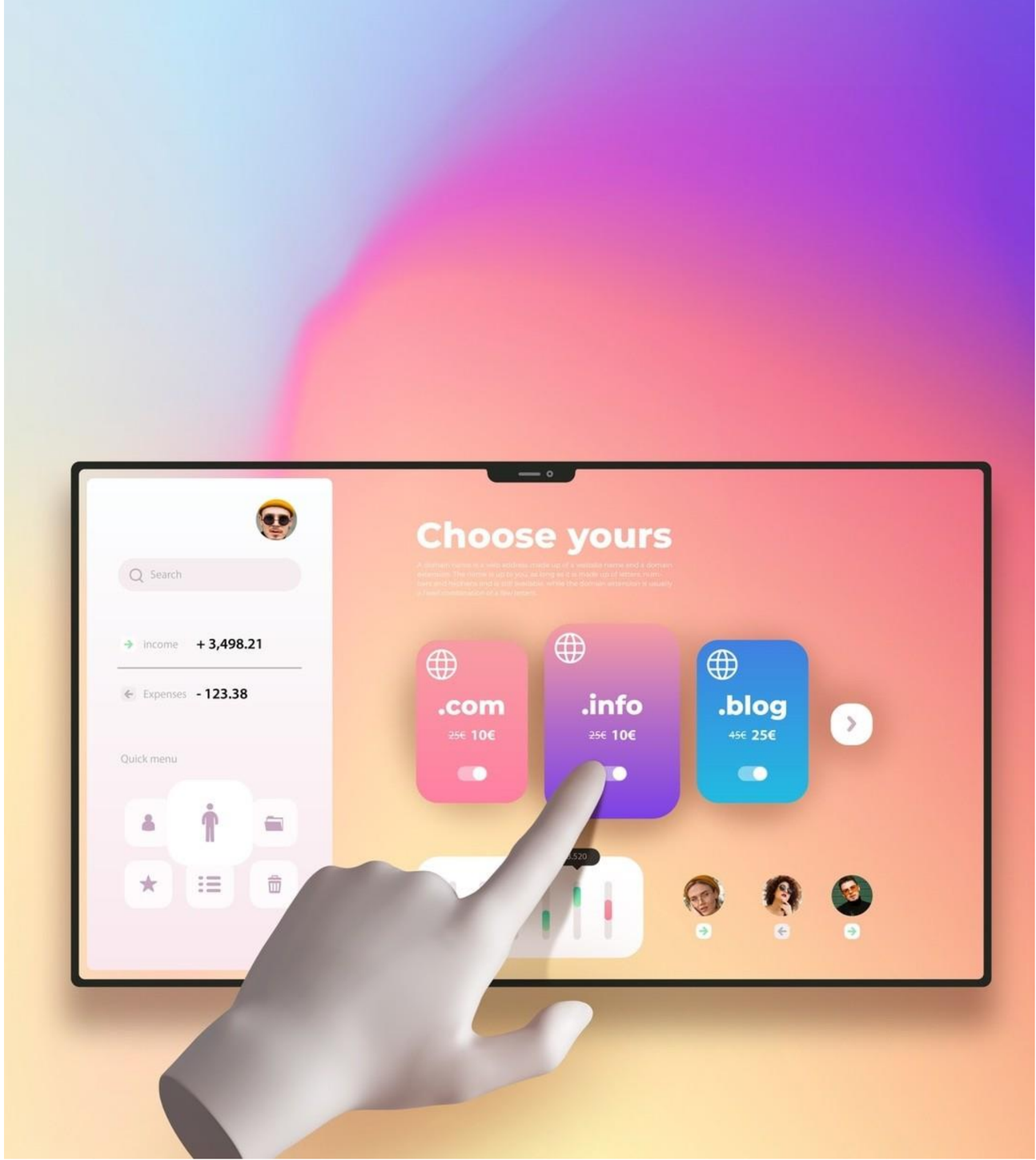
1. **Ransomware** is a type of malware that prevents users from accessing their files, systems, or networks, and demands payment to regain access. Ransomware attacks can be costly and disruptive, and can lead to loss of critical data
2. **A botnet** attack is a cyberattack that uses a botnet, a network of infected devices, to carry out a variety of malicious actions
3. **Social engineering** is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
4. **Cryptohijacking** is the unauthorized use of a computer or device's processing power to mine cryptocurrencies, often without the owner's consent or knowledge.
5. **Phishing attacks** are a form of social engineering, and are often carried out by impersonating a trustworthy entity in an electronic communication

Importance of Vulnerability Assessment

A **vulnerability assessment** is essential for identifying security weaknesses in systems. It involves scanning and analyzing systems to find flaws that could be exploited by attackers. Regular assessments help organizations prioritize remediation efforts effectively.

Vulnerability Assessment Tools

Various tools are available for conducting vulnerability assessments, such as Nessus, Qualys, and OpenVAS. These tools automate the scanning process and provide detailed reports, enabling teams to address vulnerabilities efficiently.



What is Penetration Testing?

Penetration Testing simulates real-world attacks to evaluate the security of systems. This proactive approach helps organizations understand their security posture and identify weaknesses that could be exploited by malicious actors.

Phases of Penetration

Penetration testing typically involves several phases: planning, scanning, gaining access, maintaining access, and reporting. Each phase is vital to ensure a thorough assessment of security measures and the effectiveness of defenses.

Benefits of Penetration Testing

Conducting regular penetration tests provides numerous benefits, including identifying critical vulnerabilities, enhancing incident response strategies, and ensuring compliance with industry regulations. These tests are essential for a robust cybersecurity framework.

Integrating Cybersecurity Practices

To effectively protect against cyber threats, organizations must integrate **reconnaissance**, **vulnerability assessments**, and **penetration testing** into their security strategies. This holistic approach ensures comprehensive coverage and proactive defense mechanisms.

Challenges in Cybersecurity

Despite advancements, cybersecurity faces significant challenges, including evolving threats, resource limitations, and the need for continuous training. Organizations must stay vigilant and adapt their strategies to counter these ongoing challenges.

Future of Cybersecurity

The future of cybersecurity will likely involve increased use of AI and machine learning to enhance threat detection and response. Organizations must be prepared to adopt new technologies and methodologies to stay ahead of cybercriminals.