Cyber Security

"Protection of computer systems and data from digital threats."

Introduction

Cybersecurity is the set of measures and practices designed to safeguard computer systems, networks, and information from unauthorized access, attacks, and potential risks in the digital realm.

Four Types Of Cyber Security

Network Security

Endpoint Security

Data Security

Four Types Of Cyber Security

Web Security

Network Security

Network security involves safeguarding networks from unauthorized access and threats.

Firewall Implementation

Network Monitoring

Data Security

Measures to protect data from unauthorized access, loss, or theft

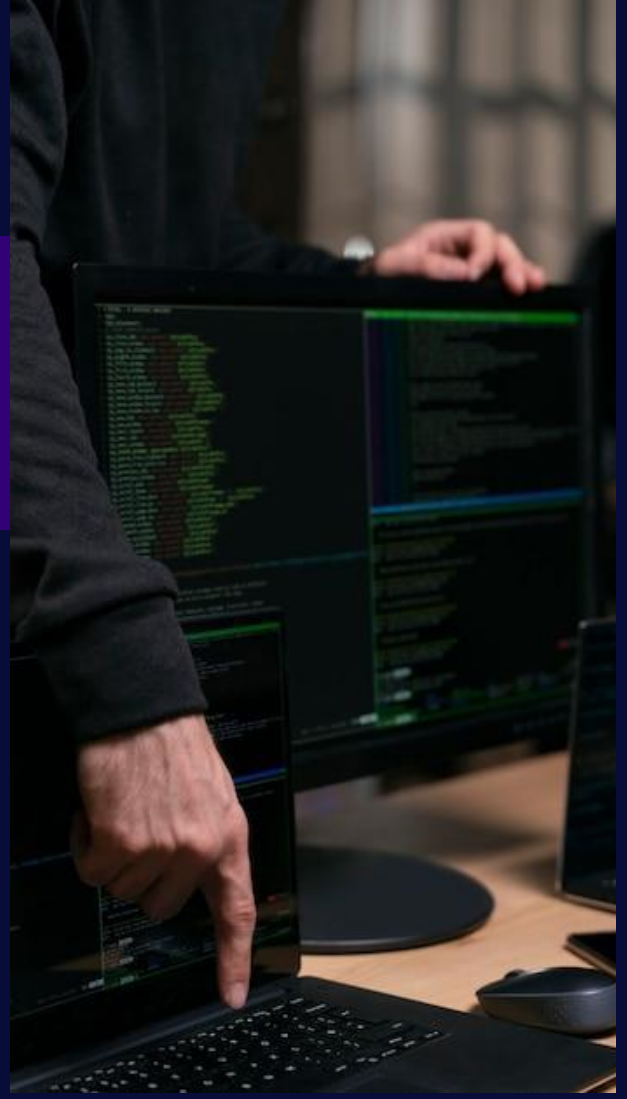
01 Encryption

02 Data Classification

03 Access Controls

Web Security

Web security is concerned with protecting websites and web applications from vulnerabilities, attacks, and unauthorized access. It involves measures such as secure coding, encryption, authentication, and secure web server configurations.



Mobile Security

Securing mobile devices and protecting against mobile-specific threats.

01

Mobile Device Management (MDM)

02

Secure App Development

03

Data Encryption On Mobile Devices

Importance of cybersecurity in today's digital world

01 Data Protection

Cybersecurity is of paramount importance in today’s digital landscape to safeguard sensitive data from unauthorized access, theft, and misuse. Organizations and individuals must prioritize robust security measures to protect personal and financial information, intellectual property, and confidential communications.

02 Privacy Preservation

It plays a critical role in preserving individual privacy. With growing concerns about data privacy, cybersecurity measures ensure that personal information remains secure and is not exploited by malicious entities for harmful purposes such as identity theft or fraud.

Importance of cybersecurity in today's digital world

03 Business Continuity

Ensuring the uninterrupted operation of businesses and critical infrastructure is significantly dependent on effective cybersecurity practices. Cyber attacks can disrupt operations, leading to financial loss, reputational damage, and compromised services, making cybersecurity an essential aspect of business continuity planning.

04 National Security

Cybersecurity is not limited to individual or corporate concerns; it also has far-reaching implications for national security. Protection against cyber threats is crucial in safeguarding critical infrastructure, government institutions, and defense systems from potential cyber warfare and espionage.

Common Cybersecurity Threats and Attacks

01 Phishing

02 Ransomeware

03 Malware

Overview of Cybersecurity Best Practices

Use of VPNs

Virtual Private Networks (VPNs) are a crucial tool for maintaining cybersecurity, especially when accessing sensitive information over public Wi-Fi networks. They encrypt data transmitted between devices and remote servers, ensuring a secure and private connection. VPNs also enable users to bypass geographical restrictions and enhance anonymity online.

Overview of Cybersecurity Best Practices

Implementing Multi-Factor Authentication (MFA)

Multi-factor authentication adds an extra layer of security by requiring users to provide multiple forms of verification before accessing their accounts. Typically, this involves a combination of something the user knows (like a password or PIN) and something they have (like a fingerprint or security token), making it significantly harder for unauthorized individuals to gain access.

Overview of Cybersecurity Best Practices

Regular Security Audits and Risk Assessments

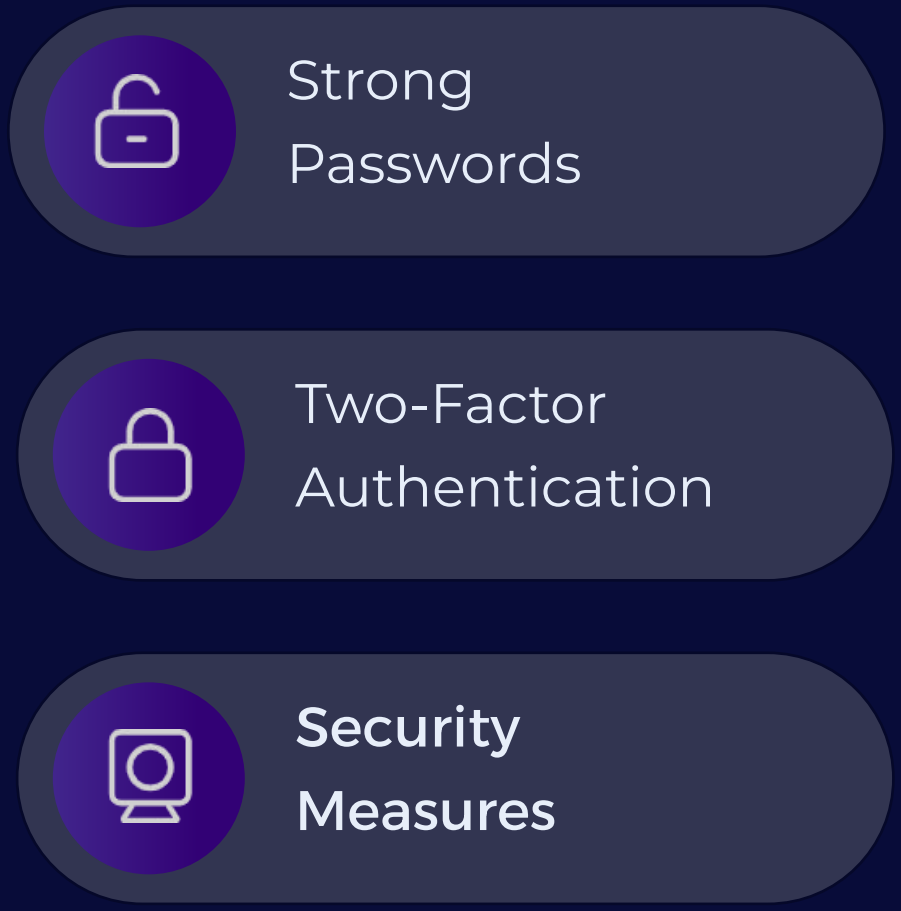
Conducting regular security audits and risk assessments helps identify potential vulnerabilities and threats within an organization's network and systems. By analyzing and addressing weak points proactively, companies can prevent unauthorized access, data breaches, and other cybersecurity incidents.

Overview of Cybersecurity Best Practices

Establishing Incident Response Plans

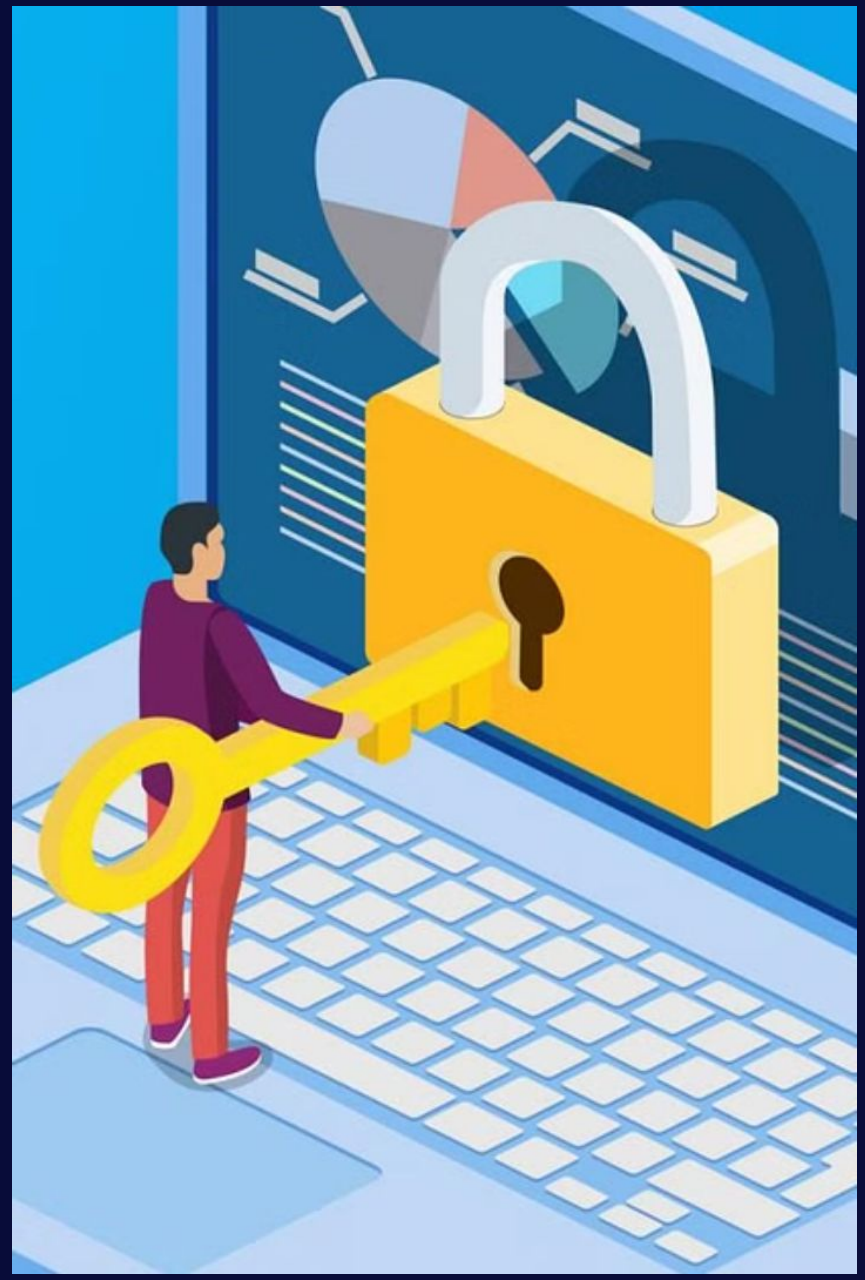
Having a well-defined incident response plan is essential for swiftly and effectively addressing security breaches or cyber-attacks. This plan outlines the specific steps to be taken in the event of a security incident, including communication protocols, data recovery procedures, and necessary legal or regulatory reporting.

Importance of Strong Passwords and Two-Factor Authentication



Role of Encryption in Protecting Data

Encryption plays a critical role in safeguarding sensitive data from unauthorized access and nefarious activities. By converting plain text into ciphertext using complex algorithms and keys, encryption ensures that even if data is intercepted, it remains indecipherable to unauthorized entities. This process secures sensitive information such as personal details, financial records, and confidential communications.



Importance of Regular Software Updates and Patches

1

Identifying Vulnerabilities

Regular software updates and patches play a critical role in identifying and addressing vulnerabilities in software applications and operating systems. These updates often include bug fixes and security patches that help secure systems from newly discovered vulnerabilities.

2

Preventing Exploitation

By keeping software up to date with the latest patches, organizations can prevent potential exploitation of known vulnerabilities. Attackers often target outdated software with known security weaknesses, making regular updates essential to thwart their efforts.

3

Mitigating Security Risks

Failure to install software updates and patches can lead to significant security risks, including data breaches, malware infections, and unauthorized access. Regular updates help mitigate these risks by keeping systems resilient against evolving cyber threats.

Employee Awareness And Training

Employee awareness and training focuses on educating and empowering employees to recognize and mitigate cybersecurity risks, promoting a culture of security and responsible online behavior within an organization.

Emerging Trends In Cybersecurity

Exploration of current and future trends in cybersecurity

01 Artificial Intelligence In Cybersecurity

02 Internet Of Things (IOT) Security

Conclusion

In an increasingly connected world, cyber security is paramount. Protecting our systems, networks, and data is essential to safeguarding privacy, preventing cyber attacks, and ensuring trust and stability in the digital landscape.

THANK YOU!

PRESENTORS:

ATAR, RITCHIE JR. M.
CORALES, JAYVIE N.
MENDIOLA, MARY JEAN S.
PARA-ASE, DIANNE B.