horizontal line

Project report on Encryption

Techniques and Approaches



**By: Sukhvir Sahota**

TABLE OF CONTENTS

[**EXECUTIVE SUMMARY 1**](#_stnvg3ujrs8x)

[**INTRODUCTION 2**](#_u12cp96z9hxu)

[Objectives of This Report 2](#_2fs1dyq171yk)

[**UNDERSTANDING THREATS 2**](#_jqvvu7dd0srh)

[**TECHNIQUES AND APPROACHES 6**](#_sn4s8z1o392l)

[Strong password 6](#_q1aitfqt4q5v)

[Role in Company Security 7](#_9avznf58fdwc)

[Characteristics of a Strong Password 8](#_v3sw1dctxlbh)

[Implementation Strategy 8](#_umqk8mxf7ilz)

[Benefits of Strong Passwords 8](#_y4nest48qx9f)

[Password expiration policy 9](#_4qim041coubw)

[Benefits of password expiration policies: 9](#_syc4uijwbzgd)

[Multi-Factor Authentication (MFA) 10](#_d8r1wzzepdvz)

[Types of Multi-Factor Authentication 10](#_wkmzvmt6htif)

[Benefits of MFA 11](#_ialqj6mar6bv)

[Secure Email with Personal Certificate 11](#_l8ghtj5kib9o)

[Benefits of Secure Email with Personal Certificates 12](#_xh100hllwtul)

[VPN IPSec on the laptops 13](#_nbcrawmcov7i)

[Components of IPSec 13](#_inudn19r1y1i)

[How IPSec VPN Works 14](#_s6ztex7szaqb)

[Benefits of Secure VPN IPSec on the laptops 14](#_7vjv2nrjanp)

[Encrypting hard drives and portable storage devices 15](#_ftuqvfz6vtpu)

[Encryption tools 15](#_cr29sahsj6lt)

[Benefits of Encrypting hard drives and portable storage devices 15](#_fijhkvh46zgu)

[**SUGGESTED BEST APPROACHES 16**](#_jjehepxgmauk)

[**CIA TRAID IMPACT 17**](#_3xti9i4zrmi9)

[**CONCLUSION 18**](#_xjjt7tvi8gjb)

[**APPENDIX : Definitions 18**](#_dvhcbo2h6vft)

[**REFERENCES 22**](#_203oo9wae8k)

# 

# EXECUTIVE SUMMARY

In today's digitally interconnected world, cyber security is paramount for safeguarding sensitive information, maintaining trust, and ensuring business continuity. This report provides an overview of fundamental security practices aimed at enhancing our company's cyber security posture. Various cyber threats pose risks to organizations, including phishing, malware, ransomware, DDoS attacks, MITM attacks, insider threats, and brute-force attacks. These threats can lead to data breaches, financial losses, and reputational damage.

To combat cyber threats effectively, a multi-layered defense strategy is essential. This includes practices such as implementing strong passwords, enforcing password expiration policies, using MFA, securing email with personal certificates, employing VPN IPSec for remote access, and encrypting hard drives and portable storage devices. Each security practice contributes to enhancing the organization's security posture by addressing different aspects of the CIA triad: confidentiality, integrity, and availability.

We propose several essential practices to achieve this goal. First, strong passwords with complex characters and minimum lengths will be enforced. Additionally, hashing algorithms like bcrypt, Argon2, or scrypt will be used for secure password storage. Multi-factor authentication (MFA) will add another layer of security by requiring additional verification steps beyond passwords. For secure email communication, we recommend using S/MIME or PGP/GPG to encrypt email content and validate message integrity with digital signatures. To ensure secure remote access, VPN IPSec with AES encryption will be implemented on laptops. Finally, data at rest on hard drives and portable devices will be protected using full-disk encryption (BitLocker, FileVault, LUKS) or hardware-based encryption.

Implementing these measures will significantly enhance our overall security posture by reducing the risk of data breaches, unauthorized access, and data manipulation. Additionally, this plan ensures compliance with relevant industry regulations and data privacy standards. By fostering a culture of cybersecurity awareness and responsible practices, we can achieve the highest standards of data protection for our organization.

# INTRODUCTION

Cyber security is crucial for safeguarding our digital assets in today's interconnected world. With increasing cyber threats, companies must implement robust security measures to protect sensitive information, maintain customer trust, and ensure business continuity. As cyber threats evolve, so must our security strategies.

## Objectives of This Report

This report aims to provide a comprehensive overview of fundamental security practices that can significantly enhance our company's cyber security. The focus will be on:

* Implementing strong passwords
* Enforcing a password expiration policy
* Deploying multi-factor authentication (MFA)
* Securing email communications
* Using VPN IPSec for secure remote access
* Encrypting hard drives and portable storage devices

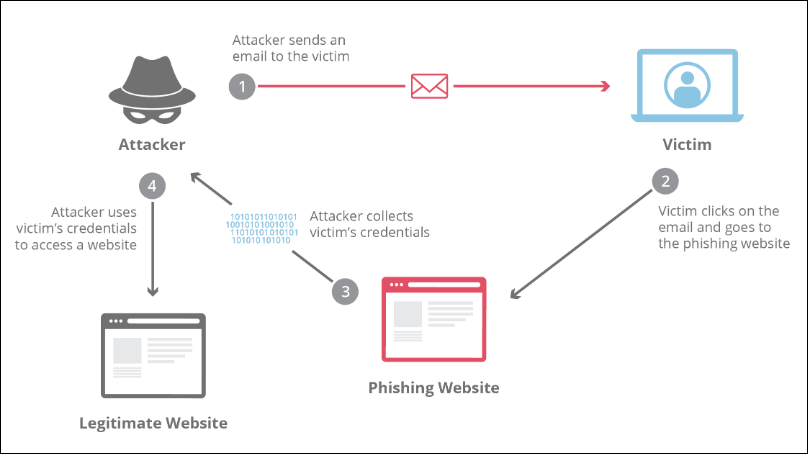
# 

# UNDERSTANDING THREATS

The digital age has brought tremendous benefits, but it has also introduced new threats and vulnerabilities. Cybercriminals use various tactics to gain unauthorized access to sensitive information. These tactics include phishing emails, malware downloads, and exploiting software vulnerabilities. A successful attack can lead to data breaches, financial losses, and reputational damage. The most common cyber threats are:

### Phishing

[“Phishing”](https://www.cloudflare.com/learning/access-management/phishing-attack/) refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information, or other important data to utilize or sell the stolen information.



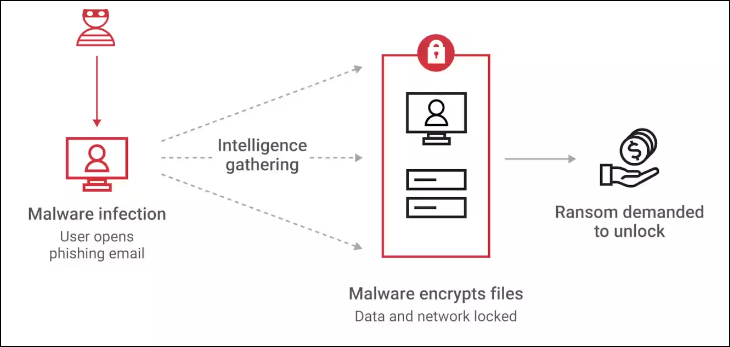
Phishing involves tricking employees into providing sensitive information by masquerading as a trustworthy entity, typically via email. These attacks can lead to credential theft, financial loss, and unauthorized access to company systems.

### Malware

[Malware](https://www.fortinet.com/resources/cyberglossary/malware) is software designed to infiltrate, damage, or disable computer systems. It includes viruses, worms, trojans, and spyware. Malware can steal sensitive information, corrupt files, and provide unauthorized access to attackers.

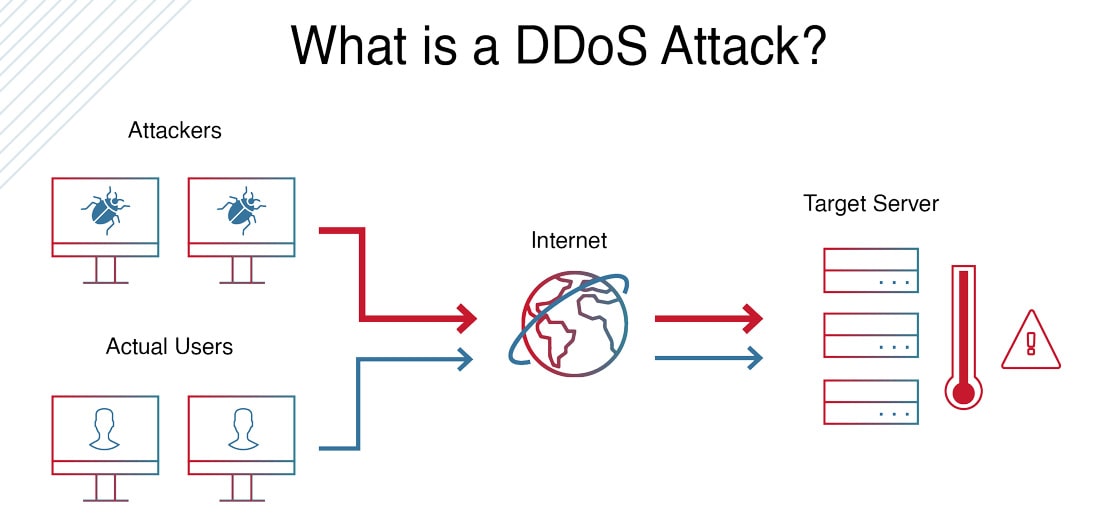
### Ransomware

[Ransomware](https://www.akamai.com/glossary/what-is-ransomware) is a type of malware that encrypts an organization’s high-value data, such as files, documents, and images, and demands a ransom from the company to restore access to that data. To be successful, the ransomware malware needs to gain access to a target system and encrypt the files. This can severely disrupt business operations and lead to significant financial loss and reputational damage.



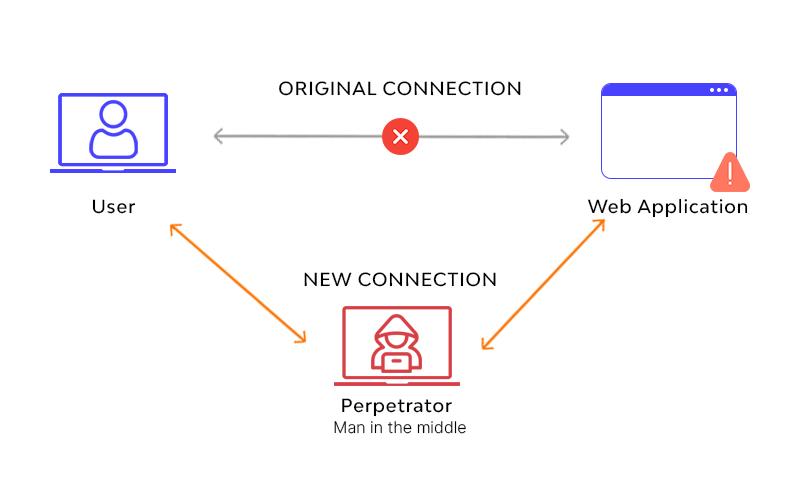
### DDoS attacks

A Distributed Denial-of-Service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks are executed using multiple compromised computer systems as sources of attack traffic, often leveraging botnets.



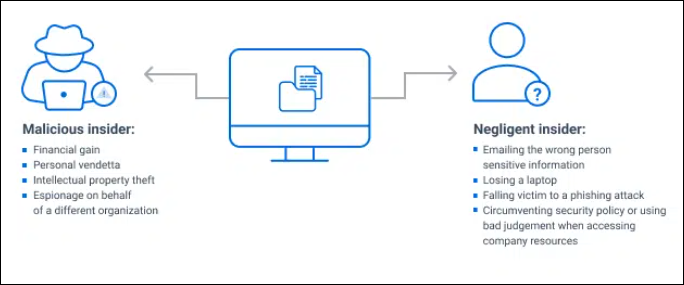
### MITM attacks

[Man-in-the-middle (MITM)](https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack) types of cyber attacks refer to breaches in cybersecurity that make it possible for an attacker to eavesdrop on the data sent back and forth between two people, networks, or computers. It is called a “man in the middle” attack because the attacker positions themselves in the “middle” or between the two parties trying to communicate. In effect, the attacker is spying on the interaction between the two parties.



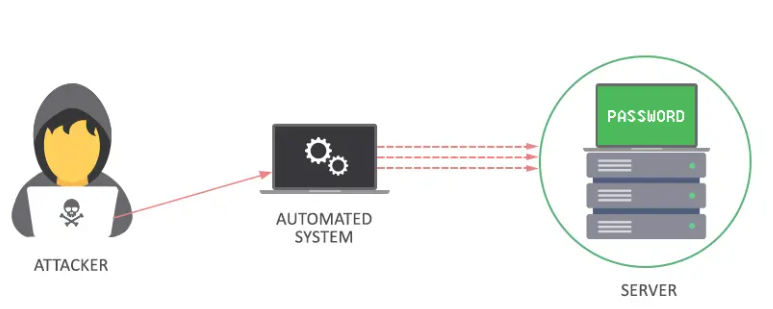
### Insider threats

An insider threat is a type of cyberattack originating from an individual who works for an organization or has authorized access to its networks or systems. These threats can be intentional (e.g., data theft) or unintentional (e.g., accidental data leakage).



### Brute-Force Attacks

Brute-force attacks involve attackers using automated tools to guess passwords until they find the correct one. These attacks exploit weak passwords and can lead to unauthorized access to accounts and systems.



These are just a few examples, and cybercriminals are constantly developing new techniques. It's crucial to stay vigilant and adapt our security measures to address evolving threats.

# 

# TECHNIQUES AND APPROACHES

To combat the cyber threats, we need a multi-layered defense strategy. Here's a breakdown of essential security practices we can implement:

1. Strong password.
2. Password expiration policy.
3. MFA.
4. Secure email with a personal certificate.
5. VPN IPSec on the laptops.
6. Cryptografied hard and flash disks to protect portable/mobile devices.

## 

## Strong password

Strong passwords are important because they help prevent unauthorized access to personal information and accounts. This is especially important for accounts containing sensitive information, such as financial email and social media accounts.

People know password reuse is insecure, yet they do it anyway. Some research has found that 45 percent of Americans use passwords of eight characters or less, which are not as secure as longer passwords.

### Role in Company Security

Strong passwords are essential for protecting user accounts and preventing unauthorized access to company systems. 81% of company data breaches are due to poor passwords according to the [2018 Verizon Data Breach Investigations Report](https://www.verizon.com/business/resources/reports/dbir/).

Many employees are reusing home passwords in the workplace, even though nearly all of them know that reusing passwords across multiple platforms is malpractice. According to [Trace Security](https://www.tracesecurity.com/blog/articles/weak-passwords-cause-data-breaches), 59% of people use the same password for everything, both at home and at the workplace. Password seems not very important factor to many but, when it is exploited, the financial burden to businesses can be huge.

The [Dropbox breach in 2012](https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach) was the result of an employee reusing a password at work and ended in 68 million users' credentials being stolen and sold online to malicious hackers.

Strong passwords play a critical role in company cybersecurity policies for several reasons:

* **First Line of Defense:** Passwords are the initial barrier preventing unauthorized access to company accounts, systems, and data. A strong password makes it significantly harder for attackers to guess or crack through brute-force methods.
* **Reduced Risk of Breaches:** Weak passwords are a major vulnerability exploited in data breaches. Enforcing strong password policies significantly reduces the risk of successful breaches and the potential consequences like financial loss, reputational damage, and regulatory fines.
* **Improved Overall Security Posture**: Strong passwords complement other security measures like firewalls and intrusion detection systems. They create a layered defense, making it more difficult for attackers to gain access even if they bypass other controls.
* **Compliance with Regulations:** Many industries have regulations mandating minimum password requirements for data security. A strong password policy ensures compliance with these regulations and avoids potential legal issues.
* **Encourages User Accountability:** A policy requiring strong passwords emphasizes the importance of cybersecurity to employees. It fosters a culture of security awareness and encourages users to take responsibility for protecting company resources.
* **Mitigates Social Engineering Attacks:** Social engineering tactics often attempt to trick users into revealing passwords. Strong passwords make it less likely that stolen credentials will be effective in gaining access.

### Characteristics of a Strong Password

The [best practices](https://www.security.org/how-secure-is-my-password/#:~:text=How%20To%20Create%20Secure%20Passwords) for creating secure passwords are:

* A password should be atleat 12 characters or more.
* A password should include a combination of *uppercase and lowercase* *letters, numbers, and characters.*
* A password shouldn’t be shared with any other account.
* A password shouldn’t include any of the user’s personal information like *name, birthday,*  *address,* or *phone number*. It’s also best not to include any information that can be accessed on social media like *kids’ or pets’ names*.
* A password shouldn’t contain any consecutive letters or numbers.
* A password shouldn’t be the word *“password”* or the same letter or number repeated.

### Implementation Strategy

To enforce strong passwords:

* Utilize password management tools to help employees generate and store complex passwords.
* A tool like [Secuiry.org](http://secuiry.org) can be used to check the strength of the passwords.
* Implement policies requiring the use of strong passwords across all systems and applications.

### Benefits of Strong Passwords

**Enhanced Security**: Strong passwords make it significantly harder for attackers to guess or crack through brute-force methods. This complexity adds significant time and effort to hacking attempts, discouraging cybercriminals and reducing the overall risk of successful attacks.

**Mitigation of Brute-Force Attacks**: Complex passwords are harder for attackers to guess or crack using automated tools.

**Reduced Attack Surface**: By enforcing strong password usage, you significantly reduce the number of potential entry points for attackers. This minimizes the vulnerabilities within your company's IT infrastructure.

## Password expiration policy

A password expiration policy is a set of rules that mandate how often users must change their passwords. This policy is designed to enhance security by minimizing the risk that compromised passwords can be used over an extended period.

*Note*: It’s important to note that NIST recommends resetting passwords only when necessary. While many organizations traditionally enforce a [NIST password policy](https://sprinto.com/blog/nist-password-guidelines/#:~:text=No%2C%20it's%20important%20to%20note,expiration%20as%20a%20general%20practice.) where passwords expire every 60 to 90 days, NIST diverges from this approach. NIST does not recommend password expiration as a general practice.

The main elements of a password expiration policy include the frequency of required password changes, notification periods before password expiration, and the restrictions on reusing previous passwords.

While the effectiveness of password expiration policies is debated, some organizations might still choose to implement them. Here are the key components to consider if you decide to move forward with a password expiration policy.

| **Key Components of a Password Expiration Policy** | |
| --- | --- |
| ***Expiration Interval*** | Determine the time frame for password expiration. This could be anywhere from 30 to 90 days, but consider the trade-off between security and user frustration. |
| ***Notification of Expiration*** | Users should be notified in advance when their passwords are about to expire to give them adequate time to create a new password. |
| ***Enforcement of Password Changes*** | The policy must enforce the change by preventing users from continuing to use an expired password. |
| ***Restrictions on Password Reuse*** | Users should not be able to reuse their recent passwords to ensure they create a new and different password each time. |
| ***Grace Periods*** | Implement a grace period after password expiration to allow users time to change their password before account lockout. |

### 

### Benefits of password expiration policies:

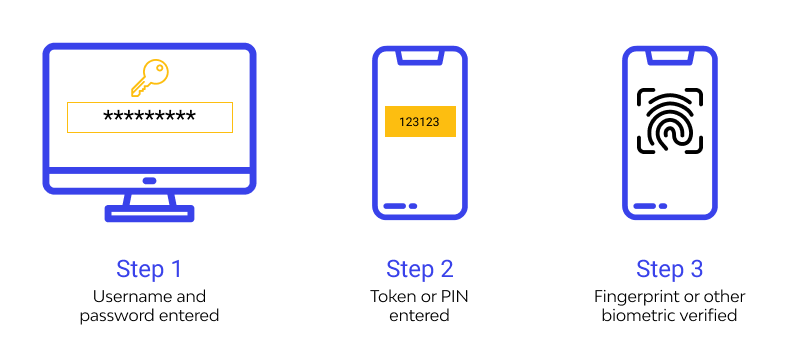
**Reduced Risk from Compromised Credentials (Limited)**: If an attacker gains access to a user's password, enforcing regular changes lessens the time they have to exploit it.

**Compliance with Regulations:** Many industry regulations and compliance standards, such as the Payment Card Industry Data Security Standard ([PCI DSS](https://www.itgovernance.co.uk/pci_dss#:~:text=The%20PCI%20DSS%20(Payment%20Card%20Industry%20Data%20Security%20Standard)%20is,security%20controls%20around%20cardholder%20data.)), Health Insurance Portability and Accountability Act ([HIPAA](https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html?CDC_AAref_Val=https://www.cdc.gov/phlp/publications/topic/hipaa.html)), and General Data Protection Regulation ([GDPR](https://gdpr.eu/)), require organizations to implement password expiration policies. By adhering to these regulations, organizations can avoid penalties and demonstrate their commitment to data security and privacy.

## Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) is a security technique that adds an extra layer of protection to your accounts and systems. Instead of just relying on a password for access, MFA requires users to provide two or more verification factors before granting access. These factors typically fall into three categories:

* **Knowledge Factor**: Something the user knows, like a password or PIN.
* **Possession Factor**: Something the user has, like a smartphone or a security token.
* **Inherence Factor**: Something the user is, like a fingerprint or facial recognition.



### Types of Multi-Factor Authentication

There are several types of MFA methods that organizations can implement:

* **Time-Based One-Time Password (TOTP)**: Users receive a temporary code via an authenticator app like Google Authenticator.
* **SMS or Email Codes:** A code is sent to the user's mobile phone or email, which they must enter to complete the login.
* **Biometric Authentication**: This includes fingerprint scans, facial recognition, or even iris scans.
* **Hardware Tokens:** Physical devices that generate unique codes, often used in high-security environments.

### Benefits of MFA

**Enhanced Security:** MFA significantly strengthens security by requiring multiple pieces of information for authentication. Even if a hacker manages to obtain one factor (e.g., a password), they would still need the other factor(s) to gain access. This makes it much harder for unauthorized users to breach accounts or systems.

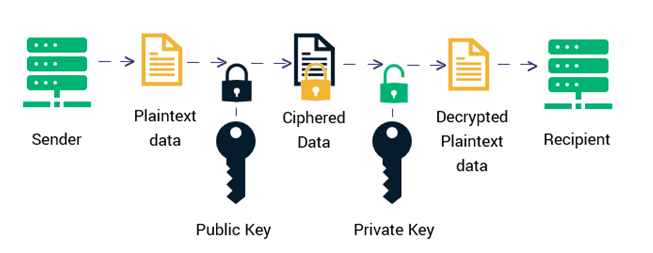
**Secure Remote Access**: With the rise of remote work and mobile computing, secure access to corporate resources from outside the traditional network perimeter is essential. MFA provides an additional layer of security for remote access, helping to protect sensitive data and systems from unauthorized access over potentially insecure networks.

## 

## Secure Email with Personal Certificate

A [Secure Email Certificate](https://cheapsslweb.com/email-identity), commonly known as a S/MIME certificate, is a security certificate issued to businesses and individuals who wish to protect their emails from hacks and cyber attacks. Email is a primary communication tool within the company, often used to exchange sensitive information.

Secure email practices protect this information from interception and tampering. The email security certificate allows users to send sensitive and crucial data over mail through a protected mechanism.



An email signing certificate works on public key infrastructure (PKI). All the email addresses that use a secure email certificate have a set of asymmetric keys i.e. a public and its corresponding private key.

* As the name suggests, the public key is available publicly, meaning that anyone can access it.
* The public key is used to encrypt the email’s contents.
* The encrypted email travels via insecure internet and reaches to the recipient’s server.
* The private key is safely stored on the email recipient’s server. When the content of the email is encrypted using a public key, only its corresponding private key can decrypt it.

The internet is likely always going to be insecure. Without encryption, anyone could potentially get access to your email messages and their contents. But when your emails are encrypted, no one can read or modify them until they reach the intended party.

Personal certificates enable secure email communication by:

* **Encrypting Email Conten**t: Ensuring that only the intended recipient can read the email. This ensures the confidentiality of sensitive information transmitted via email. There are multiple methods of doing the encryption, see Appendix B for some popular once
* **Digitally Signing Emails:** S/MIME uses digital signatures, similar to electronic fingerprints, to verify the sender's identity and ensure the message hasn't been altered during transmission. This helps prevent email spoofing and phishing attempts.
* **Non-Repudiation:** Digital signatures in S/MIME provide non-repudiation, which means both the sender and recipient have proof that the email originated from the claimed source and hasn't been tampered with.

### Benefits of Secure Email with Personal Certificates

**Data Tampering Prevention**: The technology ensures your message arrives exactly as you sent it. Any modification during transmission is detectable, preventing forgeries or manipulations.

**Sender Verification**: Recipients can be confident the email genuinely originated from a valid sender by checking the digital signatures. This combats email spoofing tactics used in phishing scams.

**Non-Repudiation**: Both parties have proof of the email exchange, demonstrating who sent the message and when. This can be helpful for legal or contractual purposes.

## VPN IPSec on the laptops

[IPsec](https://www.cloudflare.com/learning/network-layer/what-is-ipsec/) is a group of protocols for securing connections between devices. In "IPsec," "IP" stands for "Internet Protocol" and "sec" for "secure." IPsec helps keep data sent over public networks secure. It is often used to set up virtual private network (VPNs), and it works by encrypting IP packets, along with authenticating the source where the packets come from.

A VPN (Virtual Private Network) with IPSec (Internet Protocol Security) ensures secure remote access to the company's network, protecting data in transit from interception and eavesdropping. IPsec is secure because it adds encryption and authentication to this process.

### Components of IPSec

* **Authentication Headers (AH):** AH is like a security seal on a package that shows the package is from a trusted sender and hasn't been tampered with. However, it doesn't hide what's inside the package from prying eyes; it only ensures that the package is genuine and unchanged.
* **Encapsulating Security Payload (ESP):** Provides data encryption, data integrity, authentication, and anti-replay protection. ESP is like wrapping a package in a locked, opaque box. It hides both the contents and the shipping label, making it hard for anyone to see what's inside or where it's going. If you're using a simpler mode, ESP only locks up the contents and leaves the shipping label visible. ESP also adds its own label and packing slip to each package for extra security.

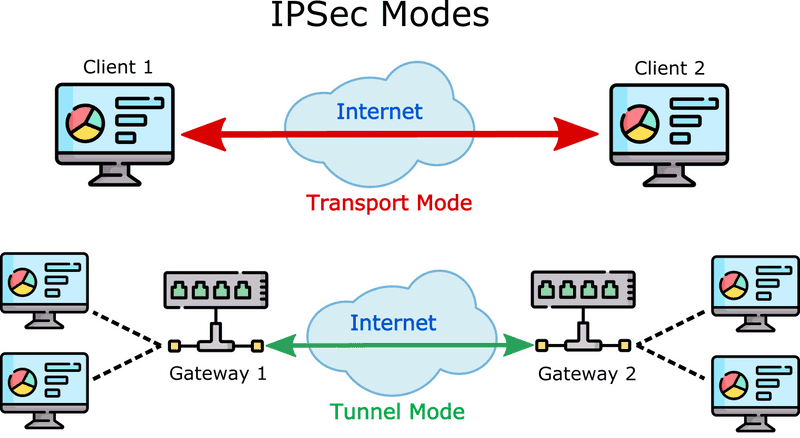
ESP is the more commonly used component as it provides both confidentiality and integrity. AES is a widely used encryption standard that can use key sizes of 128, 192, or 256 bits for ESP.

* **Security Associations (SAs)**: SA is like a set of rules and agreements between two people about how they will lock their packages and which type of locks they will use. One of the common methods they agree on is called Internet Key Exchange (IKE), which helps them decide on the locks and keys.

### How IPSec VPN Works

IPSec operates in two main modes:

* [**Tunnel Mode**](https://www.firewall.cx/networking/network-protocols/ipsec-modes.html#:~:text=IPSec%20tunnel%20mode%20is,to%20the%20remote%20network%3A)**:** [IPSec tunnel mode](https://www.firewall.cx/networking/network-protocols/ipsec-modes.html#:~:text=IPSec%20tunnel%20mode%20is,to%20the%20remote%20network%3A) is the default mode. It encrypts the entire IP packet, including both header and payload. This means IPSec wraps the original packet, encrypts it, adds a new IP header and sends it to the other side of the VPN tunnel (IPSec peer). This mode is commonly used for *network-to-network communications* or *remote access VPNs.*



* **Transport Mode**: Encrypts only the payload of the IP packet, leaving the header untouched. In transport mode, encrypted traffic is sent directly between two hosts that previously established a secure IPsec tunnel. This mode is typically used for *end-to-end communication* between two devices.

### Benefits of Secure VPN IPSec on the laptops

**Secure Communication:** IPSec encrypts data packets transmitted over the internet, ensuring that the communication between a laptop and the corporate network is secure. This prevents unauthorized access and eavesdropping on sensitive information being sent or received.

**Data Integrity**: IPSec ensures data integrity by using hashing algorithms ( such as [SHA- 256](https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm#:~:text=Lesson%20%2D%2061-,A%20Definitive%20Guide%20to%20Learn%20The%20SHA%2D256%20(Secure%20Hash%20Algorithms,1%20family%2C%20which%20was%20slowly%20losing%20strength%20against%20brute%20force%20attacks.,-The%20significance%20of), [SHA 512](https://komodoplatform.com/en/academy/sha-512/#:~:text=SHA%2D512%2C%20or,the%20BitShares%20network.)) to verify that data packets have not been altered during transit. This protects against data tampering and ensures that the information received is exactly what was sent.

**Cost-Effective Security**: Implementing IPSec VPNs is often more cost-effective than other security measures, such as leased lines or private circuits. It allows organizations to leverage the public internet for secure communication without compromising security.

**Protection Against Network-Based Attacks**: IPSec VPNs protect against a variety of network-based attacks, such as [man-in-the-middle attacks](#_bxz6pa3ji9me), replay attacks, and packet sniffing. By encrypting and authenticating data packets, IPSec ensures that data remains secure and protected from these threats.

## Encrypting hard drives and portable storage devices

Portable devices, such as laptops and USB drives, are susceptible to loss or theft. Encrypting these devices ensures that the data stored on them remains secure and inaccessible to unauthorized users. This ensures the confidentiality and integrity of your data, both at rest (stored on devices) and in transit (being transmitted over networks).

### Encryption tools

* **Full Disk Encryption (FDE)** : Encrypts the entire contents of a hard drive, rendering all data unreadable without the decryption key. This includes the operating system, applications, files, and folders. Following tools are commonly used for full disk encryption:
  + BitLocker (Windows)
  + FileVault (macOS)
  + LUKS (Linux)
* **Hardware-Based Encryption**: Utilizes built-in encryption capabilities of some portable storage devices like external hard drives and USB flash drives. Encryption and decryption are handled by a dedicated chip on the device itself. Examples :
  + Self-encrypting drives (SEDs)
  + Hardware-encrypted USB drives

### Benefits of Encrypting hard drives and portable storage devices

**Data Confidentiality**: If a hard drive or portable storage device (like a USB drive) is lost or stolen, encryption ensures that the data on it cannot be accessed without the correct decryption key or password. This protects sensitive company information from unauthorized access.

**Protection of Sensitive Information**: Companies often store confidential data such as financial records, personal employee information, intellectual property, and strategic documents on hard drives and portable devices. Encryption ensures that this sensitive information remains confidential even if the device is compromised.

**Protection During Transport:** Portable storage devices are often used to transport data. Encryption protects the data during transit, ensuring it remains secure even if the device is lost or stolen on the way.

**Secure Data Erasure**: Encrypting data from the outset means that when it's time to dispose of the device, simply deleting the encryption keys renders the data permanently inaccessible. This is much more secure than trying to wipe or physically destroy the storage device.

# 

# SUGGESTED BEST APPROACHES

The table below shows all best approaches for each security practice discussed above.

| **Security Practice** | **Approach** |
| --- | --- |
| ***Strong Passwords*** | ***Hashing Algorithms***: Use [bcrypt](#_j0um63v1k49g), [Argon2](#_dp5h37fu9h8d), or scrypt for hashing passwords, which are designed to be computationally expensive and resist brute-force attacks. |
| ***Password Expiration Policy*** | ***Hashing and Salting:*** Ensure that expired passwords are [hashed and salted](#_bxlr6wxdyf5) to prevent them from being easily compromised. |
| ***Multi-Factor Authentication (MFA)*** | ***Encrypted Communication***: Use TLS (Transport Layer Security) for secure transmission of one-time passwords (OTPs) via SMS or email.  ***TOTP Applications***: Use applications like Google Authenticator which securely store shared secrets. |
| ***Secure Email with Personal Certificate*** | ***S/MIME:*** Secure/Multipurpose Internet Mail Extensions (S/MIME) encrypts the content of emails and provides digital signatures using a public key infrastructure (PKI).  ***PGP/GPG:*** Pretty Good Privacy ([PGP)](#_6owobs6rsm87) or GNU Privacy Guard ([GPG](#_6owobs6rsm87)) can also be used for encrypting and signing emails. |
| ***VPN IPSec on the laptops*** | ***AES Encryption:*** Use [AES](#_lcoepal0uwd2) with key sizes of 128, 192, or 256 bits for encrypting data packets.  ***IPSec Protocols:*** Use Encapsulating Security Payload ([ESP](#_dt06mylreays)) for both encryption and authentication. |
| ***Encrypting Hard Drives and Portable Storage*** | ***Full Disk Encryption (FDE)***: Use tools like [BitLocker](#_lzx5lbgrccw3) (Windows), [FileVault](#_josyho32wfr) (macOS), and [LUKS](#_qf85ac6tpzv1) (Linux) for encrypting the entire disk.  ***Hardware-Based Encryption***: Use self-encrypting drives ([SEDs](#_pa1ei4eqtggw)) and hardware-encrypted USB drives which have built-in encryption capabilities. |

# CIA TRAID IMPACT

Each security practice contributes to a multi-layered defense strategy, enhancing the overall security posture of the organization. Implementing these practices together creates a comprehensive approach that addresses different aspects of the CIA triad.

| **Security Practice** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| --- | --- | --- | --- |
| ***Strong Password*** | Prevents unauthorized access to sensitive data | Reduces risk of data tampering through compromised accounts | Minimal, as long as password management is effective |
| ***Password Expiration Policy*** | Limits time compromised passwords can be used | Ensures fresh passwords, reducing chance of repeated attacks | Can cause temporary access issues during expiration periods |
| ***Multi-Factor Authentication (MFA)*** | Adds an extra layer of protection beyond passwords | Reduces risk of data alteration by verifying user identity | Potential delays during authentication, but overall improves access security |
| ***Secure Email with Personal Certificate*** | Encrypts email content to prevent unauthorized access | Ensures emails are not tampered with in transit | Minimal, but requires proper management of certificates |
| ***VPN IPSec on the laptops*** | Encrypts data in transit to prevent interception | Ensures data integrity by authenticating sources | Can slow down network speeds slightly, but ensures secure access |
| ***Encrypting Hard Drives and Portable Storage*** | Ensures data remains unreadable if device is lost or stolen | Prevents data tampering by protecting data at rest | Potential slight delay in accessing encrypted data, but overall enhances data protection |

These security practices improve the confidentiality, integrity, and availability of data for an organization. They mitigate the risk of data breaches, unauthorized access, and data tampering. However, some of these practices may introduce minor inconveniences for users, such as requiring more complex passwords or additional login steps.

# 

# CONCLUSION

Implementing these fundamental cyber security measures will significantly enhance our company's ability to protect sensitive information and secure employee activities. By adopting strong passwords, regular password updates, MFA, secure email practices, VPN IPSec, and encrypted storage, we build a resilient defense against cyber threats. As we strive to maintain a secure environment, continuous education and vigilance will be paramount in sustaining our cyber security posture.

This report serves as a blueprint for our revised cyber security policy, which will be presented to the board for approval and subsequently communicated to all technical teams for implementation. Together, we will ensure the highest standards of data protection and cyber security across our organization.

# APPENDIX : Definitions

##### **Bcrypt**

Bcrypt is a password-hashing function designed to be slow and computationally intensive, making it resistant to brute-force attacks. It uses the Blowfish encryption algorithm internally.

*Purpose:* It's commonly used for securely storing passwords in databases, ensuring that even if the database is compromised, it's difficult for attackers to recover the original passwords.

##### **Argon2**

Argon2 is a password-hashing function that won the Password Hashing Competition (PHC) in 2015. It's designed to be memory-hard and resistant to both brute-force and side-channel attacks.

*Purpose*: Argon2 is considered state-of-the-art for password hashing and is recommended for securely storing passwords in databases.

##### **Scrypt**

scrypt is another password-based key derivation function that's designed to be memory-hard and computationally intensive. It aims to provide more resistance to parallel attacks compared to traditional hash functions.

*Purpose:* Like bcrypt and Argon2, scrypt is used for securely hashing passwords, particularly in situations where memory usage is a concern.

##### **Hashing and Salting**

Hashing is the process of converting an input (such as a password) into a fixed-size string of characters using a cryptographic hash function.

Salting involves adding a random value (the salt) to each password before hashing, making it more difficult for attackers to use precomputed rainbow tables for attacks.

*Purpose:* Hashing and salting are used together to securely store passwords in databases. Even if two users have the same password, their hashed values will be different due to the unique salt added to each password.

##### **PGP/GPG: Pretty Good Privacy (PGP) or GNU Privacy Guard (GPG)**

PGP and GPG are encryption programs that provide cryptographic privacy and authentication for data communication. They use asymmetric encryption to encrypt messages and files, as well as provide digital signatures for verifying the authenticity and integrity of data.

*Purpose:* PGP/GPG are widely used for securing email communication, encrypting files, and verifying the authenticity of software distributions.

##### **AES Encryption**

AES (Advanced Encryption Standard) is a symmetric encryption algorithm widely used for securing sensitive data. It's a block cipher that operates on fixed-size blocks of data and supports key sizes of 128, 192, or 256 bits.

*Purpose:* AES is used in various security protocols and applications, including VPNs, disk encryption, and secure communication over the internet.

##### **IPSec Protocols**

IPSec (Internet Protocol Security) is a suite of protocols used for securing internet communications by encrypting and authenticating IP packets. It includes protocols like Authentication Header (AH) and Encapsulating Security Payload (ESP).

*Purpose:* IPSec is commonly used for setting up VPNs, ensuring confidentiality, integrity, and authenticity of data transmitted over IP networks.

##### **BitLocker**

BitLocker is a full-disk encryption feature included with Microsoft Windows operating systems. It encrypts the entire contents of a disk drive to protect data from unauthorized access.

*Purpose:* BitLocker is used to enhance data security on Windows computers, particularly for protecting sensitive data stored on internal and external drives.

##### **FileVault**

FileVault is a disk encryption program included with macOS. It encrypts the entire contents of a disk drive using XTS-AES-128 encryption.

*Purpose:* FileVault provides data protection on macOS systems by encrypting the startup disk, protecting user data from unauthorized access.

##### **LUKS**

LUKS (Linux Unified Key Setup) is a disk encryption specification for Linux systems. It provides disk encryption capabilities and supports multiple user passwords or keys for decrypting the disk.

*Purpose*: LUKS is used to encrypt entire disk partitions on Linux systems, protecting data stored on the disk from unauthorized access.

##### **Self-Encrypting Drives (SEDs) and Hardware-Encrypted USB Drives**

SEDs are hard drives or solid-state drives (SSDs) with built-in encryption capabilities. They automatically encrypt data written to the drive and decrypt data read from the drive, using encryption keys stored in the drive's hardware.

*Purpose:* SEDs and hardware-encrypted USB drives provide transparent encryption for data stored on the device, protecting it from unauthorized access in case of loss or theft. They are commonly used in enterprise environments to secure sensitive data.

# REFERENCES

*2024 Data Breach Investigations report*. (n.d.). Verizon Business. <https://www.verizon.com/business/resources/reports/dbir/>

Administrator. (n.d.). *Understanding VPN IPSEC tunnel mode and IPSEC Transport mode - what’s the difference?* <https://www.firewall.cx/networking/network-protocols/ipsec-modes.html#:~:text=IPSec%20tunnel%20mode%20is,to%20the%20remote%20network%3A>

GDPR.eu. (2019, February 19). *General Data Protection Regulation (GDPR) Compliance Guidelines*. <https://gdpr.eu/>

Gibbs, S. (2017, February 21). Dropbox hack leads to leaking of 68m user passwords on the internet. *The Guardian*. <https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach>

Gracy, M. (2024, April 15). *NIST Password Guidelines: All you need to know*. Sprinto. <https://sprinto.com/blog/nist-password-guidelines/#:~:text=No%2C%20it's%20important%20to%20note,expiration%20as%20a%20general%20practice>.

*Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. (2024, May 15). Public Health Law. <https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html?CDC_AAref_Val=https://www.cdc.gov/phlp/publications/topic/hipaa.html>

Jena, B. K. (2023, August 29). *A definitive guide to learn the SHA-256 (Secure Hash algorithms)*. Simplilearn.com. <https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm#:~:text=Lesson%20%2D%2061-,A%20Definitive%20Guide%20to%20Learn%20The%20SHA%2D256%20>(Secure%20Hash%20Algorithms,1%20family%2C%20which%20was%20slowly%20losing%20strength%20against%20brute%20force%20attacks.,-The%20significance%20of

*PCI DSS | What it is and how to comply | IT Governance UK*. (n.d.). <https://www.itgovernance.co.uk/pci_dss#:~:text=The%20PCI%20DSS%20(Payment%20Card%20Industry%20Data%20Security%20Standard)%20is,security%20controls%20around%20cardholder%20data>.

Security.org. (2023, October 12). *How secure is my password? | Password Strength Checker*. <https://www.security.org/how-secure-is-my-password/#:~:text=How%20To%20Create%20Secure%20Passwords>

*What is a man-in-the middle (MITM) attack? Types & Examples | Fortinet*. (n.d.). Fortinet. <https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack>

*What is a phishing attack? | Cloudflare*. (n.d.). <https://www.cloudflare.com/learning/access-management/phishing-attack/>

*What is IPsec? | How IPsec VPNs work | Cloudflare*. (n.d.). <https://www.cloudflare.com/learning/network-layer/what-is-ipsec/>

*What is Malware? How to Prevent Malware Attacks?* (n.d.). Fortinet. <https://www.fortinet.com/resources/cyberglossary/malware>

*What-is-ransomware*. (n.d.). <https://www.akamai.com/glossary/what-is-ransomware>