1847Financial | HTK

Understanding Encryption

WHAT IS ENCRYPTION?

Encryption is the process of converting readable data into an unreadable, encoded form to keep it secure during transmission or storage. It uses algorithms and keys to scramble the data, making it unreadable without the decryption key. Encryption protects confidential data at rest (storage) and while in transit (point-to-point).

WHY IS ENCRYPTION IMPORTANT?

- Encryption ensures that only authorized individuals can access sensitive information. It prevents unauthorized parties, such as hackers or eavesdroppers, from understanding or using the data even if they intercept it.
- This protection is especially critical for sensitive information such as personal data, financial records, and intellectual property.
- Many regulations and standards require organizations to encrypt certain types of data to protect privacy and maintain compliance.
- Encryption secures communication channels, including emails, messaging apps, and online transactions, safeguarding sensitive information from interception or eavesdropping.
- Encryption is used in digital signatures and authentication protocols to verify the authenticity of messages, ensuring that they come from trusted sources and have not been altered in transit.
- Implementing encryption demonstrates a commitment to security, building trust with customers, partners, and stakeholders. It enhances an organization's reputation and reduces the risk of data breaches.

HOW CAN YOU ENCRYPT YOUR DATA AT REST?

Encryption at rest involves securing data while it's stored on physical or digital storage devices, such as hard drives, databases, or cloud storage. This security measure ensures that even if unauthorized individuals gain access to the storage medium (such as a hard drive), they cannot read or decipher the stored data.

Activating encryption typically involves using built-in encryption features or third-party encryption software.

Here's some additional information on encryption methods:

1. Use Built-in Operating System Encryption:
    a. Windows devices often come with BitLocker, a built-in encryption tool.
    b. macOS offers FileVault, a built-in encryption feature.
2. Purchase third-party encryption software if your laptop doesn't have built-in encryption features or if you prefer additional encryption options.
3. Cloud Storage Encryption can be used if you store sensitive data in the cloud, consider using cloud storage services that offer encryption options.
    a. Enable encryption settings within the respective service's settings or preferences.

HOW CAN YOU ENCRYPT YOUR DATA AT TRANSIT?

Encryption in transit secures data as it moves between devices or systems over networks. By encrypting data (called packets) during transmission, this process ensures confidentiality and prevents unauthorized access, even if intercepted. Common protocols like TLS and SSL encrypt data, maintaining privacy and security during communication.

1847Financial | HTK

Here are some additional information on encryption methods:

1. Send all emails containing confidential information encrypted or securely.
    a. For company provided email address, you can do this simply by typing the word “secure” in square brackets i.e. **[secure]** anywhere in the subject line of your email.
    b. For non-company email addresses, please reach out to email provider for advisement.
2. Use secure and trusted Wi-Fi sources when working remotely that enable encryption protocols such as WPA2 or WPA3 to secure communication between devices and access points.
    a. Work with your internet provider to ensure that your internet gateway or router default password has been updated to a strong and unique password.

Important Reminders about Encryption:

- Password protect all of your personal devices is one of best safeguards in case your device is stolen or missing.
- If confidential data and files are unencrypted there is a risk that if they are sent to the wrong person, lost or stolen, any third party could gain unauthorized access to that data. Encryption adds an additional layer of protection.
- Always work with a trusted vendor if you need technical assistance with encryption settings