FileVault Disk Encryption

Objectives:

At the end of this episode, I will be able to:

1. Describe the purpose and function of Apple FileVault
2. Differentiate between FileVault v1 and v2
3. Encrypt a computer running macOS using Apple FileVault

> Additional resources used during the episode can be obtained using the download link on the overview episode.

- Security Limitations
  - Most security measures can be bypassed
    - User password can be reset from recovery
    - Firmware password can be bypassed by removing the disk
  - Encrypting your data mitigates most of those scenarios
    - Exception would be post-login attacks
- FileVault
  - Allows encryption of the entire disk
  - Current version is FileVault v2
  - "Legacy FileVault" is v1
  - Legacy FileVault only encrypted your home folder
  - Legacy FileVault maintained a "Master Password" to allow for emergency description
  - `Apple Menu` -> `System Preferences` -> `Security & Privacy` -> `Legacy FileVault`
  - Apple recommends decrypting your Legacy FileVault and re-encrypting with the new FileVault
  - FileVault 2 uses XTS-AES 128 encryption
  - Technical Details (https://support.apple.com/en-us/HT204837)
- Firmware Password
  - Booting a Mac to recovery allows for resetting user passwords
  - Anyone with physical access could do that
  - A firmware password protects from that
  - To enable:
    1. Boot to recovery
    2. `Utilities` -> `Firmware Password Utility`
    3. Set a password
  - If the firmware password is lost, you will need to take it to an Apple store to be reset

---

External Resources:

During this episode, you can reference the following external resources for supplementary tools and information:

- Apple FileVault Technical Details (https://support.apple.com/en-us/HT204837)