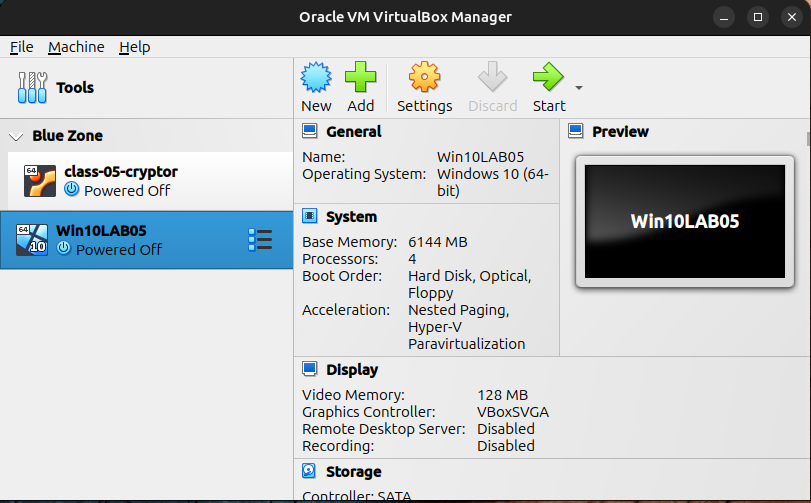
Hélio Ferreira 21/05/2024  
  
**Lab: Protecting Data at Rest**

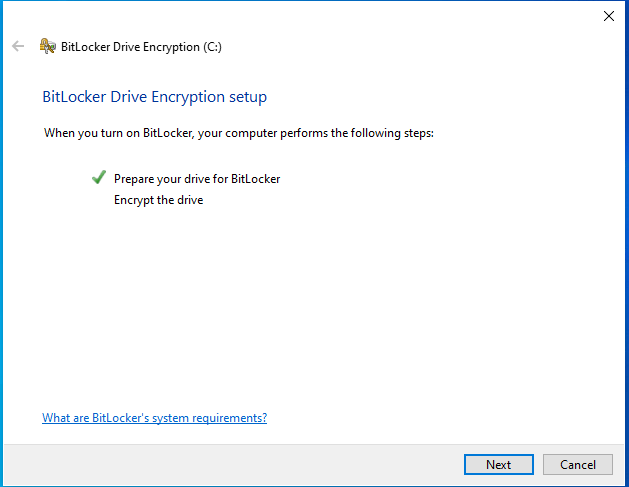
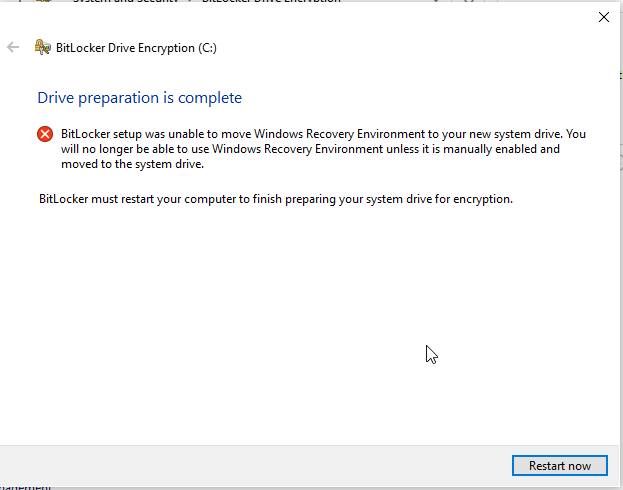
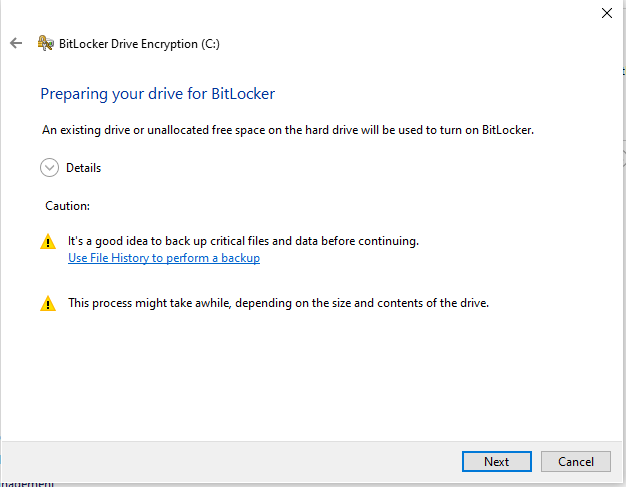
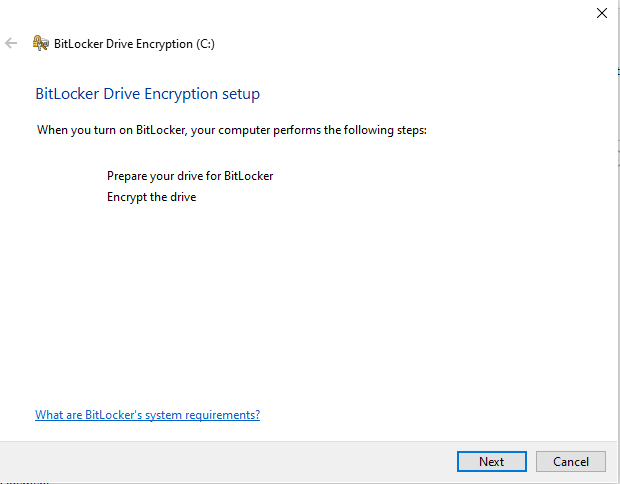
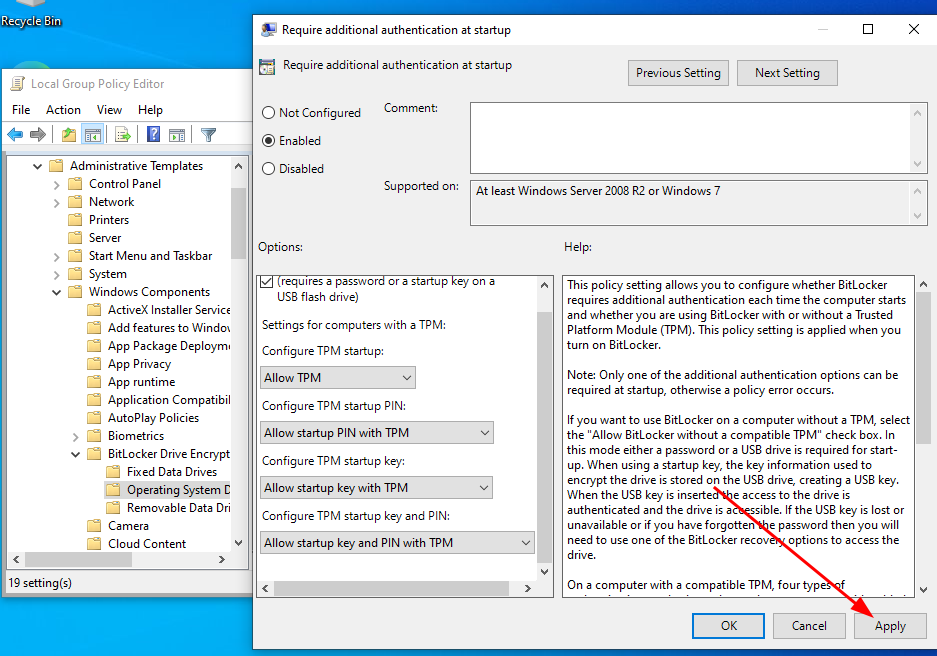
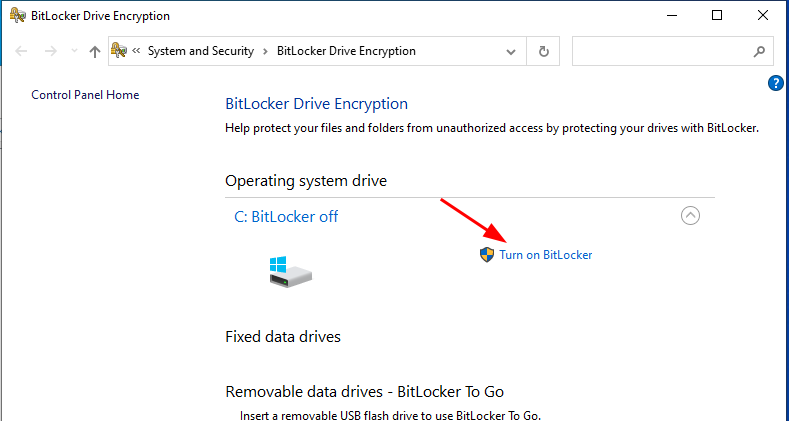
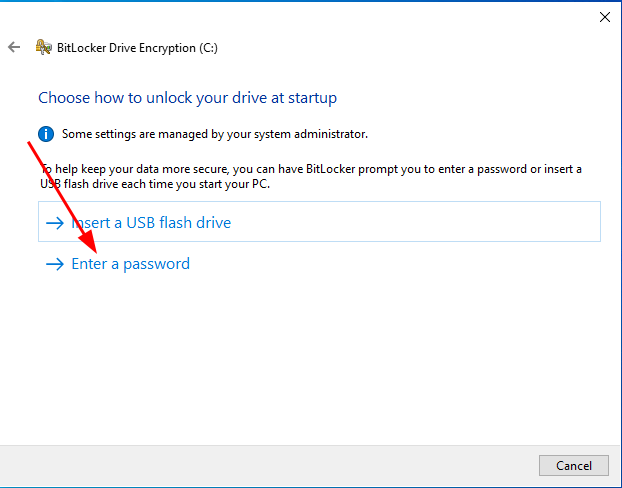
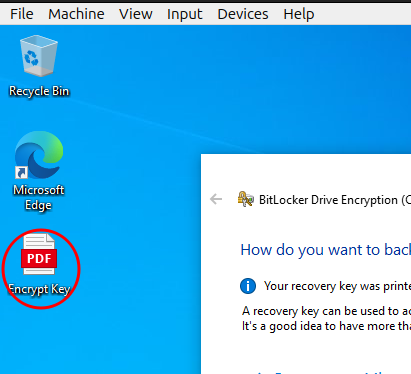
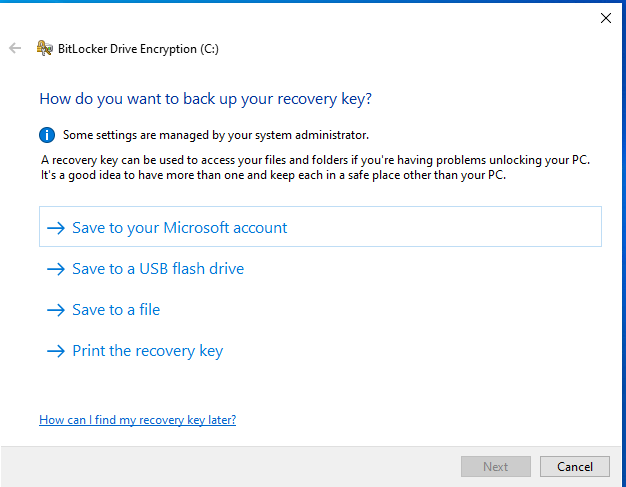
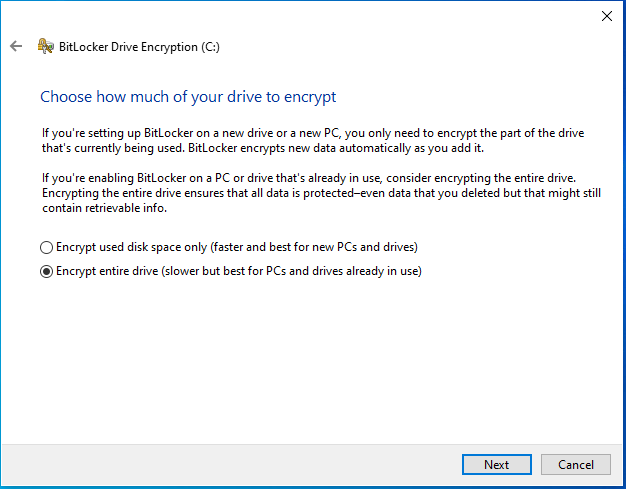
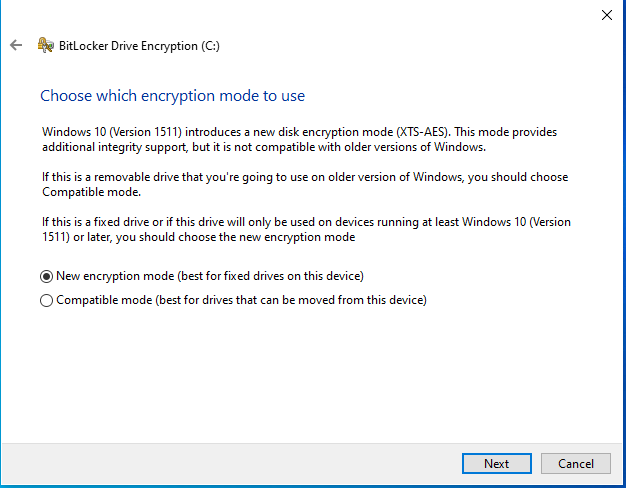
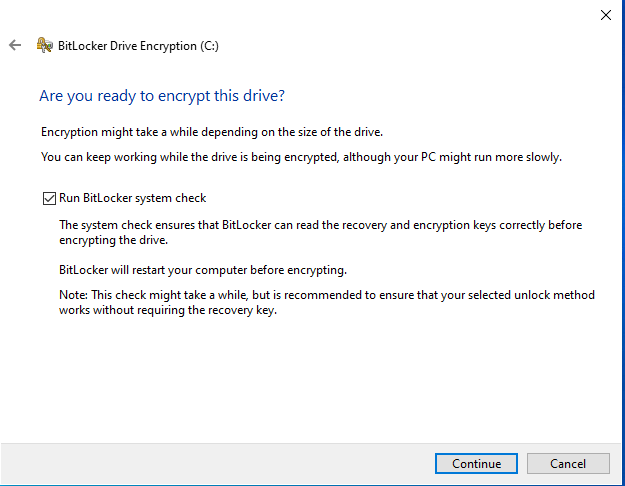
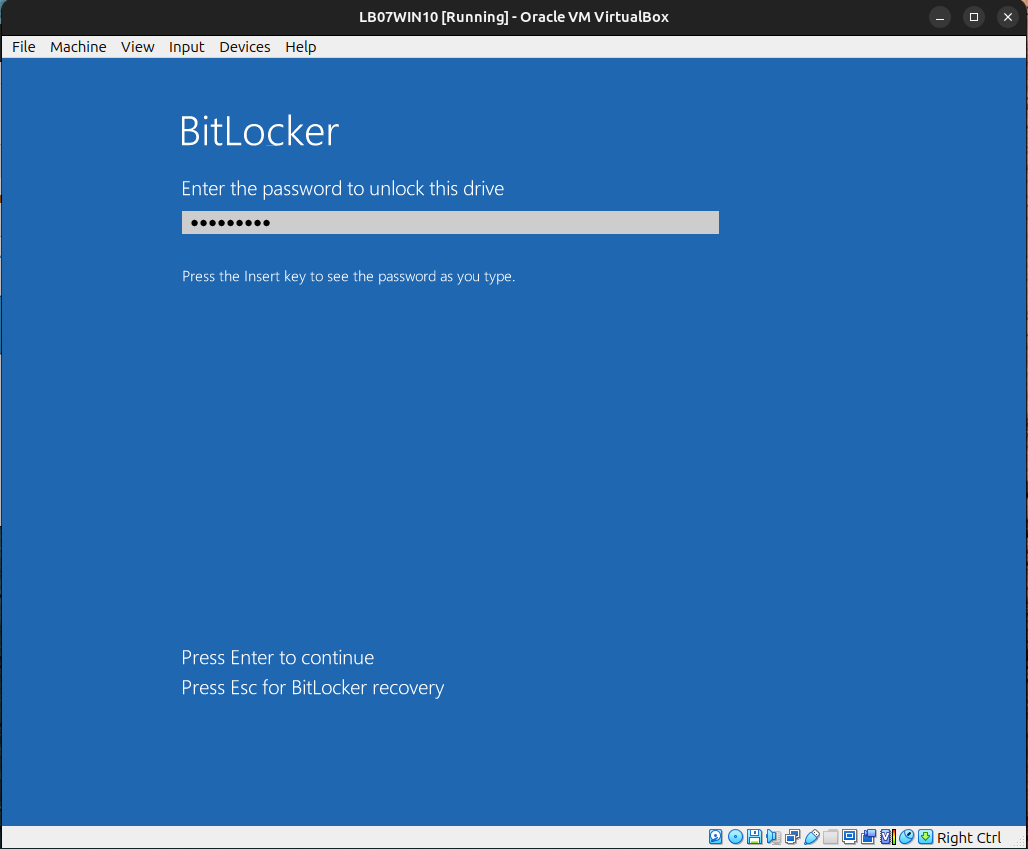
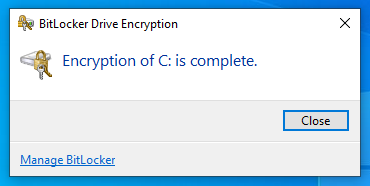
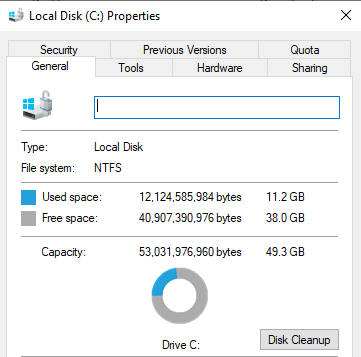
### **Part 1: Staging**

To complete this lab, you will need:

* Class-05-cryptor VM
* Windows 10 VM

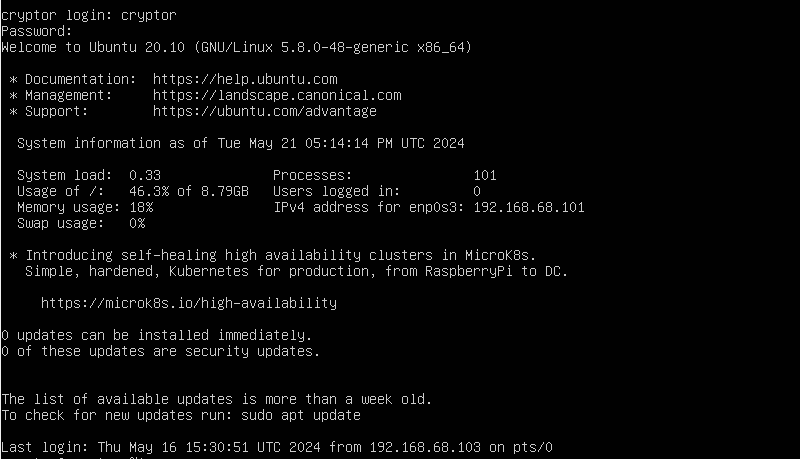
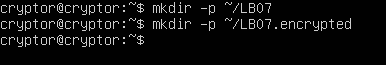
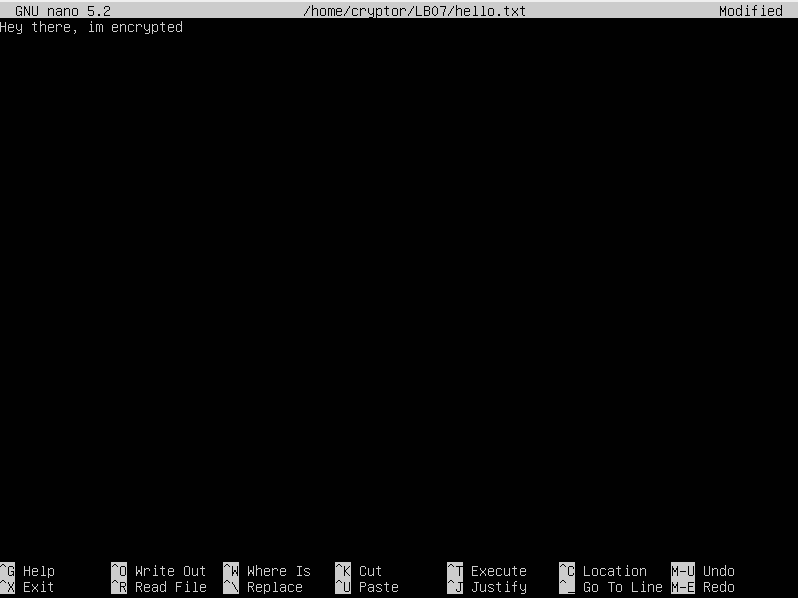
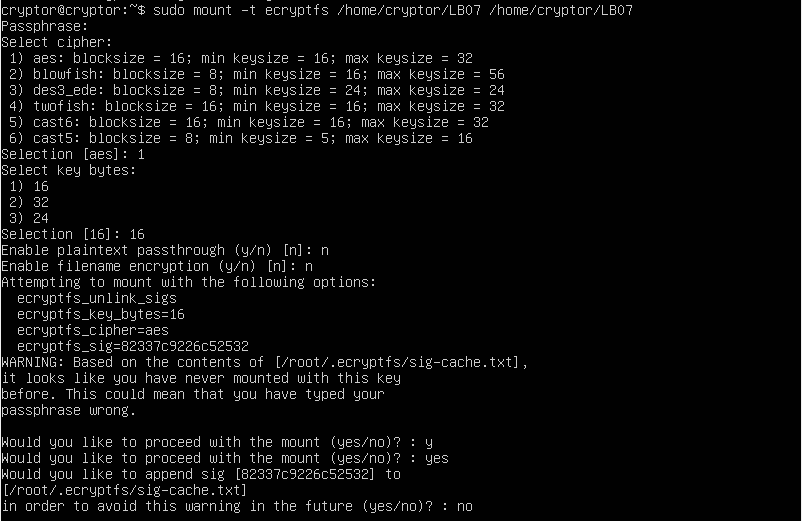
### **Part 2: Windows FDE**

To turn on BitLocker, edit the local group policy using **gpedit.msc** and navigating to Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives instead.

* Save state your Windows 10 VM before proceeding.
* Find BitLocker settings in Windows 10 and toggle it on.
* Under “Choose how to unlock your drive at start” select “Enter a password” and enter your usual password.
* Under “How do you want to backup your recovery key” select “Print the recovery key” and save a PDF to your Desktop for now. In a production environment you’d want to save this to a backed up file server for recovery in the event of lockout  
  .
* Select “Encrypt entire drive” since we’re attempting FDE.  
  
* Select “New encryption mode”
* Tick the box for “Encryption check” option.
* Reboot. Grab a screenshot of “Enter the password to unlock this drive.”
* After entering the password, it will take you to the normal user login. Login as normal. On the system tray at the bottom right, BitLocker should now begin encrypting your Windows C: drive. You’ll want to take a screenshot when it completes, but for now, feel free to move onto Part 3 while you wait for the FDE procedure to complete.
* Verify your C: drive is in an encrypted state.

### **Part 3: Linux Directory Encryption**

Sometimes you may only need to encrypt part of a file system. The Linux tool eCryptfs allows us to encrypt directories in a Linux system. This software packages comes preinstalled on class-05-cryptor VM, which is where you’ll perform this part of the lab.

* SSH into class-05-cryptor using cryptor/cryptor credentials.
* Mount a new encrypted directory using eCryptfs.
* Create a new .txt document within the encrypted directory.
* Try viewing the document. You should be able see the document because the directory is currently mounted.
* Unmount the directory with the **umount** command.
* Try viewing the document. You should now only see the ciphertext. Include a screenshot of the ciphertext on your submission.

### **Part 4: Reporting**

* **What is the purpose of the TPM chip and why is it normally required in order to operate BitLocker on a Windows 10 PC?**  
    
  A Trusted Platform Module (TPM) chip acts like a secure vault for your computer. It's a special chip on your motherboard that enhances security by storing encryption keys and performing cryptographic operations. This hardware-based security helps protect your data even from sophisticated attacks.

Here's why BitLocker relies on TPM:

Secure Storage: BitLocker uses encryption to scramble your hard drive contents, making them inaccessible without the proper key. The TPM chip safely stores these encryption keys, adding an extra layer of protection compared to just software-based encryption.

Platform Integrity: The TPM can also verify the integrity of your system's startup process. This ensures that your computer boots up with the same trusted operating system and hasn't been tampered with by malware, making it more difficult for attackers to bypass BitLocker.

Since TPM provides these critical security features, it's become a requirement for enabling BitLocker on most modern Windows 10 machines.

* **Are laptop computers secured against theft out of the box? What precautions can be taken to insure data confidentiality in the event of laptop theft?**  
  Laptops out of the box have some security measures, but they primarily focus on data security, not physical security against theft. Here's a breakdown of both:

Out-of-the-box Security:

Encryption: Some laptops may come with features like disk encryption enabled by default. This scrambles your data, rendering it unreadable without a decryption key.

Passwords: Most laptops require a login password to access the system. This protects your data if the laptop is lost or stolen while turned off.

Physical Security:

Out-of-the-box: Laptops generally lack built-in theft protection.

Precautions to Enhance Data Confidentiality:

Enable Encryption: If your laptop doesn't have full-disk encryption by default, consider enabling BitLocker on Windows or FileVault on Mac. These features encrypt your entire hard drive.

Strong Passwords: Use complex and unique passwords for your login and encryption. Don't write them down or share them with anyone.

Remote Wipe: Some software allows remote wiping of your laptop's data in case of theft. This ensures even if they bypass encryption, your data is destroyed.

Backups: Regularly back up your important data to an external drive or cloud storage. This way, even if your laptop is stolen, you have a copy of your data.

Physical Security Measures:

Cable Locks: Physically secure your laptop to a desk or other immovable object using a cable lock.

Tracking Software: Consider installing software that tracks your laptop's location if stolen.

Security Software: Antivirus and anti-malware software can help prevent malware that might steal your data even if the laptop isn't lost.

Be Mindful: When working in public places, be aware of your surroundings and avoid leaving your laptop unattended.

By combining strong data security practices with physical security measures, you can significantly reduce the risk of data exposure in case of laptop theft.

* **What data theft scenarios do today’s tools *not* defend against?**

Security tools are great, but they can't stop everything. Here's the short version:

People can be tricked (Social Engineering). Don't click on suspicious links or share your password.

Hidden flaws (Supply Chain Attacks, Zero-Day Exploits) can open doors. Software updates are essential.

People on the inside can steal stuff (Insider Threats). Keep an eye on who has access to what.

Skilled attackers are patient (APTs). Layered security makes it harder for them.

Unsecured connections leak data (Unsecured APIs, Data in Transit). Use strong encryption, especially on public Wi-Fi.

Physical access is a big risk. Don't leave your laptop unattended and consider encryption.

Stay informed, use common sense, and keep your software up to date. This will make it much harder for thieves to get your data.

* **Consider data at rest VS data in motion. How do these two categories affect how you approach securing data?**  
    
  Data security depends on whether your data is at rest (stored) or on the move.

**Data at rest:** Imagine a locked safe. You need encryption (combo), access controls (who has the key), and tamper detection (security camera).

**Data in motion:** Imagine carrying valuables. You need encryption (scrambling the valuables), secure protocols (armored car), and firewalls (security checkpoints).

By securing both data at rest and in motion, you make it much harder for thieves to steal your data.