



Guide to Encrypting Your Devices

Encryption uses complex math problems to scramble your data. In order to use the code to unscramble the data, you need a private key. In most cases, this is a password you set. If you lose an encrypted device or if it is stolen or confiscated, the contents will be meaningless without your passcode.

Encrypting a Phone or Tablet

If you have an iPhone or a newer Android, your phone is automatically encrypted once you set a passcode. Your phone uses the passcode to unlock your phone and to decrypt its content. We recommend using the maximum number of digits possible for your passcode to make it harder to crack.

On an iPhone, you can turn on your passcode or make a stronger passcode by going to Settings > Touch ID & Passcode > Turn Passcode On OR Change Passcode. You can also choose to have your data automatically erased after 10 failed passcode attempts. To do this, scroll down past the passcode settings and toggle on "Erase Data".

On an Android, go to Settings > Security > Lock Screen (the path may differ on some devices). Select PIN or Passcode and choose the most secure option possible (maximum length). Scroll down to "Encrypt phone/tablet," then tap "Encrypt SD card" to tick its checkbox. Tap the Next button and confirm your choice on the next screen by typing your PIN or password when prompted. Tap the "Encrypt phone/tablet" button to begin encryption.

Initial encryption can take 30 minutes to about an hour, depending how much data you have. Your phone or tablet will reboot a few times during the process; this is normal.


Be sure to choose a passcode you can remember – without it, you will not be able to decrypt your data. You can save it in a secure note in your password manager or on a piece of paper in a locked drawer, for example. The more you enter it, the better you'll remember it, so try to choose to use your password instead of Touch or Face ID.

If you are going to an event or another occasion where you are nervous about police interaction or a third party using your fingerprint or face to unlock your phone, turn those features off to require use of your passcode.

digital defense fund

Encrypting a Laptop

If you have an **Apple computer**, you can encrypt it using a built-in feature called FileVault.

1. Choose Apple menu > System Preferences, then click Security & Privacy.
2. Click the FileVault tab.
3. Click , then enter an administrator name and password.
4. Click Turn On FileVault.

FileVault offers a few recovery options. Be sure to save your passcode and your backup recovery key somewhere safe, like in a secure note in your password manager or on a paper in a locked drawer.

If you have a Windows computer:

Windows offers two built-in encryption options: device encryption and Bitlocker. Device encryption is only available on supported devices, and Bitlocker is only available on Windows Pro subscriptions or above.

To see if you can use **device encryption** (below information copied from [Microsoft's support page on device encryption](#)):

1. In the search box on the taskbar, type **System Information**, right-click **System Information** in the list of results, then select **Run as administrator**. Or you can select the **Start** button, and then under **Windows Administrative Tools**, select **System Information**.
2. At the bottom of the **System Information** window, find **Device Encryption Support**. If the value says **Meets prerequisites**, then device encryption is available on your device. If it isn't available, you may be able to use standard BitLocker encryption instead.

If device encryption is available on your device:

1. Sign in to Windows with an administrator account (you may have to sign out and back in to switch accounts). For more info, see [Create a local or administrator account in Windows 10](#).
2. Select the **Start** button, then select **Settings > Update & Security > Device encryption**. If **Device encryption** doesn't appear, it isn't available. You may be able to turn on standard BitLocker encryption instead.



digital defense fund

3. If device encryption is turned off, select **Turn on**.

If you Windows Pro or above, you can use **BitLocker** to encrypt your device. To enable it, go to the Control Panel and locate the BitLocker Drive Encryption system preference and click the link to Turn On BitLocker. Follow the prompts to create a recovery password to unlock the drive. Next, decide how you wish to back up your recovery key, and lastly, choose how you wish to have the drive encrypted. This will run a check on the system and begin the encryption process on your device.

If neither Windows's device encryption or BitLocker is available for your device, then you can use the open source software **VeraCrypt** to encrypt your device.

Installing **VeraCrypt** for Windows:

1. You can [download VeraCrypt here](#).
2. Follow the step-by-step instructions with screenshots for installing it [here](#).
 - a. You may be prompted to turn off fast startup. It is advised to turn off Windows Fast Startup if you are using VeraCrypt.
 - b. You can use VeraCrypt to encrypt just part of your data (creating a "volume") or your entire hard drive ("Encrypt a Windows System Drive Using Veracrypt"). The [instructions we link to](#) contain step-by-step screenshots for both options. Note that if you encrypt your whole Windows System Drive, there is a risk of your data becoming corrupted due to VeraCrypt not being a built-in Windows application. Weigh the risk of losing your data versus the risk of not encrypting your entire device.
 - c. No matter which VeraCrypt option you choose, be sure to back up your data in case of technical difficulties or data loss. You can back up to a physical hard drive (thumb drive, or a larger [portable drive](#) - you can encrypt these external drives with VeraCrypt as well - instructions [here](#)) or to the cloud (Google Drive, or for end-to-end encrypted cloud options, [Tresorit](#), [NordLocker](#), [ProtonDrive](#), etc.).

No matter which option you use for encrypting your Windows device, be sure to save your passcode and your backup recovery key (if backup options are offered) somewhere safe, like in a secure note in your password manager or on a paper in a locked drawer.

Last updated 8/30/21