

 Wallet Walkthrough – Hands-on Wallet Setup

**Objective/Aim:**  
  
 The primary objective of this exercise is to successfully install, create, and secure a non-custodial cryptocurrency wallet using the Trust Wallet application. This hands-on process aims to provide a practical understanding of wallet creation and the critical importance of managing a secret recovery phrase.

Upon completion, you will be able to:

* Install a mobile cryptocurrency wallet from an official source.
* Generate a new, unique wallet.
* Securely back up the 12-word Secret Recovery Phrase.
* Understand the basic wallet interface for sending and receiving digital assets.
* Differentiate between a public address and a secret phrase.

**Apparatus/Software Used:**

* Laptop
* Browser-brave
* Trust wallet
* Internet for research

**Theory/Concept:**

 **What is a Cryptocurrency Wallet?** A cryptocurrency wallet is a software application that allows users to interact with blockchain networks. It does not "store" your digital currency in the way a physical wallet stores cash. Instead, it holds your **keys**—the cryptographic information needed to access your assets on the blockchain and authorize transactions.

 **Non-Custodial (Self-Custody) Wallets:** Trust Wallet is a **non-custodial** or **self-custody** wallet. This means that **you, and only you, have full control and ownership of your private keys and Secret Recovery Phrase**. Unlike keeping funds on a centralized exchange (which is custodial), there is no company or third party that can access, freeze, or lose your funds. This grants you complete financial sovereignty but also places the full responsibility of security on you.

 **The Secret Recovery Phrase (Seed Phrase):** This is the most critical piece of information for your wallet. When you create a new wallet, it will generate a unique **12-word Secret Recovery Phrase**. This phrase is the master key to all the funds managed by that wallet.

* **Function:** It can be used to restore your entire wallet and all its assets on any new device if your current device is lost, stolen, or broken.
* **Security:** Anyone who gains access to your 12-word phrase can gain access to your funds and steal them. **It must be kept absolutely secret and secure.**

 **Public Address vs. Private Keys:**

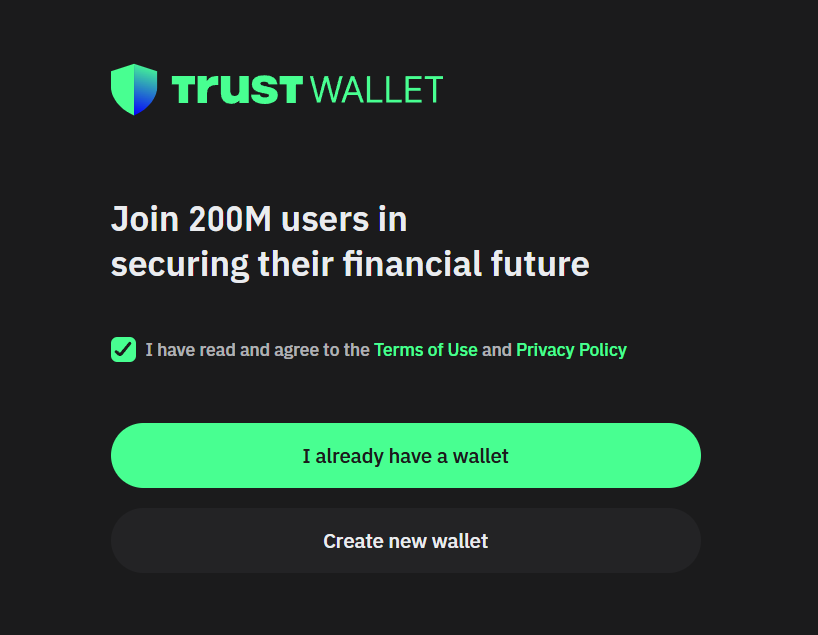
* **Public Address:** This is like your bank account number. It is a string of characters that you can safely share with others to receive cryptocurrency. Each coin in your wallet (e.g., Bitcoin, Ethereum) will have its own public address.
* **Private Keys:** These are the "passwords" that prove ownership and authorize outgoing transactions from your address. Your 12-word Secret Recovery Phrase is a human-readable master version of all your private keys. You should **NEVER** share your private keys or your Secret Recovery Phrase.



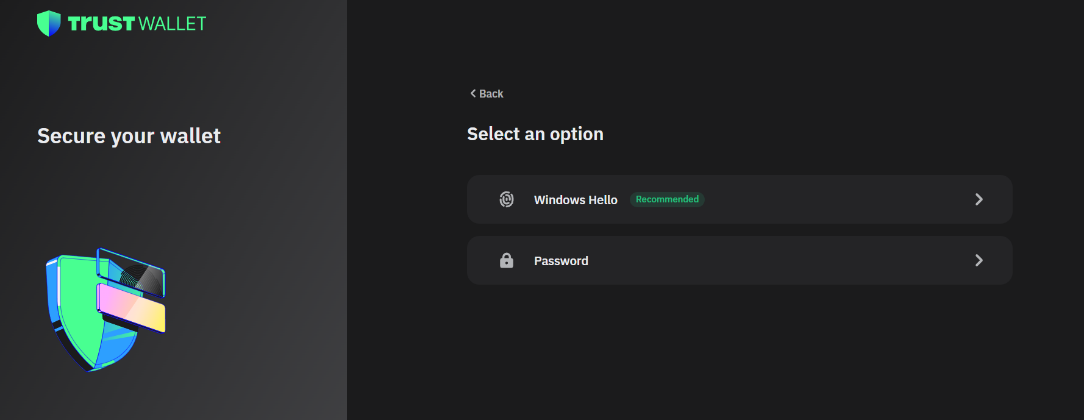
**Procedure:**

**Step 1: Download and Install Trust Wallet**



1. On your mobile device, open the official **Apple App Store** (for iOS) or **Google Play Store** (for Android).
2. In the search bar, type Trust Wallet.
3. Verify you are downloading the official app. The developer should be **"DApps Platform, Inc."**. Look for the official shield logo.
4. Tap "Install" or "Get" and wait for the application to download and install on your device.

**Step 2: Create a New Wallet**

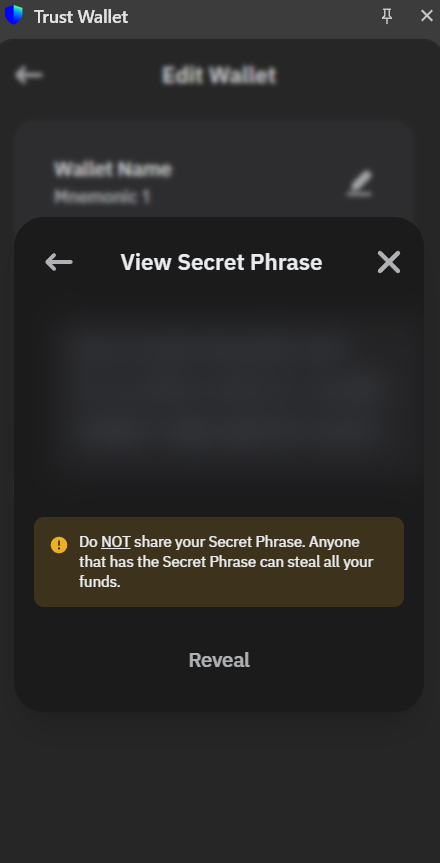
1. Open the Trust Wallet application.
2. You will be presented with two options: "Create a new wallet" and "I already have a wallet". Tap on **"Create a new wallet"**.
3. Read and accept the Terms of Service and Privacy Policy by ticking the checkbox. Tap **"Continue"**.

**Step 3: Securely Back Up Your Secret Recovery Phrase** This is the most important part of the entire process.

1. The app will display a screen with critical warnings about your Secret Recovery Phrase. Read them carefully and tick the box that says, "I understand that if I lose my secret phrase, I will not be able to access my wallet." Tap **"Continue"**.
2. Your unique **12-word Secret Recovery Phrase** will now be displayed on the screen.
3. **Immediately write down these 12 words on a piece of paper, in the exact order (1-12) they are shown.** Double-check the spelling and the order.

**CRITICAL WARNINGS:**

* + **DO NOT** take a screenshot of your phrase. If your phone is hacked, it could be compromised.
  + **DO NOT** save the phrase in a text file, in your notes app, in an email, or on any cloud storage service (like Google Drive or iCloud).
  + **NEVER** share this phrase with anyone, including support staff. Trust Wallet will never ask for it. Anyone who has this phrase can steal your funds.

1. Store the physical paper copy in a secure, offline location where no one else can find it (e.g., a personal safe, a locked drawer, or a safety deposit box). Consider making a second copy and storing it in a separate secure location.

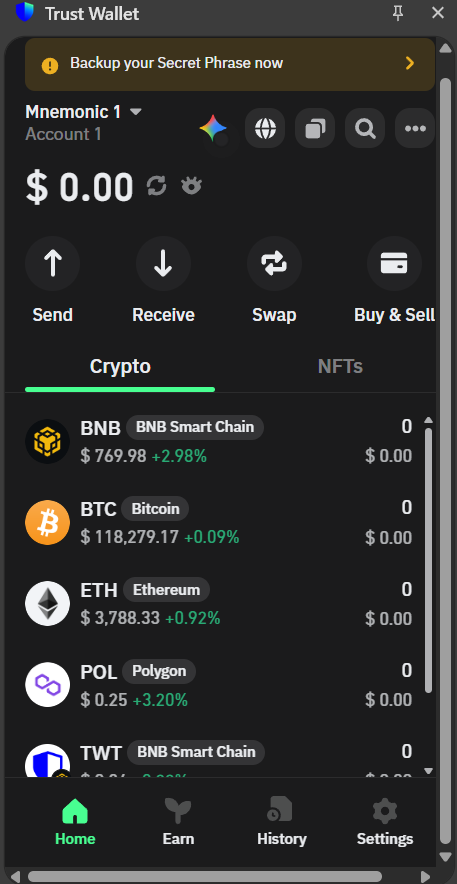
**Step 4: Verify Your Secret Recovery Phrase**

1. After you have written down your phrase and stored it, tap **"Continue"**.
2. Trust Wallet will now ask you to verify your phrase by tapping on the words in the correct sequence (from 1 to 12).
3. Tap the words in the correct order.
4. Once all 12 words are selected correctly, a "Well done!" message will appear. Tap **"Done"**.

**Step 5: Your Wallet is Ready**

1. Your wallet has now been successfully created. You will be taken to the main dashboard.
2. To find your receiving address for a specific cryptocurrency (e.g., Ethereum), tap on **"Ethereum"** from the main list.
3. Tap the **"Receive"** button.
4. A QR code and your public wallet address (a long string of characters) will be displayed. This is the address you can share with others to receive funds. You can use the "Copy" button to copy it to your clipboard.

You have now successfully set up a secure, non-custodial cryptocurrency wallet.



**Observation Table:**

 **Do** write down your 12-word Secret Recovery Phrase on physical paper.

 **Do** store that paper in a secure, **offline** location (like a safe or locked drawer).

 **Do** consider making a second physical copy and storing it in a separate secure location.

 **Do** double-check the recipient's wallet address is correct before sending any funds.

 **Do** download the wallet app only from the **official** Google Play Store or Apple App Store.

 **Do** start with small transactions to ensure everything is working as you expect.

 **NEVER** share your Secret Recovery Phrase with anyone, for any reason.

 **NEVER** take a **screenshot** of your Secret Recovery Phrase.

 **NEVER** store your phrase in a digital format (notes app, email, text message, cloud storage).

 **NEVER** enter your phrase into any website, pop-up, or Google Form. This is how phishing scams steal your funds.

 **NEVER** trust anyone in a direct message (DM) or email claiming to be from "support" who asks for your phrase or private keys.

 **Don't** click on suspicious links or connect your wallet to untrusted DApps (Decentralized Applications).

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |