



---

The Trezor Model One is the world's first hardware wallet, a device that allows its user to safely store sensitive data, such as cryptographic keys used in authentication. Invented to protect owners of Bitcoin and other cryptocurrencies, it makes it easier to manage your portfolio while greatly reducing the risk of losing coins to many common attacks, including malware and phishing.

## **How does the Trezor Model One work?**

The Trezor Model One is a portable device that holds your cryptocurrency private keys, encrypted in its flash memory. The device has no onboard power source and draws its power via the microUSB port when it is connected to a computer or phone.

To access cryptocurrency stored at a certain address you own, connect your Trezor and use the Trezor Suite interface to enter the details of a transaction. Your Trezor makes you physically confirm details about the transaction directly on its touchscreen, protecting you from common threats like keyloggers, malware or other forms of spyware.

When you are ready to send a transaction, it will show you exactly what transaction you are confirming and let you see if someone has tried to manipulate the data in any way. The private key will only be used to sign a valid transaction that has been repeatedly verified by the user and will never be exposed to the internet, with the whole signing process taking place on the device's dedicated chip.

## **Security processes and benefits**

All the core technologies that make up the Model One are open source, including its physical hardware. This allows for anyone to test and verify the code and components, allowing the Trezor to constantly react to new threats and upgrade its security.

The benefits of this process of constant community security audits is logged in detail on the Trezor security landing page, where you can browse the many bounties we have rewarded to pentesters and researchers who have responsibly disclosed security issues and helped propose a fix.

[More about security and bounties](#)

## What does a hardware wallet do?

The essential function of a hardware wallet is that it keeps your private key isolated from the internet at all times, even when signing a transaction. The Trezor Model One does this transparently with open-source code and hardware, so everyone can verify that their keys are safe on the device.

To improve usability and privacy, the Model One has many other features. These include a unique PIN entry procedure, passphrase-protected accounts, U2F and 2FA security token support, and discreet mode to protect you in the Trezor Suite app. The Trezor Model One supports over 1000 coins and tokens and can also be used in a multisignature setup for securing custody of shared funds.

### Protection from Online Attacks

Trezor hardware wallets are designed to accept only a limited number of external commands. This means that it is only capable of performing a number of functions, and always requires the user's input to do so. When sending a transaction, for example, the device will be given the destination address, transfer value, and any associated fees. It will only show the correct information used for the transaction to the user, so it is plain to see if the destination address appearing on their computer has been switched or in any way manipulated.

### Protection from Physical attacks

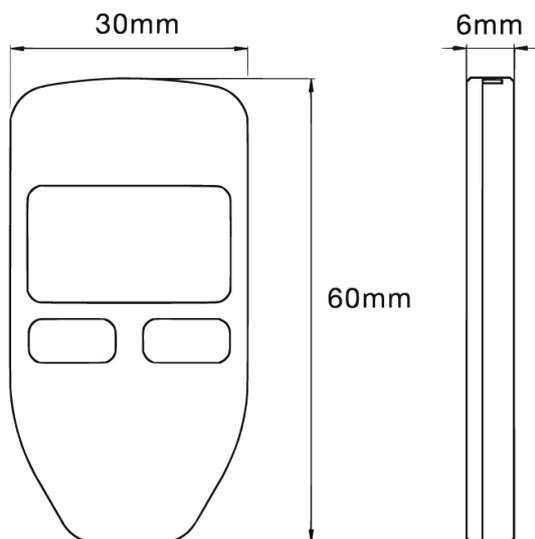
Should an attacker get their hands on your device, two protective mechanisms are in place to prevent access to your funds. Both these features can be disabled but are highly recommended.

Firstly, using a PIN to unlock the device is recommended, which stops anyone from using the device. Trezor's unique, randomized PIN entry layouts make it more difficult for anyone to observe you enter it.

Secondly, the device is protected from more advanced attacks directed at the chip itself, by a passphrase which encrypts the private seed data. Unlike the PIN, your Passphrase is not stored anywhere on the device and not vulnerable to extraction. As an extra benefit, entering the wrong passphrase will simply create an empty account, which could be used as a decoy when needed.

## Differences between the Model One and Model T

Feature	Model One	Model T
<b>Bitcoin-only firmware</b>	Yes	Yes
<b>Shamir backup</b>	No	Yes
<b>Password Manager</b>	Yes	Yes
<b>U2F authentication</b>	Yes	Yes
<b>FIDO2 authentication</b>	Yes	Yes
<b>Encryption via GPG</b>	No	Yes
<b>SSH</b>	Yes	Yes
<b>Data &amp; file encryption</b>	No	Comming soon
<b>microSD card</b>	No	Yes



---

## Where are Trezor hardware wallets sold?

The Model T is available directly from the [Trezor shop](#), as well as Amazon and through [trusted resellers](#).

## Are there accessories for the Model One?

Yes, Trezor sells a range of accessories especially for the Model One. Premium silicone cases that offer protection from scratches and impact are available in a range of colors. Trezor lanyards, which can be fixed directly to the device to let you keep your Trezor on you wherever you need it, are also for sale, as are a range of charging cables, and third-party accessories to backup your recovery seed, such as Cryptosteel capsules.