Self custodial wallet: what new users should secure before receiving crypto

Understanding the foundation of a self custodial wallet

A self custodial wallet gives you direct control over your digital assets. Unlike wallets managed by an exchange or a third-party service, a self custodial wallet puts the responsibility for security squarely on you. This means no one else can freeze your funds, restrict access, or interfere with your transactions. But it also means you must take specific steps to protect your wallet before you send any cryptocurrency to it. For newcomers, the process can feel unfamiliar, but getting the basics right from the start makes everything else much simpler.

When people first hear about self custody, they often focus on the convenience of managing their own money. But the real shift is in how you handle security. With a custodial service, the provider guards your private keys. With a self custodial wallet, you are the only one who holds those keys. That shift changes what you need to do before you receive your first deposit. You need to secure your recovery phrase, set up device-level protections, and understand how your wallet address works. Doing these things in the right order prevents common mistakes that lead to lost funds.

What is a self custodial wallet and how does it work?

A self custodial wallet is a software or hardware tool that stores the cryptographic keys needed to sign transactions on a blockchain. The wallet itself does not hold your coins; it holds the keys that prove ownership and allow you to move those coins. The most important key is the private key, which should never be shared with anyone. The wallet also generates a public address, which you can share freely to receive funds.

When you create a new wallet, the software produces a recovery phrase, also called a seed phrase. This is a set of 12 or 24 words that can regenerate your entire wallet on any compatible device. If you lose access to your wallet, this phrase is the only way to recover it. If someone else gets hold of it, they can take everything. So the first thing any new user should secure is this recovery phrase.

Secure your recovery phrase before anything else

Before you even think about sending crypto to your wallet, write down your recovery phrase on paper. Do not store it in a digital file, take a screenshot, or save it in a cloud service. If your device is compromised, a digital copy of the phrase gives an attacker full control. Write it by hand, and store that paper in a safe place. A fireproof safe or a safety deposit box works well.

Some people split the phrase into two parts and store them in separate locations, but that adds complexity. For most users, one secure physical copy is enough.

Do not share your recovery phrase with anyone. No legitimate service, support team, or wallet provider will ever ask for it. If someone contacts you asking for your phrase, it is a scam. Also, avoid typing it into any website or app, even if it looks official. The only time you should enter the phrase is on the wallet software itself, and only when you need to recover access.

Set up device security and biometric locks

Once your recovery phrase is safely stored, turn your attention to the device that runs your wallet. Whether you use a mobile app or a desktop application, the device itself is a potential weak point. Install the latest operating system updates, enable a strong screen lock, and consider using a biometric lock if your device supports it. Biometric locks, such as fingerprint or facial recognition, add a layer of protection that is hard for thieves to bypass.

Many self custodial wallets allow you to enable additional security within the app itself. For example, you can set a PIN code that must be entered before the wallet opens. Some wallets also let you require a biometric check for every transaction. Turning on these features means that even if someone gets hold of your unlocked phone, they still cannot move your funds without your fingerprint or face.

Understand your wallet address and how to use it

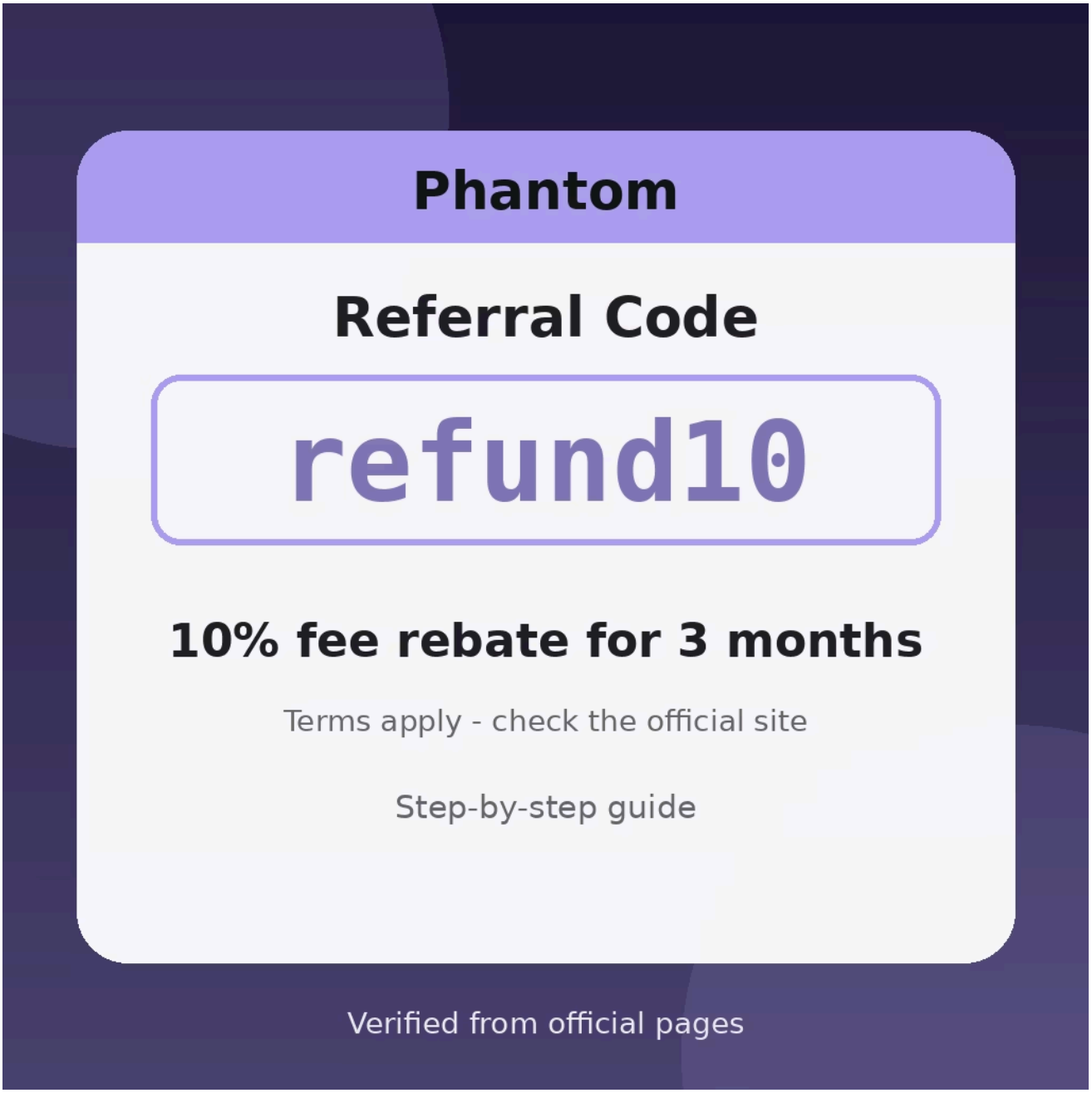
Your wallet address is a long string of letters and numbers that identifies your account on the blockchain. You generate this address from your public key, and you can share it with anyone who wants to send you crypto. But addresses can look similar, and a small typo can send funds to the wrong place. Always copy your address directly from the wallet app, and paste it into the sending field. Never type it manually. Many wallets also display a QR code that you can scan to avoid errors.

Some blockchains support multiple address formats. For example, Ethereum and Bitcoin use different formats, and within Ethereum there are both "0x" addresses and ENS names. Before you share your address, confirm that it matches the blockchain your sender is using. Sending Bitcoin to an Ethereum address, or vice versa, usually results in lost funds. A self custodial wallet typically shows which network each address belongs to, so check that before you give it out.

Make a backup copy and test your recovery

Having one backup of your recovery phrase is good; having two is better. Consider making a second handwritten copy and storing it in a different secure location. If one copy is destroyed

in a fire or flood, the other still exists. Avoid digital backups like photos or text files. Even encrypted digital files can be compromised if your device is hacked.



Before you deposit any significant amount, test your recovery process. Do this by uninstalling the wallet app and reinstalling it, then using your recovery phrase to restore the wallet. This confirms that your phrase is correct and that you can regain access. It also helps you spot any mistakes in the words you wrote down. If the recovery fails, you have time to fix the issue before you put funds at risk. Many tutorials on gamma.app walk through the exact steps of recovering a wallet, which can be helpful for first-timers.

Consider a hardware wallet for larger amounts

A self custodial wallet that runs on your phone or computer is called a hot wallet, because it is connected to the internet. Hot wallets are convenient for daily use, but they are more vulnerable to malware and phishing attacks. If you plan to hold a meaningful amount of crypto, consider moving it to a hardware wallet. A hardware wallet is a dedicated device that stores your private keys offline. It signs transactions only when you physically confirm them, so even if your computer is infected, your keys stay safe.

Hardware wallets cost money, but they are one of the most secure options available. They work with many wallet interfaces, so you can still use the same app you are familiar with. The device itself generates and stores your recovery phrase, and you back it up the same way: on paper. For long-term storage or larger balances, the extra cost is worth the peace of mind.

Watch out for phishing and fake apps

Scammers know that new users are eager to get started. They create fake wallet apps that look like the real thing, and they set up phishing sites that steal your recovery phrase. Always download wallet software from the official app store or the developer's verified website. Check the number of downloads, read recent reviews, and look for a verified developer badge. If something feels off, it probably is.

Never enter your recovery phrase into a website, even if it claims to be a wallet recovery service. Legitimate wallets never ask for your phrase outside of the app itself. Also, be cautious of browser extensions that claim to improve your wallet. Some are malicious and can drain your funds. Stick to well-known wallets that have a track record of security.

What receiving crypto means for your privacy

When you receive crypto, your public address is recorded on the blockchain. Anyone can see that address and its transaction history. If you reuse the same address for every deposit, it becomes easy for others to track your holdings. Many wallets generate a new address for each transaction, which helps preserve privacy. You can use any of your past addresses to receive funds, but using a fresh one each time is a good habit.

Some blockchains, like Bitcoin, are pseudonymous, meaning your real identity is not directly tied to your address. But if you ever link your address to your name, for example by posting it on social media or using it on an exchange, your privacy is reduced. Be mindful of where you share your address and what information you pair with it.

Final checks before your first deposit

Before you hit send on your first transaction, double-check that your wallet is fully set up. Confirm that your recovery phrase is written down and stored safely. Make sure device security

features are enabled. Test the recovery process if you have not done so already. Verify the address you are sending to, and confirm the network matches. A small test transaction is a wise move. Send a tiny amount first, wait for it to arrive, and then send the rest. This confirms that everything works and that you are comfortable with the process.

Self custody is a shift in mindset as much as a technical step. You take on responsibility that was previously handled by someone else. But the freedom that comes with it, the ability to control your own funds without asking permission, is worth the effort. With the right preparations, you can receive your first crypto with confidence, knowing that your assets are secure and accessible only to you.