What to Do When Your Seed Has Been Compromised

Jeff Hong ⋮ 3-4 minutes

October 24, 2021

What is a compromised seed?

A compromised seed is one that has been exposed or has the potential to be exposed by a third party (in other words, if someone else has seen it or someone might be able to see it in the future).

Exposed is self-explanatory:

- You took your seed out and someone saw
- Someone else found your seed
- You entered your seed in a malicious software application or website

The potential to be exposed is a bit more vague. It means that there is **a higher possibility or chance** your seed might be seen by someone else.

The most straight forward example of this is losing a copy of your seed and the potential someone else finds it in the future.

A more unconsidered example of this is entering/typing your seed on device connected (or has been connected) to the internet. This can include your computer or your phone.

The potential comes from the possibility there is malicious software on the device (key loggers, screen captures) that can copy your seed and send it to a third party. There is also the possibility that a third party can gain access to your device in the future and is able to obtain your seed.

Thus, a seed generated on an internet-connected device (by default) has the potential to be exposed.

So what do you do if your seed has been compromised?

The best thing to do is to send your coins to a newly generated seed.

Even if you think the potential to be exposed is low but it's still in the back of your mind, it's better to send your coins to a new seed. It's psychological relief and will let you sleep at night.

How do I do this?

There are many ways but we'll share the most straight forward.

Send your coins to an exchange (of your choosing) and back to a new wallet (this will incur fees twice):

1. Generate and copy a receiving address from your exchange account.
2. Send your coins to the exchange receiving address (incur fees).
3. Ensure you see your coins in your exchange account completely transfer over.
4. Reset your wallet device.
5. Create a new wallet (on the same device) and generate a new seed.
6. Copy down your new seed.
7. Generate and copy a receiving address from your new wallet.
8. Send your coins to the receiving address from the new wallet (incur fees).
9. Ensure you see your coins in your exchange account completely transfer over to your new wallet.
10. Dispose of your old seed.

Send your coins directly to a new wallet (this will incur fees once):

1. Ensure you are able to and have experience in successfully restoring your wallet with your seed.
2. Reset your wallet device.
3. Create a new wallet (on the same device) and generate a new seed.
4. Copy down your new seed.
5. Generate and copy a receiving address from your new wallet.
6. Reset your wallet device again.
7. Restore your old wallet with your old seed.
8. Send your coins to the receive address from the new wallet (incur fees).
9. Reset your wallet device again for the second time.
10. Restore your new wallet with your new seed.
11. Confirm your coins transferred to the new wallet.
12. Dispose of the old seed.

Note: It is imperative you are comfortable restoring your old seed since you'll be resetting the device before moving your funds. If you never tested or restored your seed before, this is not recommended.