Bitcoin Safety Checklist

Before you do anything with Bitcoin.

The Golden rules

NEVER:

- Never share your **seed phrase** with anyone. If someone asks for your seed phrase, assume they are trying to steal your Bitcoin.
- Never photograph your seed phrase.
- Never screenshot your seed phrase.
- Never store your seed phrase in notes, email, cloud storage, a password manager, or any internet-connected device.
- Never type your seed phrase into a computer or phone simply because a website/app tells you to.
- Never send Bitcoin because someone claiming to be "support" tells you to.
- Never trust an address displayed only on your computer; verify it on your hardware wallet when possible.
- Never rush a Bitcoin transaction.
- Never assume a transaction can be reversed.

ALWAYS:

- Verify.
- Read what your hardware wallet is asking you to sign (ex: check sending address).
- Keep your seed backup offline.
- Test your backups.
- Use small amounts while learning.
- Double-check addresses and amounts.
- Download wallet software from the official source and verify it when practical.
- Keep your setup understandable enough that you can recover it yourself.

Be extremely suspicious of:

- Unsolicited DMs
- "Wallet verification”
- "Seed synchronisation”
- Fake firmware updates

- Giveaway doubling schemes
- Recovery services asking for your seed
- People impersonating wallet manufacturers
- Fake wallet software downloads
- Search advertisements impersonating legitimate websites
- Anyone creating urgency
- Anyone asking you to screen-share while your seed/private information is visible

1. Creating a new wallet

Before you begin

- For meaningful savings, prefer a reputable open-source hardware wallet or another properly designed offline signing device.
- Obtain hardware wallets from the manufacturer or a trusted source.
- Download the wallet software from the official website.
- Verify software downloads/signatures when possible.
- Make sure you're in a private environment.
- Check for cameras: phones, laptops, webcams, security cameras, smart-home cameras, etc.
- Make sure the seed is generated on your device.

Generating the seed

- Generate the seed using the hardware wallet/offline method you have chosen.
- Write the seed words down **in the exact order shown**.
- Check every word carefully.
- Never photograph the seed.
- Never read the seed aloud around microphones/voice assistants.
- Never copy it into your computer clipboard.
- Never send it to yourself.
- Never print it using a normal network-connected printer.
- Never type it into a website.

Before depositing Bitcoin

- Verify your backup.

- Perform the wallet's **seed/recovery backup check** before relying on it.
- Understand whether you're using a passphrase.
- If using a passphrase, understand that **a different passphrase creates a different wallet** and that losing it can mean losing access to the intended wallet.
- Generate a receiving address.
- Verify the address on the hardware wallet's own screen.
- Consider sending a small test amount first.

2. Storing your seed phrase

Your seed phrase gives complete access to all the Bitcoins it controls.

Someone who obtains your seed phrase can then reconstruct your wallet and be able to take your Bitcoin **without possessing your hardware wallet**.

DO:

- Keep the seed completely offline.
- Store it somewhere protected from unauthorised access.
- Consider fire/water-resistant backup methods for significant holdings.
- Consider geographically separated backups when appropriate.
- Make sure your backup can actually be read years from now.
- Periodically make sure the backup still exists and is legible.
- Have an inheritance/recovery plan appropriate to the amount being secured.

DON’T:

- Take a photo.
- Store it in iCloud/Google Drive/Dropbox.
- Put it in notes.
- Email it to yourself.
- Store it in a normal text file.
- Send it through WhatsApp/Signal/Telegram.
- Tell “support."
- Enter it into a website offering to "verify" or "validate" your wallet.
- Keep your only backup somewhere vulnerable to the same fire/theft/disaster as your hardware wallet.

3. Restoring a Wallet

Before entering a seed anywhere:

- Ask yourself why the seed needs to be entered.
- Confirm you are using a trusted recovery process.
- For hardware wallets that support device-side recovery, enter the seed **on the hardware wallet itself**, not into a computer/website.
- Check for cameras.
- Make sure you're in a private environment.
- Make sure nobody is screen-sharing or remotely connected to your computer.

NEVER enter your seed because:

- Your "wallet needs verification."
- Your account is supposedly “locked."
- Someone from "support" requested it.
- You received an email saying your wallet needs upgrading.
- A website wants to "synchronise" your wallet.
- Someone DM'd you offering help.

4. Receiving Bitcoin

Before giving someone an address

- Generate a fresh receiving address when practical.
- Verify the address on your hardware wallet screen.
- Make sure you're using the correct Bitcoin network.
- Copy the address carefully.
- If communicating the address digitally, consider verifying part/all of it through another trusted channel for large payments.

After receiving

- Check that the transaction actually appears in your wallet.
- Understand the difference between **unconfirmed** and confirmed Bitcoin.
- For meaningful payments, wait for an appropriate number of confirmations (at least 6) before treating the payment as final.
- Remember that an address appearing in a block explorer does not by itself prove that **you control its private key**.

Privacy

- Remember that Bitcoin's blockchain is public.
- Avoid unnecessary address reuse.
- Be careful about revealing addresses alongside your identity.
- Understand that combining UTXOs can reveal relationships between previously separate coins.

5. Sending Bitcoin

Before pressing send, verify:

- Recipient - Who am I actually paying?
- Address - Does the address displayed on my hardware wallet match the intended recipient address?
- Amount - Am I sending 0.01 BTC or 0.1 BTC?
- Network - Am I actually making the type of payment I intend to make? (Ex: Segwit or Taproot?)
- Fee - Is the transaction fee reasonable?
- UTXOs - Do I understand which coins I'm spending?
- Change - If your wallet shows change information, does the transaction make sense?

NEVER:

- Trust only the address displayed on your computer.
- Copy an address and immediately click Send without checking it.
- Send because somebody is pressuring you.
- Assume "support" can reverse the transaction.
- Sign something you don't understand.

For large transactions, consider sending a small test payment first.

6. Passphrase

A Bitcoin wallet passphrase is not simply a password protecting your seed backup.
Different passphrase ➡ different wallet.

Before using one:

- Understand exactly how your wallet implements passphrases.
- Use something with sufficient entropy for your threat model (We have a template available to create entropy offline using dice).
- Verify you can reproduce it exactly.
- Understand capitalisation, spaces and characters matter.
- Verify the resulting wallet/address before depositing significant Bitcoin.

- Have a recovery strategy for the passphrase.

NEVER:

- Assume forgetting the passphrase can be fixed with the seed alone.
- Use a passphrase you aren't confident you can recover.
- Deposit significant Bitcoin before testing recovery.

7. Multi-signature wallet

Three seed phrases alone do not necessarily constitute a complete, convenient multisig recovery plan.

Before depositing Bitcoin:

- Understand the signing threshold (ex: 2-of-3 or 3-of-5?)
- Verify every hardware wallet/key.
- Back up all required wallet configuration information, not just seeds.
- Keep copies of the wallet descriptor/configuration.
- Test spending.
- Test recovery.
- Store keys/backups so one incident can't destroy enough keys to make the wallet unrecoverable.

If you need a second opinion before taking action, don’t hesitate to contact us.