Cryptocurrency security and safety best practices

Digital currencies are by nature… well, digital. This is a good thing because it enables the encoding and flexibility that make cryptos appealing

However it comes at the cost of being accessible from the internet, and therefore vulnerable to the same security threats as anything else on the web.

Anytime you are online, take steps to protect yourself, your information, and your money. The following is a list of the Top 10 security measures you should heed to protect your investments.

1. **Update Your Devices.** It is vital that your computer and electronic devices are current with the latest updates, especially if you're running Windows / iOs or

Android. Occasionally a new virus will surface that exploits an operating system security hole, and in turn, an update is created to patch this security gap. Without these updates, your operating system will not be able to protect you.

2. **Use Anti-Virus Software.** This software is designed to detect and remove viruses and other malicious software. It is absolutely critical to have this installed and kept up-to-date. There are several different companies that offer antivirus software for free, such as AVG, Avast, and Kaspersky. You can also get a paid version for advanced functions like daily system scans.
3. **Use Anti-Malware Software.** This software protects you from malicious infections such as keyloggers, spyware, and adware that a virus scanner might not find. It is recommended that you have at least one anti-malware program installed, and a second one is a good idea too because the scan results may differ between the programs. Some popular options are Malwarebytes, SuperAntiSpyware, and Spybot.
4. **Utilize Firewalls.** Firewalls let you control the incoming and outgoing communications from your computer to various applications. You can set the firewall to allow known applications like Exodus wallet or Adobe Updater to communicate freely to an IP address or domain while blocking any incoming communication from unknown IP addresses. Firewalls help prevent malicious attacks to your system by catching them before they get in. Windows has a built-in firewall, which is an acceptable option, but there are several other free applications that are easier to use and have better features. Examples are Comodo Firewall and AVS Firewall.
5. **Consider a VPN.** A Virtual Private Network (VPN) is a secure service to safely and anonymously access the internet. VPNs create a private tunnel that ensures no one can see what websites or servers you are exchanging data with, and some allow you to change your IP address to a different region around the world so that

it looks like you are accessing the internet from a whole different country. VPNs can also help prevent hackers from attacking your device at your real IP address. There are many free VPN services available, but these are limited in terms of their functionalities. Some of the best, paid options include NordVPN, PureVPN, and HMA.

6. **Choose Brave Browser.** Using the right web browser can have a huge effect on your overall online security, so it’s a good idea to choose one that is easy-to-use and extensible. Brave Browser has Adblocks and it is also private. Always bookmark the web address of each exchange so you can prevent phishing. There are many Browser extensions that can enhance your security and protect you from unwanted ads, trackers, popups, etc Some examples include Adblock, Ghostery, DotVPN, and LastPass. Remember, if you come across a suspicious ad, banner, or website: do not click on it! If you accidentally do, close the browser window immediately or kill the program using **Task Manager**.

7. **Always Backup!** Whether it’s your personal documents, pictures, or private keys, backing up your data is essential. From your hard drive crashing to dropping your phone in the toilet (my 4 year old actually did this) anything can happen to your device, so you should prepare for the worst. There are two main solutions to consider:
    1. **Local** – While hard drives are generally very reliable, they do sometimes fail. So storing the data on your local hard drive and/or an external backup is an important step in your security, but is not always sufficient unless you use a RAID system for your backup. RAID utilizes multiple hard drives to store all of the data simultaneously, so if one hard drive fails, the data is still saved on the remaining drives.
    2. **Cloud** – RAID systems are expensive, so the next best option is backing up your data on the cloud. This way, even if your hard drive crashes all of your information will still be accessible. However, this also presents a security

issue. **Anyone who gains access to your cloud account would gain access to your files, so you might want to password encrypt them as well.** Free, albeit limited, options for cloud storage include Google Drive, Apple iCloud, while some paid cloud solutions include IDrive, Carbonite, and Acronis.

8**. Backing Up Private Keys.** A simple way to keep track of your private keys is to create a new document for each one. Copy and paste the wallet address, private key and QR code into the document. Save and store it in a safe place. Additionally, you should consider locking that folder with a password or compiling your documents into a password protected zip file. But even these could theoretically be hacked, so another option is to print those documents and create paper wallets, laminate them, and store in a safe or deposit box. However, a hardware wallet like the Ledger is the most secure way to protect your cryptocurrency assets.

9. **Use Two Factor Authentication (2FA).** 2FA is an extra layer of security that requires a piece of information beyond just a username and password to log into an account. It's among the easiest and most powerful steps you can take to protect your online accounts. Many exchanges either offer or require 2FA to log in and make withdrawals. The most popular version of this is called a time-based one-time password (TOTP), which creates a unique 6 digit code that resets every 60 seconds. The code is generated by an app, such as Google Authenticator. Download the app, scan the QR code from that website you will be logging in to, and a code generator for that site will automatically be added to your app. Be sure to take note of your 2FA secret key before going any further. It is usually located near the QR code on the same page and lets you restore the same 2FA access on a different device if you lose your current one.

> You should also consider enabling 2FA for your Google and Facebook accounts, just in case there is any personal information on those platforms that could compromise your crypto assets. The amount of information to process and protect in today's digital world can seem daunting at times. But if you take the time to set up these various tools and secure your cryptocurrency assets, you can rest easy knowing that your devices and data are secure.

10. **Do Not Store Your Coins on an Exchange.** Unless you are planning to actively trade on an exchange, it is generally a bad idea to store your coins on an exchange. Exchanges can be and have been, hacked — just look at Mt. Gox and Bitfinex. Without proper security on your end, your account on the exchange can be hacked through a personal device or even a simple phishing scam. Governments can seize whole exchanges, and there is no guarantee that you would be able to reclaim your coins if that happens. An exchange called BTC-e was seized on suspicion of activity related to the Silk Road and other dark web marketplaces. Lastly, users can have their accounts suspended for a variety of reasons, and are not always able to retrieve their coins.

Buying a Nano Ledger S or Trezor is a better alternative.

Also only buy it from the official website.

Regardless of the size of your investment, the risk of losing your coins is not worth the convenience of leaving them on an exchange. Having your own private wallet(s) where you control the private key is truly the best way to protect your long-term investments.

If you do decide to keep your coins on exchanges, please follow these best practices to lower your risk:

- Enable all security mechanisms (2 Factor Authentication, IP whitelisting, using secure encrypted email like protonmail.com, using extra email confirmation, turning ON all security options on exchanges etc.).
- Distribute your coins across multiple exchanges.
- Only keep as many coins on the exchanges as you are comfortable losing

Implement all 10 of these cryptocurrency security recommendations and you'll be in good shape.