7

Safety Precautions.

Before you get some crypto in your hot little hands, you need to ensure that it doesn't slip out of your hot little hands. I'm talking about hackers and scammers.

It's very simple. Take five actions in advance, and if you do, you'll be protected from 99% of the criminals out there. (I'll show you how to protect yourself from the final 1% in →CHAPTER15: "*CRYPTO IS FULL OF SCAMMERS*")

Do not skip this chapter!

1. HAVE A GOOD ANTIVIRUS APP

You probably don't have an antivirus app installed on your smartphone. No matter whether you use a smartphone or tablet, desktop or laptop computer, you need to have a good antivirus app installed.

Crucially, it needs to have *realtime protection*. Some of the free ones don't.

It also needs to be particularly good at handling spyware. Do a websearch for 'best antispyware with keylogger protection'. Spyware is a hidden program on your device which can record what you're doing. The most dangerous kind of spyware is a *keylogger*. This records everything you

type, including your PIN number.

Spyware isn't a crypto problem *per sé*. It can compromise your Visa or Apple Pay transactions too. The difference is that, with credit cards, you have some kind of safety net. Maybe the bank will reimburse losses. With crypto, you're screwed. The responsibility is all on you.

2. GET AN E-MAIL ALIAS.

You need an e-mail alias.

Actually you need a new e-mail address too, one for just crypto websites and apps.

In theory, you could use your existing address with an alias. However, in practice, your existing address will be spread all over social media.

To get a new e-mail address:

1. At `tuta.com` >Create Free Email Account
2. Proceed through the various steps; they are self-explanatory.
3. Write your password on a piece of paper and keep it hidden well.

I recommend **Tutamail**, but you can use whichever e-mail service tickles your fancy. One advantage of Tutamail is that it does *not* have password recovery. If you lose your password, you're screwed. Why is this a good thing? It cuts out the easiest way hackers get into accounts nowadays. Hackers used to try to trick you into revealing your password. Now they simply go to the website and click on 'forgotten password' with your e-mail address.

To get an alias:

1. Sign up to `simplelogin.io`. (Use your new e-mail address)
2. Verify with the weblink that SimpleLogin sends to the e-mail you entered in step 1.
3. Login to `simplelogin.io`.
4. >Create New Alias

5. In the upper left box, type in any name you wish.
6. In the upper right box, choose your domain, e.g. `@simplelogin.com`
7. >`Create`
8. When you receive an e-mail from someone who uses this alias, just reply as usual– it will automatically use your alias.

When asked for an e-mail address, just use your alias.

The alias is the key to protecting yourself from hackers and scammers. No one can log into an alias. If a hacker finds out your alias somehow, then it's useless to him or her. Only the good people at `simplelogin.io` know that your alias goes to your real address.

It's like a criminal finding out your home address, supposedly, but going there only to find that there is no such street.

It works so long as never publish your new **Tutamail** address anywhere. Only use an alias (or three, or four...)

3. TURN ON ERASE AFTER FAILED ATTEMPTS ON YOUR PIN

If someone steals your phone, he or she can try every PIN combination and break into your phone within a few days. Then, repeat with your crypto app. True, by this time, you might have used a 'Find my phone' feature. But I think the simplest solution is best. It covers extreme situations.

Make it so after a certain number of incorrect PINs, your phone is wiped. You can easily reinstall your crypto app later [→CH.14].

Apple iphones:

`Settings`, >`Touch ID & Passcode`, >`Toggle grey→green Erase Data`

(Note that on newer iphones, it's 'Face ID & Passcode')

Android phones:

Download and install Zygote's **Locker** app.

4. TURN OFF ONLINE STORAGE FOR YOUR DEVICES.

By 'online storage' I mean iCloud, Google Drive, Samsung Cloud, Microsoft Onedrive, or whatever is built into your devices. All these services think they are being helpful by being on by default. To some extent they are, because losing all your data when your phone falls in the toilet is a bummer.

Nevertheless, this is a major security risk. Basically, you will be blissfully unaware that despite all your security procedures (see previous step), your iPhone or Mac or Samsung or whatever will be uploading private information in the background.

Hackers know this very well and have programs to scan your iCloud, Google Drive etc. Once they have broken into your account, they *always* check your online storage within seconds.

Here's the basics for each kind of online storage.

How to turn off **iCloud** on an **iPhone**:

1. Settings, >[your name]
2. >Sign Out
3. Confirm by accepting a few more 'Turn Off'? Questions.
4. >Toggle grey→green any switches for data you wish you save on your device. Otherwise your data will be deleted.
5. > Sign Out

How to turn off **iCloud** on a **Mac**:

1. System Settings, >Internet Accounts, >iCloud
2. Turn off iCloud Drive, iCloud Mail, Passwords & Keychain
3. Turn off 'Access iCloud Data on the Web'
4. Account Storage >Manage
5. Delete data from iCloud Drive, iCloud Mail,

Passwords & Keychain.

How to turn off **Google Drive** on **Windows:**

1. In a webbrowser go to drive.google.com. Sign in.
2. For any files you want to keep >[Download button]. (It looks like an arrow pointing down to a tray). Save these on a USB drive or SD card.
3. Delete all files and sign out.
4. In the Windows tray, bottom right, find your Google Drive app– it looks like a green, yellow, and blue triangle. Click it.
5. >[Cog Symbol]
6. >Preferences
7. >[Cog Symbol]
8. >Disconnect Account

How to turn off **Google Drive** on an **Android smartphone:**

1. Repeat steps 1-3 from just above.
2. Open the Google Drive app.
3. >[Profile Picture] (on the top right)
4. >Manage Accounts On This Device
5. >Remove From This Device

How to turn off **Samsung Cloud** on an **Android smartphone.**

1. Use the My Files app to back up anything important to a Micro SD card.
2. Go to Settings (cog icon)
3. >Accounts & Settings
4. >Backup Data

5. >Toggle blue→grey off for all.
6. Note: For step 4, it might say >Samsung Cloud
7. Go back to step 3.
8. >Accounts
9. >[Your Samsung Account] (e-mail address)
10. >Personal Info
11. >[Three Vertical Dots]
12. >Sign Out
13. Verify this action by responding to the e-mail.

Note that this will also remove the function to find your phone if it's lost. You might want to weigh up the pros and cons of this. Check out preyproject.com for an alternative.

How to turn off **Microsoft One Drive** on **Windows**:

1. Right click on the One Drive app. (White cloud in bottom right)
2. >Settings
3. >Unlink PC
4. Open your web browser. onedrive.live.com. Sign in.
5. Tick the files to delete.
6. >Delete

Never just assume your online files are useless.
Back them up anyway!

5. ALWAYS USE A VPN.

Buy a good VPN (*Virtual Private Network*) and use it always when using crypto apps.

Think of using a VPN like using a P.O. box. It hides your real address.

You have probably entered your postal address a few times online, e.g. on Amazon. What's the risk here? This is different. Your computer advertizes a computer address (*IP Address*) for everything you do online. You have no control. It's like walking around in a t-shirt advertizing your home address. A VPN puts another t-shirt over the top with a fake address.

Lately, it's become trendy to bash VPNs. There's no shortage of clickbaity Youtube videos claiming that VPNs are next to useless. I certainly wouldn't put the family jewels in the hands of a VPN.

A VPN is nevertheless necessary because your real, physical location is at risk otherwise. It's not easy, but your IP address can be matched to your street address. Better to be safe than sorry. It's best to protect yourself against the unlikely event that some criminal finds out your street address via your IP address. VPNs mask your IP address.

It's important to clarify something. In step 2 above, I wrote:

> *It's like a criminal finding out your home address, supposedly, but going there only to find that there is no such street.*

The process I'm describing here with VPNs is kind-of the opposite. I'm describing the process whereby the criminal does find your real world location. (He or she doesn't know anything else about you at that stage). As I said, it's very rare, but the criminal could geolocate a crypto-user down to a handful of houses and then investigate who lives there. A VPN prevents such a geolocation. On a map, your'e going to look like you live in Switzerland or Latvia or somewhere like that.

Get in the habit of turning on your VPN every time you do

anything with crypto.

While you're at it, turn on the built-in features which limit tracking. These obscure certain parts of your smartphone which are easy to identify. For iPhones, Private WiFi. For Androids, Use Randomized Mac.

These settings help especially when you're out and about. It's analagous to putting your wallet in your front pocket rather than back pocket. Not great security, but better than not. The exact wording of these settings changes with different versions of iOS or Android, so best do a websearch.

Do your own research with VPNs too. Look for a VPN with a strict 'no log' policy, and check that this policy has been audited by a reliable third party. Logs render you vulnerable to inside jobs. Avoid free VPNs. They're free for a reason and it's contrary to your interests.