November 2020

Digital Security Tips for Hong Kongers

CHINESE HUMAN RIGHTS DEFENDERS

Copyright © Chinese Human Rights Defenders 2020

There is *no perfect way* to protect yourself online.

No tool can completely protect you. However, you can adopt some tools and behaviors to try and mitigate some risks.

Copyright © Chinese Human Rights Defenders 2020

Some Questions to Ask Yourself

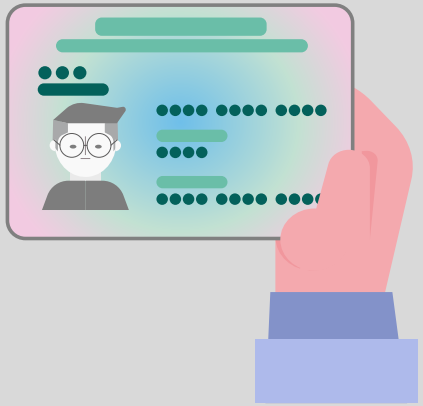
- What do I want to protect?
- Who do I want to protect it from?
- How bad are the consequences if I fail?
- How likely is it that I will need to protect it?
- How much trouble am I willing to go through to try to prevent potential consequences?

More on how to develop a personal security plan from Electronic Frontier Foundation (English):
https://ssd.eff.org/en/module/your-security-plan

Copyright © Chinese Human Rights Defenders 2020

Risks in Hong Kong

Hong Kong has high physical security risks, which make digital security risks greater as police can obtain devices and/or physically force access.



Police can **stop and search** anyone on the street for no cause to check ID

Police can **search properties without a warrant** under the new National Security Law's implementing rules

Authorities can **prevent** a person suspected of "endangering national security" **from leaving Hong Kong**

Copyright © Chinese Human Rights Defenders 2020

Surveillance Risks

Your phone is a **tracking device**.

It always sends location info to the phone company.

Police can likely access that data.

GPS/location services can store data on where you have travelled on your phone including metadata on photos.

If you are detained, **police could access it and know your movements**.

Copyright © Chinese Human Rights Defenders 2020

Tips to Protect Yourself

Try to limit your use of your phone.

- View it only as a communication device.
- Don't save a lot of messages and emails on it.
- Don't download or store sensitive files on it.

Use strong end-to-end encrypted apps with disappearing messages.

For extra sensitive trips, consider leaving your phone at home or covering it with a faraday bag/two layers of aluminum foil.

Copyright © Chinese Human Rights Defenders 2020

8 Tools for your Digital Security

Passcode

Password Manager

Virtual Private Network (VPN)

Encrypted Messaging Apps

Secure Email – Protonmail

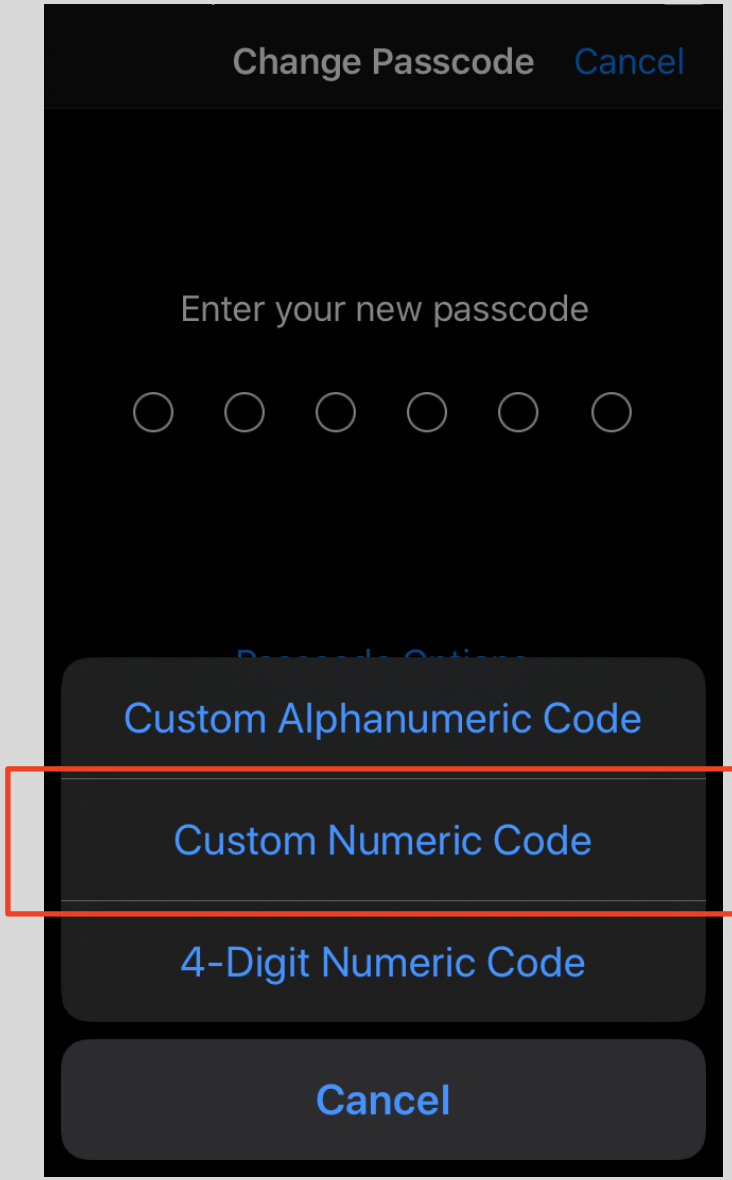
Encryption – Files and Cloud Storage

Delete Files

Advanced – GPG Encryption

Copyright © Chinese Human Rights Defenders 2020

01 Passcode *iPhone*



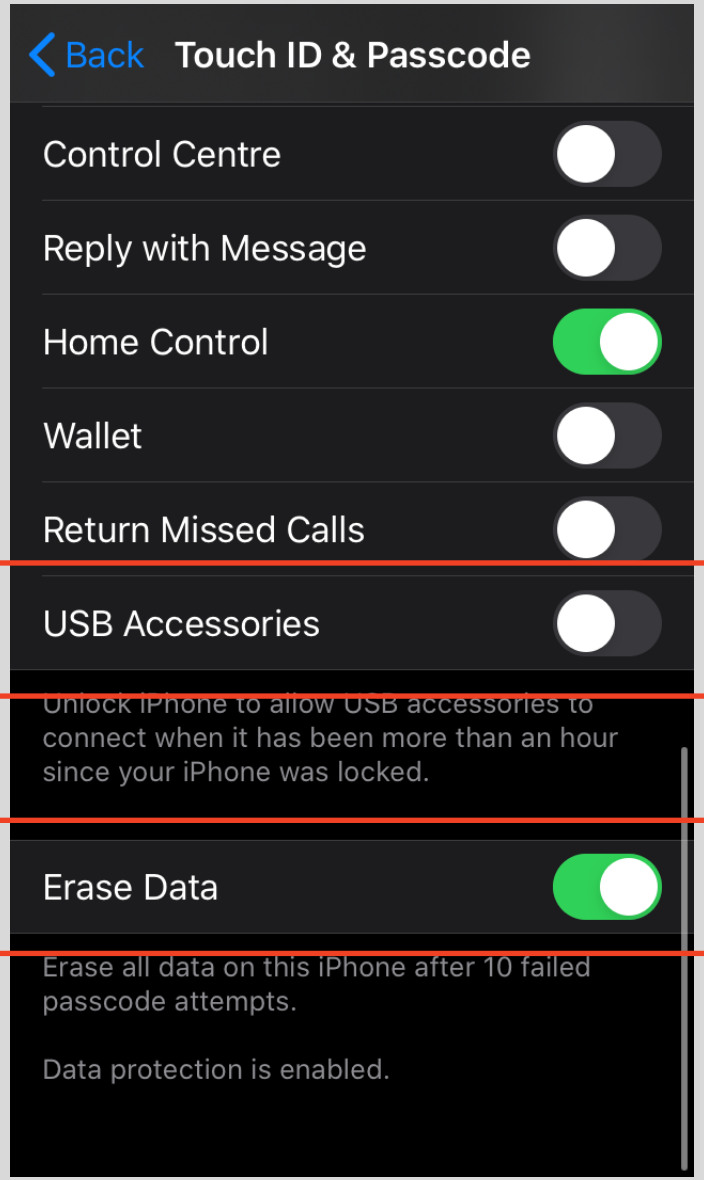
Do not use face recognition and Touch ID as they can be easily used to open your device

Change your passcode to over six-digit (ideally 10 digits).

If have iPhone 5S or later, full disk encryption is automatically turned on once you have added a passcode.

Copyright © Chinese Human Rights Defenders 2020

01 Passcode *iPhone*

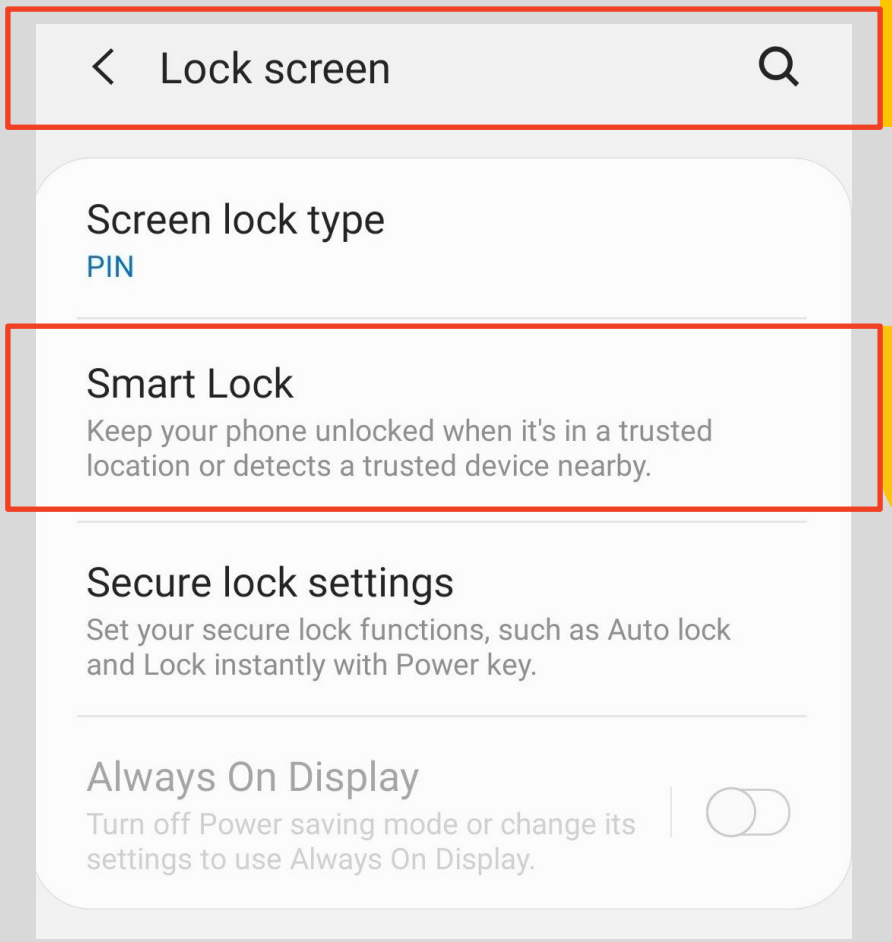


Make sure USB Accessories is ***toggled off*** to prevent access to your device through a USB cable

Can set up phone to erase all data after 10 failed passcode attempts

Copyright © Chinese Human Rights Defenders 2020

01 Passcode
Android

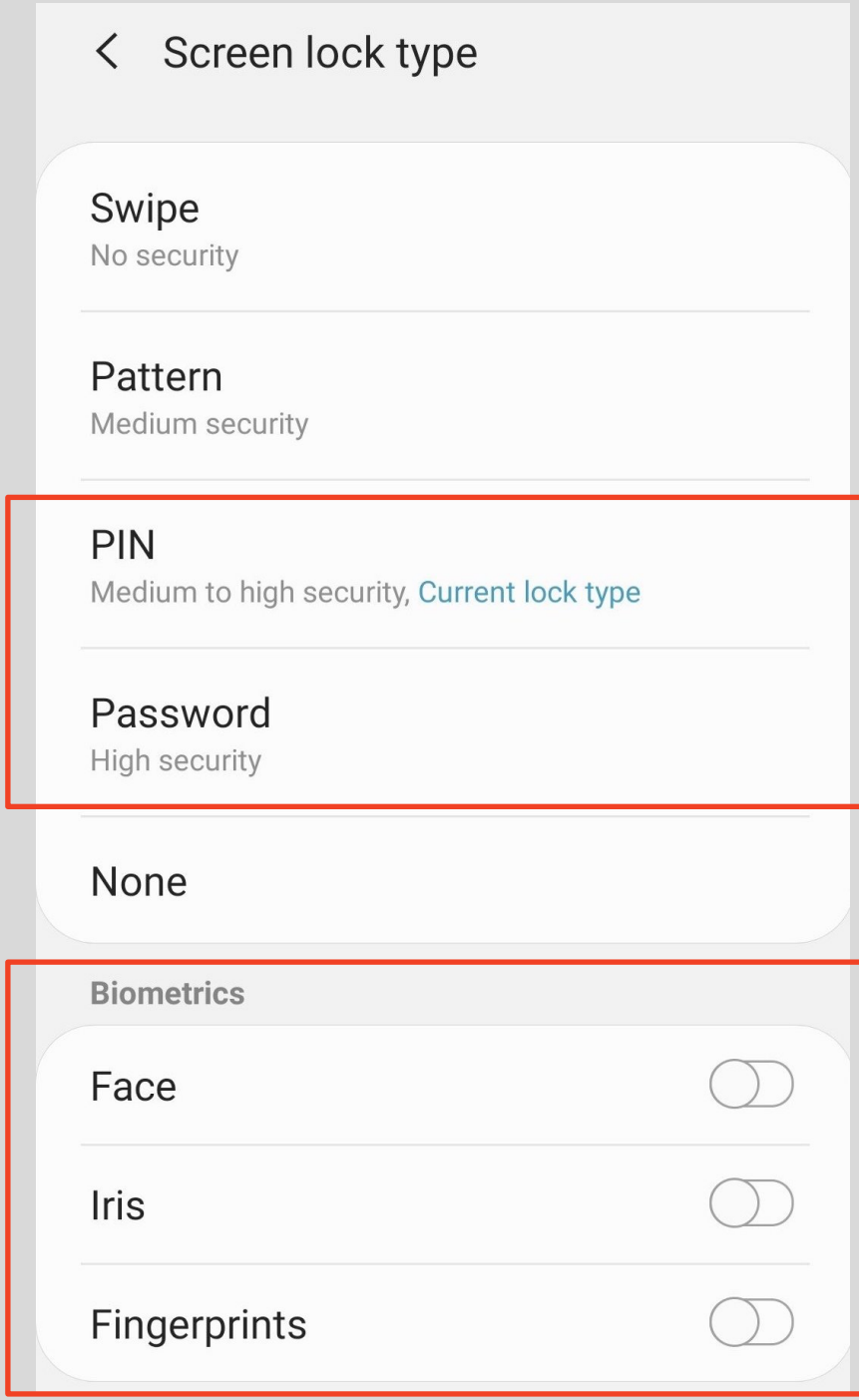


Android phones have different system settings, but most have passcode option under lock screen.

Don’t use any smart lock options

Copyright © Chinese Human Rights Defenders 2020

01 Passcode *Android*

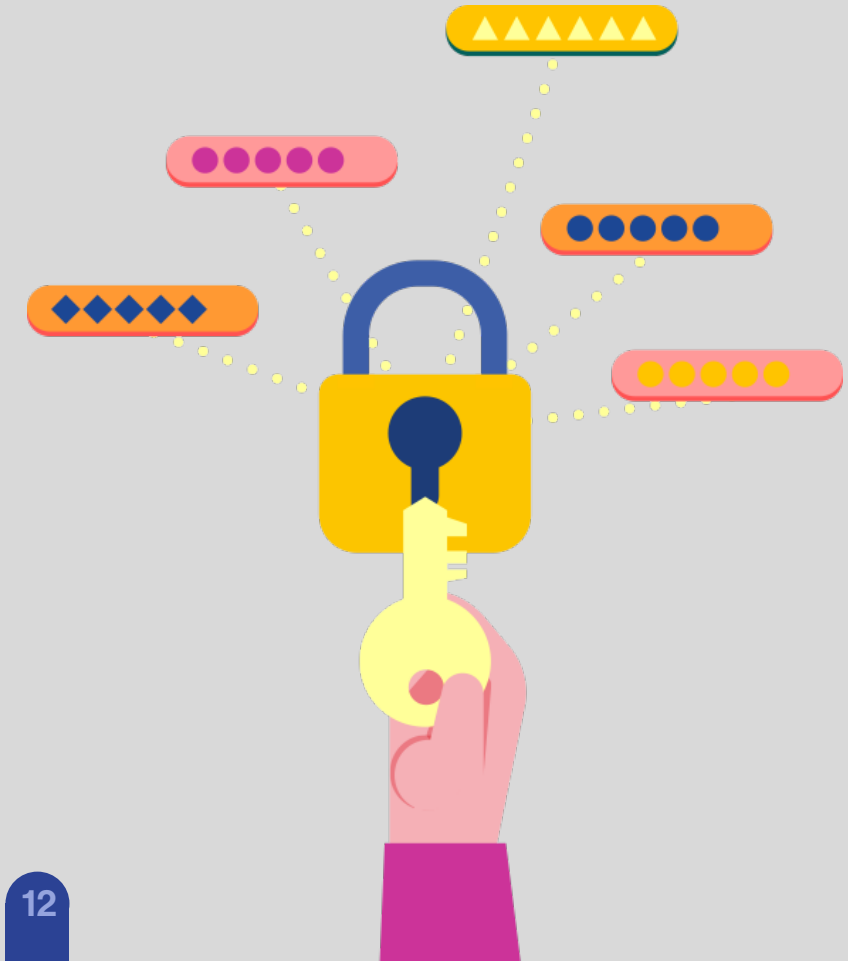


Make sure to use a pin or password as those are the most secure

Be sure to **turn off** biometric unlock options.

Copyright © Chinese Human Rights Defenders 2020

02 Password Manager



- A ***strong password for each account*** is one of the best tools you can use to protect yourself online
- Most people cannot remember multiple passwords and use the same password for several accounts. ***This is extremely insecure!***
- Password managers help you to have a strong, secure password for all your accounts
- Only need to remember one password

Recommended application: **KeePassX**
https://www.keepassx.org/

More on passwords:
https://ssd.eff.org/en/module/creating-strong-passwords

Copyright © Chinese Human Rights Defenders 2020

03 Virtual Private Network (VPN)

- Install and use **VPN on phone and computer**
- Especially important to use VPN whenever connecting to **free public WiFi**
  - Your device could be accessed through a free public WiFi connection. Any WiFi without a password is insecure and puts your phone at risk of being hacked

- Some resources to help select a VPN:

https://freedom.press/training/choosing-a-vpn/

https://thatoneprivacysite.net/

- More advanced users can consider using Tor Browser (computer and Android only)

Copyright © Chinese Human Rights Defenders 2020

04 Encrypted Messaging Apps

	Wire wire.com	Signal signal.org	WhatsApp whatsapp.com	Telegram telegram.org
End-to-end encrypted (E2EE)	✓	✓	✓	Not by default
Disappearing messages	✓	✓	✗	✓
Can register with email	✓	✗ *Can use VoIP number	✗ *Can use VoIP number	✗ *Can use VoIP number
Passcode for app	✓	✓	✗	✓
Can remove group members	✓	✓ *New group only	✓	✓
Channels to distribute content widely				✓
Notes:	Recommended	Recommended	Owned by Facebook	Incidents in mainland question strength of encryption (e.g. Jiang Tianyong case)

Copyright © Chinese Human Rights Defenders 2020

05 Secure Email

Consider using **ProtonMail** mail for more sensitive communications and can keep other emails for less sensitive mail

ProtonMail

https://protonmail.com/

Advantages of using a free secure email like ProtonMail:

- End-to-end encryption to other ProtonMail accounts
- Disappearing emails (timers set by sender), which allows sensitive information to automatically be delete from the inbox/sent folder
- Servers which are not run by corporate interests
- Two-factor authentication
- Easy to use interface that allows for searches and available on mobile app (which allows to set up a Pin to open the app

Copyright © Chinese Human Rights Defenders 2020

06 Encryption *Local Files*

Create an encrypted folder on your computer.

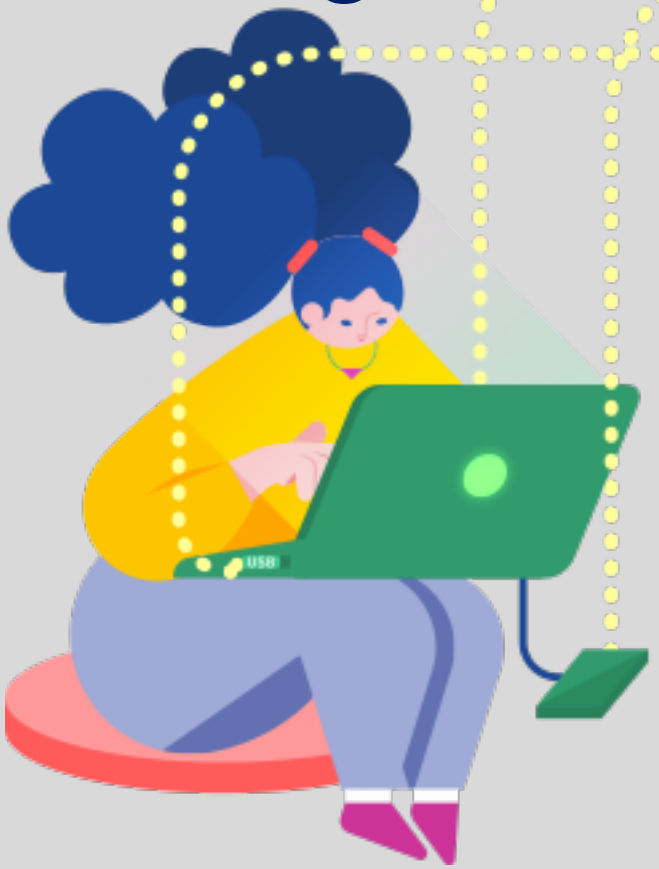
- Folder can be stored on your computer, external harddrive, or USB.

1. Download and install Veracrypt: https://www.veracrypt.fr/en/Downloads.html
2. Create new volume
   - Follow tutorial for step-by-step instructions: https://www.veracrypt.fr/en/Beginner%27s Tutorial.html
   - Note for Mac users: need to have FUSE installed
3. To store files: Open Veracrypt, mount volume (folder), place files inside, and dismount folder.

Reminder:
If you are detained and your device is seized by police, they can potentially physically force you to decrypt files

Copyright © Chinese Human Rights Defenders 2020

06 Encryption *Cloud Storage*



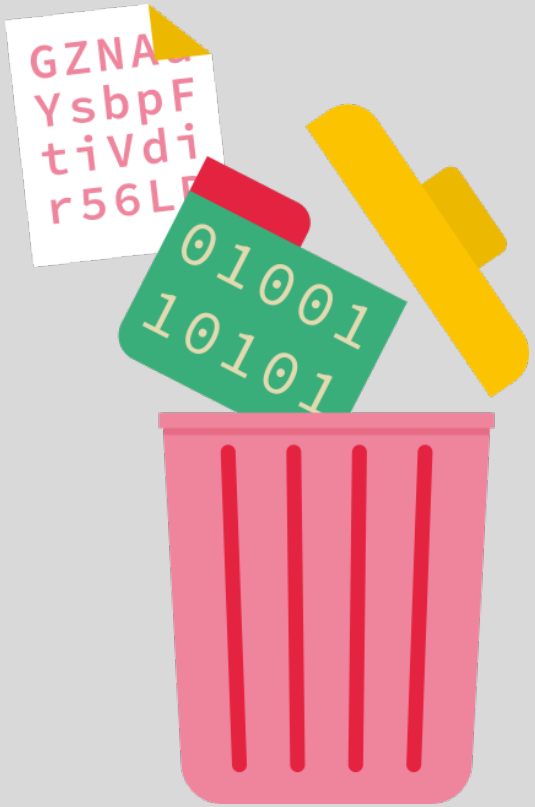
Cryptpad https://cryptpad.fr/ is a free, open source and end-to-end encrypted cloud drive

Folder can be stored on your computer, external harddrive, or USB.

- Can register anonymous accounts
- Limited storage (50MB for free account)
- Document/files can be set to disappear

Copyright © Chinese Human Rights Defenders 2020

07 Delete Files



Normally when you move a file to trash, your computer saves a version of it which someone could restore.

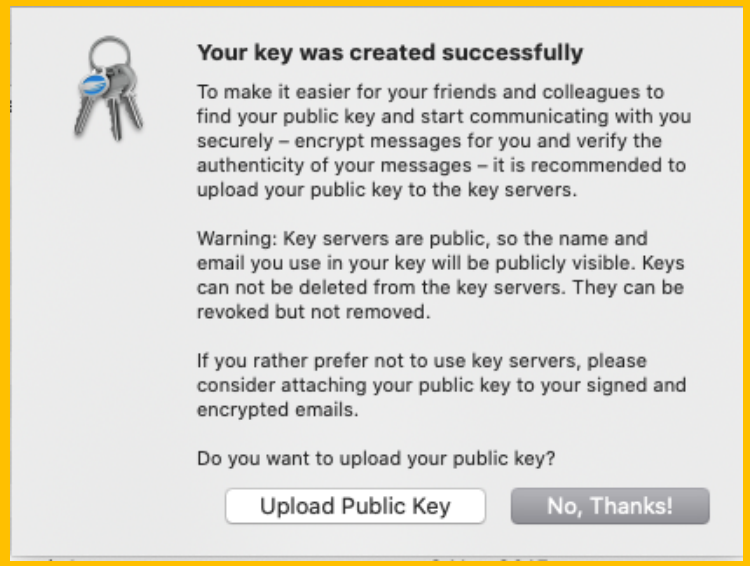
To **permanently remove** the file, you need an application which will write over the file.

- Further reading: https://securityinabox.org/en/guide/destroy-sensitive-information/
- On Windows: https://ssd.eff.org/en/module/how-delete-your-data-securely-windows
- Note for Mac: This cannot be done with newer Mac computers because they use an SSD drive, which cannot be written over. Best bet is to encrypt your files
  - Explanation: https://ssd.eff.org/en/module/how-delete-your-data-securely-macos#SSDs

Copyright © Chinese Human Rights Defenders 2020

08 Advanced: *GPG (set up a key)*

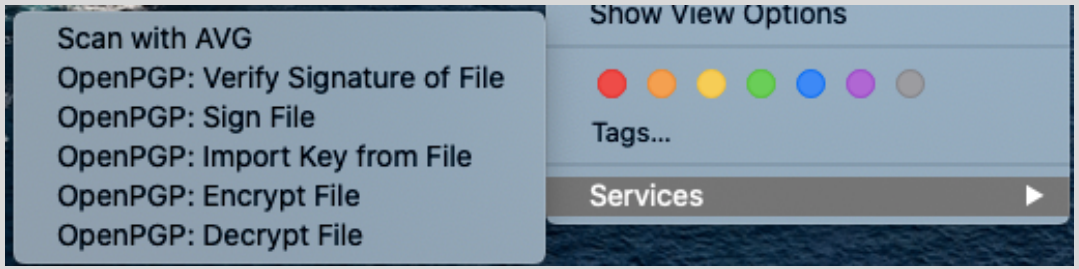
1. Download and install GPG Suite (which includes the GPG Keychain): https://gpgtools.org/
2. To set up a key:
   Open up “GPG Keychain” → go to “File” → “New Key” add relevant info including email address and strong password and click “Generate Key”
3. Exchange public keys with trusted partner:
   Right click and select “export” to generate key file.
   Do not include secret key in exported file.
   Send your public .asc keyfile to other people to encrypt files and emails with them
4. When you receive a key, double click the .asc file to import into your GPG keychain
5. Exchange fingerprints to verify key. Afterwards, double click on imported key after confirming fingerprint and set ownertrust to “full”.



Make sure to NOT upload your key to the keyserver when given this prompt.

08 Advanced:
GPG (encrypted emails and files)

After installing GPG Keychain and creating a key...

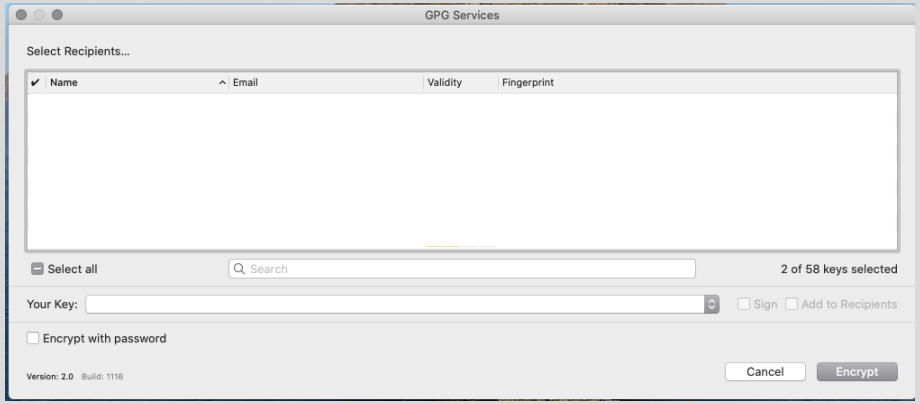


1. Right click file you wish to encrypt, go to services and select “encrypt file”.

2. Select key and click encrypt.

3. Your file is encrypted. It needs the secret key and password to be decrypted.

4. **Can encrypt it with your own key but someone with access to your computer can decrypt this file.**



Copyright © Chinese Human Rights Defenders 2020