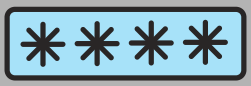
Correctly set up your WIFI

Naming your WIFI

STEP 01

Give your WIFI a name that is not directly traceable to your name.



STEP 02

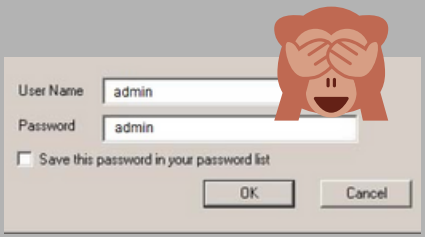
Set a strong password

Set a strong password for your WIFI, and change it regularly.

WIFI router's default administrator password

STEP 03

Change your WIFI router's default administrator password and disable the remote administrator access feature.



STEP 04

Additional safety measure: hide your WIFI name

Set your router as hidden and non-discoverable.

SET A GOOD PASSWORD

and use password manager software

A high quality password has the following elements:

Hard to hack

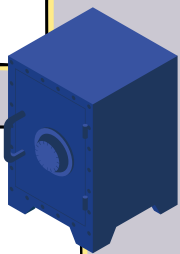
Lengthen passwords: over 10 characters.

Make your passwords complicated: a combination of uppercase and lowercase letters, numbers and symbols.

Hard to guess

Do not make it personal: do not use names, birthdays, phone numbers or identification numbers which can be easily looked up by people.

Keep them confidential: do not share your passwords.



Use a password manager

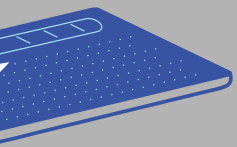
NEVER use a Post-it or word document to record passwords!That's RISKY!!!
We recommend password manager software such as KeePassXC to safely store your passwords offline.
But we don't suggest installing a password manager on your mobile phone.

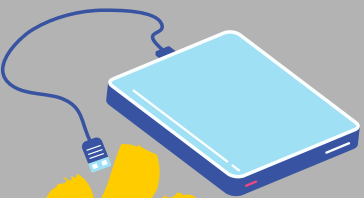
*You can find the hyperlinks of our recommended software on our official page: https://zh.amnesty.org/info-security/

Separate your communications

When you work from home, it's likely that you might be saving work-related information on networks outside of the workplace. So before you start work, ask yourself the following questions:

- Should I be using my own mobile phone for work? Or do I need a separate work phone?
- Do I need to have separate computers for private and work purposes?
- Who else has access to my work equipment apart from me?
- If working on the same computer, is it possible to separate work and private information?
- If there is only one computer/phone available, does it:
  - Have the latest updated system and software?
  - Have unnecessary/unused programmes which can be deleted?





Use secure browsers

- Firefox
- Opera

Remember:

- Make sure your browsers are updated to the latest version
- Install add-ons from browsers' official webpage

Pay attention to your email's system settings

- Set a strong password and use two-factor authentication.
- Go through your email settings carefully, such as whether your email address is included in forwarded emails; settings of email inboxes; activity of your accounts; the log in timestamps of your accounts.

End-to-end encrypted emails

Tutanota

Attention: only accounts from the same email service will have end-to-end encryption. Usually, if you're emailing an account from a different service provider, the emails will not be encrypted.

USE VPN

Use VPN if you do not want internet providers to know which servers you have been interacting with. If you need an even higher degree of anonymity or safe browsing, you can use Tor browsers.

FREE VPN

- RiseUp VPN,
- Proton VPN
- TunnelBear (limited to 500M)

PAID VPN

- NordVPN

BE AWARE

it might be illegal to use VPNs or Tor in some territories, and using them might actually increase your risk.