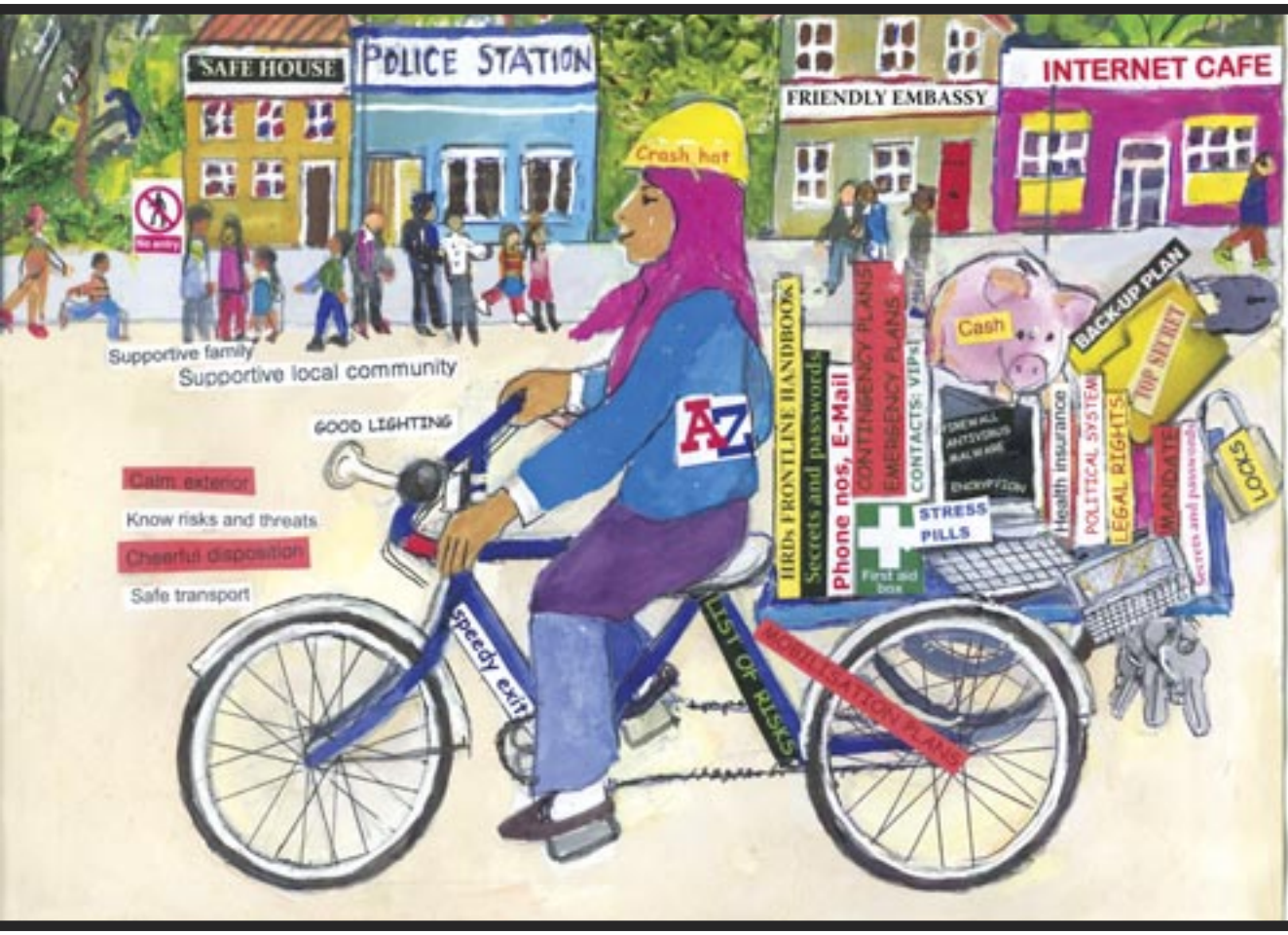
WORKBOOK ON SECURITY:

PRACTICAL STEPS FOR HUMAN RIGHTS DEFENDERS AT RISK



FRONT LINE DEFENDERS

APPENDIX 14

Computer and phone security

This check list is not intended to be a blueprint for security. Your own context is the key determining factor. Consider the risks and threats you face, and any vulnerabilities you have in order to supplement and personalise this list. It is also just a list of key points.

See Security-in-a-box https://security.ngoinabox.org/ for much more detailed information.

This information includes a number of the tips to be found in the Awareness Cards of the *Security-in-a-box* project – see the link above.

1. Protect your computer from malware and hackers

- Install antivirus software, anti-spyware and a firewall
- Do not use pirated software – it leaves you vulnerable due to lack of updates and to charges of possession of illegal software
- Consider using FOSS (Free Open Source software) such as AVAST anti-virus, Spybot anti-spyware and Comodor Firewall
- Consider using a safer browser like Firefox which has built-in security

  (see https://security.ngoinabox.org/en/chapter-1 for more information on how to protect your computer)

2. Create and maintain secure passwords

- The longer your passwords the better. Your passwords should be longer than 12 characters, contain upper and lower case letters, numbers, and special characters, and a space if possible.
- Your passwords should preferably not contain dictionary words and/or publicly available information about yourself such as birthday or friend's name – jumble up the words or replace words with special characters or numbers, or mix languages
- Consider using a phrase as your password – this can be a title of a book or an extract from a song (with characters or numbers substituted for letters)
- Change your passwords often
- Have strong different passwords for different services, update them regularly and do not share passwords (consider using KeePass to store all your passwords – see https://security.ngoinabox.org/en/chapter-3 for more information on KeePass)
- NEVER share your passwords
- NEVER let websites and programs store your passwords

  (see https://security.ngoinabox.org/en/chapter-3 for more information on secure passwords)

3. How to protect sensitive files on your computer

- Backup your files regularly and store the backup in a safe place
- Hide sensitive files with innocuous file names
- Consider encrypting your files (although encryption is illegal in some countries and could draw attention to you)
- A FOSS application called TrueCrypt can both encrypt and hide your file
- Deleted files can still be retrieved from your computer by an expert – consider using a secure deletion tools such as CCleaner (to wipe temporary files) and Eraser
- If possible check the reputation of your ISP or the place where you plan to connect to the internet, such as internet cafés
- Make sure the people you communicate with are also privacy and security aware. Communication is a two-way process. It does not make sense if only one party is concerned with privacy and security.

  (see https://security.ngoinabox.org/en/chapter-4
  and https://security.ngoinabox.org/en/chapter-6 for more information)

4. Keep your Internet communication private

- Many webmail accounts are insecure (including Yahoo and Hotmail) and provide your IP address in the messages you send. Gmail and Riseup email accounts are more secure (although Google has in the past conceded to the demands of governments that restrict digital freedom).
- Using Internet cafés can expose you to surveillance - be very aware of the risks, and whom you are contacting with what information. Delete your password and browsing history after use.
- Use "https" instead of "http" when connecting to your online services, whenever possible, so your username, password and other information is transmitted securely
- Do not open email attachments from someone you don't know, or which look suspicious
- Be especially aware when sending, receiving and viewing sensitive information on the internet
- Consider using a proxy service or application to anonymise you on the internet. This allows you to access and communicate on the internet using another computer's IP address.
- Instant messaging (chat) is also not normally secure, although Skype is probably more secure than others

(see https://security.ngoinabox.org/en/chapter-7 and http://security.ngoinabox.org/en/chapter-8 for more information)

5. Social networking

- Think carefully about the information you share about yourself, your whereabouts, friends etc
- Get consent if posting information, documents, pictures and the locations of others
- Make sure your passwords are secure and changed regularly.
- Be careful when accessing your social network account in public internet spaces – only use them if you are sure they can be trusted. Delete your password and browsing history after using a public browser or computer.
- Read and understand the End User License Agreement (EULA), Terms of Use and/or Privacy Guidelines documents. These documents may change in the future, so it is important to revisit them regularly.
- Make sure that you are familiar with the privacy settings of your social network account. Don't rely on the default settings – customise your settings and review them regularly as the service may make changes.
- Use caution when installing applications suggested by social networking services. Use these applications only if you trust their source, understand what information they will expose, and are able to control the outflow of your information.

(see https://security.ngoinabox.org/en/chapter-10 for more information)

6. Mobile phone security

- The current setup and technology around mobile phones (including SMS and voice calls) are insecure – your location can be tracked and your communications intercepted, so always consider the safest way to communicate important information.
- The safest mobile phone is a cheap, unregistered, pay-as-you-go phone which you discard after use
- Activate your mobile phone's password or pin lock
- Don't save sensitive information on your phone, or if you have to, encode it
- Be continually aware of your environment when using your mobile phone, and refrain from this in risk prone places and situations
- Make sure all your information is deleted on your mobile before selling it or having it repaired
- Destroy unusable phones and old SIM cards before discarding them
- When working with individuals and organisations transmitting sensitive information, consider having separate phones and SIMs for work and personal use.

(see https://security.ngoinabox.org/en/chapter-9 for more information)