2. Digital Security

Many people do not recognize the importance of digital security until they are faced with government officials having access to their digital information. As an activist you should be much more concerned about cyber security than the average citizen because if your information is compromised it will put other activists at risk as well.

No one can say with certainty what level of digital security is ideal for you. Should you use a complicated encryption system or are simpler measures sufficient? Do the benefits of carrying a cell phone outweigh its risks? You know best how sensitive and risky your activities are and after educating yourself on digital security, you are the best person to answer these questions.

Even if you believe your level and form of activism is not very risky, as a citizen of an authoritarian country, the actions of cyber crime offenders and government threaten your personal information.

It is necessary for activists to be up-to-date about the latest cyber security issues and techniques. A practice that is considered safe today can be very risky tomorrow. "An Introduction to Digital Security[1]" and "Advanced Digital Security[2]" written by Nima Rashedan and published by the Tavaana Institute are two indispensible resources.

1 https://tavaana.org/sites/default/files/Introduction%20to%20Digital%20Safety_1.pdf
2 https://tavaana.org/sites/default/files/Advanced%20Cybersecurity_0_0.pdf

This booklet has relied greatly on the information published in the latter source. Radio Farda's cyber security section[1], Tavaana Tech[2], and Amin Sabeti's weblog[3] are also good references. If you are fluent in English or Arabic, a booklet published by Access[4] for Middle-Eastern citizens is also a valuable documents.

Do Not Save Sensitive Information: Memorize phone numbers, addresses, and other information that could be incriminating. Do not write them on paper or save them electronically.

Categorize Information in Different Emails: Keep a number of email accounts and categorize the information based on level of confidentiality. Use one email only for personal and non-activism related exchanges. Use another email to communicate information that is sensitive. Set up the second email under another name. If the information is highly confidential you can go beyond the security provided by Gmail and use PGP (Pretty Good Privacy) for maximum protection. For more information about PGP review the article listed in footnote seven[5].

Do Not Text Confidential Information: Never use texting to communicate sensitive information. Any form of communication with a phone is unsafe and text messaging is one of the least secure forms of communication. For example, if your phone conversations are not recorded or monitored when an exchange is taking place, it is very difficult to determine what was said. On the other hand, the history of your texts is usually retrievable months and even years later.

1 http://www.radiofarda.com/section/cyber_security/1978.html
2 https://tech.tavaana.org/
3 https://aminsabeti.net/
4 https://www.accessnow.org/pages/protecting-your-security-online
5 deepdotweb.com/2013/11/11/pgp-tutorial-for-newbs-gpg4win

Delete Classified Information Quickly: When you receive a sensitive email or electronic message, delete it from both your inbox and trash as soon as you read it.

Do Not Save Sensitive Information: Memorize phone numbers, addresses, and other information that could be incriminating. Do not write them on paper or save them electronically.

Follow Internet Cafes Strategies: Be mindful of security cameras in Internet cafes. If you want to send a confidential email, open a new account under another name. Internet cafes can easily trace your activities; therefore if you are at a cafe do not check the emails that you use for your activism. If you have to send a confidential email, open a new account under another name and make sure you are not revealing your identity in the message. Furthermore, be sure to use private browsing, which is explained in more detail in the section titled Computer Security.

Delete Information: Periodically use software that thoroughly erases the information you wish to delete from your computer. Often, when you delete a file from your computer the information is not erased and can be retrieved. Use software like File Shredder to thoroughly remove the unnecessary files.

Be Aware that Your Phone's Location Could be Traced: Since your cell phone location can be traced, your location can be easily determined when you carry your phone. If you are going to a secret meeting, either leave your phone at home or turn it off and take the battery and SIM card out.

Password Security

Use Strong Passwords for your Computer, Cell Phone, Emails, and Social Media Accounts: A strong password is no shorter than eight characters. Do not use words that can be found in an English or Persian dictionary, or personal information that are easily accessible, such as date of birth, telephone numbers, or names of family members and friends. It is very important to use upper and lowercase letters, numbers, and special characters.

- Use different usernames and passwords for your profiles.
- If you have a Gmail account, use the two-step verification for accessing your account.
- Do not enable your computer or cell phone to auto-fill your passwords; otherwise anyone who gains access to your computer could also access your emails, and other accounts.[1] If you think you will forget your different usernames and complicated passwords, use password management software such as LastPass or 1Password.

Give Your Password to a Friend: Tell a trusted friend, preferably one that lives abroad, the passwords to your email, Facebook, and other accounts and ask the friend to change your passwords as soon they are notified of your arrest. This friend should not change the passwords to your personal and non-confidential accounts. Allowing your interrogator access to your personal email could be an effective way of gaining his trust.

1 http://www.pcpd.org.hk/english/publications/files/computer_wisely_e.pdf

Use HTTPS: One method of secure communication is using https (and not http). The “s” in https stands for secure. The https scheme protects the exchange of information between the user and the website being visited. It constantly checks the website’s server through the user’s browser and thus, recognizes if the connection is being intercepted. There are HTTPS Everywhere add-ons for Google Chrome and Firefox.

Bypass Filtering: For bypassing Internet censorship use Tor, Psiphon, or other known and reliable Virtual Private Networks (VPN). Make sure that the circumventing software that you are using is genuine and not an imitation. Recently a circumvention software named Psiphone (with an added “e”) was able to gain access to users’ private information.

Computer Security

- Keep all your software up-to-date. Outdated software is the main entry for hackers. Operating systems, anti-viruses, firewalls, browsers, and popular software like Acrobat and JavaScript should be updated frequently. If you have confidential information saved on JavaScript it is best to erase the software in its entirety.
- When storing information on USB flash drives make sure to encrypt them by using software like BitLocker, so that in case you lose the flash drive your information is not easily retrievable.
- If you have to save any confidential information use Google Drive instead of your computer's hard drive.
- Your computer saves your Internet history. To prevent this, use the private browsing feature of Web browsers: Incognito in Google Chrome, Private Browsing in Mozilla Firefox and Safari, and In Private in Internet Explorer.
- Use CCleaner for encrypting your files, deleting cookies, and making your files irretrievable. CCleaner is also capable of erasing traces of recently used documents.
- Routinely erase your browser's temporary files by deleting site history and downloads in your browser's preferences.

Security in Social Media

The security of your social media accounts is as important as your email.

- Use strong passwords for your accounts.
- Activate the option of ID verification for entering your Facebook account.
- Access your Facebook only from one computer and register it as a “recognized device,” so that if someone attempts to access your account from another computer, you are notified.
- On Facebook, be very mindful of what statuses and pages you “like,” since many of them could be public and seen by anyone.
- Always assume that among your Facebook friends there are people whose accounts are accessible by the government. Therefore the authorities can see your private profile and postings through these friends.
- Do not reveal your geographic location, date of birth, and city in your profiles.
- Routinely check the IP addresses and computers that have recently accessed your account.
- Do not accept friend and connection requests from people that you do not know.
- Whether on social networks, other websites, or in your email do not open links that appear to be scams.
- Do not use others’ laptops, desktops, cell phones or tablets to access your social media accounts.
- Always logout after accessing your accounts.
- On websites like Facebook, configure your setting so that the names of your friends are not displayed. Simply displaying your connections could create a serious risk for other advocates.

Cell Phone and Tablet Security

The most important measure for keeping your mobile secure is making sure the operating system is up-to-date.

- Only use applications that are well known. Lesser-known applications often pose the highest security risks.
- Install a reliable mobile security app and firewall on your phone and tablet.
- Choose strong passwords for your smartphone and tablet and make sure to lock your phone and tablet as soon as you are done using them.
- Only connect to secure WiFi connections and do not connect to networks you do not know.
- Purchase your apps from well-known and reliable app stores.
- Before purchasing an app, read the online reviews and comments to see whether users have had security concerns.
- Pay attention to access permissions an application requests. Some applications gain access to most of your information once you agree to their terms and conditions.
- If you want to carry your phone with you to a potentially sensitive event because you think you might need to take a video, remove your SIM card.
- If you are going to use your cell phone for keeping or communicating sensitive information, do not use jailbroken phones.
- Only have your Bluetooth on when you are using it.
- Download software that enables you to erase your phone contacts in case it is lost or stolen. For android phones you can activate this software on your Google Account[1].
- Do not activate app features that access your GPS location. If you ever choose to share your location, deactivate the feature immediately after use. This way you do not leave a history of your locations on various sites and services.

1 https://www.google.com/android/devicemanager