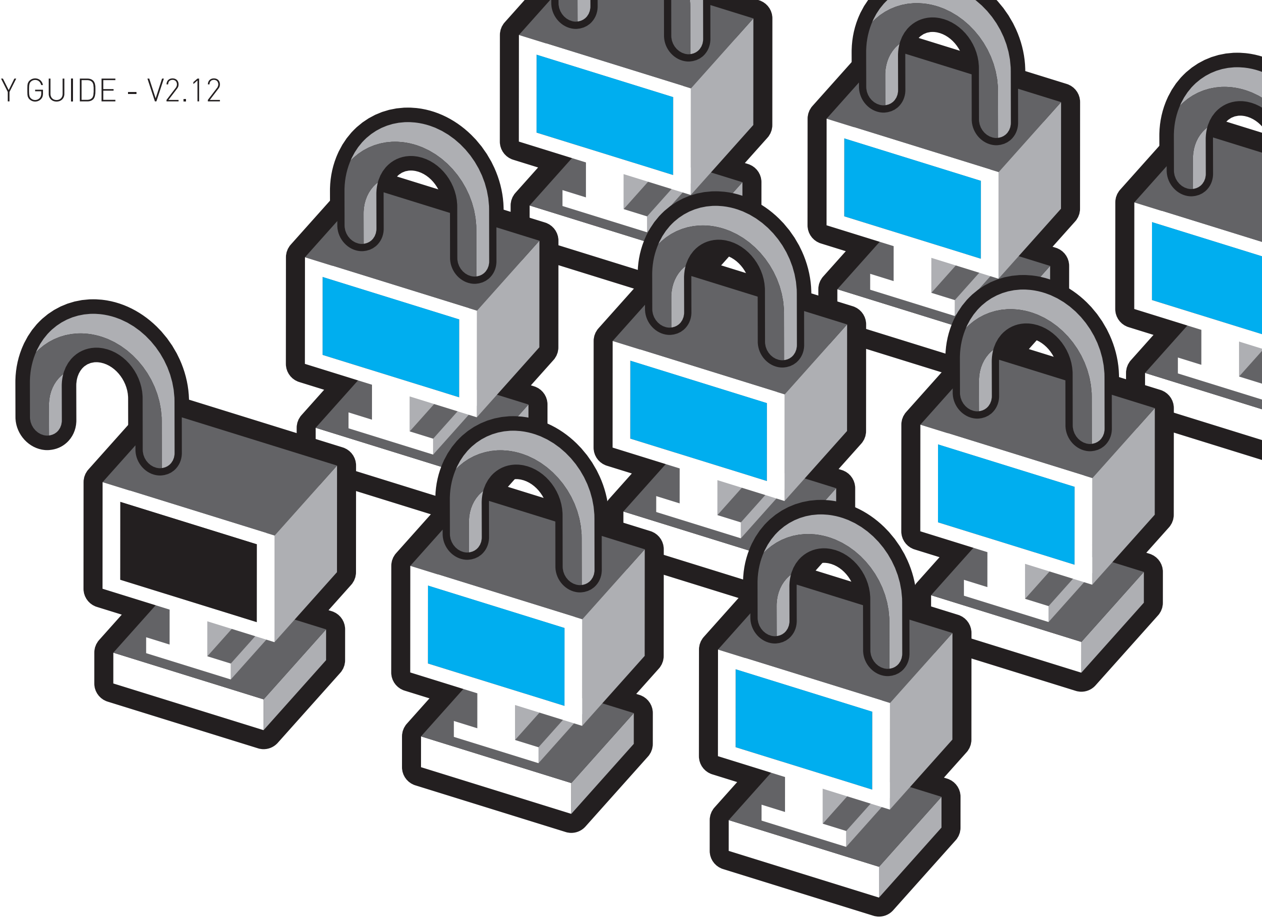


A PRACTICAL GUIDE TO PROTECTING YOUR IDENTITY AND SECURITY ONLINE AND WHEN USING MOBILE PHONES

FOR CITIZENS IN THE MIDDLE EAST, NORTH AFRICA AND BEYOND

This guide is written for citizens in the Middle East and North Africa who want to use technology safely to communicate, organize, and share data (news reports, information, media, etc.) – but it can be used by anyone online anywhere who wants to protect their privacy and security. It is written for a wide audience with average computer literacy who would like to know what steps they can take to be safer online and when using mobile devices. This guide has tips and tools for reducing surveillance and monitoring, protecting privacy, and dealing with censorship. It covers: secure use of email and chat, good password habits, how to keep your computer free of viruses and spyware, how to get around censorship online while remaining anonymous, tactics for using mobile phones safely, and has links to more in-depth resources.

While all of the information in this guide is considered accurate and has been checked as of July 2011, protecting yourself online is a complex process that changes as new technologies and vulnerabilities emerge. There is no silver bullet to guarantee complete security and privacy, but these tools and strategies will definitely help make you safer.

This document has been drafted and peer-reviewed by a range of organizations and individuals specializing in online and mobile security. If you identify problems in this document or have suggestions for improvements, email info@accessnow.org.

(If you have problems accessing any of the links in this document due to blocked sites after using the circumvention tools mentioned below, please email info@accessnow.org and let us know what you'd like to be sent via email).

Some Critical Basics

Securing your Email

Of the most popular free email services, Hotmail and Gmail offer secure email services that provide connection encryption (HTTPS) between you and the email service provider.

Gmail now has HTTPS as its default setting, but you need to turn it on for Hotmail if you haven't already been prompted to do so (go to Account > Other Options > Connect Using HTTPS > Use HTTPS Automatically). At this time Yahoo Mail is not secure; although it's a hassle, we recommend you establish and use an alternative email account that has HTTPS for your communications, especially for anything sensitive. Remember that HTTPS secures the connection between you and your email provider only and delivery towards the final destination can still be unencrypted and vulnerable if the recipient is not using HTTPS, or they use a different email provider. Other secure email service options are Riseup.net, and Vaultletsoft. In addition, an excellent system for encrypting and digitally signing your email is PGP and GPG (read more in English and Arabic).

If you use Gmail and would like to learn more about other security features (2-factor authentication, IP history), please see their Gmail Security Checklist. If you use Hotmail, you can learn more about their security features, including their 1-use passwords for use on public computers here.

Making Passwords Safer

One of the most important things you can do is create good, strong passwords and use good password behaviors. Some basic tips:

- Think of a phrase, rather than a single word.
- Make your passphrases twelve or more characters long; this makes it harder to crack using various software programs.
- Use a combination of symbols, numbers, uppercase and lowercase letters. One way is to include symbols and numbers for words and letters in a passphrase, which can be a saying or a line from a song or poem.
- Don't use the same password for every account; if your password is easily intercepted when inputted online in a place that doesn't offer HTTPS, it's easy to intercept your log-in information and use it to access your other accounts.
- Change your passwords every 3 months or more often if you use internet cafe systems or computers other than your own.
- If you have problems remembering passwords, use a secure encrypted program like KeePass to keep track of them.
- Some accounts are compromised via lost password recovery systems.
  Be sure your security questions and answers for your accounts are not simple and easy to guess.

Anti-virus and anti-spyware

A critical issue for most computer users is the utilization of pirated software, especially Microsoft Windows. When you obtain software illegally, you save a few bucks but you also leave yourself open to vulnerabilities that are not addressed by receiving updates and patches from the software manufacturer. If you cannot obtain official, legal versions of software and operating systems, you should at least run effective anti-virus and anti-spyware software in order to minimize your risks. But if at all possible, try to get official copies of software if you can for your own security.

- If you aren't currently running effective software, an excellent free anti-virus program for Windows is Avast, which helps protect the data on your computer from being damaged and infected. Malwarebytes is another program that runs in safe mode if your computer has already been infected.
- Equally important is anti-spyware software, which identifies and removes malicious software that can track all your activities on- and offline; a free and effective anti-spyware program is Spybot.
- To reduce your exposure to viruses and spyware, don't open up emails and attachments from unknown or untrusted sources. If you're unsure of an attachment, file, or website, you can upload to test it at VirusTotal or email it to scan@virustotal.com with "SCAN" in the subject field (or SCAN+XML if you want your results in XML format.)
- Another common entrypoint for malicious code is scripts you encounter when browsing the web. We strongly recommend that you download and use the NoScript add-on to use with your Firefox browser, which allows you to block most scripts and allow those you trust.
- Another common entrypoint for viruses and spyware is USB sticks and other removable media. Don't put removable media into your computer unless it comes from a known and trusted source. Also use anti-virus and anti-spyware like Spybot and Avast to scan removable media.

Consider switching to Linux-based operating system Ubuntu unless there is a critical reason for continuing to use Windows. Ubuntu allows for an encrypted hard drive by default and is essentially free from viruses and malware. Targeted attacks notwithstanding, a user of Ubuntu is much more secure than a user of an unpatched, pirated, or outdated copy of Windows. Mint is another Operating System based on Ubuntu that allows usage of a wider range of applications.

Secure Instant Messaging

Skype and Google Chat inside HTTPS-secured Gmail are good options if you believe that your accounts will not be targeted by hackers. A much more secure option is using Pidgin to access a number of chat clients (Google Talk, etc.) with the Off The Record (OTR) plug-in -- this ensures that even with your encryption keys, any previously logged data will be worthless. Read more about OTR's security properties to understand an example of Privacy by Design.

Secure your online presence in other ways:

- In order to keep your identity secret when participating in online activist activities, you can create aliases when asked to identify yourself online on social networking and media sites. The degree to which you anonymize is up to you: it's common to create an anonymous handle on Twitter, but most people will have accounts under their true names for social networking sites like Facebook. This is up to you and your sense of how likely you are to be targeted online for in-depth surveillance. It's important to know that for Facebook, you will have to create a convincing fake name instead of an obviously fake one-word pseudonym, which Facebook will remove for violating their terms of service agreement.

- If you do decide to use your real name on Facebook and use HTTPS to access/use the site, it's important that you not provide additional pieces of sensitive personal information such as your phone number.
- There are increasing options for utilizing GPS technology in order to demonstrate your physical location when online. This can be a powerful tool when used as part of a coordinated campaign to map out reports from the ground using mobiles during a crisis or key event, but it also gives out incredibly sensitive information about your location and activities. We recommend you turn GPS tracking off for programs such as Twitter and Bambuser unless it's temporary and critical to an activist project you're working on. Even if the GPS is not displayed, it is critical to disable the collection of this information in your web browser or other client.
- When you send sensitive information to others, keep in mind that they may not be secure; their contact lists, emails, and other communications could be monitored. Be especially careful when communicating with parties when you have not verified their identity. In addition, any direct messages you send to someone (known or unknown) via Facebook and Twitter can be read if they have not taken certain steps (see more about HTTPS and circumvention tools to the right).
- Keep your usage of third-party applications that access your accounts to a minimum or don't use them at all (e.g., apps that access your accounts for Twitter, Facebook, Gmail, etc.) They frequently have security vulnerabilities and are used to hack into otherwise secure accounts.

Online Security

The internet is heavily censored in many countries throughout the region, such as Bahrain, Kuwait, Oman, UAE, Qatar, Syria, and Saudi Arabia. It is also monitored, although to an unknown extent. If you are able to circumvent the censorship, it is not the same as circumventing the monitoring, which is harder to do. You should try to use a secure, anonymizing proxy with the assumption that your activity can be monitored and recorded. In addition, we strongly recommend that you don't use Internet Explorer as your web browser, as it has a number of vulnerabilities, especially in unlicensed versions of the software. An excellent free alternative with a number of useful add-ons is Mozilla's Firefox.

Encrypting your activities online using HTTPS

If you are engaging in activism online, it's important to do so in a way that keeps your identity and passwords safe. We recently saw Tunisia carry out a massive phishing campaign where they exploited a vulnerability in order to gather the log-ins and passwords for citizens accessing Facebook. Fortunately, Facebook responded by enabling HTTPS, which helps. When possible, you should always use HTTPS. If you are unable to use HTTPS, it is critical that you use a secure proxy system of some kind. A censor can target specific users or specific sites and deny access to HTTPS sites. If you use an anonymizing proxy like Tor, it will be very difficult if not impossible to perform such targeted attacks.

HTTPS

An excellent and easy-to-use add-on you should use is HTTPS Everywhere. This is a Firefox add-on that "forces" a site to use HTTPS if available. **Downloading this should be one of the first things you start to use in order to have end-to-end encryption for sites such as Facebook, Twitter, Google Search, and more.** It will also reduce your vulnerability to having your passwords captured when sharing open or unsecured wifi networks.

- If you haven't already, download the most recent version of Firefox. Then download HTTPS Everywhere and/or Force TLS, restart Firefox, and set preferences. Note: HTTPS Everywhere has a number of default sites that that can be customized. Force TLS involves more customization, requiring the user to create a list of sites to force HTTPS.
- If you use Google Chrome, download KB SSL Enforcer Extension. *(Note: This is not as effective as the add-ons for Firefox mentioned above. There are still some bugs with SSL Enforcer, although we assume it will improve over time.)*

Facebook

Although the Firefox add-ons described above force HTTPS for a number of sites, if you use Facebook often, it's also a good idea to ensure that Facebook is set to HTTPS as a default, especially if you access it on multiple computers.

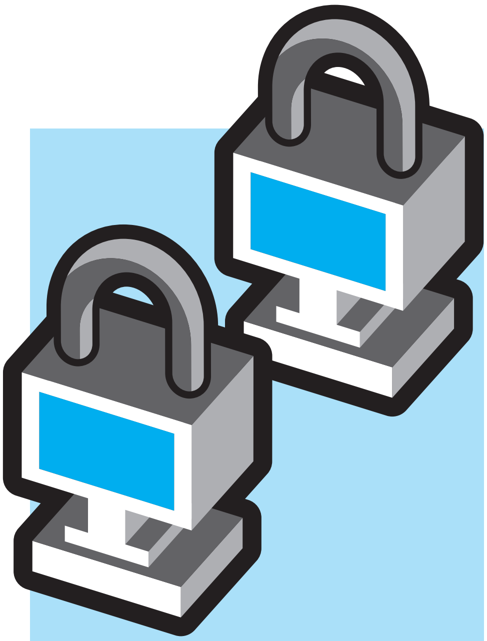
- In order to enable HTTPS for Facebook, go to Account in the top right corner > account settings > on settings tabs, select account security "change" > check box next to "secure browsing (HTTPS)"
- The use of some games or other facebook add-ons will disable the use of HTTPS.
- Facebook also now has other security features you can use, including remote log-out and log-in notifications that allow you to limit the devices that can access your account. A video reviewing their security features can be found on their site. Another comprehensive guide to using Facebook securely can be found here.

Twitter

Although the Firefox ads-ons described above will force HTTPS for Twitter as well, it's a good idea to change your Twitter settings to HTTPS by default whenever you connect, especially if you access Twitter on multiple or public computers.

- In order to enable HTTPS for Twitter, click on your Twitter handle in the top right corner > settings > scroll to the bottom of the page and check the box next to "Always use HTTPS".
- Note: Changing your Twitter account's setting to "always use HTTPS" does not currently force HTTPS on mobile devices as well. Until this is fixed, always go to https://mobile.twitter.com.

Circumvention: Visiting sites that are blocked



A number of countries in the region engage in heavy filtering of a large number of websites and blogs and it is reasonable to suspect that this filtering indicates a great deal of surveillance as well, although the level of surveillance will vary from country to country. In order to visit and upload any media to blocked sites, you can use circumvention tools. It is important to note that there is a difference between encryption and privacy/anonymity: good circumvention tools encrypt traffic between a user and the circumvention provider, but they cannot encrypt the traffic between the circumvention provider and the site being visited. This is why it is important to use HTTPS whenever possible, as it provides end-to-end encryption. But using HTTPS alone will not help you access a site that has been blocked, which is why circumvention tools are important. Your IP address is always stored by the remote service - only with an anonymizing proxy (such as Tor) is your IP address actually and safely hidden. Many services will reveal your last logins and thus if your account is hacked, your previous locations will be revealed.

Jumping the firewall

Simple web-based proxies allow users to access blocked sites via web page forms. A user will visit a proxy site and enter in the URL for a site they wish to visit, and the proxy will retrieve and display the page. HTTP/SOCKS proxies funnel web traffic through protocols that enable passage through firewalls. The IP addresses and port numbers found on public proxy directory sites and are entered into a browser's configuration.

Although simple web-based proxies and HTTP/SOCKS proxies are commonly used to circumvent filtering, they do not provide anonymity (your usage of them can be seen/monitored) and it is rarely known who provides them. There are a number of risks associated with them, so it's advisable to use a system like Tor, which can provide circumvention and anonymity.

Another proxy-based solution is Psiphon. It comes in several different configurations. Psiphon 1 is a lightweight web proxy that runs on MS Windows and Linux computers. Psiphon nodes (or 'psiphonodes') are not usually open public proxies. Instead the intention is for average people without specialist computer hardware to provide proxy-based circumvention capability to a small number of 'friends' located in another country where site blocking is in effect. This is known as a web-of-trust model, as the 'friend' who provides the psiphon proxy will be able to access any traffic passing through their psiphonode and thus there needs to be a trusting relationship between the provider of the psiphonode and those utilizing the node. **Psiphon does log data on users, but the IPs are anonymized.** Psiphon 2 is a centrally managed cloud-based solution run by Psiphon Inc. comprised of link-rewriting proxies. Psiphon 1 and 2 have difficulty dealing with HTTPS and Web 2.0 sites. These limitations have been addressed in the newer PsiphonX.

Tor: Anonymity online

Tor is an excellent, sophisticated tool for circumventing Internet filtering and helping protect your anonymity online, however its main drawback is it can be slower than other solutions for browsing. Tor Browser Bundle takes care of all the setup and using a Tor Bridge may help get access in a heavily filtered environment.

While there are multiple ways to use Tor we suggest you download the Tor Browser Bundle, which lets you use Tor on Windows, Mac OS X, or Linux without requiring you to install multiple applications. Just launch the Tor Browser Bundle, and a custom version of Firefox will start along with Vidalia, the Tor controller application, pre-configured to connect to and send all traffic through the Tor network. You can install the Tor Browser Bundle onto a USB flash drive, so that you can use it on any computer where you might need it. For Browser Bundles with or without secure IM in multiple languages (including Arabic and Farsi) visit the Tor download site. As the use of Tor can slow the web browsing experience we recommend the use two browsers, one with Tor for accessing sensitive or blocked information and another browser for all your other non-sensitive web browsing. If left connected Tor will improve its efficiency over time and you should notice an improvement in speed. If you find accessing web sites with Tor is still too slow and the content you wish to view is text-based, you can turn off image and javascript loading in your browser. Doing this may dramatically speed up loading the pages through Tor.

Unfortunately, the main Tor website that is linked to above is usually blocked in most countries in the region. You can still access the software by:

- Visiting the Tor website with HTTPS - https://www.torproject.org/
- Finding a torproject.org mirror by googling "tor mirror". You can also view the official list of mirrors if you google "site:torproject.org mirrors" and view the cached result of the "Tor Project: Mirrors" page.
- Or you can request a bundle by sending an email to the "gettor" robot at gettor@torproject.org. Note: for best security and results use an HTTPS protected Gmail account to email gettor@torproject.org. Select one of the following package names and put the

Mobile Devices

package name anywhere in the body of your email:

- tor-im-browser-bundle for Windows
  (Tor & instant messaging)
- tor-browser-bundle for Windows
  OR Intel Mac OS X OR Linux (Tor browser)

Shortly after sending your email, you will receive an email from "Gettor" robot with the requested software as a zip file. For further help with Tor, email tor-assistants@torproject.org.

Another option for circumvention that encrypts communications and provides anonymity is a VPN network. You can read more about how to set one up here, or download the free version of the VPN Hotspot Shield here or by emailing hss-sesawe@anchorfree.com (the subject line of your message must contain at least one of the following words "hss", "sesawe", "hotspot", "shield").

Other widely used circumvention tools include Ultrasurf and Freegate. All three of these VPNs are good tools for accessing sites that are blocked, but it's important to note that like simple web proxies or HTTP/SOCKS proxies, they are not anonymizers (e.g., they do not hide your identity when you are using them.) Additionally, these services are known to filter and block sites that their operator does not support or like. Furthermore, these sites are known to log data about all users. They are commercial enterprises and generate revenue by targeting advertisements to you on the basis of your personal information (the sites you view, the search terms you use, etc.) -- this is a critical issue for those seeking anonymity or simply privacy in their use of circumvention software.

Important Note: When a government has the ability to control the Internet services in a country, they can use a number of other strategies to compromise your security and privacy via code and security certificate injections. To address this, use the tools and tactics above, and try to follow the news or alerts from online activists in your country who may recognize these types of tactics and provide early alerts.

More resources: Video tutorials for how to use various circumvention tools in English and Arabic (12 pm Tutorials).

Many activists have been tracked via their mobile phones, and some countries conduct surveillance more extensively than others. Egyptian activists experienced a high level of surveillance at all levels, and Egyptian authorities used a type of technology to remotely turn phones into listening devices in their environments, even if they were off at the time. You need to assess the risk for your own activities given the practices used in your country, how high-profile your work is, and what others in your community have experienced. Phone companies have the capability to track and collect information about your use of mobile phones, including your location, and may share that information with the government if so requested. There is also the possibility of installing surveillance software on a phone that runs in the background without the user noticing. There is a risk of this, if your handset has been physically out of your hands for a period of time.

When your phone is on, it is constantly communicating the following information with towers nearby:

- The IMEI number – a number that uniquely identifies your phone's hardware.
- The IMSI number – a number that uniquely identifies the SIM card - this is what your phone number is tied to.
- The TMSI number, a temporary number that is re-assigned regularly according to location or coverage changes but can be tracked by commercially available eavesdropping systems.
- The network cell in which the phone is currently located. Cells can cover any area from a few meters to several kilometers, with much smaller cells in urban areas and even small cells in buildings that use a repeater aerial to improve signal indoors.
- The location of the subscriber within that cell, determined by triangulating the signal from nearby masts. Again, location accuracy depends on the size of the cell - the more masts in the area, the more accurate the positioning.

Mobile Devices (Continued)

Because of this, when your phone is on and communicating with the network towers, it can be used as a surveillance device for those with access to the information that telecoms collect, including:

- Your phone calls received and sent
- Your SMS received and sent, including the information of senders and recipients
- Any data services you use (e.g., web browsing activities if not using HTTPS, unsecured instant messaging) as well as the volume of data transferred e.g., "did you upload to YouTube")
- Your approximate location (from within a few meters to a few km depending upon density of towers)

It is important to note that if you think you are being tracked, it is not always enough to switch SIM cards, as you can be tracked by the ID (IMEI) of your mobile device/handset alone.

There is also a lot of information on your phone that may be used against you if the phone is confiscated or taken from you. All mobile phones have a small amount of storage space on the SIM card, as well as internal phone memory. (In addition, some phones have a SD (or microSD) storage card for multimedia files.) In general, storing data on the SIM card and SD card (if available) is better than storing internally on the phone, because you can more easily remove and destroy the data on the SIM or SD card.

Data stored on your SIM, internal phone memory, and SD storage card (if present) include:

- Your phone book - contact names and telephone number
- Your call history - who you called, who called you, and what time the call was placed
- SMS you have sent or received
- Data from any applications you use, such as a calendar or to-do list
- Photos or video that you have taken using the phone camera, if your phones has one. Most phones store the time the photo was taken, and may also include location information.

For phones that allow web browsing, you should also consider how much of your browsing history is stored on the phone. If possible, do not keep a browsing history. Emails are a further potential danger should an attacker obtain access to the SIM card or phone memory.

Like the hard drive in a computer, the SIM memory of your mobile phone keeps any data ever saved on it until it is full, when old data gets written over. This means that even deleted SMS, call records and contacts can potentially be recovered from the SIM. (There is a free application to do this using a smartcard reader). The same applies to phones that have additional memory, either built into the phone or using a memory card. As a rule, the more storage a phone has, the longer deleted items will be retrievable.

So what does this mean for you?

Mobile phones can be powerful tools for activists, but they can also be incredible liabilities if the government or security forces are actively working with telecoms to track you. If you are in a country that uses mobiles extensively for surveillance, especially if you think you are being closely watched for high-profile activities, it's recommended that you don't use mobile phones to communicate. Conduct meetings face-to-face.

Ultimately, the risks you take are up to you: if you don't think you're being targeted as a high-profile activist or as part of a larger surveillance campaign and want to use your phone to communicate with fellow activists, record photos and video, or pass on information, you can use the following tactics:

- Create and use a code word system to communicate with fellow activists.
- Use "beeping" as a system for communication with fellow activists (calling once or twice and hanging up in order to let

Mobile Devices (Continued)

someone know you've arrived at a location, are safe, etc.)

- Don't use the real names for fellow activists in your address book; give them numbers or pseudonyms. This way if your phone or SIM card is taken by security forces, they don't have your entire network of fellow activists in hand.
- Bring back-up SIM cards with you to protests if you know they are being confiscated and it's important that you have a working cell phone with you at an event. If you have to get rid of a SIM card, try to physically destroy it.
- If your phone can be locked with a password, use it. This can also be your SIM card's PIN number: SIM cards comes with a default PIN number; if you can, change the default PIN number and enable PIN locking on your SIM. You'll then be required to enter a password (your PIN number) each time you use your phone.
- If you think a protest is going to meet with an increased crackdown by security forces, you may want to put it in airplane mode while at an event; you won't be able to send or receive calls, but you can still capture video and photographs and upload them to online sites later. This tactic is also useful if you think security forces are cracking down on everyone with a cell phone at an event. Later on the government can request call/SMS or data records for all individuals who were in a particular location at a particular time in order to perform mass arrests.
- Turn off location tracking and geotagging for various applications unless you are using this feature as part of a targeted project to geotag certain media at an event as part of an action. If you are using your cell phone to stream video live, turn off the GPS/geotagging option (Directions for Bambuser.)
- If you have a phone that runs on the Android Operating System, you can use a number of tools to encrypt web browsing, instant messaging, SMS, and voice calls via the tools created by the Guardian Project and Whispersys.
- When using your mobile device to browse the web, use HTTPS whenever possible.

More resources:

- Tactical Tech's Mobiles in a Box (English)
- MobileActive's Mobile Security Risks Primer (English)

Note for BlackBerry users:

BlackBerry-maker Research in Motion (RIM) provides two types of accounts with corresponding levels of encryption. For ordinary individual consumers, there has never been true end-to-end encryption on your BlackBerry communications – RIM or your mobile provider can always intercept your calls, emails, SMS, web browsing, etc. By way of contrast, enterprise users whose company uses a BlackBerry Enterprise Server (BES) will have end-to-end encryption on their email, messenger (BBM), and web browsing. However, if you're an Enterprise user, keep in mind that whoever runs your company's server, typically your IT admin, has the means to decrypt all of your communications, and there are a variety of legal (and not so legal) processes which a government can use to get your decrypted communications.

Recently the UAE tried to force Research in Motion to give them the mechanism to decrypt all BlackBerry communications, but RIM has refused to do so. BlackBerry users should keep up to date on any news of negotiations between their government and RIM on these issues. They should also be aware of other attempts to intercept encrypted BlackBerry communications. In 2009, UAE's Etisalat sent BlackBerry users an unofficial "update" that allowed the telecom to receive copies of all users' messages. RIM soon sent users an update that removed the fraudulent software, but BlackBerry users should be aware of any suspicious software updates that do not come directly from RIM.

Other

Blogging

If you have a blog or want to start one, there's a number of resources for setting one up. Your main concern is keeping your identity safe and making sure people can read your blog in case it becomes blocked by the government. Below are further resources on setting up and mirroring your site in case it becomes blocked at its original URL:

- Anonymous blogging with wordpress and Tor (Global Voices)
- Mirroring a censored wordpress blog (Global Voices)
- Tips on how to blog safely (EFF)
- Handbook for Bloggers (Reporters Without Borders)

Recording Video

Book: Video for Change in Arabic
& Video: How to Create Videos for Change with Arabic subtitles (Witness)

More resources on security and digital activism:

Tactical Tech & FrontLine:
Security in a Box: Arabic English

The Electronic Frontier Foundation:
In-depth guide: Surveillance Self-Defense
& Briefer: International edition of SSD
(both in English)