Cyber Security Guide

Published by the World Association of Newspapers and News Publishers
for the Arab Free Press Forum
November 2013
Written by Alan Pearce

If law enforcement or the intelligence agencies want to monitor anybody's Internet access – read their emails and social media postings, harvest their contacts, find out what they are searching for and downloading, and listen in to their calls – then they can, regardless of the niceties of court orders and warrants. This means that absolutely everything is open to inspection.

Generally, they gain access to computers and smartphones by so-called "social engineering", the art of enticing users to malicious websites and then tricking them into giving out confidential information or by secretly planting malware in their system (known as a "drive-by download"), and via email.

Be aware of social media posts and emails with enticing links, many of which are often shortened so you don't know where you are heading. Short URLs can be enlarged at LongURL.org.

Never open attachments or click on links if you are unsure of their origin. If you must open a suspicious attachment, disconnect from the Internet first and run it through an anti-virus 'sandbox'.

If you are in the habit of reading sensitive documents and suspect you may be being observed, use a separate computer not connected to the Internet, known as "air-gapping".

It is essential to secure your home and office wireless networks by changing the administrator password for the wireless router.

You can easily attract attention by researching sensitive subjects on the Internet or by simply being on a suspect's contacts list.

Suddenly, the Internet is a very dangerous place for journalists.

However, by being alert to the dangers and by using a combination of the tools and techniques listed below it is possible to stay beneath the radar and not attract attention in the first place.

When choosing a password, select a memorable phrase rather than an actual word that can be found in a dictionary. For example, I Like Lots Of Vinegar On My Fish And Chips can be written as ILLOVOMFAC. You should add to this some numbers and non-alphanumeric characters, plus a mix of upper and lower case, making it very difficult to crack by brute force.

If it's not too late, never post any personal information on the social networks – birth dates, family connections, location, travel plans, identifying photographs, etc.

Free, open source software is generally preferable to the paid-for variety because it can be tested by developers and any logging devices or backdoors can be identified. All proprietary encryption software should be treated with the upmost caution.

All of the links given in this guide should open in your browser. Deep Web links marked <!> can only be opened in a Tor-Firefox browser, which you will learn to configure below.

Be alert that no single system or piece of software is 100% secure or safe.

Setting up Defences

Arguably the most security-conscious browser is Mozilla Firefox, available in Arabic. But first spend a minute or two adjusting the *Settings*:

- Click the Firefox logo and select *Options/Options.*
- In the dialog box, open *Privacy* then tick the option *Tell websites I do not want to be tracked*. There is an option to *Always use Private Browsing mode.* Untick *Accept cookies from sites*. Tick *Clear history when Firefox closes*. Under *History* select *Use custom settings for history* and select *Never remember history*.
- Under *Security*, tick *Warn me when sites try to install add-ons*. Remove all exceptions. Tick *Block reported attack sites*. Tick *Block reported web forgeries*. Untick *Remember passwords for sites*.
- On the *Advanced* tab, under *General* tick *Warn me when websites try to redirect or reload the page*. Under *Network* tick *Tell me when a website asks to store data for offline use*. Tick *Override automatic cache management* or set Cache Size to 0.

There are a number of free security add-ons for Firefox. Install the following:

HTTPS Finder or HTTPS Everywhere
Do Not Track Me
BetterPrivacy
QuickJava
DownThemAll

Do not use Google for sensitive searches; use Secret Search Labs or iXQuick.

For quick, anonymous browsing use AllNetTools, Guardster or Anonymouse. Free Virtual Private Networks (VPNs) include FreeVPN and ProXPN.

Erase your tracks with CCleaner and remove sensitive data permanently with the Heidi Eraser. Install free anti-virus software from AVG or Avast.

Using Tor

Tor is a hidden network of the Deep Web where users' identity and location are encrypted and masked, providing very good anonymity. Begin by downloading the free Tor/Firefox bundle. An Arabic version of the browser can be found here. This is safe and easy to install. Simply follow the on-screen instructions and a gateway to the Deep Web can be configured in minutes with no special skills. Also, add an HTTPS enforcer, such as HTTPS Everywhere. Also add Do Not Track Me.

On the opening page, where is says '*Your IP address appears to be…'* are a set of numbers that in no way connect to your computer. You are now anonymous and free to explore Tor or branch off to the Surface Web with minimal risk of being monitored.

Deep Web Entry Points

- The Hidden Wiki <!> http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main_Page
- Tor*Dir* <!> dppmfxaacucguzpc.onion
- Tor*Link*s <!> torlinkbgs6aabns.onion
- Tor*Help* Forum <!> http://zntpwh6qmsbvek6p.onion/forum/

If you have difficulty opening a Deep Website, just try again later and it may reappear. Deep Website availability can be checked at *Is it up?* <!> http://zw3crggtadila2sg.onion/downornot/

To be extra safe, access Tor directly from a USB drive, SD card, portable hard drive or CD/DVD. These can be used on any Internet-ready computer. Install Tor/Firefox and other useful programs directly to the device.

Recommended Free Portable Apps

- PortableApps.com – wide range of open source software for portable devices
- KeePass Portable
- Notepad Portable Text Editor
- VLC Media Player Portable
- IrfanView Portable
- GIMP Portable
- Sumatra PDF Portable
- Eraser Portable
- 7-Zip Portable

Secure Communications

Email: continue using your existing email account for general use so the agencies have something to monitor and without arousing suspicion by going quite. For sensitive correspondence, use Tor or a VPN and sign up anonymously with a web-based free email service (avoid companies like HotMail, Gmail, etc). Consider using a separate computer for these activities.

Email can also be encrypted within the message, along with any attachments, but this in itself may draw attention.

Disable the email's HTML settings and set to *plaintext*.

Secret Messaging: PrivNote, free self-destructing messages. SpamMimic, converts simple messages into *spamtext.* PasteOnion <!> http://xqz3u5drneuzhaeo.onion/users/boi/, paste and share text, images, etc, on the Deep Web.

Private Messaging: Tor*PM* <!> http://4eiruntyxxbgfv7o.onion/pm/. Simple*PM* <!> http://4v6veu7nsxklglnu.onion/SimplePM.php.

Deep Chat: Tor*Chat* <!> http://lotjbov3gzzf23hc.onion/index.php/group/torchat, peer to peer instant messenger. EFG Chat <!> http://xqz3u5drneuzhaeo.onion/users/efgchat/index.php?chat=lobby.

Deep Social Networks: Tor*StatusNet* <!> http://lotjbov3gzzf23hc.onion/. Tor*Book* <!> http://ay5kwknh6znfmcbb.onion/torbook/. Tor*Square* <!> http://ay5kwknh6znfmcbb.onion/torsquare/.

Smartphones & Mobile

Never leave your smartphone or any digital device unattended. If officials or others want to examine it, do not leave them alone with the device. Equally, be very cautious where you recharge your phone. It only takes a few seconds to insert spyware into the device.

For Android users, a good free option to protect against viruses, malware and spyware is AVG Mobilation. Lookout protects iOS or Android devices from unsecure Wi-Fi networks, malicious apps, fraudulent links, etc.

A Mobile VPN will help mask you in public. Hotspot Shield encrypts all smartphone traffic through a Virtual Private Network to hide your identity and prevent tracking. It also allows you to view banned content and access Twitter and Facebook mobile if their services are ever blocked locally.

- Put a security code on your smartphone in addition to the SIM code and engage the auto-locking feature.
- Disable network connections and switch off bridging connections. Do not broadcast the Bluetooth device name and disable automated Wi-Fi connections.
- Turn off Geotagging and GPS location via *Settings*.
- Whenever possible, access 2G, 3G or 4G networks in preference to free Wi-Fi services.
- When covering demonstrations, etc, replace the SD card in the phone with a spare that does not contain personal data and contacts in case of arrest. Also, switch to Airplane Mode to avoid being tracked.
- Avoid connecting personal devices to the office network or computer.
- Update models regularly to keep the operating system in line with security enhancements.

- Remove battery or leave your phone behind when meeting contacts, etc.

Security Apps

You can take your smartphone onto Tor and keep everything off-radar using apps for Android and iOS with access to both Deep and Surface Webs, plus PM and email without being monitored or blocked.

- **Secret Messenger** —Heml.is secure messaging system for iPhone and Android. Secret SMS for iOS will encrypt messages between users and hide them.
- **Secret Cameras** — Secret Video Recorder Pro for Android and iOS. Secret Camera for iOS and Mobile Hidden Camera for Android.
- **Secret Audio** —Secret Audio Recording for Android and Spy Recorder for iOS.
- **Record Calls** — Top Secret Call Recorder for Android and Call Log Pro for iOS.
- **Secret Compartment** — secret folders for Android and iOS.
- **Remove Evidence** — there are shredders for Android and iOS.

Hiding and Transferring Secret Data

- Onion File Hosting <!> http://f4om2jzqkad5zpxv.onion/hosting/login
- Anonyshares <!> http://4eiruntyxxbgfv7o.onion/anonyshares.html
- Onion File Sharing - <!> http://f3ew3p7s6lbftqm5.onion/
- sTORage - <!> http://utovvyhaflle76gh.onion/
- QicPic <!> http://xqz3u5drneuzhaeo.onion/users/qicpic/
- OneSwarm
- Pastebin

Recommended Free Programs

- Comodo Personal Firewall
- Lavasoft's Ad-Aware
- Spybot Search and Destroy
- Anti-Trojans
- Crap Cleaner
- Avast Free Antivirus
- AVG Anti-Virus Free Edition