

Cyber Security Tools



Climate Conference 2022



Index

- 1- Why this guide?
- 2- Ground Rules
- 3- Encryption - encryption and why you have to care?
- 4- Before you come to Egypt
- 5- Encryption of operating systems
- 6- Airport and hotel
- 7- Data

- Encryption
- Share
- Secure Deletion and disposal of data

- 8- VPN
- 9- Bonus Content ++

- Browsers
- Browsers: Cookies
- Browsers: Digital Fingerprint
- Browsers: Addons
- Metadata
- Password managers
- Two-factor authentication/two-step verification
- Secure Communication: Conversations & Webinars



Why This Guide?



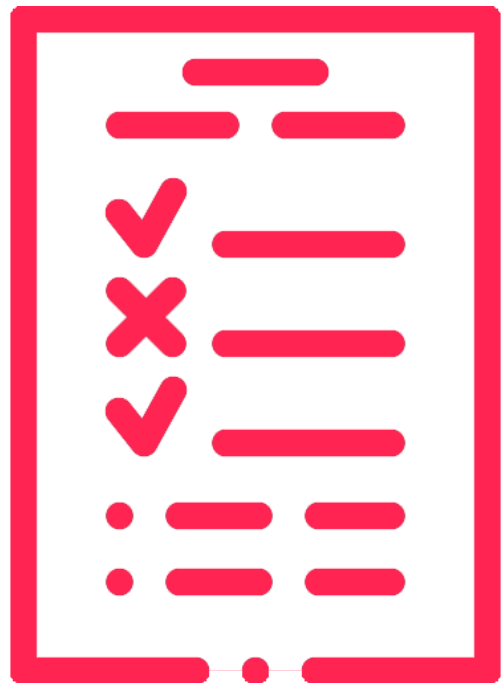
In November 2022, Egypt will host the 27th Conference of the Parties of the UNFCCC (COP 27), with a view to building on previous successes and paving the way for future ambition to effectively tackle the global challenge of climate change.

In anticipation of the technical or security problems that participants may face while using the Internet, This guide came to help maintain the digital integrity of the participants during the use of the Internet due to the blocking policy adopted by the Egyptian Government from 2017.

This Guide contains a set of tools that help you maintain your digital security anywhere in the world and not just Egypt.

Ground

Rules



1. As far as possible, do not leave your devices with a strange hand.
2. Use a VPN.
3. Disable WiFi and Bluetooth when you don't use them.
4. If you are using a business travel laptop, make sure the operating system and soft wares are up to date.
5. Do not keep your personal and business data in the same device
6. Use cloud storage services as much as possible and limit using USB Flash Drives.
7. Avoid connecting your device to any unreliable pieces or accessories such as hard drives, USB Flash Drives or printers.
8. Encrypt the operating system on your laptop and smartphone.
9. Use licensed operating systems and softwares
10. Avoid using pirated software.
11. LGBTQ people are subjected to security prosecution, same-sex relationships may lead to imprisonment, and homosexual dating apps are sometimes used by law enforcement to monitor and target users, so care must be taken before using them.
12. If you receive digital gifts such as data storage media, do not use them before you inform the technical support staff about them after you return home.

Encryption

Why should you care?



Encryption is like your home key to your Home and the Vault where you save what you don't want others to see, a wall of repulsion that prevents you from intruders and hackers and protects you from extortion and other Cyber violence.

Encryption can simply be defined as a way of mixing data so that only authorized parties can understand information, it is the process of converting ordinary human-readable text into incomprehensible text. Decryption can be done by a key. This key is the only way you can decrypt text or data and access it.

Before you come to Egypt



In this guide, we aim to advise you about what digital tools you should put in your bag before you arrive in Egypt. The Internet may seem to you unlike what you are used to, and you may have difficulty browsing a number of sites or slow access to some services or perhaps redirect you to other pages.

>> So.. Before You Come:

1. Contact the Technical Officer of your Organization, who will provide you with advice for your Cyber security during your journey
2. If you're using an Organization's Laptop or other devices, make sure you understand the security rules you have to follow within your Organization's policy.
3. Activate all passwords on your devices and smartphone and encrypt Operating Systems.
4. Keep important data and information on cloud storage, and encrypted Flash drives.
5. Review the data and information you keep on your devices and how much risk you may be exposed to. Once viewed/leaked?
6. Do not take devices such as external hard drives that you will not need during your trip.
7. The average internet speeds in Egypt on 4G networks will not exceed 50 Mbit/s, and the average speed is 20 Mbit/s depending on the quality of coverage. The VDSL broadband has a maximum of 100 Mbit/s, the average speed is 30 Mbit/s, and upload will not exceed 10 Mbit/s.
8. Check with your service provider offers and roaming rates.

6 Airports & Hotels



1. Keep all your digital devices with you, during the inspection time.
2. Turn off your devices during airport inspection.
3. If you are using public Wi-Fi networks at the airport or elsewhere, make sure that the VPN service is activated.
4. Activate Wi-Fi and Bluetooth only when using them.
5. Do not leave your personal devices in the hotel room and do not leave the data storage devices such as hard disks unencrypted, Otherwise, it is considered to have already been viewed/copied.
6. If one of your devices is confiscated, you have to assume that it is no longer safe to use.
7. If you have to leave your devices in the hotel room make sure they are closed and encrypted.

Encryption of Operating Systems



Full hard disk encryption is the most important digital habit to protect you in the event that your devices are confiscated or stolen.

Full hard disk encryption refers to converting all the files it contains into an unreadable (encrypted) form, which cannot be accessed without the password to decrypt them.

8 Encrypt Windows



>> Windows device encryption:

1. Sign in to Windows with an administrator account.
2. Select the Start button, then select Settings > Update & Security > Device encryption. If encryption doesn't appear, it isn't available.
3. If device encryption is turned off, select Turn on.

>> Standard BitLocker encryption:

1. Sign in to Windows with an administrator account.
2. In the search box on the taskbar, type Manage BitLocker and then select it from the list of results. Or, select Start > Settings > Privacy & security > Device encryption > BitLocker drive encryption.
3. Select Turn on BitLocker and then follow the instructions.

Encrypt

Mac OS



1. On your Mac, choose Apple menu > System Preferences > click Security & Privacy > then click FileVault.
2. If the lock at the bottom left is locked, click it to unlock the preference pane.
3. Click Turn On FileVault.
4. You might be asked to enter your password.
5. Choose how to unlock your disk and reset your login password if you forget it:
6. iCloud account: Click “Allow my iCloud account to unlock my disk” if you already use iCloud. Click “Set up my iCloud account to reset my password” if you don’t already use iCloud.
7. Recovery key: Click “Create a recovery key and do not use my iCloud account.” Write down the recovery key and keep it in a safe place.
8. Click Continue.
9. If your Mac has additional users, their information is also encrypted. Users unlock the encrypted disk with their login password.
10. If there’s an Enable Users button, you must enter a user’s login password before they can unlock the encrypted disk. Click Enable Users, select a user, enter the log in password, click OK, then click Continue.



Encrypt

Linux



Linux operating system can be encrypted during the installation process, whether the whole hard drive, or one or more of hard disk partitions.

While similar to the steps of the encryption process, they may vary according to the type of inauguration program used by the distribution you wish to install, whether Ubuntu or Fedora, for example. See the Distribution Directory on its website or contact your organization's technical support team, or contact us via the [HelpLine](#).

Encrypt

ios



1. Go to Settings > Touch ID & Passcode.
2. Press “Turn Passcode On” if not enabled already.
3. Press “Passcode options” to choose a custom numeric or alphanumeric code (recommended).
4. Confirm your device is encrypted by scrolling to the bottom of the Settings > Touch ID & Passcode screen. You should see the “Data protection is enabled” message.

Encrypt

Android



1. Enter the settings > Security > Encryption.
2. If the phone is automatically encrypted there are no additional steps.
3. If it is not encrypted make sure to back up your data and charge the phone up to 80% and then start the encryption process.
4. The process may take some time depending on the size of the data and the speed of the device.

Data encryption helps protect private and sensitive information and data. Even if an unauthorized person or entity has access to it, they will not be able to read it.


>> **Cryptomator:**

The type of encryption used by cloud stores such as Google Drive and Dropbox does not prevent them from accessing data and therefore if a hacker or leak of data may jeopardize your data, here is the role of [Cryptomator](#) that helps you make a folder inside the cloud fully encrypted.

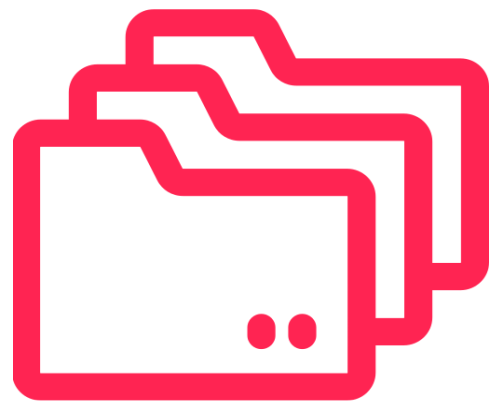
>> **VeraCrypt:**

helps you [encrypt](#) your files, hide them in a fake file, encrypt them at a flash drive or hide an encryption within an encrypted by creating a file with two passwords, each password that opens a locker, which is a step for disguise.

13 Data Encryption



Data Sharing



>> MegaSync:

One of the best cloud storage providers and uses a type of encryption that encrypts data on your device before it is sent to the company's servers. You can use it for cloud storage as well as sharing files via extracting a file link and sharing it.

>> Onion share via tor:

You can use the software to share files and conduct conversations as well as darkweb sites hosting. The software is easy to use.



Deleting data in the traditional way does not actually delete it. As it remains on the hard drive or data storage. To get rid of it permanently it is preferred to write or fill in empty spaces. The proposed programs here rewrite random data in the blank spaces to reduce the ability to recover deleted data.

>> Bleachbit:

Works on Linux, Windows, and Mac OS, and you can permanently delete one or more files and rewrite more than once on the empty parts of the Hard Drive.

>> Shreddit:

It performs the same function as Bleachbit but on Android phones.

>> Apple's Operating systems:

According to Apple's official website If you're an administrator or user, you can locally or remotely erase an iPhone, iPad, and Mac—in most cases using the option Erase All Content and Settings. On the device, erasing (or wiping) obliterates all the keys in effaceable storage and renders all user data cryptographically inaccessible.

16 Virtual Private Networks



VPN's provide a secure connection to the service provider's servers located in different countries around the world, and secure communication between you and the server via an "encrypted tunnel".

By connecting to the Internet via a VPN you can browse the Internet away from censorship, restrictions and blocks practiced by a number of countries. For example, if you are visiting or moving to live in a country like China you will not be able to use Google's services or browse social media sites such as Facebook because of the blocking policy, or what is known as the Great Firewall, similar to the Great Wall of China.

Note: The VPN service provider replaces the ISP here where they can see the sites you are trying to visit or what you do on those sites if they are not encrypted through the HTTPS protocol and collect information about you.

VPN Services that can be connected from Egypt

Egypt blocks traditional protocols for VPN communication and therefore we Recommend a service provider that provides communication via protocols that go beyond blocking.

Virtual Private Networks



>> NordVPN

Provides servers that use a protocol that helps bypass dpi and block connection to their servers, known as Obfuscated servers.

>> AirVPN

Provides a set of protocols that help to bypass the denial of service, most notably OpenVPN over Tor.

>> Torguard

Provides more than one way to bypass blocking. You can learn about it from [here](#).

>> Astrill

Known as one of the best VPN providers whose services operate from within China with high efficiency.



Bonus Content

18 Browsers



Chrome, Google's browser, controls a large share of the browsers market, with Firefox in second place. There are other browsers but they are built on one of the browsers such as Opera, Brave, and Tor.

In all its services, Google collects a great deal of data about users, starting with search history, sites visited, geographical location, etc.

In contrast, [Firefox](#) collects a specific and clear amount of data, unlike Chrome, as most users install Chrome, which is the closed source version based on the "Chromium" open source project of the browser, unlike Firefox browser.

Both browsers provide enough protection and security for users and respond quickly to vulnerabilities, but at [Tech Mentor](#), we recommend that you put your privacy history under the selection of different services.

Bonus Content

Cookies & Fingerprint



>> Browser: Cookies

Cookies are small text files that websites store on your computer, mobile device (smartphone) or tablet when you visit their website. Cookies usually bear the name of the website they came from, and how long the cookies are active (how long they will be effective on your device).

There are “third party cookies”, which are cookies placed by the site you are visiting for the benefit of advertisers to collect data about your use.

>> Browser: Fingerprint

Each user has a unique fingerprint, enabling companies like Google to recognize and track the user on any platform they use.

A set of information describing the content of a particular item such as the photos you take, most notably the date the file was created or modified, the name of the person who edited it, or in the case of the photos the type of camera or smartphone from which they were taken, the time, date, dimensions of the images, aperture and geographical location.

Bonus Content

Metadata



>> To delete Metadata through Android:

- [ObscuraCam](#)
- [Imagepipe](#)

>> through an iPhone:

- [Pixelgarde](#)

>> through an iPhone:

- [ExifCleaner](#)

We recommend using these add-ons to provide better security and privacy, while browsing.

Bonus Content

Browser addons



- 1. Ublock origin** [firefox](#) | [chrome](#) | [edge](#)
Ad blocker helps you browse without pop-ups or other ads, which sometimes infect your device with malwares.
- 2. ClearURLs** [firefox](#) | [chrome](#) | [edge](#)
Automatically removes tracking from URLs to help protect your privacy while browsing the Internet.
- 3. Decentraleyes** [firefox](#) | [chrome](#) | [edge](#)
It protects you from trackers on websites that use free services to deliver their content.
- 4. Cookie AutoDelete** [firefox](#) | [chrome](#) | [edge](#)
Automatically deleted after you close the tab and you can add sites whose cookies you wish to keep.
- 5. Privacy badger** [firefox](#) | [chrome](#) | [edge](#)
Stops advertisers and other third-party trackers from secretly tracking where you go.
- 6. Canvas Blocker** [firefox](#)
Prevents websites from taking the user's fingerprints. and providing a fake fingerprint.

Password Manager is an application that takes the hassle out of saving more than one password for each account you own, and also helps you stop using one password for each account you own, all you have to do is save one password for the application or file of the password manager program and through Save all passwords, and specify a different password for each account and service you use.

Bonus Content

22 Passwords Manager



>> Bitwarden:

An integrated open source password management solution for individuals, teams, and organizations. Provides their application on all platforms, as well as as add-ons for Google Chrome and Firefox browsers.

>> Keepassxc:

Does the same task, but unlike Bitwarden the program provides the encrypted database file and you can save either on an External/cloud storage.

Works on Mac, Linux and Windows operating systems, and you can use the same database for alternative applications.

Android: [Keepassdx](#) and **iPhone:** [lesspass](#).

Bonus Content

2fa & Auth



It is a second step that complicates the attempt to hack your accounts. If the hacker can access your password and try to access your account, he will not be able to because of the obstacle of the second step that Facebook will require, for example, to confirm the entry.

You might think they're the same thing, but two-factor authentication is using a tool like a fingerprint scanner, and two-step verification is like the code you get via a text message from Google to confirm your Gmail login.

There're programs that help to provide the same step without having to use a phone number, you can use the [Aegis app](#) on **Android** phones, and [Raivo OTP](#) on the **iPhone**, and you can use the same functionality on the password management apps we recommended. However, we recommend using separate programs with separate passwords.

The use of instant conversations and remote meetings is the basis of communication between individuals and friends as well as between different work teams, since the covid-19 pandemic and following preventive measures and social distancing, and therefore we recommend safe and open source applications that use end-to-end encryption, which is the best type of encryption that can be used at the present time.

Bonus Content

Conv. & Webinar



>> Signal Messenger:

Works on all different platforms and operating systems and provides real-time conversations between two parties, as well as video and voice chats for up to 40 participants. It is the best alternative to WhatsApp.

>> Jitsi Meet:

With it, you can make voice and video calls, share your screen, and conduct digital meetings with up to 100 participants, and it is the best alternative to the Zoom application. It is completely free and you can use the software on your own server. Just share the room link and activate a password for it if you want.

Tech Mentor.

