DIGITAL SECURITY GUIDELINE FOR HUMAN RIGHTS DEFENDERS AND JOURNALISTS IN ETHIOPIA

Atnafu Brhane

This digital security guideline, developed to help human rights defenders and journalists in Ethiopia, provides essential information on how to use mobile phones, computers, email, and the Internet in a safe and secure manner.

Licensed under a Creative Commons Attribution ShareAlike 4.0 International License
Is my computer at risk?

Human rights activists and journalists must make significant efforts to ensure their computers remain safe and secure. Unfortunately, many computer threats exist that may put you and your data in danger. This guide can help you minimize these threats and increase your online safety.

What kind of threats exist?
- **Malware** (also known as Malicious Software): Malware is a program just like any other except it is designed to make changes to the way a computer operates. In doing so, it damages the computer on which it is run. Malware includes computer threats such as viruses, worms, spyware, Trojan horses, and ransomware (amongst others). Email, text messages, USB memory sticks, and malicious webpages can all be used to spread various types of malware onto your computer.

Why is malware a threat for human rights defenders in Ethiopia?
CitizenLab, a Canadian-based academic research lab focused on the study of digital threats, listed the Ethiopian government as a potential user of spyware in its 2015 report. A leaked document revealed that the Italian spyware company Hacking Team sold spyware software to the Ethiopian government. In turn, the CitizenLab report claims the Ethiopian government is using this software to spy on domestic dissenting voices and as well as critics who travel abroad (Read More).
2 How do I protect my computer from malware?

Online attackers will use all sorts of different tricks to try to get you to install malware on your computer. Accordingly, you must take active steps to protect your computer from malware attacks. The steps below should be followed:

**Turn on your Window Defender:** If you are using a Windows operating system on your computer, make sure the Window Defender is on and updated.

**Download and use Stethoscope:** For best practice security settings on your Windows or Mac computer, use Stethoscope software (available for download on either Windows or Mac). After you install the software and run it, the Stethoscope will immediately start assessing your device’s information and show you the results (screenshot below).

The Stethoscope result shows that the system being reviewed is up-to-date, firewall is enabled, disk encryption is enabled, screen lock is enabled, automatic updates are enabled, and remote login is disabled. According to the above Stethoscope result, the computer has the required security settings. Your Stethoscope results should be similar.
Digital Security Guideline For HRCo

Make sure your operating system is up-to-date:
Make sure you have the latest version of the operating system installed on your computer, and make sure the automatic update setting is ON. You can find this setting on: Select the Start Menu → Type Windows Updates in the search box → select Window Update from the result → in the left select Change Settings → under Important Updates select Update Automatically.

Enable a firewall:
A firewall helps prevent unwanted programs (like malware) from entering your computer. Enabling a firewall will increase the security of your computer. To enable a firewall on your computer:

Write Firewall on Window start search bar → Select Windows Defender Firewall and a dialogue box will appear → select Turn Window Defender Firewall ON or OFF (see figure 1.2 below).

Figure 1.2 Windows Defender Firewall
From a Customize Windows Dialogue box, select the “Turn ON Windows Defender Firewall” Check Box. (See figure 1.3)

This setting will generally protect your computer from a malware attack as long as your Windows system is up-to-date.

2.1 Phishing attacks

A phishing attack is a social engineering attack used to steal an individual’s sensitive information (including online activities and user credentials).

How do phishing attacks work: In general, phishing attacks work by impersonating a legitimate organization and then stealing your data, personal information, and other login information. Research indicates that over 5% of the Ethiopian population use Facebook (a frequent site of phishing attacks), putting at risk the sensitive personal information of millions of Ethiopians. Hackers often impersonate the Facebook website to steal user information. The figure below shows how hackers can target Facebook users by creating imposter Facebook webpages.
As shown in figure 1.4, above, hackers can create a Facebook login page that looks exactly like the real www.facebook.com – but in this case the URL is not actually Facebook’s. Instead, if you look closely, you will see that the hackers replaced the letter “b” with the letter “l” (making the address www.facelook.com). If a user types their login information into the fake page, the hackers who set up this phishing attack will gain access of all of that user’s Facebook information, including messages, photos, and other personal details.

Accordingly, to best protect yourself, always make sure the URL that is written in the address bar is indeed the true website before providing any passwords or usernames in a login page.
3 How do I protect sensitive data on my computer?

Many of us leave sensitive documents on our computer without using any method to protect our data from being stolen. And although having a password on Windows is better than not having one at all, this measure alone is not enough to secure your data. To make your information and documents truly inaccessible to those who would wish to steal them, you need to be familiar with a term called encryption.

Encryption is a mathematical process of making documents inaccessible except to a person who has the password key to decrypt. There are two common types of encryption: (1) data in transit encryption and (2) data at rest encryption.

Data in transit encryption:
Data in transit is data actively moving from one location to another location, through the internet or local network. There is many way to protect data in transit while traveling from one network to other. One of the way to protect data in transit is to use secure cloud storages and use encrypted communication i.e. HTTPS, SSL, TLS...

Data at rest encryption:
Data at rest are a data stored on a hard drive, laptop, memory stick, or any other storage device. In Ethiopia, where Internet penetration is below 15%, most people store their data offline. At the same time, however, most people do not know how to protect their inactive data from theft or hackers. The best way to protect data at rest from being stolen is to employ full disk encryption (discussed below). Enabling full disk encryption on your device will encrypt all the data stored in your computer and protect it from individuals seeking to gain unauthorized access.
For years, police and security personnel in Ethiopia have targeted human rights defenders and stolen their data. The police have used inactive data from the computers and memory sticks of human rights defenders to incriminate them. Thus, full disk encryption should be employed to protect your data from theft by coworkers and colleagues who are forced to spy you by police. With full disk encryption you will also be protected if you lose your device.

You can use encryption in three ways:

- **Full disk encryption** encrypt all data stored on your device.
- **Drive Encryption** encrypt a specific drive on your device.
- **File Encryption** encrypt only a specific file on your device.

### 4 How do I use BitLocker to employ full disk encryption?

As discussed above, employing full disk encryption is essential for protecting the personal and sensitive data on your device. Here, we will show you how to do this by using the “turn ON BitLocker” command on your Windows operating system. This function will encrypt your whole computer, making it much more difficult for unauthorized individuals to access your information.

**Note:** If you cannot find an option to use BitLocker, we recommend upgrading your version of Windows. BitLocker only comes with WINDOWS 10 PRO. The upgrade usually costs around $50 USD. We recommend getting this upgrade instead of using lower cost workarounds like Hasleo BitLocker Anywhere. If you cannot upgrade, try to use the latest version of VeraCrypt for full disk encryption in Windows, or to create a VeraCrypt “encrypted file container” (both discussed below). Encrypted file containers are like new drives on your computer (for example, a T: drive). Anything you move into the encrypted file container will be protected by a password and will only appear once you open the encrypted file container in VeraCrypt. Notably, an encrypted file container can be made to look like anything, even an mp3 file, adding an additional layer of security.
To begin: Go to Control Panel → Click on System and Security → Click on Bit Locker Drive Encryption

1. Under BitLocker Drive Encryption → Turn ON BitLocker
2. After you turn ON BitLocker, you will find an option asking how you want to unlock your drive when Windows starts. If you choose a USB flash drive to start your computer, the USB flash drive will need to be with you all the time (or in any extremely secure location). If you lose the USB flash drive, you might lose access to your computer. If you choose to use a password, you will need to create a strong password that is a combination of letters, numbers, and characters that you can remember easily. In this example, we will use the password option:

3. Enter your password in this dialogue box:
After you press “Next”, you will be given options to save your recovery key. This recovery key will help you to access your data in case you lose your password. You can save your recovery keys on a flash drive, you can print it out, or you can save it on your Microsoft account. If you choose “Save to USB Flash Drive,” make sure your USB flash drive is plugged into the USB port. If you lose your flash drive or if someone steals it, be aware that it is very likely you will lose access to your computer. In this example, we will choose to save our recovery key on our Microsoft Account. This option prevents the recovery key from being stolen physically.

4. Choose how much of your drive you would like to encrypt. Choosing to only encrypt used disk space is fast and recommend for new computers, however, you can choose the specific amount based on your specific scenario. In this example, we will choose to encrypt only the used disk space.
5. Choose which encryption mode to use. In this example, we will use New Encryption Mode. Please note this option is only used on Windows 10 and above.
6. Check the box that says "Run BitLocker system check". This option ensure that BitLocker correctly read the recovery and encryption keys before encrypting the device.

Next, restart your computer in order to start encrypting your drive.

7. When restarting, the BitLocker dialogue box will pop up to let you enter the encryption password to unlock the drive. If you forget your password, you will need to retrieve the recovery key from wherever you saved it. In this example, we saved the recovery key on the Microsoft account.
8. When the encryption process is complete, you will be able to see a lock icon on the encrypted drive when you open File Explorer:
5 How do I use VeraCrypt to encrypt my computer?

Another easy way to encrypt your hard drive, USB flash disk, or other personal files is to use the open source encryption software VeraCrypt. With VeraCrypt you can encrypt your whole partition, drive, or USB flash disk by creating a virtual encrypted disk inside of a file. VeraCrypt helps protect your data from theft via strong security keys. It also supports both standard encrypted volumes and hidden volumes. And you can hide your more sensitive data inside hidden volumes, adding extra protection. If you are somehow forced to reveal your password, the sensitive file that you put inside a hidden volume will remain inaccessible.

To install VeraCrypt:
1. First go to https://www.veracrypt.fr/ or download the software by clicking here.
   • Before downloading the software, make sure you have the compatible software for your operating system. Because the majority of users in our context use Microsoft, we will use the Windows version of VeraCrypt in this example.
   • If you are using a Mac operating system, use this link to download VeraCrypt.
   • If you are using a Linux operating system, click here to download VeraCrypt.
2. To launch VeraCrypt, double-click on the file Veracrypt.exe or click on the shortcut file in the Windows Start menu. Follow the red rectangle for instructions.
3. Click “Create Volume”.

4. Now VeraCrypt Volume Creation Wizard will appear. In this step, you need to choose where you want the new VeraCrypt volume to be created. This step has three options:

4.1 A VeraCrypt volume can reside or be placed in a file, also known as container. For this example, we will use this option to create a VeraCrypt volume.

4.2 A partition drive, to encrypt an external hard disk or flash drive.

4.3 Encrypt a system partition. This option encrypts the whole system, similar to the BitLocker encryption example above.
5. The VeraCrypt Volume Creation Wizard lets you choose a volume type, either a Standard VeraCrypt volume (this option is marked by default) or a Hidden VeraCrypt volume.

- For this example we will use a Standard VeraCrypt volume, which is a normal volume.
- A Hidden VeraCrypt volume helps you to create a hidden encrypted file container inside a normal encrypted volume. This option helps you when you are forced to give away or reveal your encrypted file container password.
Digital Security Guideline For HRCo

6. Now select where you want the file container to be created.
   • A VeraCrypt container can be created on USB flash disk or external hard drive, or you can provide a different location path in your computer, such as desktop or document. This means the file container can be moved or deleted like any normal file. Every file container has a file name with a file extension. The file extension lets you to choose what kind of icon your file container will have. For this example, we will use the .mp3 file extension, which is an audio file extension, with the file name HRCo.mp3. Whoever sees this file will assume it is an audio – not an encrypted file container.

7. Now the encryption option lets you select the encryption algorithm. Choose the default encryption algorithm for the guide.
8. Input the size of the file container that you wanted to create. In this example we created a 1 GB file container. That means up to 1 GB of data will be able to be placed in this container and encrypted. Larger, and smaller, containers can also be created depending on your specific needs.
9. Next put in your password. Your password should be long and made up of special characters. Do not forget to re-type your password on the field provided. Then press **Next**:

![Volume Password screenshot](image)

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ % + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 64 characters.

10. On the next dialogue box, move your mouse as randomly as possible within the VeraCrypt Volume Creation Wizard window at least for 30 seconds. The longer you move the mouse, the more secure your files will be. Once you are finished, press **"Format"** to create the container.
11. You have just created a file container! After you click “OK” make sure to **EXIT** the dialog box.
12. To access your new file container, launch VeraCrypt from the Windows Start menu shortcut. Once the dialog box appears, select a drive letter from the list. This will be the drive letter to which the VeraCrypt container will be mounted. For this example, we selected drive letter T. When you select the file, you have to remember the file name and the location which the file container created. Remember in step 6, we created the file container in the document folder with the name HRCo and the file extension.mp3. Let’s click on “Select File”.

13. Find the file container. In our case, it is an audio file with the name HRCo. Click “Open”.
14. As in the picture below, select the file container. Then click the “Mount” prompt that appears.
15. Type your password (*created in step 9*) and click “OK”.
16. In this example we mounted the container as virtual disk T. Double-click on virtual disk T and open the file. This virtual disk is fully encrypted. Now you can save your work or document in this file container and it will be secure. After you finish working with this file container, don't forget to “Dismount” the container. When you decide to access your encrypted file container again, you must go through the same process above of mounting putting in your password.
According to EthioTelecome's recent report, over 12 million people use smartphone in Ethiopia. The majority of those users are Android operating system customers. In this section, we will review how you can best secure your smart phone using an Android OS.

Note that all phones are designed to give away information like where we are, who we are calling, and who we are texting. Because of this, using a smartphone can be a little like having a spy in your pocket. At the same time, however, using a smartphone provides tremendous benefits. This guide seeks to help you utilize these benefits while reducing your risks as much as possible.

To securely use your Android device:

1. Turn OFF device location unless it is necessary to use.
2. Use messaging applications that support end-to-end encryptions. Make sure the applications you use for calls and messages are from open source software. For best practices of calls and messages, download Signal Private Messenger and Wire Secure Messenger applications from Google Play Store or Apple Store. Make sure the applications you download from the Apple Store or the Google Play Store are verified and real.
3. Review and follow the five subparts below when operating your Android phone.
6.1 Secure message and call applications

**Signal Private Messenger** is a free open source software that supports end-to-end encryption. All communications such as video calls, text messages, group chats, and file sharing are encrypted through the application.

**Signal supports:**
- End-to-End encrypted video calls.
- End-to-End encrypted text messages (both groups and one-on-one communication).
- End-to-end encrypted file or document sharing (both in groups and one-on-one communication).
- Self-disappearing messages.
- Can be locked with a passcode.
- Can be used on other desktop devices, such as laptops.
- Users can download Signal Private Messenger from the Google Play Store or Apple Store, depending on their device's operating system.
- Allows for two-factor authentication.

**Wire Secure Messenger:** Unlike Signal, Wire allows anyone to create an account with an email address or a phone number (Signal only works with phone numbers).

**Wire Secure Messenger supports:**
- End-to-end encrypted video calls.
- End-to-end encrypted text messages (both group messages and one-on-one communications).
6.2 Phone encryption

iOS usually has encryption by default as long as you set a strong passcode for your device. For Android phones, however, you must go to Settings and turn ON device encryption.

• Follow these Steps to encrypt your Android phone:
  Go to Setting → Security → Tab Encrypt Phone → Enter your phone Pattern or Password (it is recommended to use a password to lock your phone)
  Note: The encryption setting varies depending on the version of your Android phone. For security reasons, it is always best to update your Android version whenever an update becomes available.

• End-to-end encrypted file or document sharing (both in group and one-on-one communication).
• Self-disappearing messages.
• Can be used on other devices, such as laptops.
• Users can download Wire Secure Messenger from the Google Play Store or Apple Store, depending on their device’s operating system.
• Users can log out and log in from multiple accounts.
6.3 Circumvention tools

To combat Internet blockage and ensure safe online communications, it is advisable to use circumvention tools such as **Psiphon** and **Orbot**.

**Psiphon**: Once you install Psiphon on your phone or laptop, all your online communication will be encrypted. You can install Psiphon from the Google Play Store or Apple Store. Psiphon was designed to combat Internet censorship. All blocked applications and websites are accessible through Psiphon. The tool is available in Amharic language.

**Orbot**: An anti-surveillance tool that encrypts your Internet traffic. It can also be used to bypass censorship. You can find Orbot at [www.torproject.org](http://www.torproject.org) or on the Google Play Store.

**RiseUp VPN**: Allows you to bypass censorship and encrypt your internet traffic on your phone.

6.4 DuckDuckGo

DuckDuckGo is a secure browser and search engine. The search engine is fully encrypted and (unlike other engines) does not send your search information or what you type to different sites. You can use DuckDuckGo by typing [www.duckduckgo.com](http://www.duckduckgo.com) into any web browser or downloading the DuckDuckGo browser from Google Play Store.
6.5 Secure camera use

Install **CameraV** to ensure secure camera use. CameraV is an encrypted and password-protected camera application that allows you to encrypt all the videos and photos you take on your phone. Secure camera use is particularly important in Ethiopia where activists have been targeted for simply documenting human rights abuses.

Police usually confiscate the phones of human rights defenders and delete all documented pictures. In this context, CameraV is a highly recommended application for human rights defenders to use on a daily basis. You can download CameraV from the Google Play Store.

7 Secure email communications

Securing your email is an essential step for securing your social media account, bank activities, and any other online service that requires your email address upon registration. Many threats target emails, most notably phishing emails which ask users to provide personal information and login credentials by impersonating legitimate organizations or individuals. To combat this threat, it is important to always check and make sure you are receiving emails from real organizations and people.

Additionally, it is important to use email services that support end-to-end encryption to prevent your emails from being intercepted. The following four entries are user-friendly secure email services that support end-to-end encryption.
7.1 Set up two-factor authentication for your Gmail account

Emails coming or going through Gmail are encrypted, making it a very secure email application. You can, however, also set up two-factor authentication (2fa) to protect your account from unauthorized access. Follow the steps in this link to set up 2fa (detailed below).

**Note:** You can set up 2fa in three different ways. The most common way is to get a code through text message (selecting the most suitable verification method will depend on each user’s specific context).

- **2-Step Verification**
  - Set up at least one backup option so that you can sign in even if your other second steps aren’t available.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticator app</td>
<td>Use the Authenticator app to get free verification codes, even when your phone is offline. Available for Android and iPhone.</td>
</tr>
<tr>
<td>SET UP</td>
<td></td>
</tr>
<tr>
<td>Voice or text message</td>
<td>Get codes by text message or phone call.</td>
</tr>
<tr>
<td>SET UP</td>
<td></td>
</tr>
<tr>
<td>Security Key</td>
<td>A Security Key is a small physical device used for signing in. It plugs into your computer’s USB port. Find out more</td>
</tr>
<tr>
<td>ADD SECURITY KEY</td>
<td></td>
</tr>
</tbody>
</table>
7.2 Riseup

RiseUp is a hosting and email service provider that supports secure communications over Secure Socket Layers. Users who wish to use email services from RiseUp must obtain an invitation code from a friend in order to create RiseUp email account. Please try to get the code from the person who is being assigned to digital security matters.

RiseUp Provides:

- Transfer your login information and emails through encrypted channels.
- Support secure group email communication.
- Provide document editing platform called EtherPad.
- Once you get Invite Code, you can request account.
- Allows you to share documents securely: Share Riseup
- Provides internet traffic encryption service through RiseUpVPN.

7.3 Tutanota Mail

Tutanota Mail is a free and open source email service provider. Every email communication and all data in Tutanota is encrypted. Tutanota does not save your login information and allows for anonymity Sign Up. It also removes the IP addresses from all emails.

7.4 ProtonMail

As with Tutanota and RiseUp, all communications sent through ProtonMail are end-to-end encrypted. ProtonMail has an option to set emails to expire after a specific date. The provider also allows you send encrypted emails to non-ProtonMail Users. More information is available at: https://protonmail.com/
How do I stay safe on public WiFi?

It is generally unsafe to connect to the Internet in a public place like a coffee shop, hotel, or airport. That’s because whenever you connect to a public WiFi network the network administrator might be able to see your online activities. Accordingly, if you decide to connect to a public network, you should always follow these steps:

- Enable your Windows Firewall.
- If possible, use a VPN (this allows you to tunnel all of your communications).
- Don’t access a website that stores or requires your personal information.
- Only access secure websites that uses the HTTPS encryption protocol. You can easily identify whether or not a website is secure by looking for the lock key in the address bar.
- Install the HTTPS Everywhere plugin on your browser.