

# DIGITAL SECURITY TRAINING



**DEFENDDEFENDERS**

East and Horn of Africa Human Rights Defenders Project



## ABOUT THIS GUIDE

DefendDefenders present: A simple guide to enhancing your digital security with free tools and easy actions.

DefendDefenders is the East and Horn of Africa Human Rights Defenders Project.

We seek to strengthen the work of human rights defenders (HRDs) throughout the region by reducing their vulnerability to the risk of persecution and by enhancing their capacity to effectively defend human rights. DefendDefenders works in Burundi, Djibouti, Eritrea, Ethiopia, Kenya, Rwanda, Somalia (together with Somaliland), South Sudan, Sudan, Tanzania, and Uganda.

For **Emergency help** please see

<https://www.defenddefenders.org/get-help/> or

Call our 24/7 Emergency Phone Line on +256-783-027611



Text ICT Helpline/Signal/WhatsApp on +256-787-556560

## DEVICE SECURITY

We will guide you through some areas where you should check your devices and accounts for your personal & data security.

### Windows



Most of these settings can be found easily from the start menu. To get to them, press the Windows Key  > In the Search Box  Type here to search > Type Control Panel > Click on Systems and Security > Check the Security Status of Window Defender Firewall, Bitlocker Drive Encryption to make sure they are turned on.

### Mac



Go to Apple menu (🍏) > System Preferences, click Security & Privacy, then click General. For more details on how to enable security settings, go to: <https://apple.co/365i2KA>

### Android



Go to 'Settings'. Enable settings like password/biometric, disable location tracking where need be. For more details on how to enable security settings on Android: <https://nr.tn/3f1BQ9J>

### iPhone



Go to Settings > Touch ID & Passcode and type in your passcode. Then, scroll down and ensure that USB Accessories are not permitted on the lock screen, so make sure the setting is Off. For more information, go to: <https://zd.net/3nXf94p>, and <https://apple.co/2J1bc03>





## BACKUP

A backup is a second copy of your files, kept in a different place than the originals. This means that if you lose your files, because your device was broken or stolen for example, you have only lost the device, and not your data.

### For Windows & Mac:



**Google Drive Synctool** is a good choice with at least 15GB of free storage.



**Microsoft OneDrive** also offers 5GB of free storage, and an easy sync tool - useful if you mostly use Microsoft Office products, as it integrates very easily.



**Dropbox, Degoo, and Sync.com** all offer limited free storage and easy setup. We advise that you choose a tool which suits your needs (if you're not sure, start with Google Drive!) and make sure it is set to back up your files automatically when you are online.



### For mobile devices:

iPhone / iPad: Settings > Apple ID (top option) > Choose your device > iCloud Backup

Android: Varies by make & model, but usually integrates with the Google account you are signed into the phone with. Open your phone's settings app > Tap System > Backup > Turn on your backup service. For more information, go to: <https://bit.ly/3nXhHQ1>

## ONLINE SECURITY



### Phishing

Is the fraudulent attempt to obtain sensitive information, data, and user credentials.

#### Be wary of emails with

- Suspicious attachments
- Grammar mistakes
- Questionable greeting language
- Requiring an immediate response

For more information, go to:

<https://bit.ly/3666qqj> and <https://bit.ly/3q5EIT1>



### Vishing

Social Engineering by Phone (Voice-Phishing = Vishing)

For details, go to:

<https://nr.tn/3q3hnnK>

To see what others could find out about you, use sites such as [ThreatCrowd.org](https://www.threatcrowd.org), [HaveIBeenPwned.com](https://www.haveibeenpwned.com), and [OSINTFramework.com](https://www.osintframework.com) to search your online usernames, email addresses, phone number, and your name. You might be surprised by the results!

### If you find anything you don't want to be public:

- Change your social media settings for whichever service you found your data in.



- Change what you post in future, as information is very difficult to get rid of once it is online.





## ENCRYPTION

Always make sure your device is fully encrypted:




### Windows:

Press the Windows Key  > In the Search Box  Type here to search > Type Bitlocker > Click Manage Bitlocker > Turn on Bitlocker. Put the recovery key into your Password Manager (discussed on the next page) in case you need it later!

If you run a type of Windows which doesn't have the Bitlocker feature, you can also visit VeraCrypt, a free encryption tool with excellent how-to guides found here, <https://bit.ly/3q2Ndh0>.



### Mac:

Choose Apple menu () > System Preferences, then click Security & Privacy > Click the FileVault tab > Turn on FileVault Go to <https://apple.co/39ir7ld> for more information.



### Android:

Go to Settings > Security > Encryption > Click Encrypt Phone. For more information, go to <https://bit.ly/39isi47>



### iPhone:

Go to Settings > FaceID/Touch ID Passcode > Turn Passcode On > Enter your passcode Setting any passcode / password automatically encrypts your device - great feature!



## PASSWORDS & 2 FACTOR AUTHENTICATION

A password manager will store and assist you to create new passwords for all of your accounts (online/offline). This means you can use very long, secure passwords, different for each website, without having to remember them!

We recommend **LastPass** or **Bitwarden** as an online password store, as it has a good range of features in its free version, and is available on a wide variety of platforms. Other good offline alternatives include **PasswordSafe** or **KeePass**.



Multi Factor Authentication (MFA) commonly known as Two-Factor Authentication (2FA) is an authentication method that requires the user to provide two or more verification factors to




gain access to a resource such as an application, online account. Use an authenticator app like **Authy** or **Google Authenticator** instead of receiving codes by SMS. You can have **Authy** on multiple devices by setting the 'Allow Multi Devices' option - that means that unlike Google or Microsoft authenticator apps, you can make sure you always have your codes available on a laptop, phone, tablet etc - all the devices you use.

Get as many accounts as you can under your Password Manager and 2 Factor Authentication - however, if you need to make quick choices, prioritise your email accounts and anywhere that sensitive data affecting human rights is stored.



## MOBILE & COMMUNICATIONS

### Instant Messaging:

Whatsapp , Signal  and Telegram  all provide end-to-end encryption and should be regarded as secure communications channels.

Some consider WhatsApp less secure, but this is not really about whether the actual communication security is secure (it is), but is more about 3 key factors in how the apps get used by people:

- Don't message groups with members you don't know and shouldn't necessarily trust - always keep secure communications to a minimum audience
- Other apps can set timeouts to automatically delete messages later
- Other apps like **Wire** can let you talk to contacts without knowing their real phone number

The most important point is to use one of these tools and **Avoid the Use of SMS where at all possible** - especially if you think you may be targeted, it is not at all secure, and is easy for your mobile provider or related entities to intercept your messages.

There are also desktop & web versions of all these apps, so you can easily use them to copy/paste files and large pieces of text to replace email if you need to.



## MOBILE & COMMUNICATIONS

### Email:

Email is insecure by default, so be cautious with using it for anything requiring security unless you have done some of this setup first - see the previous page on WhatsApp, Signal, Wire & Telegram for free, easy & secure options which can often help to replace Email for many purposes.

**PGP** is a common method of securing email, but it's configuration is notoriously complex for novice users - we would suggest that if you already know how to manage your own PGP keys, this guide is not for you!

However, in recent years there have been efforts to make using PGP much more usable with tools such as Mailvelope and FlowCrypt.



Mailvelope is used across all email systems such as gmail and yahoo. Step by Step use is as: <https://bit.ly/3fDBiBX>



One common method we suggest for users of Gmail is a browser extension called FlowCrypt. Visit [FlowCrypt.com](https://FlowCrypt.com) and follow the easy installation steps to see how you could be using secure email in less than 5 minutes!



## ACTION PLANNING

---



Take an hour or two to sit down with your laptop & phone, and to go through your settings and accounts. You may find it useful, particularly if you are responsible for doing this at an organisation, to make a 'SMART' action plan.

Online you might see various options for what SMART can stand for, but they all focus on a similar key idea: a SMART objective is one which you can easily use to track your progress, prove to key stakeholders that work is progressing, and will help everyone involved stay focused on what is to be done, by when, and who is responsible.

Thank you and Good Luck with securing your devices and your work!

Check <https://www.projectsmart.co.uk/smart-goals.php> for further ideas and information.



© DefendDefenders 2020