Digital Security Guide

Improved Cybersecurity for Activists

Land is Life

October 2022

Table of Contents

Digital Security Guide for Sub-Saharan Africa 3
- Introduction 3
  - General Cybersecurity Practices 4
  - Basics of Cyber Security 6
- Staying Safe from Attacks - Our Recommendations 8
  - Brief Context about Recommendations 9

- Securing Data, Media, Devices from Break-ins 10
  - Hard Drive and Computer Encryption 11
  - Destroying Hard Drives 16
  - Password Security 17
  - Cloud Backups 19

- Online Digital Privacy 20
  - How To Approach: Email Security and Phishing 21
  - Using Anti-virus 23
  - VPN Usage and Safe Browsing 24
  - Multi-Factor Authentication (MFA) 26
  - Messaging Apps 28

- Physical Security and Security in Activism 30
  - Physical Security Questionnaire 31
  - Security Questionnaire for Protests 33
  - Monitoring Your Org's Security 35
  - Monthly Privacy Tool 37

Appendix 39
- Browser Settings 39
- Extra Password Security 41
- Protection against Physical Threats 50
- Protecting Your Local Network 58
- Protect against Theft, Tampering, and Confiscation 63
- Tools 67

Digital Security Guide for Sub-Saharan Africa

Introduction

In this guide, you'll find recommendations on how to best secure your organization. This guide is specifically crafted for indigenous organizations local to Cameroon, Kenya, and Uganda.

High-level Takeaways:

- Verify, don't trust!
- Think before you click!
- Protect your personal information
- Share the guide with others in your network
- Have meetings with your team to discuss the contents of this guide
- Routinize practices from the guide (look at it regularly and establish an everyday security practice)

General Cybersecurity Practices

Digital security requires attention, effort, and care. Making sure that you, your information, and personal devices are safe from attackers should be a daily consideration.

Below are some of the most common practices that you can follow to improve your digital security.

Best Practices

- Before you open a link someone sends to you, try to look at it to see if it leads to where you want to go.
    - Hold your mouse over it or your finger to see what the actual link is! For example, https://twitter.com/home looks safe but http://twiter.io/home does not!

- Never leave your devices unattended. Attackers can use a number of different tools to get information from your devices.
    - Always knowing where your devices are and making sure people don't have access to them is a big step towards digital safety.

- Be careful with what information you share online.
    - Attackers are most successful using phishing emails and texts (pretending to be someone they are not). Things to check:

        - The email address/phone number of the person you are talking to.
        - The website URL you are trying to access.
        - Incorrect information from the person you are talking to.
        - Unusual behavior from the person you are talking to.
        - Try not to share personal information or your credentials online if possible.
        - Never share your personal information if you are not certain of the source or the person behind the phone.
        - Do not be afraid to confirm the identity of the person you are communicating with.

    - 3 places to check before you respond or add your information:[1]
        - The phone number, email address, or website address (URL)
        - The language of the sender (does it sound like them?)
        - The topic of the communication (is it unusual?)

- Find and update the right software.
    - Updating your software keeps your information and devices secure. Software updates include bug fixes and solutions for vulnerabilities that can make your information less secure.
    - Types of software you can update:
        - Operating system (e.g. Windows, Android; they will tell you when they want to update - Follow their instructions!)
        - Applications (e.g. WhatsApp; these applications will also tell you when they are ready to update - Follow their instructions!)

[1]https://blog.malwarebytes.com/101/2018/06/five-easy-ways-to-recognize-and-dispose-of-malicious-emails/

Basics of Cyber Security[2]

1. **Backup & sync your files**
    a. It's important to backup your data. External hard drives are fine, but backing up to the cloud is better.
    b. Backups protect you from ransomware,[3] or from accidentally deleting something, or from hardware failure. Those last two things happen a lot!

2. **Active device security**
    a. Anti-virus, Password Managers, Encryption Tools.
    b. Your browser, your email service, your anti-virus program - all of these might warn you about threats. Pay attention to these warnings!

3. **Safe browsing habits**
    a. Avoid suspicious websites, and understand what your browser saves.
    b. If it's too good to be true, it probably is. Be suspicious when a site requires you to install a program, or to save a download.
    c. Unless you change the settings, a browser will save what you visit. It will be easy for any other site you visit or any other user of your device to see.

4. **Keep devices up to date**
    a. Computers and their software; phones and their apps.
    b. Hackers love to attack devices that are not updated because they are easy targets. When your device says it's time to update, listen to it!

---

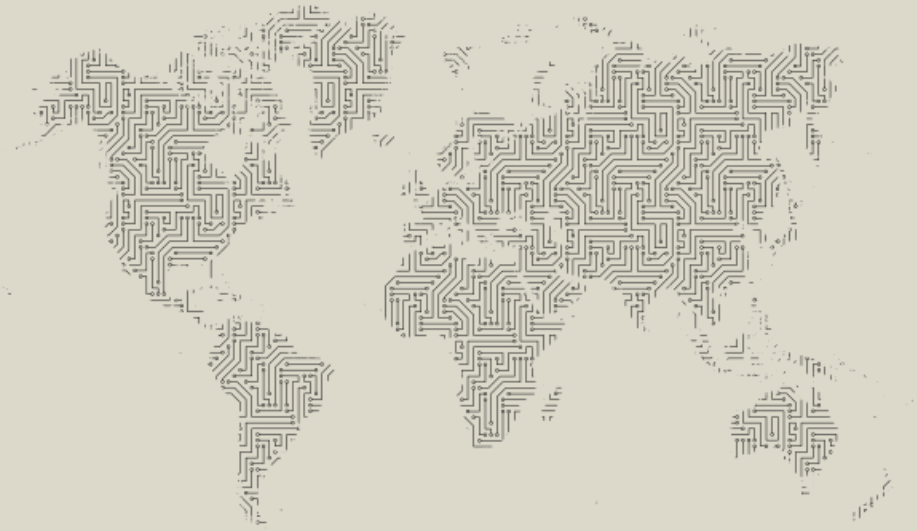
[2] You can find more on these topics in the sections below!
[3] To know what ransomware is, and the definitions of other cybersecurity terms, try the SANS Institute.

5. **If you want to know more about the latest cyber threats like…**
    a. These include ransomware, phishing, malware, and others.
    b. Visit a reputable site, like The CyberWire.

6. **Final Words**
    a. When in doubt, throw it out!
    b. Something strange about that link, or that file, that text, or that email you received? Trash it. If it's important and legitimate, the person who sent it can send it again.

Staying Safe from Attacks

Our Recommendations



Brief Context about Recommendations

The recommendations presented in this section address specific threats of data theft, surveillance, digital hacks on websites and social media, and possible harassment and arrests by governments, policemen, militaries, and private corporate associates in Cameroon, Kenya, and Uganda.

The following security questions will be addressed:

1. How can I prevent data from being stolen/lost if my device is taken by the government or the police, or if they have access to my cloud files? (Encryption pg 11)
2. How to get the data back? (Backups pg 19)
3. How can I help secure my websites and social media accounts from hacks, attacks, and takeovers? (Multi-factor Authentication pg 26)
4. How can I maintain my privacy when being spied on by the government and police? (VPNs pg 24, Safe Browsing pg 25, Physical Security pg 30)

Securing Data, Media, Devices from Break-ins

Threats and Vulnerabilities Addressed

- Data theft from break-ins
- Unsecure electronic devices and hard drives
- Unsecure cloud data

Recommendations

- Hard Drive and Computer Encryption
- Destroying Hard Drives
- Password Security
- Cloud Backups

Tip

If you use flash drives or external hard drives, be sure to lock them or put them out of sight when not in use - may deter an intruder or an attacker

Hard Drive and Computer Encryption

Protect Your Data: If someone takes your hard drive out of your computer, they can read the data unless it is protected by encryption. This is NOT the same as having a password to log into your Windows computer. It is a separate setting.

Keep in mind: This is only available on Windows Professional, Education, or Enterprise editions, not on Windows Home. These versions are usually more expensive than Windows Home, but they make encrypting your computer so easy that it is worth the cost. If you already have Windows Home, you can upgrade to Professional or Enterprise editions.

1. Click on the search button near the lower left corner of the Windows toolbar (it looks like a magnifying glass)

2. Type "Control Panel" in the search bar and click on it when it comes up.

3. Click on "System and Security"

4. Click on "Device Encryption" or "BitLocker Device Encryption".

5. Click on Turn on BitLocker. If BitLocker is already turned on, then you will see an option to "Back up your recovery key". (Instructions about this are at Step 11 below).

6. BitLocker will scan your computer and give you instructions before protecting your hard drive. For example, it might ask you to remove USB flash drives, or to turn on TPM security hardware

7. When it is ready, it will prompt you to shut down.

8. Restart your computer. You may have to do this more than once.

9. BitLocker will resume automatically and encrypt the hard drive.

10. BitLocker will ask you to set a PIN. You will need to enter this PIN each time you start your computer. We suggest saving your PIN in your password manager (see instructions for Password Managers). (You can also use a Startup Key, which is a USB drive with a code on it that allows the computer to start up. We do not recommend this because it may get complicated in use.)

11. You have the option to print or save the recovery key to a file. You can save the file on an external drive, or you can print it out and save the paper. It is important to have this recovery key in case you forget your PIN. However, a copy of your recovery key may be in your online Microsoft account.

External Drive Protection (Encryption)

If your external drive is taken (whether it is a hard drive, or a USB thumb drive, or a flash drive), it will be easy for someone to read everything on the drive, unless it is encrypted. Encryption is a way to store the files in a code that can only be decoded with the right key (such as a password). We suggest using the free service VeraCrypt to encrypt your external drives.

Creating your VeraCrypt drive

1. Download VeraCrypt from this site: https://www.veracrypt.fr/en/Downloads.html (The version you most probably want is the Windows MSI file under the "latest stable release. However, any of the options under Windows should work to install VeraCrypt on your Windows computer.)

2. After it has downloaded, double click on the file to start the installer. Follow the instructions on the installer (give it permission to make changes).

3. Plug in the drive that you want to encrypt.

4. When you have VeraCrypt installed, start VeraCrypt by finding it in the Start Menu (click on the Windows icon in the lower left of the toolbar).

5. Select the drive letter you want to use. We suggest using "V:" for VeraCrypt so that you don't confuse it with any other drive you have plugged in.

6. Click the Create Volume button.

7. Select "Encrypt a non-system partition/drive". Click Next.

8. Select "Standard VeraCrypt volume". The other option "Hidden VeraCrypt volume" is for advanced users and you may find it useful depending on what is threatening you. If you feel that someone may force you to enter your password to open an encrypted drive, the "Hidden VeraCrypt" volume could be helpful. Click Next.

9. Select the Volume Location. Click on the "Select Device" button. Find your external drive among the options. Note, this will never be "Harddisk 0" or your "C:" drive. It will be one of the Removable Disks. It's better to only plug in the one external drive you want to encrypt to

make sure you select the correct drive.

10. Volume Creation Mode. If the drive you are using already has data that you want to keep, select “Encrypt partition in place”. If the drive is empty or it does not have any data that you want to keep, select “Create encrypted volume and format it”. If you select this option, everything on the drive will be gone and you will NOT be able to get it back!

11. Encryption Options. Select AES. (The other options are also acceptable.) Click Next.

12. Volume Size. Verify the size of the “partition”. The partition is the part of the hard drive you want to encrypt. Usually, an external drive has just one partition which is the size of the whole drive.

13. Enter password. (See our password section to pick a good password and store it!)

14. You may also use a keyfile. This will create a file that acts as a second password. If you use this option as well, you will need BOTH the password and the keyfile to access your VeraCrypt drive. Click Next.

15. Answer whether you will have files larger than 4 GB. Click Next.

16. Volume Format. Select the Filesystem. Windows can read FAT, NTFS, and exFAT. We suggest NTFS. Click Format.

To access your new VeraCrypt drive:

1. Plug in the drive to the USB port.

2. Click Cancel if Windows asks you to format the disk.

3. Start VeraCrypt by finding it in the Start Menu. (click on the Windows icon in the lower left of the toolbar).

4. Select the drive letter for your VeraCrypt drive. (We use "V:")

5. Click on the Select Device button. Select the correct partition and click OK. Note, this will never be "Harddisk 0" or your "C:" drive. It will be one of the Removable Disks. If you have more than one Removable Disk and you're not sure which Removable Disk the VeraCrypt drive is, then unplug all of the other drives and Exit VeraCrypt. Start from Step 3.

6. Click the Mount button. Enter your password. If you used a keyfile, check that box and search for the keyfile.

7. VeraCrypt will take about one minute to get your drive ready.

8. Open Windows Explorer and look for the drive labeled "V:" (or whichever letter you selected for your VeraCrypt drive in Step 4). You should now have access to the files there. Note that you can open files in the VeraCrypt drive, change them, save them, etc.

Destroying Hard Drives

If you want to get rid of an old hard drive, it is not enough to just delete the data. A skilled person can read deleted data off a hard drive, even if it doesn't work anymore. Below we show how to destroy two different kinds of drives. Remember, your computers (desktop and laptops) have hard drives inside them. Remove them before giving away or throwing away your computers, and follow the instructions below.

Hard disk hard drives. These are the heavier hard drives that have a round disk ("platter") that spins while it is being read and written to. They are either 100 x 70 mm or 147 x 102 mm.

The best way to destroy these is to take a power drill and drill holes in the drive until the round platter shatters. Or, you can try to shatter the drive with a hammer. The last option would be to encrypt it as you would solid state hard drives that you want to throw out. (See the "Hard Drive and Computer Encryption" section for instructions.)

Solid state hard drives (also known as flash drives). These are the lighter drives. They can be very small, like a USB thumb drive, or the same size as hard disk drives.

These are more difficult to physically destroy, so we suggest encrypting the drive with a long password that you do not keep. (See the "Hard Drive and Computer Encryption" for instructions.). Then you can dispose of the flash drive any way you wish and it will not be readable.

Password Security

Complex and strong passwords are difficult to hack.

Here's a quick table of how long it takes a hacker to guess your password in 2022. (source)

Character Count	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper, and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 sec	7 sec	31 sec
8	Instantly	Instantly	2 min	7 min	39 min
9	Instantly	10 sec	1 hour	7 hour	2 day
10	Instantly	4 min	3 days	3 week	5 month
11	Instantly	2 hour	5 month	3 year	34 year
12	2 sec	2 day	24 year	200 year	3k year
13	19 sec	2 month	1k year	12k year	202k year
14	3 min	4 year	64k year	750k year	16m year
15	32 min	100 year	3m year	46m years	1bn year
16	5 hour	3k year	173m year	3bn year	92bn year

17	2 day	69k year	9bn year	179 bn year	7tn year
18	3 week	2m year	467bn year	11tn year	438tn year

Here is a password generator you can use to create new passwords.

If you have trouble remembering your passwords, be sure to explore different password manager options available to you.

Cloud Backups

*Don't trust only your hard drives! They can be stolen, and they **will** stop working eventually!*

Description: We suggest using a cloud storage service to back up your data. Cloud storage services offer hard drive space on their computer systems that is backed up in multiple places so you will not have to worry about losing your data, as long as you remember your login information and keep the service active. If internet access is not consistent or reliable where you work, it would be better to use these services only to back up the data (instead of working off the cloud directly).

Cloud Tips

- Common services: Google Drive; Microsoft OneDrive.

    Start free, but pay for more space.

    High quality, easy to use.

    Not encrypted - if the government might demand Microsoft or Google turn over your data, then they will be able to read it. Use BoxCryptor with these services to encrypt your cloud files.

- Encrypted Cloud Providers: NordLocker, Sync.com.

    Even the cloud company has "zero-knowledge" of your data.

    Paid service.

    Might not be as easy to use.

- Multi-factor Authentication (MFA) - don't forget to use this with these accounts!

Online Digital Privacy

Threats and Vulnerabilities Addressed

- Intercepted Communications
- Surveillance by the government and police
- Hacks, attacks, and takeovers of social media and websites.

Recommendations

- Messaging Apps
- Email Security and Phishing
- VPN Usage and Safe Browsing
- Using Anti-virus
- Multi-factor Authentication

Tip

Always use a VPN and be careful of any links you click!

Be aware of scams that are too good to be true!

How To Approach: Email Security and Phishing

Email is one of the most common ways for people to communicate today. It makes it easy to send/receive messages or files, but it wasn't designed with security in mind. Here is some more information about this topic.

Overview:

Most email service providers can see what you are using your email account for. This means that sometimes, governments can request this access.

Attackers will try to access your email account because usually people connect many websites and services through a handful of email addresses.

Ways to be more secure:

- Set up multi-factor authentication (MFA) on your email accounts. MFA just means that when you log in to your account, it will check to see if it is really you by:
    - Calling or texting your phone
    - Sending an email to your other email account
    - Asking you for a code or a physical device

- Consider creating an email account with a secure provider like ProtonMail or Tutanota. These providers are a step up in terms of encryption and not accessing your data.
    - They generally can't see the body of your email message.
    - If you communicate with others who are using the same secure email provider, the message is even more secure (via end-to-end encryption).

Phishing

What is phishing? Phishing is "the process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity using bulk email which tries to evade spam filters".[4]

What is social engineering? Social engineering is "the art of manipulating, influencing, or deceiving you in order to gain control over your computer system. The hacker might use the phone, email, snail mail or direct contact to gain illegal access."[5]

Phishing attacks will use emails, phone calls, or malicious websites to solicit your personal information. Common Indicators:

- Suspicious attachments
- Poor spelling and odd layout
- Spoofed hyperlinks and websites
- Generic greetings and signature
- Suspicious sender's address

Be aware of scams that are "Too good to be true."

[4] KnowBe4: https://www.knowbe4.com/phishing
[5] KnowBe4: https://www.knowbe4.com/what-is-social-engineering/

Using Anti-virus

This helps prevent programs you might accidentally or mistakenly install from attacking your computer in various ways. Luckily, this is easy to set up and is built in Windows.

1. Click on the search button near the lower left corner of the Windows toolbar (it looks like a magnifying glass).
2. Type "Control Panel" in the search bar and click on it when it comes up.
3. Click on "System and Security"
4. Click on "Security and Maintenance"
5. Make sure that "Network firewall" and "Virus protection" are both enabled. If they are enabled, you will see links for "View in Windows Security" under each of those settings.

VPN Usage and Safe Browsing

VPN Usage

Why this is important: When you send and receive information over the internet, it is possible that it can be gathered by someone with their computer in between you and the website (a "man-in-the-middle"), or your internet service provider. For example, if you are using wi-fi for your internet, another person on the same wi-fi network could gather everything that you send and receive while you are connected to that network. Or the government could make your internet service provider keep track of all of your internet activity. If you use a VPN, you can make the information sent and received unreadable by anyone on the network or by your internet service provider; only your VPN company's server will be able to read it before it's sent to the site you're visiting. VPNs will also prevent a website from getting your IP address (that is, your internet location address), which can be used to pinpoint you or your location.

There are several VPN providers. We do not recommend free VPNs, with the exception of ProtonVPN. Unfortunately, the free version of ProtonVPN is not as fast as their paid versions. Other well-respected VPN providers are Mozilla, Mullvad, ExpressVPN, and NordVPN. Note that if you purchase a VPN, you will probably be able to install it on your phone and your computer with the same account. For the best security with a VPN, check the settings of your VPN software to make sure that it starts up with your computer or phone, and that it blocks internet traffic if the VPN is off.

Using Safe Browsers

There are various ways you can be attacked through your browser. First, your browser generally saves information about your internet traffic. If you do not change the settings on your browser, someone can open your browser and know what sites have visited, enter sites where you are already logged in, and even learn what information you have entered in your browser (for example, names, addresses, credit card numbers, passwords). Second, if you accidentally visit an attacker's site, a browser without protections will have a greater chance of making a successful attack on your computer or phone.

For general use, we recommend using either Mozilla Firefox or Brave browsers on your computer and the Bromite browser on your phone. We also recommend that you use "private" browsing when you don't want the browser to save what websites you visit. You can also change your browser settings for increased privacy, but changing settings is a detailed process (instructions are in the Appendix). It may be easier to use the LibreWolf browser because it has safe settings by default.

Your browser might offer to save your passwords. We don't recommend this. Use a separate password manager as we recommend above.

When it is important that your internet browsing cannot be traced back to you, we recommend using the Tor browser in combination with a trusted VPN.

You can find the Tor Browser on www.torproject.org. It helps you stay anonymous by making it difficult to trace the traffic back to your IP address, which can give your physical location. But Tor by itself does not encrypt traffic. This is one reason to use a VPN with Tor, because the VPN encrypts traffic. Tor is available on your computer and on your phone.

Multi-Factor Authentication (MFA)

(Aka 2-factor authentication or 2FA)

MFA may be the single most important thing you can do to protect your accounts.

Passwords have been hacked or stolen from websites on a regular basis. Phishing emails can trick a person into giving their passwords to an attacker's website. MFA requires more than just a password to log in. With MFA, even if someone manages to steal your password, they don't necessarily have access to your account.

You can usually find the MFA setting in the "security" settings of your account (whether it's an email account, an online bank account, or other type of online account).

Different types of MFA

There are several different types of MFA. We go over a few of them below.

Recommended:

- Authentication app. This is an app that you would install on your phone. Google Authenticator and Microsoft Authenticator are good, free options.
    - In use: After you enter your password in your account, the website or app will ask for a code. You open up your

authentication app and find the website and app in the list, and enter the code into the website.

- Hardware token. This is the most secure. But, it is also the most expensive and the least convenient. Sometimes accounts do not have this as an option.
    - In use: A hardware token (such as a Yubikey) is something that you would plug into your device when you want to log into an account. You would enter your password, and then the website or application would ask for the hardware token. Usually, you would have to touch the hardware token that is plugged into your device. The hardware token interacts with the website or the app, and logs you in.

- Email address. This method is only as secure as your email account. If your email account is protected by MFA, this may be a convenient option. However, many sites do not have this option.
    - In use. After you enter your password into your account when logging in, the website or app will tell you that it is going to send you an email. You will receive the email message with a code that you enter into the website or app.

Least recommended:

- SMS or text message. This is the least recommended option because it is the least secure. There are various ways that a skilled person or government could hack this MFA method.
    - In use. After you enter your password into your account when logging in, the website or app will tell you that it is going to send you a text or SMS message. You will receive the SMS message on your phone with a code that you enter into the website or app.

Messaging Apps

SMS/Text is NOT secure! Use end-to-end encrypted apps suggested below.

SMS or text messaging are not secure methods of communications. A government can force a mobile phone company to turn over those messages, or another group with special equipment can read those messages. There are various end-to-end encrypted messaging apps you can use so you and the person you message can read the messages.

Recommended Messaging Apps

- Signal - Most Recommended

  Signal is a secure messaging app available in your phone's app store. Secure messaging, phone calls, and video calls are all available between Signal users.

  Ability for sender to delete messages on both ends. You can do this for individual messages, or you can set a time limit to delete all messages in a conversation.

  Signal also has other benefits: groups, emojis, and limited use of "metadata" (that is other data besides your message, such as location, contacts, etc.).

- WhatsApp - Use with Caution!

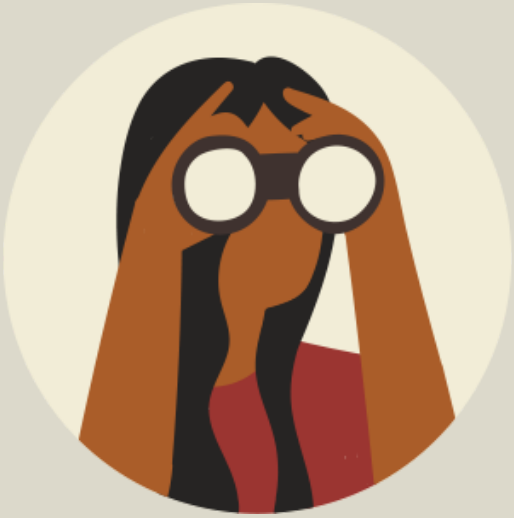
  Same features as Signal, and it uses Signal's encryption. However, we do not recommend it as highly as Signal because WhatsApp (and its owner Facebook) captures and stores a large amount of metadata. Governments may request or require Facebook to reveal that data.

  A lot of people use WhatsApp and a lot of false information and dangerous links are shared on it. Use with caution!

- Wire - Least Recommended

  As secure as Signal, but you don't need a phone to use it. Unfortunately, the free version is too limited.

Physical Security and Security in Activism



Threats and Vulnerabilities Addressed

- Physical protection techniques for activists
- Camera Surveillance
- Assaults, Kidnapping, Assassinations
- Exposure of Activist Work

Recommendations

- Checklist for Physical Security
- Checklist for Safe Protest

Tip

Plan ahead if you are planning to participate in public action.

Physical Security Questionnaire

Thinking about your physical security is an essential part of digital security. If someone gets physical access to your phone, computer, or home, they can access information about you.

General Things to Consider:

- When you are away, how do you know if someone came over?
- When you are home, how do you know if someone is there?
- What do you have at home?
- Consider installing gates around the location you want to be secure.
    - This can discourage intruders from entering your home.
    - It can also give you time to react if you hear them coming.
- Place locks on the windows and doors that can be reached from outside.
    - Be sure to check these locks periodically, based on how often you are there.
- Video surveillance (also known as CCTV), burglar alarms, and motion sensors are more options.
    - CCTV will let you see what is happening when you are away.
    - Attempts to break into the location are recorded.
    - You will have more time to react to intruders if you can hear/see them coming.

- If you use flash drives or external hard drives, be sure to lock them or put them out of sight when not in use - that may deter an intruder or an attacker from stealing them.

Security Questionnaire for Protests

Protests are an important part of civil society around the world. Here are some suggestions for how to plan ahead if you are planning to participate in public action.

Be mindful of all of the things you are bringing to the event.

- Consider bringing a notebook and a pen instead of your device.
    - The government can potentially track your location through your cell phone or other devices.
- Consider bringing a mask or scarf to cover your face.
    - The government might have access to facial recognition technology.

Who are you traveling with?

- Pairs or small groups are more difficult to detain by the police or other actors than individuals who are alone.

How will you be traveling to and from the event?

- Is your home or office secure while you are away?
- How well do you know the place you are going to?
    - Is there any way you can plan different routes on the day of the event?

        - Roadblocks and police checkpoints may appear during the event.
        - Learning different routes will help you know if you are being followed.
- What is your exit plan if you need to leave quickly?

Monitoring Your Org's Security

As part of better understanding the security environment of grantees and what solutions are effective, it's important to continue to collect information on the cyber attacks experienced by local organizations. Here's a few things you can do:

Start a security incident register.

- These are easy and practical in seeing the number of incidents you and your collective have had over a set time frame. These are used widely and help in analyzing the type and frequency of threats that people receive. Nothing is too small to register.
    - Someone suspicious outside your meetings?
    - Have you received calls from strange numbers?
    - Is someone from an opposing group taking photos at a rally?

- Include:
    - Time
    - Date
    - Description of incident
    - Who did it?

- It helps to have the time, date, description of what happened, who could have been the perpetrators and who might be the target. Just

like everything else, don’t worry about having all the information. Not having information on this at least tells you what you need to be looking for next time. However, it should be noted that adversaries can conduct the same human intelligence gathering on you.

Monthly Privacy Tool

We created this activity so that you could see what information is available online about you and people you know. You can make copies of this page and work through it every month with your team.

Search for your name on search engines in your country.

- Can you remove any of this information?
- Look for images.
- Look for a video.
- Look for your address.

Try looking for family members. How about coworkers?

- Does it say any information about you?
- Can you remove any of this information?

What information have you shared publicly recently?

- Have you posted any private information?
- Can you remove any of this information?

What applications have you been using?

- What permissions have you given those applications?
- What permissions can you change today?

Are all of your passwords in your password manager?

- Do you have a strong password for your password manager and use multi-factor authentication (MFA)?
    - Can you start using MFA?
- How many passwords do you reuse?
    - Can you change them to different passwords?

When was the last time you logged out of your accounts?

- Are you logged in at other devices?
- Can you log out of all of your accounts across devices today?

Appendix

Browser Settings

Extra privacy and security for your browser.

Your browser saves what pages you visit, where you log in, etc. This can be convenient because you don't have to log in every time you open the browser, but it also means anyone else who uses the computer can open the browser, read your email, etc. The safest way to use a browser is to use all of the following settings, but can pick and choose which ones you want depending on your risk level.

Mozilla Firefox

- Click the three-lines icon just under the "X" at the upper right of the Firefox window.
- Find Privacy and Security on the list on the left side of page that comes up

    Choose "Strict" under Enhanced Tracking Protection.

    Check the box for "Delete cookies and site data when Firefox is closed" - Note, this means that you will be logged out of your accounts when you close the browser.

    Uncheck all the boxes under "Logins and Passwords", except for "Show alerts about passwords for breached websites

    Uncheck all the boxes under "Forms and Autofill". You may also want to delete whatever has already been saved by clicking on the "Saved Addresses" and "Saved Credit Cards" buttons.

Under History, Choose “Never Remember History” after “Firefox will”. This means that when you close your browser, nothing will be saved from your previous browsing.

Check “Block pop-up windows”

Check “Warn you when websites try to install add-ons”

Check “Block dangerous and deceptive content”, “Block dangerous downloads”, and “Warn you about unwanted and uncommon software”

Under “HTTPS-Only Mode”, check the box for “Enable HTTPS-Only mode in all windows”

Brave Browser

- Click the three-lines icon just under the “X” at the upper right of the Firefox window.
- Find Shields on the list on the left side of the page that comes up

  Change trackers and ad-blocking to “Aggressive”

  Make sure “Upgrade connections to HTTPS” is on
- Find Privacy and Security on the list on the left side of page that comes up

  In “Clear browsing data”, click on the “On Exit” tab and check all the boxes. This means that when you close your browser, nothing will be saved from your previous browsing.

  In “Cookies and other site data”, select “Block third-party cookies”.

  In “Security”, make sure that “Standard protection” is selected.

  Make sure that “Always use secure connections” is on.

  Make sure that “Use secure DNS” is on.

Extra Password Security

Passwords are important tools for keeping your data and identity secure. Unfortunately, attackers know this, and they have many tricks they can use to figure out your passwords.

But you can defend against those tricks by applying a few important tools and tactics. The most effective strategy is to make passwords that are LONG, RANDOM, and UNIQUE. To do this reliably, you will need to use a secure password manager. It is also important to set up multi-factor authentication whenever possible.

If your passwords have been compromised

- Search "Have I Been Pwned" to see if your accounts are reported as compromised.
    - Change any of your account passwords you find there immediately, using the instructions for setting up a password manager below.

- Even if none of your accounts show up here, you should still follow the instructions below, as many account breaches are not reported.

Avoid common weak password strategies

Here are the most common ways attackers learn your passwords:

- They can guess your password:
    - Using your personal information such as important dates, names, famous quotes, songs or authors you like
    - Using a dictionary
    - By slightly changing passwords you have used before
    - Using software to try all possible combinations to unlock your passwords

- They can look for:
    - Where your passwords are written down (like notes around your desk)
    - What you're typing when you enter your password
    - Passwords that have already been breached and are available online

- They can trick you into:
    - Installing malware app to record your password
    - Making you type your password into a fake login page through phishing
    - Providing your passwords or other information by pretending to be a support person or someone you know (also known as social ingeneering)

Follow these guidelines to protect yourself against those tactics:

Be aware that the following strategies, on their own, DON'T make your passwords safe:

- Using words or numbers related to you or people and organizations around you, like:
    - names of people, pets, or organizations
    - dates of birth, important anniversaries or holidays
    - telephone numbers or addresses
    - or anything else a person could learn by researching you and people around you
- Using common phrases, such as famous quotations, song lyrics and poems.
- Replacing characters with a similar symbol (e.g. replacing "a" with "@" etc.)
- Putting exclamation marks, numbers, or other punctuation at the end
- Starting Each Word With Upper Case Letters
- Using single words in any dictionary (five or more words in a row is ok)

Use a Password Manager

- Get KeePassXC (for Linux, Mac or Windows), KeePassDX (for Android), or StrongBox (for iOS).
- DO NOT reuse passwords.
- Let the password manager generate and save a long, random, unique password for each of your logins.
- You may want to set up password managers together with your colleagues. You can help each other in the process.

    - You may want to familiarize yourselves with the process of sharing passwords safely. However, whenever possible, it is more secure to set up separate logins for different accounts.
- Read guides to KeePassXC and KeePassDX.

Backup your password manager's database

- How to back up KeePassXC
- How to back up KeePassDX
- How to back up Strongbox

Remember a few secure passwords

- Use the diceware method to generate passwords for your password manager and other passwords you must remember (like the password to unlock your password manager or devices):
    - Get a list of numbered words and some dice.
    - Roll dice five times to get a five-digit number (for example, 6,2,5,1,1).
    - Use the word in the list with the corresponding number.
    - Repeat this five times. Use those five words as a "passphrase" for one login.
        - Do not re-use this passphrase anywhere else.
    - Next, create a mental image using the words, in order, which will help you remember the phrase.
- Practice entering these passwords regularly, daily at first and then at least once a week. Repetition will help you commit these passwords to memory.

If there are passwords or backup codes you need to write down on paper and store securely

- If you must write passwords down on paper, store them in a locked place like a safe or desk drawer.
    - It is important that your passwords not be visible to those who pass by, or easy to find and copy.
    - Do not keep them in your wallet.
- Destroy any paper copies of passwords or backup codes thoroughly as soon as you no longer need them.

If you decide to use an online password manager

- Avoid storing highly-sensitive account information (like financial account or recovery account logins) in the online database.
- Protect access to your online database with 2-factor authentication

If you need to share passwords

Avoid sharing passwords whenever possible.

- If you must share a password with a friend, family member or colleague, change it to something temporary and share that password. Change it to something secure again when they are done using it.
- Consider creating separate accounts for each individual who needs access; many services make this possible. You can limit what actions these accounts are allowed to take, and what they can see.

- Set up your password manager so you can use it collaboratively. Password managers make this possible.

Do not give your password when someone emails, calls, or messages you

- Go to the app or site for the service that supposedly sent you the message to verify the request.
    - See guides on basic security and social media to find different services' records of alerts they have sent you.
- If it appears to be a person or office you know sending the message, contact them through another channel to verify whether they made the request.
    - For example, if the message was an email, call them.
    - Do not click links in the email or send a response.
- Be aware when a message is trying to frighten you, make you curious, make you feel you will miss an opportunity, or otherwise make you act quickly and without thinking. Pause, remain calm, and find other ways to verify messages like these.

When to change your password

- Regularly change passwords you use:
    - Online, every six months
    - Offline (for example, to log into your laptop), once a year
- Change your password immediately when:
    - it appears your account, devices, or colleagues and people around you have been victims of a breach.
    - you get a credible warning from the services you use that there was an attempt to log in from an unauthorized device or location.
        - Look for news reports about breaches.

        - If you receive an email or alert, double-check on the service provider's own website that they sent the alert.
    - you entered your password on an untrusted, shared, or public device (it might have malicious code installed).
    - you are concerned that someone watched you type your password.
    - Minimize damage by warning others who may also have been affected.
    - See these guides on social media and the basic security guides for Android, iOS, Linux, Mac, and Windows for instructions on how to change your device passwords

Mind where you are and who can see

If you're in a public space and type your password, be mindful of whether you can be seen or recorded.

- Check to see if anyone is watching your keyboard or phone while you type your passwords.
- Use a privacy protecting screen to make it harder to see what you are typing.

Use two-factor authentication (2FA or MFA)

- Check which services offer 2FA.
- It is crucial to set up 2FA for:
    - your bank accounts or money apps
    - accounts like your email address, social media, or others you would need in order to recover other accounts
- Your 2FA options may include:

    - Using an authenticator app or program like Google Authenticator, Okta, or Duo. We recommend the Aegis app on Android or Raivo OTP app on iOS/iPhone.
        - When using this option, it's important that you protect your mobile phone from malware.
- Using a hardware device--often called a security token, dongle, or USB "key"--which you can plug into your device or set up to use NFC (near-field communication).
    - Some examples are Yubikey, Nitrokey, Google Titan Key, and Thetis Key
    - Hardware devices may not be usable on mobile devices.
- You can use one authenticator app or hardware device for multiple services, or set different services up with different forms of 2FA for additional protection.
- Once you set up your device for 2FA, the above two options do not require an internet connection to generate codes. Using email for 2FA will require an internet connection.
- Ranking 2FA options in order of safety, an authenticator app or hardware device is safest, then email, then SMS.
    - SMS text messages are not encrypted and attackers have successfully intercepted these one-time codes on their way to a target's phone.
- Once you have set up 2FA, when you enter your username and password you will also use this additional way to prove you are who you say you are, by inserting your key, entering a code from your authenticator, or entering the code you are sent.
- Do not disable two-factor authentication once you have set it up. Some services may offer you the option to turn it off for a while for convenience, but consider

Keep 2FA backup codes safe and separate

- If you are given backup codes when you set up 2FA, store these codes in a password manager.
- Ideally, to keep these codes separate from other information that could be used to access your accounts, create a separate KeePass database and save it on another device.

Avoid fingerprint or face unlocks (biometrics)

- If your device is set to unlock using your face or fingerprint, change your settings to use password unlock instead.
- See the basic security guides for Android, iOS, Linux, Mac, and Windows for instructions on how to do this.

Set safer recovery questions

Many web services ask for "security questions" or "recovery questions" when you create an account. To make it less likely someone can guess these:

- Provide fake, unrelated answers to these questions.
- You can even use another random, unique code generated by your password manager.
- Save your responses in your password manager so you don't get locked out.

Protection against Physical Threats

We do a lot of digital work to protect sensitive information. But that is only one aspect of digital security. The work you do to protect your valuable devices and documents can be undone in an instant if your devices are lost, stolen, tampered with, confiscated, or damaged. Planning for physical security is as important as protecting your devices digitally.

Careful risk assessment, maintaining a safe computing environment, and writing up a security policy can help you avoid physical disasters. Both criminals and politically motivated attackers may have reasons to target your data. They might be seeking financial information, sensitive data related to your work or personal details they can use to intimidate, blackmail or impersonate you. Criminal and political attacks are often difficult to distinguish, and attempts to obtain sensitive data often look like attempts to steal valuable hardware.

Start with the steps below to develop a physical security plan.

Think about inexpensive, low-tech security measures

While it is important to budget for physical security, money is not the only way to achieve protection. Your actions, procedures, teamwork, preparation, planning, practice, time and learning are all free.

- Consider creative, low-tech protection solutions: A dog can be as good an alarm as the latest surveillance camera. Japanese castles used intentionally creaky floors to detect intruders.
- Plan for many different security measures. Like a rope, the more threads of the rope there are, the stronger the rope is.

Create a physical security policy, with colleagues and family

If you live with other people or share an office with another organization, talk to them about security. Try to determine what behaviors you can expect from one another and from visitors.

- Get to know your neighbors. Depending on the security climate where you work, this may provide one of two opportunities:
    - Neighbors could become allies who can help you keep an eye on your home or office.
    - If not, your neighbors will become another entry on the list of potential threats that you need to address.
- Set aside time to work on a policy document.
    - Coordinate with colleagues so they can participate.

    - Coordinate with family members as well to make plans for keeping safe at home.
    - Make sure everyone has time to ask questions about what they are supposed to do and why.
    - Determine what support your colleagues or family members need to make sure they are able to act on the policy, and make sure it is available.
- Set dates to revisit the policy.
- Set dates for regular security and protection capacity building
- Establish security briefing procedures and expectations about sharing information about incidents.
- Store and backup your policy documents in ways that are quickly accessible.
- Plan how you will introduce newcomers to your organization to the policy.
- See the Front Line Defenders Workbook on Security for practical advice on how to create a security policy.

Have a communication plan in case of emergency

It is important to have a plan both for your household and for your office. Consider including the following information:

- Who is in your network of allies and supporters who can come to your assistance.
- Emergency contacts and medical conditions of staff
- Who to contact in the event of a fire, flood, or other natural disaster.
- How to respond to a burglary or an office raid.
- What steps to take if a device is lost or stolen.
- Who should be notified if sensitive information is disclosed or misplaced.

- How to recover information from your off-site backup system.
- How to perform certain important emergency repairs.
- How to contact the organizations that provide services like electrical power, water and Internet access.

What goes in your plan? Assess the risks and vulnerabilities you face

- How might your information be lost or compromised?
- What would happen if it was?
- What devices do you use?
    - Make an inventory.
    - Include serial numbers and physical descriptions.
- Where are these items physically located?
    - Think broadly: not just about information at the office or at home, but in someone's luggage, in a recycling bin out back or "somewhere on the Internet" (which often means on the servers run by internet providers, social media companies, or other far-away people you do not know).
- What is your policy on people using personal devices for work?
- What communication channels do you use, and how do you use them?
    - Examples might include letters, faxes, mobile devices, landline phones, emails, video calls, social media and secure messaging platforms.
- How do you store important or sensitive information?
    - Computer hard drives, email and web servers, USB memory sticks, external hard drives, CDs, DVDs, mobile phones, printed paper and hand-written notes are all common means of data storage.

        - In each case, include information in your plan about whether or not the data are encrypted, whether and where there is a backup, and who has access to the keys or passwords needed to decrypt them.
    - See our basic security guides on encrypting your devices and setting screen locks, to stop anyone who gets physical access to your device from getting access to your files.
- How do you destroy sensitive data when you no longer need it?
    - How will you securely dispose of paper rubbish that contains sensitive information?
    - How will you remove sensitive information from devices you are getting rid of?
- What is your plan for traveling?
    - How will you, your colleagues, and family members interact with immigration and border security personnel in various circumstances?
    - How will you all handle sensitive data or software that might be seen as incriminating?
    - What information do you all need about travel insurance, if any?
    - Would it improve your security to partner with not traveling person and check in at pre-planned times?
    - What will you do if a colleague fails to check in as planned?
- What will you do in different emergencies?
    - Make simple checklists to make it easier to act under stressful conditions.
    - Include information about access to legal support.
    - Find out what legal protections you have against law enforcement personnel, landlords, and others who might try to enter your home or office.

Create an office access policy

- Your policy should include rules about key distribution, monitoring systems like cameras, alarm systems, and what to do with people delivering packages, repairing your systems, or fixing or cleaning your space.
- Think of your physical security as having the following layers, and plan for the protection of each of them:
    - The walls or fences of your site
    - Between the walls/fences and the doors and windows of your building
    - Inside your building
    - Finally, a safe room inside that building, and your evacuation plans if those other layers are breached.
- Decide which parts of your space should be restricted to visitors.
- If possible, arrange rooms for greater privacy and security:
    - Create a reception area where visitors can be met when they enter the office
    - Create a meeting room that is separate from your normal workspace.
    - If you work out of your home, this might require that you move documents and equipment into a bedroom or some other private space when meeting with visitors.
- Your printers, monitors, projectors, and other devices likely have USB or Ethernet ports. Keep them out of public areas, so nobody can plug a device into them that can spy on you.

When working outside your home or office

- Public wifi and internet cafes should be considered insecure.
    - Use a virtual private network (VPN) or the Tor Browser to prevent attacks when you connect to public wifi.
- Consider carrying your laptop in something that does not look like a laptop bag.
- Keep devices near you at all times. Do not let your device out of your site when charging, for example.
- Consider traveling with a security cable and practice finding workspaces near objects to which you can attach one. Thieves often exploit mealtimes and restroom visits to steal unattended equipment from hotel rooms and cafes.
- Remember that hotel safe deposit boxes are accessible to hotel staff who have the master key.

Consider using surveillance cameras and motion sensors

- Remember, if what you are looking for is a fast alert, low-tech solutions like bells or alarms which ring when a door opens, or a dog that will bark, can be as effective as a surveillance camera, if not more so. Closed-circuit TV (CCTV) cameras may require someone to monitor them or review footage.
- Consider whether a camera to monitor your space would put those who work there or nearby at risk, if your adversary had access to these cameras. Balance this risk against your need to know if your space has been searched, raided, or burglarized.
- Avoid using "internet of things" devices like Amazon's Ring. Many internet of things systems are notoriously vulnerable to spying. Amazon, which offers the

Ring system, has been known to share camera footage with law enforcement without users' permission, and may use your data in other ways it does not disclose.

- As an alternative, consider using Haven, which was specially created to help human rights defenders monitor their own spaces with control over their own data.
- When using a surveillance camera, you may want to transmit video to a location other than the one you are monitoring. This video should be sent encrypted and also encrypted wherever it is stored.

Protecting Your Local Network

Avoid running ethernet cables in unprotected areas

- Avoid running internet cables outside your building, as it makes it easier for someone to tamper with them when you are not looking.

Set a strong passphrase on your wireless network

- Follow our guide on creating and maintaining strong passwords.
- Set your network to use WPA2 or WPA3 security.
- The steps to secure a wireless network will depend on which router you use.

Avoid connecting unnecessary devices to your network

- Televisions, cameras, phones, printers, video game consoles and "Internet of Things" (IoT) devices are also computers. They come with many of the same risks. Think twice before connecting new equipment to your home or office network.
- Unplug devices you are not using.

Change your wifi network's name

- Give your wifi a name that does not clearly identify you, your organization or the location of the access point.

Create a separate wifi account for guests

- This way, you will not need to give them your password, and it will be easier to change the passwords if you need to.
- Ensure this account has a password. Leaving your router unprotected by a password makes it possible for intruders to tamper with your wifi.

Lock up networking equipment

- Lock networking equipment like servers, routers, switches, and modems inside a secure room or cabinet to make it hard for an intruder to tamper with them.

Make sure your servers are encrypted

- If your office runs servers, work with the person who manages them to ensure they encrypt their data (see the section on "Keeping your digital information private" for more information on this topic). If for some reason you run

unencrypted servers, ensure that at least if they are unplugged, they will encrypt their contents.

Prevent accidents and outages

- Computers, networking equipment and data storage devices can be quite delicate. The same is true of surveillance cameras, printers, "smart devices" and other hardware. Electrical fluctuations like lightning strikes, power surges, cuts to your power, blackouts and brownouts can cause physical damage to digital devices by harming electronic components or destroying data on hard drives. Extreme temperatures, dust, and moisture can also do damage.

Plug electronics into surge protectors

- Not all power strips contain surge protectors, so check this when buying new ones. A surge protector should specify a maximum voltage and list a rating in joules.
    - If your electricity is particularly unstable, you might also need a "power filter" or "line conditioner."
    - Put surge protectors, UPSs, power strips, and extension cables where they will not be unplugged or powered off when someone bumps them.

Consider installing uninterruptible power supplies (UPSS)

- These are somewhat more expensive than surge protectors, but they will stabilize your power supply and provide temporary power in the event of a blackout.
- UPSes are particularly valuable for servers and for desktop computers that do not work if they are not plugged in.
- Consider lighting that does not depend on electricity – strong flashlights, strip lighting on walls powered by batteries, solar charged lights, etc.

When moving into a new building, test the power supply

- Do this before plugging in important equipment. If the power behaves poorly with lamps, lights, and fans, it is likely to damage your digital devices.

Get good cables

- When you find yourself with access to high-quality computer cables, surge protectors, and power strips, consider picking up a few extras. Sparking power strips that fall out of wall sockets and fail to hold plugs securely can cause people physical harm, as well as damaging your devices and data.

Ventilation

- If you run your computer inside a cabinet, make sure it has adequate ventilation to prevent it from overheating.
- Computer equipment should not be housed near radiators, heating vents, air conditioners, or other ductwork.

Protect against Theft, Tampering, and Confiscation

Start with locks

If possible, install high-quality locks on your doors and windows.

- Keep an up-to-date list of how many keys were created and to whom they were distributed.
- Make plans to collect keys from anyone who no longer needs access (when people leave an organization is an ideal time to take keys back.)
- Consider purchasing a laptop safe or a locking cabinet for sensitive documents and equipment.
- Lock the devices themselves:
    - Most desktop computer cases have a slot where you can attach a padlock to stop someone from getting in and tampering with the hardware.
    - Use locking security cables, where possible, to prevent intruders from stealing desktop and laptop computers.

Don’t place equipment where it can be easily stolen or tampered with

- Avoid placing important devices, including servers and wifi routers, in easily accessible locations like hallways and reception areas, or next to windows or doors.
- Protect your building's main electrical switches with locks.

Consider risks of leaving devices behind vs taking them with you

- You know the level of risk better than anyone else, so consider: is it likely that someone will raid your space or tamper with your devices while you are out? Or is it more likely you will be detained and searched with your devices on you?
- What are you going out to do? Travel? Cross borders? Go to a protest where it is likely you will be arrested? Weigh whether the risk or search or confiscation is higher if the device is on you, or if you leave it behind.
- Scatter small objects over your device. Consider taking a picture of it before you go. When you return, compare the photo to the position of the objects, to see if the device has been moved. (One classic tactic is to leave a single thread or hair on the device if there is no breeze in the area; it can be hard for an attacker to re-create the shape of that thread or hair.)
- Consider using a monitoring app like Haven to watch your things while you are gone.
- Also consider whether a locked box could help secure your devices in case your space is searched.

Decide whether to register your devices with law enforcement

- If your local law enforcement is trustworthy, registering the model and serial number of your devices can help you recover devices if they are stolen.

Consider what can be seen

- Establish a "clean desk policy": ensure you and your colleagues do not leave sensitive information sitting on your desk, particularly passwords, paper calendars, planners, journals, address books, or sticky notes.
- Position computer screens in your home or office so they cannot be seen from outside. Remember to account for windows, open doors, and visitor waiting areas.
- Consider ways you can avoid using devices in public, where someone could look over your shoulder.
- If you often work in public, buy privacy screens. These simple plastic covers make it difficult to read a screen unless it is directly in front of you. They are available for laptops, external monitors, tablets and smartphones.
- If you need to hide your location, remember these clues can be used to figure out where you are:
    - Check what is visible on camera in video calls: architecture, signs, trees, geological features like mountains?
    - Consider what can be heard in the background: nearby traffic, sound systems, factories, children playing?
- Cover cameras when you are not using them, so they cannot be manipulated to spy on you.

Decide how you will dispose of sensitive information

- Set a regular schedule to erase devices securely, in order to ensure sensitive files do not remain on your devices, hard drives, USB memory sticks, removable memory cards (SD cards) from cameras, mobile phones or portable music players, and any other device that saves sensitive information.
- For each device you have (Android, iOS, Linux, Mac, and Windows), see our guides for basic security: specifically, the sections on securely deleting files, wiping blank space, and disposing of an old device. Incorporate these instructions into your physical security plan.
- Many paper shredders work on CDs, DVDs, and bank cards as well as paper documents. Just make sure your shredder does so before you try this!
- Dispose of the pieces in various locations far from your home or office to make reconstruction harder.
- When you are disposing of a computer hard drive, you can make it harder to get data off of it by destroying it with a power drill, a few strong blows from a hammer, or nails hammered through it. Do not burn or pour acid on a drive, and do not put it in the microwave.

Tools

Use the following tools to visit blocked websites, to help hide your online activity, and to remain anonymous online.

Psiphon

(Android, Mac, Windows)

A free application, with good user support, that provides access to blocked websites while helping to hide your online activity. Provides good user support and offers improved performance for a fee.

Download I See their guide

Riseup VPN

(Android, Linux, Mac, Windows)

A free, activist-focused application that provides access to some blocked websites while helping to hide your online activity.

Download I See their guide

Proton VPN

(Android, Linux, Mac, Windows)

A business-oriented application that provides access to some blocked websites while helping to hide your online activity. Offers improved performance for a monthly fee.

Download I See their guide

Lantern

(Android, iOS, Linux, Mac, Windows)

A free application that provides access to blocked websites while helping to hide your online activity. Offers improved access to blocked sites for a fee.

Download I See their guide

TunnelBear VPN

(Android, iOS, Mac, Windows)

An application that provides access to some blocked websites while helping to hide your online activity. Free for up to 500 MB/month on one device (or up to 10 GB in select countries). Supports additional devices and unlimited data for a fee.

Download I See their guide

Hideme VPN

(Android, iOS, Linux, Mac, Windows)

An application that provides access to some blocked websites while helping to hide your online activity. Free for up to 10 GB/month on one device. Supports additional data for a fee and accepts Bitcoin for payment.

Download I See their guide

Speedify VPN

(Android, iOS, Linux, Mac, Windows)

A video-friendly application that provides access to some blocked websites while helping to hide your online activity.

Download I See their guide

Outline VPN

(Android, iOS, Linux, Mac, Windows. Management app: Linux, Mac, Windows)

An open-source application, developed by Google, that makes it easier for individuals and organizations to administer their own secure VPN service. Administrators can then give other users access to blocked websites while helping them hide their online activity.

Setup a server and download a client I See their guide

Algo VPN

(Linux, Mac, Windows)

An open-source application, developed by the security company Trail of Bits, that makes it easier for individuals and organizations to administer their own secure VPN service. Administrators can then give other users access to blocked websites while helping them hide their online activity.

Setup a server

Remain anonymous online:

Tor Browser

(Android, Linux, Mac, Windows)

A free and open-source application that uses a network of volunteer relays to hide your online activity while providing access to some blocked websites. The Tor network might be blocked in some regions, and using it could make your connection look suspicious to anyone who might be monitoring your online activity.

Download | See this guide or their FAQ

Tails

(Linux, Mac, Windows)

Use a separate, secure operating system that you load from a USB drive. Tails communicates over the Tor network to hide what you are looking at online and offer access to some blocked services. Tails does not leave traces of your work.

Download I See their documentation