Hello Comrades.
This will be a basic guide to understanding and practicing security culture.
First of all, we should discuss what security culture does and why it must be practiced.
The utmost importance to this is for the protection of comrades and yourself as revolutionaries dedicated to the movement. We need to protect our ability to carry out the ability to serve the people and work as Marxist-Leninist-Maoists to carry out the revolution. This is critical. I recommend to practice security at all steps of the case, and learn what you can about security regarding technology. This guide will only be a basic starting point for all of us. If anyone wants to expand these basic points, then do so and add information regarding this.

Where to begin?

We have to understand this much about technology: a lot of it is run by corporations who's advertising goal is selling information and providing it to distinct corporate and government entities. For example, Microsoft's Windows 10 operating system utilizes telemetry, which essentially tracks every activity that is done on your computer under the guise of "constantly diagnosing" your computer and looking for software and hardware errors. Obviously, the data collection involved can and will be accessed by reactionaries, whether government or corporate.
Google utilizes something similar, especially since data collection is their advertising point. They largely are involved with taking in information and selling it, which again, can and will be accessed by reactionaries!

Why do we need to utilize technology though, you may ask? Why not just do everything in real life and stay offline? Well, of course. We promote limited activity online, but we also suggest utilizing the internet to have ease of access to other comrades that you may not know of, but are capable and willing to organize and work with you in your local areas!
Emails, file sharing, some means to keep in contact and produce material for activity in real life.
Say, working with a revolutionary news source, who mostly post online? We need security when dealing with collective work alongside others to produce knowledge about the conditions we live in.

What are the solutions?

There are plenty of ways to avoid or limit detection and information gathering that can wreck the movement. These can concern multiple things and their solutions.

Regarding Hardware Itself?

Phones, laptops, and the such hold different functions and can help with the movement in many ways. Coordination with contacts is largely one of them, even file storage and sharing is important and beneficial. Phones can keep good contact with other comrades from nearly anywhere, laptops are portable enough to move around different meeting areas and provide discussion through direct file holding, external hard drives are good for similar things, etc.
But we need to consider the dangers of utilizing these pieces of techs.

Phone advice

Most phones are owned and controlled by major corporations- iPhones by Apple, Galaxy by Microsoft and Samsung, etc. Alongside this, phones are where a majority of one's own data can lie, depending on how one uses this. A corporation that holds your data and has relationships to the US government can and will lend this information to the reactionary forces. What is to be done then?

Well, we can look at a few paths:

Getting secure, safe phones

Phones with kill switches are important to turn off: cameras, microphones, GPS trackers, etc. Anything that can bring a connection to your activity in any way as well as being monitored at all.

The only phone I can think of is the PinePhone from Pine64 which utilizes Linux OS! The entire phone depends off of community-driven, open source software. This could be largely useful, but I myself have no personal interactions with this other than listening to first hand reviews from friends and youtubers.

The preference that most do prefer is Android, as they are secure and cheap. In addition to the fact you can use a custom rom that allows for an open source OS.

F-droid is also something you can use on every android phone. It has only free software.

Get a jailbroken iPhone or a rooted Android phone

Although these will still have connections to Apple and occasionally, Microsoft, you have more free reign to change a lot of stuck things that are on default iPhones and Android phones, as to produce more security for yourself.

Although, I do not have experience with this either. This should be researched more on your own time.

Not using or keeping your phone near or at important places!

This is even more important. Especially if you do not have the ability, for any reason, to get yourself a new phone, or you are unable to jailbreak/root your phone. And even then, should be a safety precaution altogether, even with phones that have kill switches for hardware that can be utilized for spying.

If you stick to your iPhone or Android, then it is recommended to disconnect your political activites and even ideological perspective from wherever you are on your phone.

Use burner phones

for quick communication, you can get a burner phone for $20 USD and throw it away after using it. They are quite cheap in a lot of places and are useful for the intention of communicating under the radar.

<u>Computer advice</u>

Laptops and computers also need to have major security steps to protect yourself as a communist. Hardware itself is not very much useful to change and shift. All hardware is proprietary, but can work with open-source drivers and softwares. I recommend looking into those, but these do not pose much in regards to security. Nvida hardware forces you to use non-free software, so be wary. I don’t really think this is much worry. Especially since you can uninstall the telemetry in this software, even then, it is no major issue. They won’t be buying and selling data like Google or Microsoft.

<u>Operating System?</u>

What I do recommend heavily, is discussing your OS or operating system.

This is the software that utilizes the computer's resources- the hardware.

As I've said above, Windows should be avoided! And Mac, just as much. Or at the very least, I support using dual boot- keeping windows/mac for your own personal, non-political needs and utilizing linux for such. It really is your own choice.

The recommendation is to install Linux on your laptop or computer. Linux is safer and does not have the usage of telemetry in most distributions.

I recommend to avoid certain Linux distributions: Ubuntu, elementaryOS/ZurinOS, KaliOS, or anything that holds pre-installed applications that allow for data collections.
I recommend utilizing debian based distributions that are simple to use, like Mint, Trisquel, etc.
Trisquel uses purely and only open-source applications, which is useful for security but also has no access to apps you may regularly use and is proprietary software.
ParrotSecOS has a built in OS and is another Debian based distribution. Be sure to check it out, since it is also a very lightweight OS.
You can also use arch based distributions, although more complex. If you want to keep more in track of software that may be monitoring or external sources that can search and monitor your metadata, then go for Arch or something Arch-based.
If you do not want to go through the trouble of downloading everything manually, I recommend getting an arch installer. (personally, I recommend anarchy installer)
If you still do not want to go through this trouble, then I recommend getting Manjaro Linux, which is an arch-based distribution that is for beginners and has a lot of pre-installed, open source software. (Avoid installing "non-free drivers," but this is for Nvida hardware, so as before, you can just uninstall the telemetry in this.)
Finally, TailsOS is very useful and very secure. All you need is a USB drive that holds at least 8gb (preferably 16gb+) and the image file for tails. You install the entire OS on your USB and it is an amnesiac system, that has a short life on your computer's memory.
This is great for secure, encrypted file storage! It also is good for collective usage.
I will post resources for where to install this and how to install it at the bottom of this!

Text readers/editors?

You can utilize PDF and Docx files, as long as you have JavaScript blockers.
If you use any of the browsers below (specifically brave), this is already built in and you can access the PDF through there with no issues of security. This is the safer option.

Browsers and search engine?

You should avoid:

- Microsoft Edge
- Google Chrome
- Canonical's Chromium (Canonical is the same company that runs Ubuntu Linux)
- anything closed source, really

Utilize Brave, Firefox, Waterfox, or Tor (although Tor is funded by the US military, it does not have closed source, data stealing software.)
Brave has its own tor browser and is based on Chrome code. It has adblockers, JavaScript blocker, AND a tracker blocker. Although, it has advertisement for its own bitcoin wallets, and the owner of Brave is a transphobe who sends money to anti-trans groups.
Firefox has its own tor browser. It has open-source addons. Waterfox is based off of Firefox, although hold no differences.
LibreWolf is similar to Firefox and has many improvements alongside it.
These apps do not utilize or force you to sign into an account to save and keep history/bookmarks/etc.
Brave has a sync option that utilizes a passphrase to sign into a sync, but no account.

For any choice you take for your browser, don't use Google as a search engine! Their primary point of advertisment is data collection and sharing!

If you want a good, secure search engine that does not collect data, I deeply recommend utilizing DuckDuckGo, Startpage, or Searx. (I personally recommend DuckDuckGo since it is similar to the other major search engines!)

Contacts, messaging and emails?

For contacting and talking to others, I recommend looking into email services like, ProtonMail or Tutanota. Both have encrypted, free services based outside the US.

Although the emails are encrypted, I recommend using Tor at the same time as using a NEW encrypted email account, with a name and passPHRASE that is not connected to you or anything that can go towards comrades or suggests communist activity.

The same applies for messaging apps like Signal or Riot.

Signal does use your phone number, but this should be used for vague conversations between each other when attending events that require splitting up. Do not depend on this.

But riot is mostly, if not entirely, safe when utilizing it with the same safety precautions. But it is important not to depend on this!

Remembering passwords?

Utilize password managers. Human-generated passwords are not great, and you cannot consistently memorize them. I recommend keeping to and using password managers.

If you, for any reason (which I dont see of), don’t want to use these, then you can use a password book. Which is literally a book that you write your passwords in, these can and usually do have locks on them. Good as an alternative to firewood

Use KeePassX or BitWarden. They are very good password managers and can remember these passwords for you.

Don’t forget! Any account you can make on any application should be utilizing Multi-Factor Authentication, whether it be the two passphrases on ProtonMail or what. As long as it allows you.

I recommend constantly changing passwords and using any password manager/generator to generate new ones and keep it stored there or in the password book.

Encryption?

Encrypt files and/or hard drives/disk partitions.

This can be done manually on Linux or while installing a Linux partition, you can completely encrypt a drive, and the only access is with a passphrase.

I believe that there is only encryption options on Linux OS’s and not on Windows.

Either way, it is recommended to keep encrypted files on TailsOS or if you want your personal computer to be utilized as the basis for your information, then encrypt the Linux partition.

The simplest way to encrypt the Linux partition is to go to manual partition and choosing to format the partition as a LUKS filesystem instead of an EXT4 filesystem.

What is deeply recommended is using an external hard drive to keep all your files in and your partition itself. If you have any questions on how to do it, I will post links on how to encrypt files on Linux or encrypt your Linux partition on an external hard drive.

You can utilize cryptomount to do it manually with an already installed partition

Regarding Larger Concerns?
This is a basic understanding of all things security that can be practiced on your computer and phone and any sort of connection regarding information sharing and activity regarding organizing.

I have nothing to add, or else it would be more complex and this would be akin to a series of tutorials than advice and resources.
If you wish to learn more, ask around… ask other comrades. And if you have time before you *start* organizing with comrades and serving the people, try to teach yourself some more adanced things and check out the resources I will be posting.
Thank you for reading and concerning comradely need to protect yourself, your comrades, and the entire movement of your country.
This will be important, and be sure to spread this around and any additional links associated!

Red Salute,
SHSC