Digital Safety for Sri Lankan Journalists and Activists

Digital Safety Hand Book

IMS paving the way for good journalism

MEDIA
LAW
FORUM

Digital Safety for Sri Lankan Journalists and Activits
Hand Book
Published in Sri Lanka , March 2020

Publisher: International Media Support (IMS)

ISBN:

Authors
Lakna Paranamanna
Haritha Dahanayaka

IMS
41/2A, Pelawatte Road, Sri Lanka

Nørregade 18
1165 Copenhagen K Denmark
+45 88327000 info@mediasupport.org

Join the global work for freedom of expression and stay up to date on media issues worldwide

forfreemedia
InternationalMediaSupport

International Media Support is anon-profit organisation working to support local media in countries where conflict and political transition make it difficult for media to operate.

www.mediasupport.org

Digital Safety for Sri Lankan Journalists and Activists

Digital Safety Hand Book

Preface

Freedom to access information is a fundamental tenet of a thriving democracy; a right that should be enjoyed by every citizen of a democracy. Today, that right faces grave risks. The world wide web - a space that once nurtured freedom of expression and information flow, is being engulfed by the preying clutches of the deep state with authoritarian ambitions and capitalist mongers.

As journalists and activists operating in an era where communications have unapologetically moved into the digital sphere, accessing data, information and engagements between and among users itself have become seamless. But this age has also marked the birth of a new revolution alongside a clarion call to privacy.

While it is in the interest of every responsible citizen to be aware and lobby for internet safety the concerns for journalists, whistleblowers and activists in this regard, is graver than ever before. Although digital communications have enabled a slew of options to extract and exchange information, it has also posed a series of unique challenges including identity protection and online harassment and bullying.

While it is in the interest of every responsible citizen to be aware and lobby for internet safety the concerns for journalists, whistleblowers and activists in this regard, is graver than ever before.

Is it only a fool's hope to expect anonymity and safety online? Are there absolute protections? How can we make use of the digital tools freely available to us to strengthen the fourth and fifth estates? These are some of the questions we hope to offer answers to, through this guidebook. Our aim is to arm you with a basic understanding of how the digital infrastructure around us works, where the vulnerabilities lie and the measures we can implement to fix the loopholes - temporarily - so that your digital footprint and identity is safeguarded.

The term temporary is important in this context and it's linked to the cardinal rule that must be remembered at all times. The world wide web is an organism of sorts, ever evolving and developing - therefore, do not be complacent about your digital hygiene and safety. All we can do is to stay updated and be updated.

Good luck!

Content

01.

The six points to remember in digital safety

1.1: Asking the right questions

Questions are the most important tools you possess as journalists or even for those who lobby to uncover truth and justice. The right questions in digital safety can arm you with knowledge needed to protect your identity online.

Some of the important questions to ask yourself before setting out to draft a digital security plan are:
- What do I want to protect?
- Who do I want to protect it from?
- What will be the consequences of failing to implement protective steps?
- What steps am I willing to take to prevent the above consequences?

Once you have asked these questions from yourself, you are one step closer to creating your own customized digital security plan.

1.2: Identifying your weakest link

Remember the age old phrase, "You are only as strong as your weakest link?". That certainly rings true in terms of digital security!

Think about a home; there will be little use of installing the best door locks if you are going to leave your cracked window unrepaired.

Similarly, creating a strong password to access your digital accounts will be useless if you are going to share the password with even your closest loved ones. So ask yourself, what are your vulnerabilities?

1.3: Managing your identity!

Our email serves as the main identity point in all our transactions online. Many of us have only one, or at most two emails. We use it for official communications, to create our social media accounts, for online banking, to sign up for loyalty schemes at our favourite stores .... The uses are endless.

One of the key points to remember is that it's best practise to compartmentalize our interactions online. Create separate identities for each category - work, keeping in touch with family, banking, loyalty schemes etc. This way, a weak security set up in one category does not impact your entire identity online.

1.4: Complex and expensive is NOT synonymous with best security

It is easy to get carried away with shiny new security systems that promise best of protections. Truth however is that, higher the complexity, the harder it is to keep up. Similarly, expensive solutions don't also mean better security. You would be surprised to realize that some security steps only require simple solutions like switching to pen and paper to leave out a digital footprint and thereafter shredding them!

1.5: There is no one-size-fits-all plan!

Off-the-shelf security solutions may provide you a certain degree of protection but they will never resolve all your needs, as opposed to a digital safety plan that you customize in consideration of your security needs and ease of implementation. It's imperative to choose a plan that is convenient to you, because if it's not something you are comfortable with, chances are you will abandon the plan halfway through the process.

1.6: Stay updated!!

In this handbook, we aim to cover the dos and don'ts when it comes to your interactions online but keep in mind, we are advising you on what is best given the updates and developments. Keeping a tab on recent developments is a MUST! Starting with the very basic security measures including the updating of your apps and anti-virus software, remember to stay updated!!

02.

Passwords

To put simply, a password is a key that will unlock your digital accounts - it maybe an e-banking account, a social media account or even an encrypted document.

We all maintain at least three accounts/ profiles online but we tend to use a single password for all accounts for ease of access. But is this a safe practise? How important are passwords for our digital security?

Think of a hacker; the image that immediately jumps out is an individual in a hoodie, typing green code in the thick of dark on multiple screens... Well, it turns out the process of 'hacking' does not always have to be that complex. Your social media accounts may be hacked by a stranger who shoulder-surfed and figured out your password when you accessed it in a public location.

2.1: What is a 'strong password'?

Has to be lengthy - Longer the password, tougher it is for a 'shoulder-surfer' to remember it. It will also take longer for password cracking tools (programs with the ability to guess the combination) if the password is longer.

This is why 'pass-phrases' have risen in relevance as opposed to 'passwords'. Instead of using a word, best practises now advise a phrase - a string of words - is a better option to improve safety.

Password: cakelove
Passphrase: redcakefoxberriesfordbit
(*tip - remember to use a series of at least six random words)

Has to be complex - Simply making it longer is not enough. Making the pass-phrase complex also helps make it tougher for various programs to 'crack' it. Make sure to use a combination of uppercase and lowercase letters, numbers and symbols.

> **Let's try making the above pass-phrase complex.**
> **Eg: reD*cakE#fox$bErriEs@fordb1t**

NEVER make it personal - It is convenient to create a password out of something easy to remember - it may be a milestone in your personal life or a private detail. But this is a bad idea! With a little research, these aren't information 'interested parties' are not able to find out.

This is also a factor to remember when answering the security questions that are presented when you set up email profiles etc. It's advisable to not include accurate answers to security questions.

NEVER share - Sharing maybe caring, but not when it comes to digital security. This golden rule is applicable to even the closest members of your family. If on the off chance you happened to share your password, make sure to change it as soon as possible!

Keep changing - Make sure to update your password every few months - like all things related to digital security, passwords must also never remain static. Do follow the above mentioned steps noted to build a 'strong password'.

DON'T repeat - Don't use the same password on all your digital accounts. A vulnerability in one may expose all your activity online. The toughest challenge in using different passwords is remembering them. We will get to introducing a solution to this challenge in the next topic.

> **Exercise: What is your current password? Check how secure it is by looking up how long it takes to crack it via a web based platform: www.passfault.com**
> **Now replace your password using the above mentioned tips.**

https://password.kaspersky.com/ is one of several websites that allow you to test the strength of your passwords. Reputable services like this perform calculations on your computer and do not send anything back to their servers. They can be useful when testing the relative effectiveness of different password strategies but you should still avoid submitting your actual passwords.Do make sure to not include your actual password in the test and instead use a similar test version.

2.2: Remembering and recording secure passwords

If you are not supposed to use the same passwords for all accounts and you are not to write the passwords down on paper, how is it humanly possible to remember them all?

Fret not - we have a solution! A password manager, which you can install on your computer as well as your smart phone.

Think of the password manager like a portable vault; an encrypted vault that will keep all your passwords safe. This way you don't have to memorize your many pass-phrases; you will only have to remember the pass-phrase to your password manager account and it will automatically generate and safely store passwords to all your digital accounts.

Exercise:
Create a password manager account on:
KeePassXC (keepassxc.org) (Windows) or KeePassDX (keepassdx.com) (Android) or iOS (https://keepassium.com) and secure all your password protected accounts.
***tip - Remember to create a 'strong password' for your password manager account and keep backup of your password database.**

Resource:
Read more about KeepassXc on
https://securityinabox.org/en/guide/keepassxc/windows/

2.3: Two-factor authentication

Now that you have replaced your old passwords with strong pass-phrases, the next most important step in further securing your digital accounts, is to active two-factor authentication. This means, in addition to your password, you have to provide a secondary source of identifying information to prove your identity in order to access the account.

This secondary verification step, is carried out in several forms:
1: As a numeric code that is sent via text message
2: It may be generated off an app in your phone
3: It can also be generated using a hardware device known as a 'token or a dongle'

* However, do not forget that SMS-based verification is not encrypted and is vulnerable to interceptions. Therefore, it is better to use the second or third options to activate the two-factor authentication process.

Exercise:
An easy to use, free app to activate two-factor authentication process is FreeOTP.
It is available for both Android and IOS users.
Refer to two factor authentication information offered by:
Google (https://www.google.com/landing/2step/)
Facebook (https://www.facebook.com/help/148233965247823)

Resources:
https://twofactorauth.org – A website listing the different online services that support 2FA with instructions on how to configure.
- FreeOTP https://freeotp.github.io
- Android - https://github.com/andOTP/andOTP
- KeePass XC also supports 2FA - https://keepassxc.org/docs/#faq-security-totp

03.

Keeping your digital communication private

Communication methods currently available to us:
-Voice calls on land lines and mobile phones
-SMS messages
- Emails
-Internet-based messenger apps
- Online discussion boards and social media platforms

Whichever method you choose for your communication, you are assigned an identity - it can be your profile name, your IP assigned by your Internet Service Provider (ISP), the IMEI number of your phone or the Serial/Mac number of your laptop etc.

So it's important to keep in mind, that when you transmit a message using any of the above methods, it passes through several devices or gates and are vulnerable to interception at several points before it reaches the end user and even afterwards. In short, once you release information from your device, it is vulnerable to surveillance and exposure. Let us proceed further with that in mind.

3.1: What are the vulnerable points?

- Sender's/ receiver's device (tab, phone, laptop) - If the device has been infiltrated with malware
- Wifi router - if it is infected with malware or is hacked
- ISP or Network service provider - Either for their own use or on behalf of a third party, can happen at your end or at the receiver's end.
- At the internet backbone - if it is 'tapped' by a state actor
- Any of the websites you visit

Looking at this list, it may make you feel as if all forms of communication are risky. There is no mincing of words, it is. But there are steps you can take to secure your communication at each of these points and a first for many of these would be strong password protection, which we discussed above.

It is also important to always be mindful of what you are sharing in your message. What will happen, if in the worst case scenario, the information falls into the wrong hands? Therefore in some instances, it might make sense to take steps such as creating pseudonyms or code words to refer to important names, dates, locations and other sensitive information.

3.2: How will you know if there has been unauthorized activity in your account?

- Changes to content or account settings that you did not make
- Your contacts receiving messages that you did not send
- Inability to log into your account despite entering the correct password
- You regularly don't receive messages sent to you by your trusted contacts
- Attempts to change your password that you did not request
- Some social media platforms offer details of recent account activity and you may notice access from locations and dates that you could not have made yourself

If you notice either one or more of the above mentioned signs, take immediate steps to follow the below instructions:

- Immediately stop using the account, until you know more about the situation
- Change your password immediately, if you haven't got locked out of the account
- (remember to follow the steps to create strong passphrases)
- Log out of all sessions if you are still logged in, if you are able to do so.
- Activate two-factor authentication if you haven't already (See 2.3)
- If you are logged out of the account, contact your email provider to reclaim your account
- Consider getting expert help - reach out to agencies who can put you in touch with tech experts, security researchers etc
- Warn contacts as appropriate so that they don't fall prey to an imposter!
- Figure out what the 'weak link' was - was it your device infected by malware? Or a case of a weak password? Are there other members of your community experiencing similar issues?

3.3: Few other steps to consider in further securing your digital communications

Encryption

Encryption allows information to be hidden - from the point it is released from the sender until it reaches the receiver. Think of encryption like a 'special key' or a code. Without the code or the key, the message cannot be accessed.

It can be done using two methods: Symmetrical or asymmetrical.

In symmetrical encryption, the same key will be shared between the sender and the receiver. In asymmetric encryption, the sender and the receiver need a pair of keys to access the information shared.

If you are a Whatsapp user you may see a notification stating 'messages to this chat and calls are now secured using end-to-end encryption' This means, the information you share is encrypted throughout the entire path.

When you visit certain websites, you may notice in the URL bar that it reads https:// (hypertext transfer protocol secure) instead of http://. HTTPS also uses encryption , but of a slightly different kind. You may also notice a lock symbol at the beginning of your web address. These are all different ways to let you know that your communications are secure and it will be harder for someone to eavesdrop on your communication, so look out for these signs!

*If your website does not have https:// avoid typing in your passwords or any other identifiable or sensitive information that may make you vulnerable. If you use Firefox or Chrome as your browser, if will enable you to add https:// before a web address.

Metadata

Simply explained, metadata is 'data about data'. Take a library card for example: it will reveal details about the nature and location of the content in the book. The sensitivity of metadata is that although it may seem insignificant and is not superficially visible, it may reveal a lot of sensitive details about the sender, if not used or stored carefully.

Some ways in which metadata could reveal information is through email attachments such as word documents or images.

How to be a safe metadata sharer:

- Try as much as possible to share information in the body of the email as opposed to attachments
- Turn off geo-tagging when taking photographs of yourself in private locations
- Do not include your personal details when setting up profiles in your cameras etc

Exercise:
Create new accounts on
Protonmail - https://protonmail.com/
Wire - https://app.wire.com/

Resources:
HTTPS Everywhere: It's an extension on Firefox, Chrome and Opera that enables you to encrypt your communications with many major websites
https://eff.org/https-everywhere
Have I been pwned: enables searches across multiple data breaches to check if your email has been compromised.
https://haveibeenpwned.com

04.

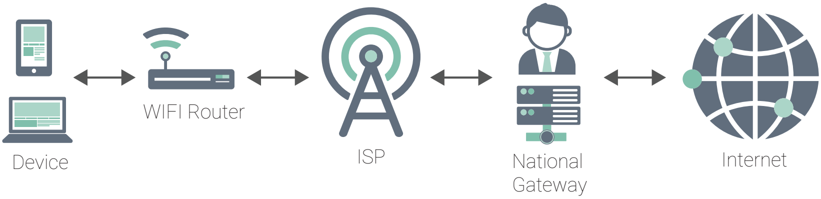
Remain anonymous and bypass censorship

Many countries have an infrastructure that prevents internet users from accessing certain websites and online services. It is a similar operation that is deployed in our offices or school networks, when users are barred from accessing certain social media sites, gaming sites or sexually explicit material.

Despite the guarantee of free access to information enshrined via Article 19 of the Universal Declaration of Human Rights, the number of countries engaged in internet censorship continues to increase.

4.1: How does internet censorship work?

It will be helpful to take a look at how your home internet connection works, before we try to understand how and where the censorships are imposed.

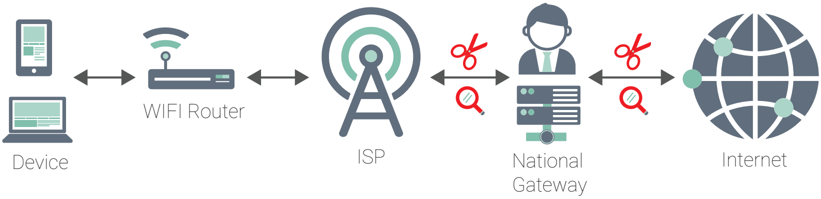


GRAPHIC: your internet connection

The ISP will have assigned an external IP address to your network. Online services will use this address to send you data. Anyone who knows your IP address can figure out the following:

- What city or region you are in
- In certain institutions, they can determine your precise location such as what building you are in - if you were using mobile data it may know your precise physical location
- If you were in an internet cafe, it maybe able to able to reveal which exact computer you were using

A number of methods may be used to block the internet user from accessing a particular site. The simplest and safest assumption is that at the ISP level or national level, a device somewhere between you and the resource you are seeking to access (Eg: a website) has decided to block your communication.



GRAPHIC: how censorship works

There are ways to circumvent and bypass these blocks and unless you have built your own internet, it is usually through circumventing tools such as TOR anonymity networks or VPNs.

4.2: TOR Anonymity network

This is the most well known and thoroughly tested public anonymity network. Each time you activate the TOR, your device will select three proxies at random and relay traffic through all three of them; these are called TOR relays. By adding a separate layer of encryption for each relay, TOR ensures that neither your ISP nor the relays themselves can determine the location of your IP address or the location of the websites you are visiting.

It is slower than other circumvention tools but it has unique features.

- You don't have to worry about trusting the organisations or individuals who run the proxies you use
- Does a good job of preventing the website you visit from figuring out who you are

*But remember, it does not hide the fact that you are using TOR and you still need to use a secure connection (https://) when visiting a website.

> **Resource:**
> **Tor is free and open-source software that enables anonymous communication.**
> **Tor is free and open-source software for enabling anonymous communication. https://www.torproject.org**

4.2.1 Things to avoid when using Tor

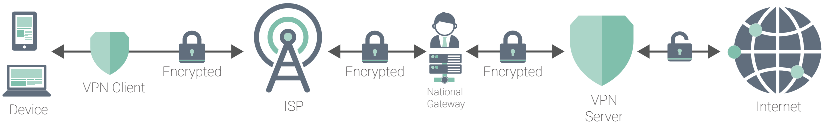
- Do NOT torrent over Tor – it renders 'onion routing' pointless
- Avoid installing browser plug-ins such as Flash, Quicktime – they could be manipulated to reveal your IP
- Avoid installing additional plug-ins or add-ons to the browser
- Tor will not protect any personal information you choose to enter in forms online
- Be careful surfing Tor's hidden or anonymous servers – some of the content maybe illegal/criminal
- Weak internet security will not make you safe even if you use Tor

Eg: Although safe from traffic analysis, its still vulnerable to attacks and exploits Leaked NSA documents have revealed most surveillance targets were "dumb users" - Tor users with poor internet security

4.2.2 How can you boost Tor browser security?

- Check if your connection to Tor browser is secure using TORCheck website

4.3: Virtual Private Networks (VPNs)



GRAPHIC: how VPN works

In some countries, it is enough just to sign up for a free or commercial VPN service run by an individual, organisation or company you trust. Some VPN services rely on functionality that is built into the operating systems such as Linux, Windows, IOs. Others require installation and configuration of the OpenVPN software. In some cases, your provider will offer a customised installer that handles everything for you.

The only problem with this approach is that basic VPNs rarely have built-in blocking resistance features, and this means once your VPN service is blocked, you may have to find a new one.

Resources:
Here are three trusted, open-source VPNs for your use

RiseupVPN - Riseup provides online communication tools for people and groups working on liberatory social changehttps://riseup.net/en/vpn

Psiphon3 is a secure, open source, public, ad-funded circumvention tool that uses VPN and SSH proxies to provide uncensored access to online content. www.psiphon3.com

ProtonVPN (https://protonvpn.com). It comes free with a limited number of VPN servers with your free ProtnMail email account.

4.3.1 Things to consider when choosing a VPN

- Check if the service assures data such as locations/activities of users are not logged.
- To ensure this, some services make available third-party audits or information on the code for the users to confirm independently
- Any mentions of locations – specifically on avoiding locations that have laws on data retention
- A kill switch – in the event a VPN connection drops, it will prevent the user from reconnecting to the internet, thereby avoiding accidental exposure of location or identity
- Double encryption

4.3.2 Limitations of VPN use

- Legal concerns – If the user is living in a non-democratic country, the use of a VPN to access blocked sites maybe punishable by law
- Location not completely concealed – Although a VPN may secure your data connection, your network service provider will still know your location
- VPN is not a panacea! - A VPN will not protect your identity made vulnerable by an insecure connection or vulnerable device
- Slower internet use – can be bypassed by choosing a service close to where you reside

05.

Security from malware and phishing attacks

Keeping your device free and secure from malware and phishing attacks is a basic step towards ensuring your device is healthy and in the eventual run, contributes towards making your device secure because malware can significantly reduce the efficacy of any other security precautions that you may implement.

5.1: What is malware?

There are many names; viruses, spyware, worms, trojans, rootkits, ransomware and crypto jackers are some. Phishing attacks are one method of infiltrating your device with malware.

Phishing is an attempt to extract your personal information by tricking you into thinking you are communicating with someone you know.

Malware can be spread via the internet through email, malicious web pages etc while some may also be spread through devices such as USB sticks, used to share information and data.

5.2: Anti malware software

Unfortunately, at present there are no full-featured, open-source anti-malware tools but there are some basic steps we can follow to minimize the risk.

- If you are using Windows, have a look at the built-in Windows Defender. Macs and Linux computers do not come with built-in anti-malware software. The same is true of Android and iOS devices, which are somewhat less vulnerable because they typically prevent the installation of software unless it comes from an official source like the Google Play, F-droid or the Apple App Store.

- Installation of reputable, free-to-use tools. Eg: Malwarebytes (Windows, Mac, Android) / Avira (Windows, Mac, Android) / AVG (Windows, Mac, Android). Most products advertised as "anti-malware" for iOS are really something else: VPNs, password managers, anti-theft trackers and other such "security" tools.
- There is one widely used FOSS anti-malware tool - ClamAV (runs on Windows and Linux; you can install it on Ubuntu and other Debian distributions, using the built-in package manager.) However, the downside is, it's only a scanner - it can be used to determine if a file or directory contains known malware but it will not monitor your system to protect you from infection.
- Another option is to purchase a commercially available anti-malware product that involves the payment of annual license fee to continue receiving regular updates.

Please check the links below about anti-virus companies collecting and selling your personal information through the installation of their free applications
- https://www.wired.co.uk/article/avg-privacy-policy-browser-search-data
-https://www.komando.com/security-privacy/antivirus-program-sells-your-data/703476/

Read the terms of service and privacy policy before installing free applications. Free applications may collect information that could reveal your identity.

5.3: Tips to keep in mind to protect devices from malware

- Do not run two anti-malware tools simultaneously - many will identify the other anti-malware program as suspicious and stop it from running. This can result in neither tool functioning properly.
- Make sure that your anti-malware program allows you to receive updates. Many commercial tools re registration and payment to receive updates after a certain point.
  NOTE: All of the software recommended here can be updated for free.

- Follow the cardinal rule in digital security -make sure your anti-malware software updates itself regularly. If possible, configure your software to install updates automatically.
- Turn on your firewall software. A firewall is like a security guard at a building entrance. It is the first program on a computer that looks at incoming data from the Internet - it is also the last program to handle outgoing data and devices, making decisions on network traffic.
  NOTE: Also make sure your router or Wifi access point has firewall enabled
- If your anti-malware tool has an optional "always on" feature, enable it.
- Run occasional scans on all of the files on your computer. This will help identify weaknesses in your anti-malware program and your security vulnerabilities.
- Anti-malware software requires full access to your operating system in order to look for infected files and detect malicious behaviour and this could at times, increase your level of risk, especially if it is poorly designed or compromised by a back door. So use it with caution and dont be heavily reliant on the software alone. Practise vigilance.
- Uninstall software that you do not use any longer. Outdated software often has security issues.
- Improve the security of your Web browser by preventing it from automatically running potentially dangerous programs that are sometimes contained within the web pages you visit.
- Be cautious when opening files that are sent to you as email or messenger attachments, through download links or by any other means. As a general rule, avoid opening files from unknown sources, though even trusted sources might inadvertently send you malware.
- Be cautious when inserting removable media like USB sticks, flash memory cards, DVDs and CDs into your computer.
- Check out Windows Basic Security Tool Guide for tips on how to do this more safely.
- NOTE: If you often need to open files or insert external media from strangers, use a compartmentalised system like Tails to prevent malware from infecting your computer or accessing your sensitive files.
- Never accept and run applications that come from websites you do not trust. Instead of accepting an "update" offered in pop-up browser windows, for example, check the relevant application's official website.
- Uninstall Adobe Flash and the Java browser plugins as described in Section 3 of the Firefox Tool Guide (Windows, Mac, Linux).

- If you hover your mouse over a link in an email or on a webpage, you will see the full website address. This can help you decide whether or not you want to click that link. If you are using Mozilla Firefox, you can install the NoScript add-on, as described in the Firefox guide. Browser extensions like Privacy Badger, HTTPSEverywhere, and uBlock Origin are also helpful.
- Stay alert when browsing websites. Glance at the website address after you follow a link and make sure it looks appropriate before entering sensitive information like your password. Watch for browser windows that appear automatically and read them carefully instead of just clicking Yes or OK.
- When possible, verify the software you download before installing it. This is not always easy, but the Tor Browser(https://www.torproject.org) Tool Guide for Linux describes one way of doing this on Linux.
- Disconnect your computer from the Internet when you are not using it and shut it down completely overnight.

5.4: How do you protect your smartphone from malware?

Smartphones and tablets are increasingly targeted by malware because they are constantly left on and there are many weak spots to attack - by gaining access to microphones, cameras and GPS hardware via third party apps etc.

- Keep your operating system and applications up to date.
- Install only from official or trusted sources like Google's Play Store and Apple's App Store (or F-droid, a FOSS app store for Android).
- Pay attention to the permissions requested by your app. If they seem excessive, deny the request or uninstall the app.
- Consider installing a reputable anti-malware tool if available for your device.
- Uninstall apps that you don't use. Developers sometimes sell their apps to other parties who may continue to improve the app or try to make money by inserting malicious code.
- See the Basic Security for Android Tool Guide for more information on protecting your Android smartphone or tablet.

5.5: How do you recover from malware?

First step is to disconnect the device from any networks it has access to, so you prevent infection of other devices.

Sometimes, cleaning out malware may be as simple as running your anti-malware software and allowing it to resolve the issue. But keep in mind, certain malware is designed to survive a full reinstallation of the operating system. Follow the below steps to ensure your device is safe to use after a malware attack:

- Do a full scan with your existing anti-malware tool.
- If the suspect device is a computer, restart it from an anti-malware rescue disk (Eg: Windows Defender Offline or the AVG RescueCD).
- Discard the USB memory stick you used to create the rescue disk.
- Restore your device to its "factory settings," if you can after backing up your important files. Do NOT backup any software. Be careful with the storage device used for backup. Make sure it is clean before plugging it into your restored device.
- If the suspect device is a computer, reinstall the operating system.
- Once again, make sure your backup disk is clean before plugging it into the device on which you reinstall the operating system. If you use a USB stick to reinstall the operating system.

Resources:
Phishingquiz Phishing is an attempt to trick you into giving up your personal information by pretending to be someone you know. Identifying these attempts can be harder than you think. Can you tell what's fake?
Visit: https://phishingquiz.withgoogle.com

Virustotalanalyze suspicious files and URLs to detect types of malware, automatically share them with the security community
https://www.virustotal.com/

Windows defender: https://support.microsoft.com/en-us/help/17466/windows-defender-offline-help-protect-my-pc /

Windows defender offline tool.https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/windows-defender-offline

06.

Protect important data on your device

If your device falls prey to a remotely operated intruder attack, or if an individual manages to access your device physically, they may be able to read or modify your data. While making sure you have implemented the above mentioned steps to improve your digital security, it also helps to maintain several layers of security.

Another important step is to protect the files themselves. That way, your sensitive information is likely to remain safe even if your other security steps fail.

There are two general approaches to the challenge of securing your data in this way ; encrypt your files, making them unreadable to anyone but you, or you can conceal them, hoping an intruder will be unable to find it.

6.1: Encrypting your information

You may want to refresh your memory on what was discussed earlier about encryption, before you move into this section. To repeat and put it simply, it's like storing your information in a vault.

One useful tool in this regard is Veracrypt - a trusted, free and open-sourced program.

Pros of using Veracrypt:

- Offers ability to permanently encrypt the whole disk of your computer including all your files, all temporary files created during your work, all programs you have installed and all Windows operating system files.
- Supports encrypted volumes on portable storage devices.
- Provides 'deniability' features (Hidden volumes and hidden operating systems. Until decrypted, a VeraCrypt partition/device appears to consist of nothing more than random data, making it impossible to prove that a partition or a device is a Veracrypt volume or that it has been encrypted.

6.2: Using VeraCrypt safely

First step is to determine the level of sensitive information you are planning to keep; unless you have a good reason to store a particular file, or a particular category of information within a file, you should simply delete it . The second step is using a trusted encryption tool such as VeraCrypt.

It is important to remember that when your VeraCrypt volume is 'mounted' (enables access of the content to you) the information stored may be vulnerable. So make sure to keep it closed if you are not actually accessing the files. After all, what is the use of a sturdy home if you are going to leave the door open?

6.3: Other tips

- Disconnect VeraCrypt when you walk away from your computer for any length of time. Even if you typically leave your computer running overnight, make sure the sensitive files are not open for access physically or remotely.
- Disconnect before putting your computer to sleep. This applies to both 'suspend' and 'hibernation' features, typically used with laptops.
- Disconnect before allowing someone else to handle your computer. When taking a laptop through a security checkpoint or border crossing, disconnect all encrypted volumes and shut your computer down completely.
- Disconnect before inserting a USB memory stick or other external storage devices, even if they belong to friends and colleagues.
- If you keep an encrypted volume on a USB memory stick, remember that just removing the device may not immediately disconnect the volume. Always dismount the volume properly, then disconnect the external drive or memory stick and then remove the device.
- If you decide to keep your VeraCrypt volume on a USB memory stick, you can also keep a copy of the VeraCrypt program with it. This will allow you to access your data on other people's computers. However: if you don't trust the machine to be free of malware, you probably shouldn't be typing in your passwords or accessing your sensitive data.

Resources:
VeraCrypt- https://www.veracrypt.fr

How to use Veracrypt: https://www.youtube.com/watch?v=cxo8xosH_TI
Veracrypt beginner’s tutorial - https://www.veracrypt.fr/en/Beginner%27s%20Tutorial.html

07.

Keeping safe when using social media

Social media platforms provide ease of connectivity and communication both online and offline. But it has left a lot of scope for various groups to abuse and exploit information shared by users.

Although social media sites are virtual platforms, the interactions we engage in have real life implications and it is imperative to keep this in mind before you share information, particularly personal details. You wouldn't offer up your personal details to a stranger you meet in real life and this practise must remain the same when you are using social media because you may be divulging more than what you intend to, if you are not being careful.

Also remember that social networking sites are owned by private businesses that make money by collecting data about individuals and selling it to third party advertisers. When you enter a social networking site, you are leaving the freedoms of the internet behind and are entering a network that is governed and ruled by the owners of the site. Privacy settings are only really meant to protect you from other members of the social network, but they do not shield your data from the owners of the service. Essentially you are giving all your data over to the owners and trusting them with it.

If you work with sensitive information and topics, and are interested in using social networking services, it is important to be very aware of the privacy and security issues that they raise as your activity and engagement on those sites can make you particularly vulnerable.

7.1: General tips for safe social media use

- Always ask the questions:
- Who can access the information I am putting online?
- Who controls and owns the information I put into a social networking site?
- Will my contacts mind if I share information about them with other people?
- Do I trust everyone with whom I'm connected?
- Always make sure you use secure passwords and when possible, the two factor authentication to access social networks. If anyone else does get into your account, they are gaining access to a lot of information about you and about anyone else you are connected to via that social network. Follow all instructions reviewed in our section about passwords in Section 2!
- Make sure you understand the default privacy settings offered by the social networking site, and how to change them.
- Consider using separate accounts/identities, or maybe different pseudonyms, for different campaigns and activities. Remember that the key to using a network safely is being able to trust its members. Separate accounts may be a good way to ensure that such trust is possible.
- Be careful when accessing your social network account in public internet spaces. Delete your password and browsing history when using a browser on a public machine.
- Access social networking sites using https:// to safeguard your username, password and other information you post.
- Be careful about putting too much information into your status updates – even if you trust the people in your networks. You may fall victim to imposters and impersonators that aim to damage your credibility!
- Most social networks allow you to integrate information with other social networks. Be particularly careful when integrating your social network accounts! You may be anonymous on one site, but exposed when using another.
- Be cautious about how safe your content is on a social networking site. Never rely on a social networking site as a primary host for your content or information as it is very easy for governments to block access to a social networking site within their boundaries if they find its content objectionable.

7.2: Sharing personal details

Social networking sites ask you for a good deal of data about yourself to make it easier for other users to find and connect to you. This is the biggest vulnerability as it opens up a slew of concerns including identity fraud and makes it easier to identify you and monitor your activities.

Ask yourself: is it necessary to post the following information online?

- birth dates
- contact phone numbers
- addresses
- details of family members
- sexual orientation
- education and employment history

7.3: Who do you interact with?

We use social media mostly to establish connections with other people. The connections may mostly comprise of those you know and trust – but you may also be connecting to an online community of like-minded individuals you have never met. Given interactions on these platforms involve inadvertently sharing a lot of information about yourself, try as much as possible limit contacts with unknown users.

7.4: Who can see your status updates

The default setting for the status update on most social networking applications is 'public' - meaning anyone on the internet can see it. If you only want your contacts to see the updates, you need to tell the social networking application to keep your updates hidden from everyone else.

Exercise:
Twitter - look for "Protect Your Tweets"
Facebook - change your settings to share your updates with "Friends Only".

Even if you switch to those settings, think about how easy it is for your information to be reposted by followers and friends. You should also think about what you may be revealing about your friends that they may not want other people to know and to ask others to be sensitive about what they reveal about you.

7.5: Revealing your location

Most social networking sites will display your location if you have enabled location services. But this isn't just limited to your mobile, even your desktop can release data about your location. Be particularly mindful of updating location settings on photo and video sharing sites. Don't just assume: double-check your settings to be sure they are not sharing your location information.

7.6: Content sharing

All social media sites already are increasingly visual oriented. The millions of photos and videos on these sites can reveal people's identities very easily. It's important that you have the consent of the subject/s of any photo or video that you post. Photos and videos can also reveal a lot of information unintentionally (remember what was discussed earlier on metadata 3.3). Photo and video sharing sites may publish this information when you upload content to their sites.

7.7: Instant chats

Many social networking sites have tools that allow you to have discussions with your friends in real time. Unfortunately, despite the convenience, they are one of the most insecure ways to communicate on the internet; because they may reveal who you are communicating with, and what you are communicating about. Connecting to the site via https:// is a minimum requirement for secure chatting, but even this is not always a guarantee of security. Eg: Facebook chat uses a different channel to HTTPS (and is more prone to exposure).

Resources:
Instead of instant chat services, we recommend you to use the below secure, internet based messenger apps;
Wire - https://app.wire.com/
Signal - https://signal.org/

Whatsapp – this is a popular messaging service in the region. But do take a look at the information below to ensure you are using the platform safely.
https://www.whatsapp.com/safety
https://www.makeuseof.com/tag/whatsapp-secure-tips/

7.8: Joining the community; creating groups, events and communities

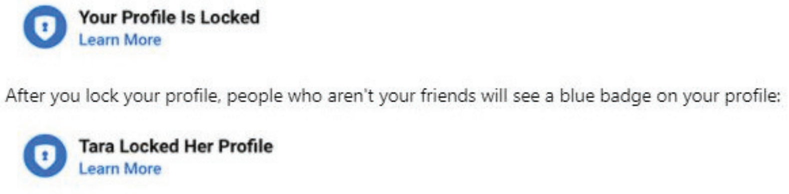
When you join a community or group online it is revealing something about you to others. On the whole, people may assume that you support or agree with what the group is saying or doing, which could make you vulnerable if you are seen to align yourself with particular political groups etc.
Also if you join a group with a large number of members that you don't know, this can compromise any privacy or security settings you have applied to your account. Alternatively, if you set up a group and people choose to join it, what are they announcing to the world by doing so?

Resources:
Google- https://about.google/community-guidelines/
Facebook- https://www.facebook.com/communitystandards/
You Tube - https://www.youtube.com/about/policies/#community-guidelines
Youtube safety tools - https://www.youtube.com/about/policies/#staying-safe

7.9: Some new features to ensure safety on social media

Facebook

Profile lock
Restricts public viewing of your profile, all content of your profile can only be viewed only by friends
Details and step-by-step guide: https://www.facebook.com/help/196419427651178



Your Profile Is Locked
Learn More

After you lock your profile, people who aren't your friends will see a blue badge on your profile:

Tara Locked Her Profile
Learn More

Instagram

'Limits'
-Feature aims to limit abusive comments and direct messages. It allows users to limit/hide comments and messages from users not on their followers list or have become recent followers.

'Hidden words'
-Something of a spam folder, the feature allows users to filter offensive words, phrases that are redirected to another 'hidden' folder.

Security Check-up
Launched in June 2021, the feature helps protect users from malware, spam and other threats that create vulnerabilities on the platform. Its a guide for users, containing simple steps with instructions on how to protect their accounts with mechanisms including checking login activity, reviewing profile info and confirming the accounts that share login information.

Link: https://about.instagram.com/blog/announcements/keeping-instagram-safe-and-secure

Whatsapp

In October, Whatsapp introduced end-to-end encrypted backups in chats. As a result, the feature will provide additional security to backups stored. Those who backup chats can now secure the data with either a password or a 64-digit encryption key in case they misplace their main device.

How to activate:
1:Open "Settings"
2: Tap chats and open "Chat Backup". Select "End-to-end encrypted backup"
3: Tap "Turn On" and follows prompt to create a password/passkey
4: Tap "Create"

TikTok

One of the key safety feature concerns on TikTok is the absence of two-factor authentication. Instead provides option to log in with a verification code sent to your phone.

Its a one-time access code. But this can also lead to phishing or ransomware attacks.

Securing TikTok
- Privacy – Choose to option to make the account 'private' to prevent exploitation of your content or identity
Go to:
1: Profile page
2: Tap three dots in the right-hand corner -- select "privact and setting"
3: Toggle "Private Account" on

Direct Messages
- Offers the user to select who can send direct messages
Go to:
1: Within "Privacy and Safety" tab, tap "Who can send messages to me"
2: Choose from among - "everyone", "friends" or "off"

Avoid linking other social accounts to your TikTok account
Always routinely update the app to benefit from any security updates