A guide to practicing basic digital safety in India

Kaarana *ಕಾರಣ* *कारण*

Table of Contents

Introduction

Are you an activist defending human, social or cultural rights? Do you rely on digital tools and platforms such as Facebook, Twitter or WhatsApp for collaborating or organising efforts? Are you a journalist with confidential sources and information to protect? Or are you a citizen who doesn't want their accounts and/or devices to be at risk of compromise?

It is not paranoid to be worried about the safety and integrity of your data and communications in our current times, and, as the recent arrests of lawyers, activists and others have made clear, standard police operating procedures includes the seizure of phones, laptops and electronic storage devices, along with demands for passwords of online accounts, for resources such as email, social media, etc., in order to gain access to private conversations and personal information of those arrested.

Minimising threats to your digital life and securing yourself online is an ongoing process, and while one cannot secure their digital footprint in every way, all the time, it is indeed possible to take steps which greatly minimise threats to both security and privacy -- offline as well as online. It is absolutely **CRITICAL**, if you believe that you may be at an increased risk for seizure of devices due to the work you do, that you take steps to protect your digital security immediately, so that if/when the police show up demanding access to your devices - you are covered.

This is a basic guide that breaks down the process of securing your digital communications and devices in various scenarios, including where they may be confiscated, illegally retained or threatened with destruction. This process also ensures that in such scenarios there is minimal loss of your communications and data and that you continue to remain in control of it.

Below, we are listing down some of the rights you as a citizen are entitled to and advisable action which you should take when faced with seizure of your devices and/or demands for your account credentials.

Citizen rights

1. **What are your rights when police demands access to mobiles or computer devices?**
    a. If the police have asked you to hand over the device via notice then you have a right to refuse.
    b. If the device is seized during a search, you cannot refuse.
    c. If the police already has custody of the device and demands access, you have a right to refuse.
2. **What are your obligations to provide passwords of devices and/or accounts to police officers?**
    a. You have a right to refuse any demand / request for passwords.
    b. The only exception to this is Section 69 of the Information Technology Act. This can only be resorted by the police in cases of national security etc. Even so, the validity of this law is questionable.
3. **Search through seizure vs search through court ordered warrant**
    a. As suggested above, if there is an FIR then you have more rights responding to a court notice than in a search and seizure operation. An accused person cannot be compelled to produce evidence.
4. **How to recover from illegal confiscation of your equipment?**
    a. The validity of a search and subsequent seizure is subject to judicial review. *Note:* Please see the 'Annex A' section of this document for information on what court-issued warrant is supposed to look like.
    b. There are two possible alternatives: challenging the order granting search warrants; or filing an application under Section 451 or 457 of the Criminal Procedure Code, depending on the facts.
5. **How will proper operational security measures benefit you in the case of arrest and seizure of devices?**
    a. Secured devices/accounts make it difficult for them to be breached without your consent.
    b. The use of weak or no passwords make it so that your devices or accounts are just like open notebooks waiting to be read.
6. **What to do before the police illegally confiscate your equipment**
    a. The basic security measures should be kept, as identified in other parts of this document.

Understanding threats to your digital safety

In Security the concept of “Threat Scenario” (also referred to as “Threat Vector”) is important to understand because a given technology solution or advice is often designed to protect you in the face only a few well defined threats. So you should evaluate the advice and tools you should adopt based on the threats you are likely to face in your specific situation and understanding how the security features and advice addresses those scenarios. For e.g. if you are a college student or a programmer, say, in a normal company you may not be worried about the police confiscating your laptop, whereas if you are a journalist covering hot current issues your security needs are different.

Here are the common threat scenarios you should be aware of with your digital security. “Malicious Actor” is abbreviated as MA in this section.

1. **Online attacks on your accounts**
    a. MA successfully guesses your email password - either because your password is too weak, or;
    b. You use the same password across more than one website, and MA gets usernames/passwords from one Service (A) and they are now able to get into other Service (B) as well - even if Service B is much more securely operated as Service A;
    c. MA sets up a “phishing site” that fools you into entering your password on the fake website; so you essentially give your password to the MA yourself;
    d. You visit an insecure website (say through a link that MA sent to you via email); the insecure website ends up installing malware on your computer;
    e. You check your email on a kiosk machine - which you should assume is basically compromised - and as you type your passwords malware on the machine captures them, so you have effectively given away your password;
    f. You use software (such as your browser or operating system) that are not up to date, and increase the number of attacks you are vulnerable to;
    g. You downloaded apps on your mobile and granted it wide access to your account data (like contacts, SMS, call history, etc.) without thinking too much about whether that app needs that access or not;
    h. You used “Login with Google” or “Login with Facebook” on some website or web application, and granted wide ranged access either because you were misled by the app or did not think too much of it.

2. **Physical security of your devices**

    a. You leave your laptop or phone unattended in a coffee shop or train (say) and MA can either steal your machine or accesses your machine in your absence;
    b. Government agency or local police confiscates your devices and asks you for passwords.

Tips for security against online attacks

Software Updates

Use a modern browser and operating system, and always update to the latest version in a reasonable time frame. Do not ignore legitimate notifications to upgrade your software as they often include fixes to known security vulnerabilities.

Passwords & Passcodes

Passwords are the gateways to our digital identities as they unlock our devices and communications. Protecting them not only prevents us from harm, but is absolutely critical for secured access.

Remember: Fingerprints can be requested or taken forcefully to unlock devices, as they fall under physical evidence. Use a password or passphrase to secure access to your devices

- **Tips for choosing strong passwords:**
    - Passwords should be 8 characters long at the very least;
    - Using a mix of letters, numbers and special characters usually makes them stronger;
    - Passwords may be derived from long phrases from your favourite book, regional/local terms, or even song lyrics to make good passwords. If you can take just some letters (instead of whole words from the phrases) to make a string that cannot be found in a dictionary, that would be better;
    - Alternatively, a password generator - such as that provided by LastPass or Random.org - may be used for generating a strong password;
    - Use different passwords for each website or service you use. This way if one Service is compromised, it does not impact your accounts with other Services;
    - Make use of a website such as https://howsecureismypassword.net/ to test the complexity of a password structurally similar to the one you want to use.

- **Things to avoid with passwords:**
    - Do not write passwords down on paper or as a note on your phone - keep passwords secret;
    - Avoid common words (like “password”, or words found in any dictionary) - not even if using numerical digits and combining of upper and lowercase letters - this would include passwords such as ‘computer’ ‘computer1’, ‘Computer!” or even ‘Computer123’;
    - Passwords should not be related to any known family, interests/hobbies, date of birth, etc.[1] - including random words may make password guessing or cracking harder, but at the same time it may make it more difficult for you to remember.

- **Password managers:**
    - Use a password manager like LastPass or KeePass to remember, store and retrieve account passwords;
    - Using a password manager makes it more convenient to use unique passwords for different services, and overall usually more secure than otherwise;
    - Please note that if you are the risk of having your device confiscated having a password manager on a phone or laptop can be risky. Ensure that your password manager times you out at periodic intervals, and the password you use to protect your password database is very strong and not written down anywhere (including your devices);
    - If you are using an “offline” manager like KeePass you can put your encrypted password database on Dropbox or Google Drive. That way you can access the same file on multiple devices, and in case your laptop is confiscated you can still access your main database and even move it around, or change the password, to protect it from unintended access from devices you have lost access to.

- **Mobile device passcodes:**
    - Phone passcodes should not contain repeating numbers or easy patterns (111111, 123456, 898989) as these take much less time to crack in comparison to passcodes with non-repeating numbers;
    - Avoid using a specific date, month or year as your passcode;
    - Passcodes should be 6-8 digits long - keep your phone’s software updated as there may be exploits which allow for your phone’s passcode to be cracked/retrieved on older versions/phones. (Ref: https://motherboard.vice.com/en_us/article/wjken4/leaked-emails-cops-hiding-graykey-grayshift-phone-hacking-emails)

[1] https://en.wikipedia.org/wiki/Wikipedia:10,000_most_common_passwords

Two-factor authentication

Two-factor authentication (also known as “Two-step verification”, or “Multi-factor authentication” or just 2FA) acts as an additional layer of protection for your accounts. The idea is when you log into a Service, you need to provide proof of two things: (a) something you know - i.e. a password, and (b) something you have - like access to a different device, or a security token etc. Here is a website which lists many prominent web services who supports 2FA.

For example, using 2FA on Twitter (say) would make it so that a user has to enter, after their account credentials, a six-digit code (which is either texted to a provided phone number, or which can also be retrieved through an offline 2FA code generator app), which is then verified to make sure that the login attempt has both **a)** the proper account credentials as well as **b)** access to the mode previously specified for 2FA.

Most popular online services support two-factor auth as it provides effective protection against common password attacks, like weak or reused passwords. The most popular form of second factor is the SMS OTP that most of us are familiar with because it is so ubiquitous in India. Unfortunately SMS based OTP suffers from many security drawbacks like SIM confiscation, wiretapping, and carrier-social-engineering. Where possible you should opt for other two factor methods, and many popular services provide users with other options. Here is an overview of generally available second factor methods:

- **Code based authenticator applications:**
    - Examples are: Google Authenticator, Microsoft Authenticator, Duo Mobile; these code base authenticator apps can be used across Services - for e.g. the Duo Mobile app can be added as a second factor for your Google account, Office 365 account and your Github account;
    - *Note:* Some of these apps will require re-initialization when you change phones, so if you lose your phone or upgrade to a different device you will difficulty getting into your accounts. This is a security feature so that SIM hijacking does not automatically compromise your app-based second factor. This means when using one of these apps you should also create backup codes if the Service supports is and put them in a locker or a password manager;
    - Create a backup of the secret key(s) used for 2FA code generation. This means, safely storing an image of the QR code that is provided at the time of setting up 2FA. Failure in maintaining a backup of 2FA secret key(s) might lead to the loss of account access.

- **Push-based authenticator applications:**
    - Examples are apps like, Google Prompt, Microsoft Authenticator, Duo Push, and often the apps often only work with specific services (like Google Prompt only works with Google services);
    - These apps do not provide a code, but show a prompt in the mobile app asking you to confirm if you are trying to log into your account at that time;
    - These are more convenient to use than code based apps and we recommend this over SMS and Code-based authenticator apps.

- **Backup codes:**
    - Some services provide the ability to generate a number of backup codes that you can print and put away safely (say in a locker) that you can use instead of one of the above methods;
    - These can be a good way to recover if you fear losing devices, but unless you secure the codes these have the potential to undermine your security.

- **Security Keys:**
    - These are the most modern and secure two-factor methods. These are the only available method today that is resistant to phishing;
    - We recommend Security Keys over any of the other methods.

It is worth pointing out that all code-based and push-based two factor methods are prone to phishing. Security Keys, on the other hand use cryptographic security and work in tandem with the browser to ensure that you are authenticating with the correct website. Security Keys are based on a standard called U2F and security keys are generally available from companies like Yubico (called Yubikeys) and Google (branded 'Titan Keys'). Feitian is a reputed Chinese company that also makes and sells security keys around the world, but we do not recommend buying direct from Feitian by ordering from India.

In summary, here are the key takeaways about 2FA:

1. Enable Two-factor auth on all services that support them;
2. Any two-factor method is better than having no two-factor;
3. Yet, most two-factor methods themselves are susceptible to phishing;
4. If you are really paranoid or need the highest security you can get a hold of, you should get Security Keys.

Allowing third party apps access to your data

Large services like Google, Facebook, Twitter, and others, have rick Application Programming Interfaces (APIs) to enable independent developers to build innovative and useful features on top of the core products. If you have linked your Facebook account with your Tripadvisor account, or use a third party mobile client for reading your Twitter feed, then you have used APIs.

These integrations mostly use a well defined protocol called oAuth 2.0 and always require the user's consent before they are allowed access to the user data in the core product. That is, unless you approve the integration to Facebook, TripAdvisor cannot access your Facebook data or your friends list. However users often do not pay a lot of attention to the level of access they provide to these apps, and that often leads to trouble.

Different services have had different problems in this space, but here are two main principles you need to follow:

1. When you grant apps access to your data, pay a lot of attention to what permissions it is asking for. For e.g. if a bus ticket booking app asks for access to your Contacts List, you should ask yourself whether this is reasonable or not
2. Facebook, Google and other API providers also provide tools for you to review the third party apps that have access to your data. Review them periodically and revoke access to apps that you no longer use. For Facebook, this page has more info. For Google you can use the Security Checkup tool.

Other service-specific advice

Email

a. If you are online, chances are you have one or more than one email identity provided by email services such as Gmail, Yahoo and/or Hotmail
b. You MUST ensure that you enable two-factor authentication (authenticator-based provides more security in case of SIM confiscation). Also see earlier section called on Two-factor authentication
c. *If you use Google:*
    i. visit the Security Checkup tool periodically and review the information there. The tool checks your account access and points out any changes you need to make, for e.g. enable two factor authentication.
    ii. If you think you are particularly at risk of targeted online attacks, you can consider enrolling in the free 'Google Advanced Protection Program', which enforces highly secure settings on your account to automatically protect your Google account from many online threat scenarios. Note that you will have to purchase two security keys before you can get into the program but there is no charge for being in the program itself. If you

are at risk of physical confiscation of your computing assets, leave one of your keys with a friend or relative.

iii. Periodically review active sessions (bottom-most in Gmail on Desktop) and log out from inactive devices. “Sign out all other Gmail web sessions” and Change password if you find unfamiliar device logged into your account.

Communication channels and applications

1. **WhatsApp**
    a. Make use of security codes (for verifying when a contact migrates to newer device);
    b. Remove unused *web.whatsapp.com* sessions;
    c. Use 2FA to prevent WA access in case of SIM being physically confiscated and put in another device:
        i. (Settings -> Account -> Two-step verification);
        ii. Choose a strong, secure 6 digit pin.
    d. Disable online backups:
        i. (Settings -> Chats -> Chat backup -> Backup to Google Drive)
        ii. Choose “Never” or “Only when I tap ‘Back up”

Ref:
https://metro.co.uk/2018/08/27/whatsapp-is-quietly-storing-your-private-messages-in-an-unencrypted-archive-where-its-feared-hackers-could-read-them-7885607/

2. **Signal**
    a. Use disappearing messages (time-limit based);

3. **Telegram**
    a. Use secret chats over regular ones with self destructing messages;
    b. Remove authenticated sessions from unused devices.;

Encrypted Calling Apps:

a. Signal
b. WhatsApp Voice
c. Threema

Documents Storage (Dropbox, OneDrive, Google Drive)

1. Google Takeout - https://takeout.google.com/ - maintain offline backups instead of online ones, as it allows you to retain more control;
2. If online backups must be made, make sure to use a reputed service which can also guarantee the security, integrity and privacy of uploaded data;

Social Media

1. Disable syncing of contacts (contact information can be compromised due to sync with Facebook/Twitter);
2. Enable 2FA on social media accounts (sensitive communications sent in private can be compromised through targeting of social media accounts);
3. Two-way conversations can be compromised from either end, so when communicating sensitive details with someone else, make sure that they too are following basic operational security procedures.

Physical confiscation and device security

Your devices are the gateways to your online identities and activity. When you lose access to your devices - because they are lost, stolen or confiscated - the precautions mentioned in the above section about *online security* are no longer sufficient.

Encrypting your electronic devices

Password protecting your devices may not be enough in some cases as it is almost always still possible for data on the device to be recovered/extracted through digital forensics techniques. In such cases of heightened risk, it is important to encrypt fully your computing device as well as smartphone. It is also important to choose a robust passphrase for the encryption of the digital device - just the same way it would be important to choose a complex pin for an analog safe with valuable goods inside of it.

A strong passphrase acts as an overarching layer of protection which can prevent your data from being wrongly accessed without your consent.

Leaving your devices unlocked - and why you shouldn't

Make sure to always close the computer lid, lock the screen, or power off the device wherever possible. Most smartphones which have screen-locking allow users to set a time limit since time of last lock before the passcode has to be entered again. This will help keep your device safe from unauthorized access.[2]

Those at an increased risk of device seizure should also make it so that their phone passcode/password has to be entered each time during unlocking, regardless factors such as proximity to a home WiFi network, or time since last unlock, through security settings available on their phone.

---

[2] Ref:https://www.businessinsider.in/The-FBI-staged-a-lovers-fight-to-catch-the-kingpin-of-the-webs-biggest-illegal-drug-marketplace/articleshow/47474146.cms

Remember: If or when the device is on and already unlocked, unencrypted and/or not password-protected at the time of seizure, none of the steps listed above may be of any considerable help.

Mobile Phones

Android Devices

1. Updated OS with a 8-character alphanumeric passcode of decent strength - NO FINGERPRINTS;
2. Disabling online backups;
3. Deactivate Google Assistant or any forms of smart unlock (WiFi/NFC);
4. *Remote wipe through Google:*
    a. Login to myaccount.google.com;
    b. Head over to https://www.google.com/android/find;
    c. Locate the device which you wish to make changes to, click 'Erase' or 'Wipe Device'.

iOS Devices

1. Updated OS with a passcode/word of decent strength - NO FINGERPRINTS;
2. iCloud-based backups should be disabled;
3. *Remote wipe through the iCloud platform:*
    a. Login to icloud.com;
    b. Head over to 'Find my iPhone';
    c. Locate the device associated with your account, then click on 'Erase iPhone'.

Note: Installing software updates is also a crucial step in protecting against unpatched vulnerabilities or techniques being successfully exploited by those attempting to gain access to your mobile device.

Contacts

- *Automatic contact backup on Google (specific to Android devices)*
    - Visit contacts.google.com;
    - Check to see if any contacts have been automatically uploaded, delete as and where necessary.

- *Using TrueCaller without compromising your contacts:*
        - Visit truecaller.com;
        - Login with an unused account, do not share contact details if logging in via Gmail
        - Look up number once logged in

Call and SMS

Clear call and SMS histories as often as you can, unless it is important that you retain them (such as for proof of financial transactions, etc). Avoid using your phone's cellular network for sensitive communications. India has a central, lawful interception system dubbed 'CMS', which can allow for most phone-based communication to be intercepted. Make use of a secure, encrypted messaging/calling platform in cases where exposure of communication to anyone except the party with whom contact was intended would have unwelcome implications.

Computing Devices

Windows: *Encryption through BitLocker on Windows*

1. *Setting-up BitLocker:*
    a. Required OS
        i. Windows 10 - Education, Pro, or Enterprise edition
        ii. Windows 8 — Professional or Enterprise edition
        iii. Windows 7 — Enterprise or Ultimate edition
2. (Start > Control Panel > System and Security > BitLocker Drive Encryption)
3. *Storing the Recovery Key:*
    a. Secure Storage
        i. Printed document kept in an unreachable place or with a trusted associate;
        ii. On a USB drive kept in an unreachable place or with a trusted associate.

Mac OS: *Using FileVault*

1. *Setting-up FileVault:*
    a. (System Preferences > Security & Privacy > FileVault)
        i. Use the 'Recovery Key' option instead of opting for iCloud-based unlocking;
        ii. Protect the Recovery Key by keeping it secret and out of reach, or with a trusted associate.

Linux/Ubuntu

1. *Using Veracrypt for disk encryption on Linux systems:*
    a. A quick guide on installing and implementing Veracrypt can be found here: https://linuxconfig.org/encrypt-a-drive-with-veracrypt-in-linux

Storage Devices

Files which are deleted from storage devices *(such as pen-drives & portable HDDs)* can be recovered if not properly overwritten. When deleting sensitive files, it is important to *purposefully* overwrite any bits which may have been left behind.

- *CCleaner:*
  - CCleaner may be used to overwrite data so that it is irrecoverable through regular capabilities. (Ref: https://www.ccleaner.com/docs/ccleaner/introducing-ccleaner/can-data-cleaned-by-ccleaner-be-recovered)

- *DBAN:*
  - DBAN is a utility which provides several methods for rendering the data on a disk irrecoverable. (Ref: https://dban.org/)

Annexe A

FORM No. 10

WARRANT TO SEARCH AFTER INFORMATION OF A PARTICULAR OFFENCE

(*See* section 93)

To

(*name and designation of the police officer or other person or persons who is or are to execute the warrant*).

WHEREAS information has been laid (*or complaint has been made*) before me of the commission (*or* suspected commission) of the offence of (*mention the offence concisely*), and it has been made to appear to me that the production of (*specify the thing clearly*) is essential to the inquiry now being made (*or* about to be made) into the said offence (*or* suspected offence);

This is to authorise and require you to search for the said (*the thing specified*) in the (*describe the house or place or part thereof to which the search is to be confined*), and, if found, to produce the same forthwith before this Court, returning this warrant, with an endorsement certifying what you have done under it, immediately upon its execution.

Dated, this day of ,19 .

(*Seal of the Court*) (*Signature*)

Form No. 10, "Warrant to search after information of a particular offence"
Code of Criminal Procedure

FORM No. 11

WARRANT TO SEARCH SUSPECTED PLACE OF DEPOSIT

(*See* section 94)

To

(*name and designation of the police officer above the rank of a constable*).

WHEREAS information has been laid before me, and on due inquiry thereupon had, I have been led to believe that the (*describe the house or other place*) is used as a place for the deposit (*or* sale) of stolen property (*or if for either of the other purposes expressed in the section, state the purpose in the words of the section*);

This is to authorise and require you to enter the said house (*or other place*) with such assistance as shall be required, and to use, if necessary, reasonable force for that purpose, and to search every part of the said house (*or other place, or if the search is to be confined to a part, specify the part clearly*), and to seize and take possession of any property (*or* documents, *or* stamps, *or* seals, *or* coins, *or* obscene objects, *as the case may be*) (*add, when the case requires it*) and also of any instruments and materials which you may reasonably believe to be kept for the manufacture of forged documents, *or* counterfeit stamps, *or* false seals, *or* counterfeit coins *or* counterfeit currency notes (*as the case may be*), and forthwith to bring before this Court such of the said things as may be taken possession of, returning this warrant, with an endorsement certifying what you have done under it, immediately upon its execution.

Dated, this day of ,19 .

(*Seal of the Court*) (*Signature*)

Form No. 11, "Warrant to search suspected place of deposit"
Code of Criminal Procedure