KEEPING YOURSELF SAFE ONLINE

VOLUME 1

DEF
DIGITAL EMPOWERMENT *foundation*

WAAT
WOMAN ACT AGAINST TROLLS

WEBAWARE
AN ONLINE SAFETY INITIATIVE BY OLX INDIA

This compilation has been adapted from Digital Security Training Kit by Digital Empowerment Foundation made under the IMPACT project and Chayn's Advanced DIY Online Safety for Every Woman

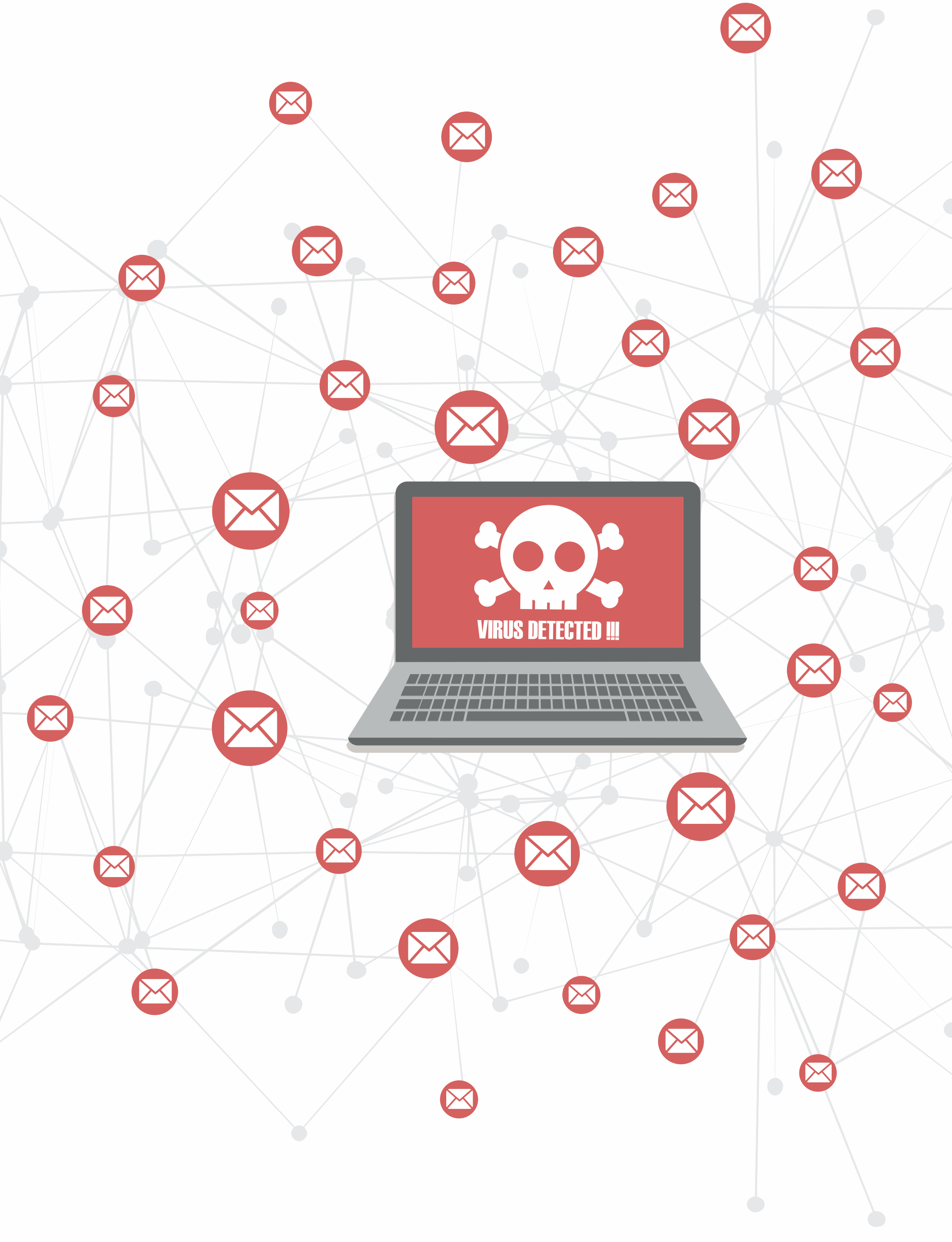
Written by Zothan Mawii
Designed by Ravi Kumar Yadav

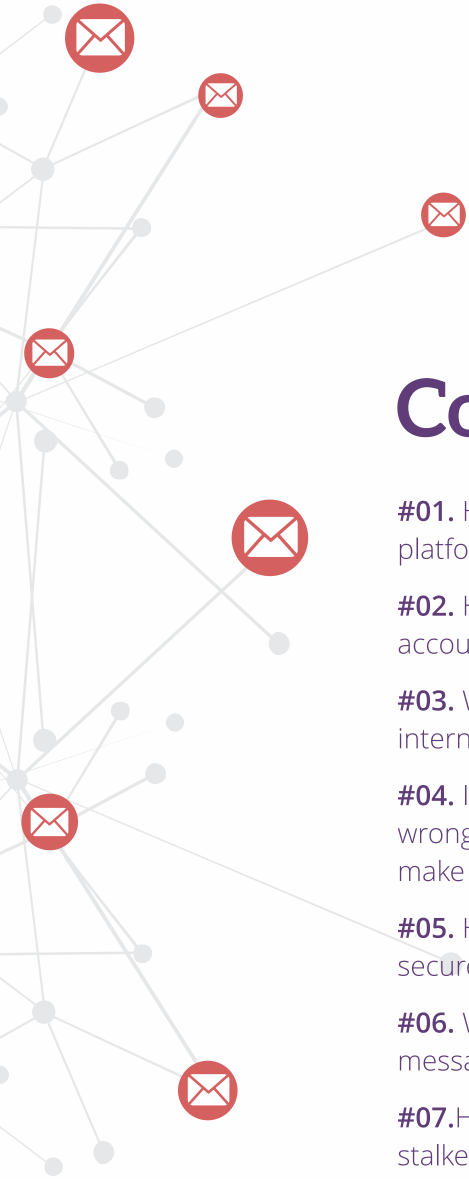
Published by:
Digital Empowerment Foundation
House No. 44, 3rd Floor,
Kalu Sarai, New Delhi-110016

To read this publication online, visit
www.defindia.org/publication-2

KEEPING YOURSELF SAFE ONLINE

Volume 1 for secondary school and college students


VIRUS DETECTED !!!



Contents

How do I use social media platforms safely?

We all use social media platforms to share our photos, stories, opinions, read and watch new content. Some of us may even be using these sites to promote our work whether for creative outreach or commercial purposes. Social media has spawned a number of commercially successful "influencers" who have monetised their social media posts and pages to a good extent.

Social media sites receive a lot of flak for a number of things – spreading misinformation, collecting data about users and sharing them to third parties, social media addiction and the list goes on. While these accusations may hold weight to a certain extent, there is no reason to completely stop using them. We just need to be mindful of the way we use them. There are some small steps that you can take to ensure that you stay as safe as you can be when you're online.

1. Set up secure passwords

When you sign up to websites and create accounts online, you are usually guided to make secure passwords according to that website's requirements.

Apart from this, it is good practice to use different passwords across different websites, applications and accounts.

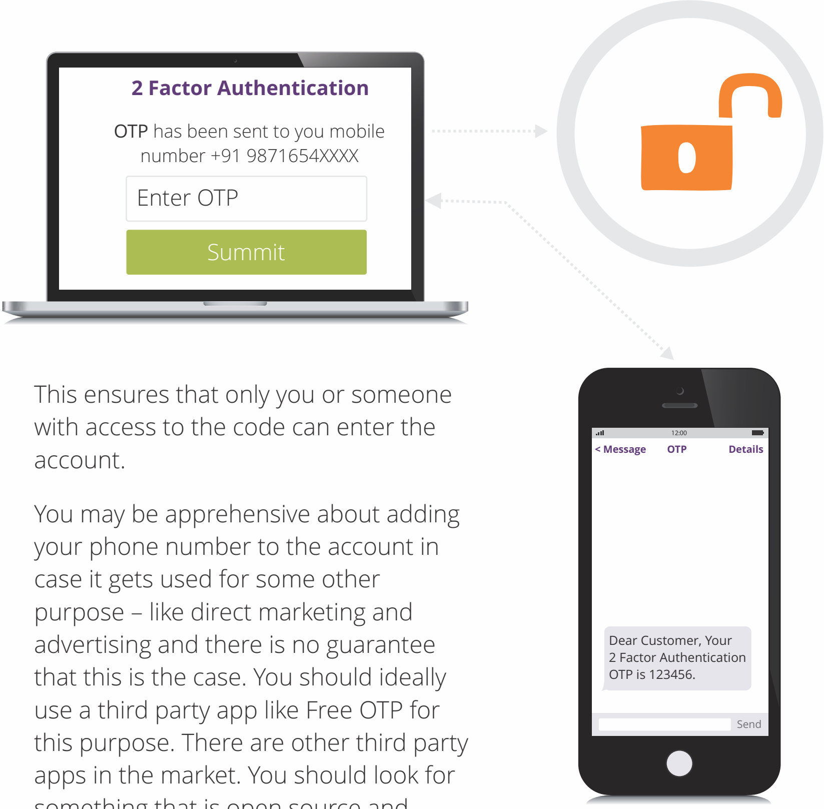
Follow the golden rule – Use a combination of numbers, upper case letters, lower case letters and special characters.

Don't store passwords as a text on your phone or email or in a notebook. These can easily come into the hands of the wrong people and compromise.

If you don't think you will be able to remember all you different passwords you can use a password manager. These can create unique and strong passwords for you and save them securely.

2. Set up 2 Factor Authentication (2FA)

Websites usually ask you to enter a password to access them. When you set up 2 factor authentication, you add your phone number as well. A unique code is sent to your phone number everytime you log in so that you can gain access to your account.



2 Factor Authentication

OTP has been sent to you mobile number +91 9871654XXXX

Enter OTP

Dear Customer, Your 2 Factor Authentication OTP is 123456.

This ensures that only you or someone with access to the code can enter the account.

You may be apprehensive about adding your phone number to the account in case it gets used for some other purpose – like direct marketing and advertising and there is no guarantee that this is the case. You should ideally use a third party app like Free OTP for this purpose. There are other third party apps in the market. You should look for something that is open source and transparent when making your choice.

3. Turn off location services

Turning on location tracking on social media sites is very convenient – you can immediately get recommendations for cafes and restaurants nearby, shops and other activities. But letting an app track your every move has a few consequences.

For example: When you go out with your friends and post an Instagram story or a Facebook photo tagging the location, you are effectively letting all your followers know exactly where you are. This could be a nuisance if you're avoiding someone or put you in danger if you have a stalker.

From a security point of view it is advisable to turn off your location and automatic location tagging.

This is a good practise to follow not just on social media platforms but on apps like Google Maps, Uber and Ola, and e-commerce sites etc. These sites can track you, the places you go to and direct ads to you based on where you are and the places you go to. When you are done using an app, make sure to quit and close the app. Some apps have been known to track your location while it is running in the background.

4. Last seen/ last read messages

Social media platforms like Facebook, WhatsApp and Instagram let users see when their contacts were last online, or if the messages they have been sent have been read. Again, this is down to personal choice but for many this can be a nuisance and cause some uncomfortable situations. Things could easily escalate if you have a stalker or an abuser.

5. Posting content online

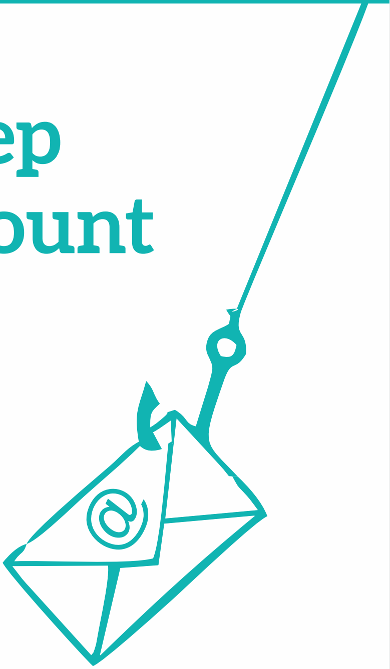
When you post content online, you should remember that your actions affect the people in your post and the people on your friend list or followers. Just as in real life, follow the adage: Do unto others as you would have them do unto you.

So if you're posting content online, ask yourself: Is it true? Is it inflammatory? Will it embarrass or anger those who are in the post? Is it appropriate to make the content public?

If people in the post object, be sure to take the post down.

Take care not to spread "fake news", fake videos, hoaxes and scams. In this age of misinformation, fake news, cyber bullying and online mobs, it is our collective responsibility to use platforms mindfully and maintain good faith online as we try to do in our offline lives.

How can I keep my Email account secure?



1. Password and 2FA

Setting up a strong password and 2factor authentication to access your email account is the first step to keeping a secure account.

2. Phishing and social engineering schemes

You may have come across phishing and social engineering scams yourself.

Phishing

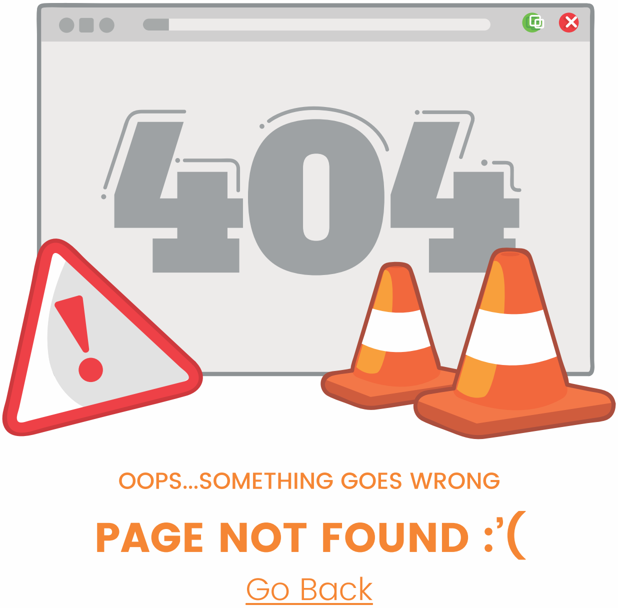
Have you ever gotten an unsolicited email from someone you may or may not know, telling you some sad story about how they have been robbed and need money, or sick and need money, or in some desperate situation where they need you to send them money immediately. This is a scam set up by fraudsters to make you send money into their accounts. Millions of users around the world have fallen victim to this scam.

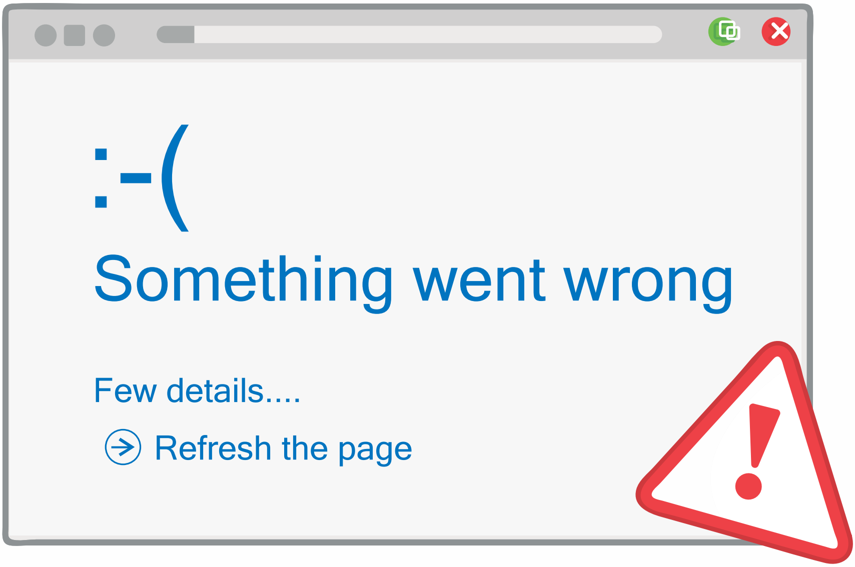
If you receive an email like this – check the sender. If it's not anybody you know – ignore it. If the sender is somebody you do know, call them or contact them through a different medium to make sure that it really is them.

Other phishing scams are designed as emails with links on them – it could be to a different website, a form or anything. Do not click on these links. Clicking could lead to a virus or malware being installed in your system or sending the same email to everyone on your contact list thus opening them up to vulnerabilities.

Social engineering

Social engineering is the act of manipulating people into making them give up sensitive, confidential information. One way that hackers, hoaxers and criminals do this is by sending emails that seem like it is from a trusted source. Like a bank, a healthcare provider or an e-commerce website that you visit frequently. The email will state some problem and ask you to sign in using the given link. The link then takes you to a legitimate looking sign in page, where you might be asked to divulge your email password, bank account details, or atm/bank card pin.





:-(

Something went wrong

Few details....

Refresh the page

You should always check the web address of the website before you enter passwords and sensitive information. For eg: www.thewire.in is a secure website, however www.thewire.in.co is not.

Always open the webpage on your browser to fill in passwords and not through a direct link. This will let you know if the webpage is genuine or not. Only when you reset your password should you follow links and re-enter passwords.

Take the necessary precautions to protect your account and information. As regular users of email and social media you will quickly learn to discern the genuine from hoaxes but you should always exercise caution.

What can I do to browse the internet safely?

Whatever web browser you may be using, there are a few things you should to make sure that your personal information is protected and you are safe online.

1. Use an ad blocker

Whether you're using Google Chrome or Firefox, you should use an ad blocker. This way you won't have to see pesky ads on the pages you visit. Ads online have a way of following from one website to the other. You may have noticed that when you click on an ad on Facebook or Instagram, you start seeing those on ads on other pages you visit all around the web. When you install an ad blocker, it disallows advertisers and third parties from tracking your activity and the pages you visit. We recommend using an extension like Privacy Badger—it's free, protects your privacy and ensures that you stay secure online.

2. Do not auto save passwords

Auto saving passwords means that anyone with access to that system will be able to log in to your accounts. This is especially dangerous if your device gets stolen or you are using a public computer.

3. Do not auto fill forms

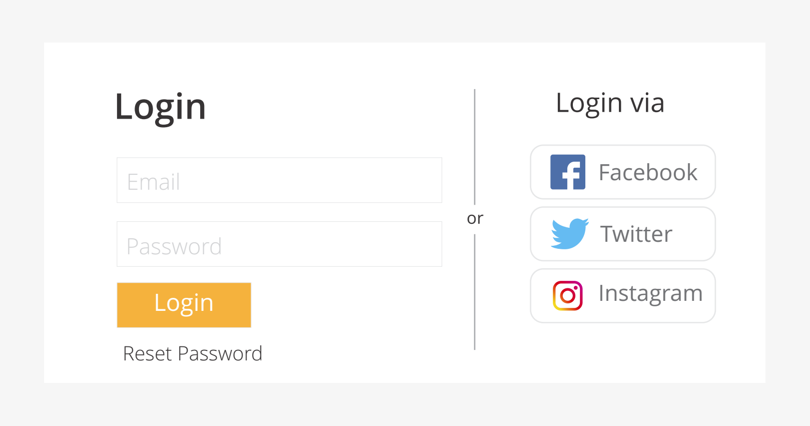
Auto fill forms also contain sensitive personal information like your address, DOB or financial information that you should not save on your browser. In addition to strangers and hoaxers getting hold of this information, some third party trackers and service providers have been known to use this information to track users and use the information maliciously.

4. Clear cache regularly

It's good practice to clear your cache regularly. This way cookies that track your behaviour are deleted and will not have a very long history of your usage patterns. Of course cookies once deleted can be reinstalled, so it is not a fool proof step. But it is good practice to regularly delete cookies.

5. Avoid social log in

Some websites require that you sign up or become a member in order to access it. Most websites nowadays allow you to sign up using your social media account and credentials but you should avoid doing this. When you use social log in, the website has access to your social media data and can track your behaviour while you're on it and target ads to you depending on your actions there.



6. Use a VPN

For enhanced security you should use a Virtual Private Network. This prevents ISPs and third parties from tracking your browsing history and routes. However, a number of commercial VPNs in the market now collect user data and use it for advertising purposes. You should research your options well before you start using one.

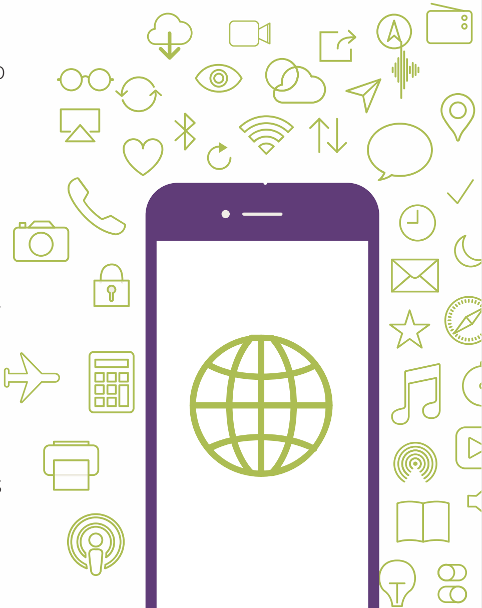
I use a lot of applications. What's wrong with that and what can I do to make it safer?

Every service, from shopping to entertainment to health advice is available on some app or the other now. This surely makes everything easy. Playlists are curated according to your preference, books and clothes displayed based on your previous purchases or browsing history. You do need to be careful about certain things when using these apps.

1. Collecting, storing, and sharing information

Apps collect a huge amount of information like the details you have to enter, financial information so you can buy things and your behaviour on the app to offer you good service. Terms and conditions are lengthy and complicated and most times users don't have an option but to accept the app's terms to continue using the app. Many times apps don't inform users the full list of data they collect.

Usually when you download an app from Google Store or App Store, you can the list of apps that the app needs access to. Most commonly these are:



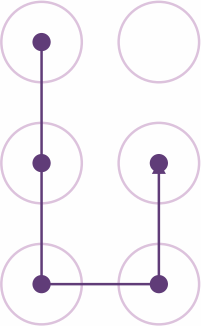
Contact list, camera and photo gallery, microphone, location. You should turn off location services from your phone and only allow apps to use it when you specify it. You can change these setting on your phone by going to Settings > Location > Disable locations service.

2. Check security, privacy and other settings on your apps regularly.

Apps and websites keep updating their products to give users better features and service. You should regularly check your apps to make sure your privacy and security settings are up to date. Facebook is good about this with users receiving prompts when a new feature is introduced.

How do I keep my device secure?

We've talked about browsing the web and using social media securely. Now let's talk about keeping your devices secure



1. Always use a pin lock or password

Set a number pin or pattern lock on your phone to prevent other people from accessing your devices without your permission. This is especially helpful if you're phone gets stolen.

On iOS devices, this acts as a layer of encryption. Meaning that people will not be able to access the content of your device, or read your messages.

2. Install an anti-virus and disk cleaner

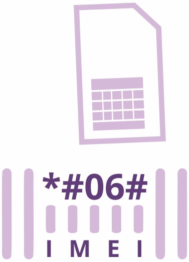
Install an anti-virus like Norton or McAfee to keep your laptops and tablets safe from viruses and malware.

You should also install a disk cleaner like C cleaner and periodically remove unwanted files from your computer.

3. Encrypt your devices

Encrypt your devices so that the data on them remains secure. iOS and Android phones are encrypted so long as you enable it and use a pin. The data on your phone remains encrypted so long the attacker does not have access to the pin and the data remains switched off. However, data stored on the cloud is vulnerable to hacking and attacks.

4. I've lost my phone what do I do now?



Dial *#06# to recover the unique IMIE number. This number can be used by law enforcement to track the phone now.

Unfortunately if you have lost your phone there is little you can do to protect data on it. The pin lock on most Android phones can be overwritten giving access to the person who has your device.

However, you can remotely backup your data to the cloud so you don't lose precious photos and such forever. You can also wipe your phone clean so that your sensitive data remains secure.

What can I do to make sure my messages or calls stay private?

You should use communication apps with end-to-end encryption.

1. Secure messaging apps

Messaging apps like WhatsApp, Signal and Wire have end-to-end encryption. This means that messages you send remain between you and the person/people you sent it to. Law enforcement authorities, hackers or platform owners cannot access the messages. For enhanced privacy you should use an app like Signal since it is open source and one can always check the security of the code.

2. Use VoIP for calling

Again using an app like WhatsApp, Signal, Jitsi for calling can help keep your conversations secure and ensure that nobody is listening to your conversations or recording them.

Help! I'm being stalked/bullied/abused on social media. What can I do?

Online abuse

There are a bunch of things you can do if you are being stalked or abused on social media. The action you want to take depends on you and the severity of the situation. Based on that, here are a few things you should do.

1. Report abuse

The first step you should take is to report the account that is threatening you. Most social media sites and apps have a mechanism by which you can report a person for not following “community guideline”. The person's account based on the severity of the abuse will be removed for a while or permanently if they have previous complaints against them.

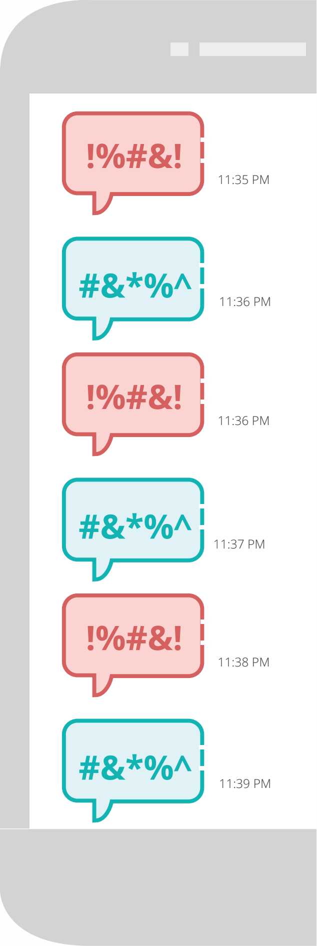
2. Block the user on social media and your phone

Block the user on the platform so that they cannot contact you.

3. Tell someone you trust

Share your story with somebody you trust. It could be a close friend, a parent or siblings or anyone really. Having a good support system will help you deal with the mental agony you may be facing. If you can't talk about it with anyone you know, you could call some of the helplines listed below

- Women's Helpline: **1091**
- National Commission for Women (NCW): **011-23219750**
- Anti Stalking/Obscene calls: **1096**
- Arambh: **arambhindia.org**
- Women's Helpline in Mumbai: **1298**



4. Keep proof of abuse

You may want to legal action against the perpetrators. If you decide to you will need substantial proof of wrongdoing.

Take screenshots: This will help you demonstrate the abuse you faced to authorities

Keep a diary: You will need to remember little details if you are planning to pursue a case

Record voice calls: If your abuser is calling you, record voice calls. In India, in most cases, the law will accept recordings of voice calls as proof of wrongdoing. There are apps and features on your phone that will help you do this.

5. Build a support system

Facing abuse can be harrowing and many times perpetrators will make you feel ashamed and as if you asked for it. It's important that you build a support system of confidantes – people you can talk to and turn to about these issues. There are a number of communities online where you can do this. It's just a matter of finding the right one for you.

KEEPING YOURSELF SAFE ONLINE

Keeping Yourself Safe Online Vol 1 has been compiled keeping in mind the security and safety needs of secondary school and college students. This kit contains basic online safety measures that should be adopted by everyone to have a safe and secure online experience.

DEF
DIGITAL EMPOWERMENT foundation

WAAT
WOMAN
ACT AGAINST
TROLLS

WEBAWARE
AN ONLINE SAFETY INITIATIVE BY OLX INDIA