



UP POLICE WOMEN POWER LINE 1090



FICCI SMART POLICING AWARDS 2019
TO WOMEN POWER LINE



HANDBOOK ON PREVENTING & DEALING WITH **CYBER BULLYING OF GIRLS**



OUR PARTNERS



unicef



Cyber Peace
Foundation



Google™



TECHNOSYS SERVICES

PREFACE



Anju Gupta, IPS

Additional Director General of Police
WPL 1090 Lucknow

The Internet has become a vital resource for everyday use by a large population of India. The online resources have created faster, reliable and multiple channels for people to connect, chat, share ideas, learn new things as well as seek and provide services. It has brought the world together as a global community that can freely share information directly and indirectly. A lot of personal information about people gets posted online through a variety of activities in cyberspace every day.

The rise of Internet has also given rise to significant concerns about safe use of cyberspace. These concerns include online frauds, impersonation, cyber bullying, defamation and data theft. However, cyberbullying of women is emerging as a real serious challenge for female users of the Internet.

The UP Police has set up a 24@7 Contact Centre (CC) in Lucknow, called the Women Power Line (WPL) 1090. The CC receives a large number of complaints of harassment and other crimes from women from across the State. The complaints include a large number of complaints of cyberbullying, most of which pertain to misuse of social networking platforms.

The CC has set up a Cyber Forensic Unit that is well equipped to redress such complaints to the satisfaction of victims. Keeping in view ever growing technological advancements, we are in process of augmenting our capacity and capability, especially in the field of open source intelligence and analysis.

In addition, we have been conducting awareness campaign for girl students across few districts of UP. UNICEF and Google India have supported our initiative and the Cyber Peace Foundation provided us trainers. A lot of material, jointly developed by WPL1090 team and CPF team for the awareness campaign, has formed the basis of this handbook. We have trained over 30,000 girls so far.

In the months ahead, we will be conducting more workshops for girls as well police personnel to help them understand basics of cyberbullying. We will be distributing copies of this handbook and would also upload it on our website to make it available to countless users. We hope these efforts of WPL1090 will go a long way to make Internet safer for women.

We deeply appreciate valuable contribution of 1090 Team, especially Dy.S.P Monika Yadav, Inspector Soni Sachan and Satyavir Sachan.



CONTENTS

Women Power Line 1090 : An Introduction

1. Decoding Cyberbullying

- 1.1 Bullying
- 1.2 Cyberbullying
- 1.3 Vulnerabilities in Cyberspace
- 1.4 WPL1090 Data : Quantum, Typology and Other Analysis of Cyberbullying

2. Identifying Cyber Bullying and Perpetrators

- 2.1 Practical Examples of Cyberbullying
- 2.2 Is Cyberbullying punishable in India?
- 2.3 Can perpetrator be traced, tracked and caught ?

3. Dealing with Cyberbullying

- 3.1 Approaching Law Enforcement
 - a. Registering a formal complaint with local Police station
 - b. Registering a formal complaint with UP Police Women Power Line 1090
- 3.2 Reporting to Platforms
- 3.3 Supporting authorities catch cyber bullies
- 3.4 Getting Content Removed

4. Online Safety and Prevention

- 4.1 The three pillars of online safety
- 4.2 Minimize Risk by Adopting Responsible Cyber Social Behaviour

Cyber Security Tips



WOMEN POWER LINE 1090

The WPL1090 can be reached primarily over phone (1090), Twitter (@wpl1090) and Email (1090police@gmail.com). The complaints are also received from other helplines integrated with WPL1090 such as UP112, UP GRP and 181 through APPs developed by WPL1090. The API integration of WPL1090 and UP112 is in the pipeline.

The Service Delivery Mechanism

The WPL1090 is manned by female and male police officers and a small contingent of outsourced women staff. Referred to as operators, they are trained at the Centre to fully appreciate the delivery mechanism to provide relief and justice to girls in distress.

The service delivery mechanism has been designed to address the core concerns of girls, including reporting matters about harassment, accessing justice from Police, maintaining anonymity and getting full redressal. The key elements of the service delivery mechanism are as follows:

- Every complaint is received only by a female operator.
- A complaint can be lodged only by a victim or any other female on her behalf with her consent. The operator directly contacts the victim to confirm a complaint, unless it is a report about a matter requiring emergency response from police and victim cannot be contacted. In that case, the operator reports it to UP 112 and advises the complainant too.
- A registration number is automatically generated and sent to the mobile of the victim as an SMS. A victim can call up the Centre again with this number as a reference number.
- The identity of a victim is never disclosed unless she wants active police intervention on the ground by UP112 or by police stations across UP.
- A victim is never called to any Police Station or to the Centre unless she lodges a police case.
- The WPL 1090 remains in touch with a victim till the final resolution of her complaint. This usually entails making few feedback calls to the victim up to a month and sometime even beyond.

Resolution Mechanism

The 1090 Centre has been built its capacity and capability to fully resolve complaints pertaining to bullying over phone and in cyberspace. Apart from sophisticated

technological cloud based platform, which enables processing of huge number of complaints until the final resolution, a dedicated Cyber Forensic Cell at the Centre has been well equipped to handle all forensic aspects pertaining to cyberbullying through social media and other online platforms.

Any complaint that requires emergency services of UP Police is sent to UP-112 on real time basis and the complainant is advised about the same. Similar procedure is adopted with regard to complaints pertaining to the UP GRP. The complaints about stalking and crimes are forwarded to police stations and district control rooms on a real time basis. In addition to phone calls and messages, in 2018, the WPL1090 has also got developed a dedicated APP (1090APP) which links the WPL e-platform with all the police stations (PSs), district control rooms (DCRs) and senior police officers across 75 districts of UP. The 1090APP provides an online, real time mechanism to forward complaints to multiple levels within district police and to receive back a short Action Taken Report (ATR). At present, a majority of PSs and DCRs are electronically linked to WPL1090 platform.



1. DECODING CYBERBULLYING

1.1 BULLYING

In order to appreciate cyberbullying, let us recall our own experiences of facing or witnessing 'bullying'.

Bullying can be described as aggressive behaviour of a person who uses some kind of power (physical, information about other person, one's own influence/clout/position etc.) to control, intimidate, insult or harm others.

Bullying may manifest in verbal actions (name calling, body shaming, inappropriate sexual or other remarks, threats etc), or through physical actions (use of force, damage to things belonging to other person, rude gestures or signs etc) or through social interactions (deliberately forcing a person to leave a group, spreading rumours, saying or doing something to embarrass any person etc). We all can definitely recall such moments.

Many of the acts of bullying are punishable as offences under the Indian laws. For example under the Indian Penal Code (IPC), stalking of a female or forcibly trying to contact a female is described as an offence under Section 354D. Another example is of criminal intimidation, which is defined as an offence under Section 506.

However, every act of bullying may not have been defined as a penal offence. For example, deliberately forcing a person to leave a group through mocking the person or saying something mean are examples of bullying, but may not attract any penal provisions of the Indian laws.

1.2 CYBERBULLYING

The bullying which takes place over the internet is called cyberbullying.

It involves use of digital devices, including computers, laptops, phones and is perpetuated through a variety of communications such as messages, mails, social media accounts etc. Broadly, it includes posting or sending or sharing harmful or misleading or unwarranted information about a person or group without any explicit consent of the person/group. Such information can be accessed from publically available sources or may be obtained through private sources through deceit or collusion or other wrong means.

Many of the acts of bullying are punishable as offences under the Indian laws. For example, abusive and mean messages can be covered under section 67 of the IT Act and section 354D of IPC. For example, abusive and mean messages can be covered under section 67 of the IT Act and section 354A of IPC.

1.3 VULNERABILITIES IN CYBERSPACE

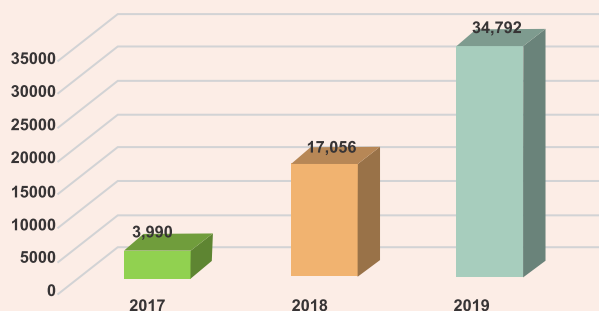
There are five inherent vulnerabilities of cyberspace which are exploited by offenders to bully innocent girls and they are:

- The anonymity of account holders in cyberspace, which, many times, cannot be readily unmasked by a victim.
- The ease of sharing content and forwarding the same, which can go viral in no time.
- It is not easy or always possible to delete content from everywhere in cyberspace. When shared over messaging applications, content may be downloaded and saved on devices and may be reused.
- An offender may use online information to perpetrate offline trouble for a user.
- Logging off and deleting profiles do not always help getting an offender to stop cyberbullying others.

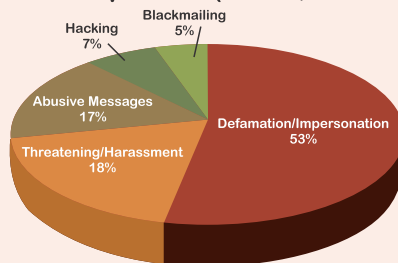
1.4 WPL1090 DATA: QUANTUM, TYPOLOGY AND OTHER ANALYSIS OF CYBERBULLYING

The WPL1090 is the lead Agency of UP Police entrusted with the responsibility of solving the complaints of cyberbullying reported by girls from across the State. The Centre has established a well equipped Cyber Forensic Unit of trained personnel who deal with such complaints to identify the perpetrator and get the content removed. Thereafter, the regular police personnel of the Centre counsel (warn) the perpetrator and take feedback from victims. The resolution rate of the Centre is over 99% for 2018 and 2019. The Graphs and Charts below indicate the trends of cyberbullying:

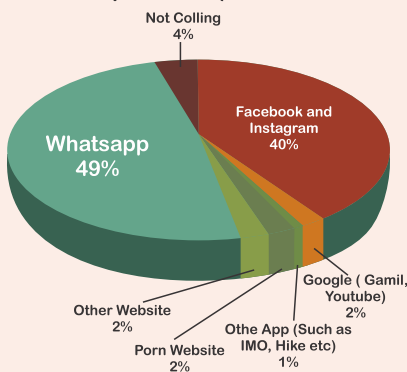
Cyber Complaints Reported to WPL1090 (2017 to 2019)



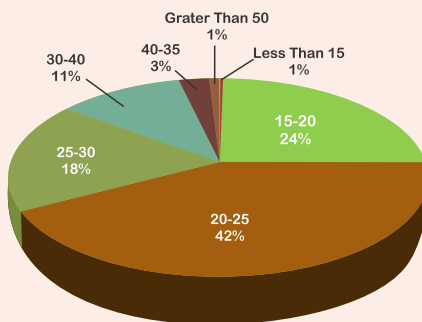
Typology of Cyber Complaints (Jan 1, 2018 to Dec 31, 2019)



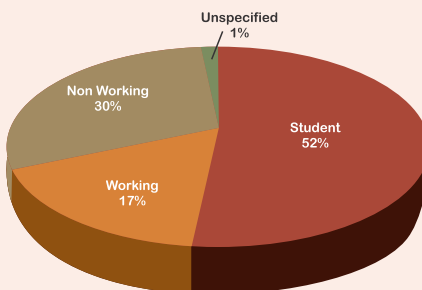
Platforms of Cyber Complaints (Jan 1, 2018 to Dec 31, 2019)



Age Profile of Victims of Cyber Complaints (Jan 1, 2018 to Dec 31, 2019)



Work Profile of Victims of Cyber Complaints (Jan 1, 2018 to Dec 31, 2019)



2. IDENTIFYING CYBER BULLYING AND PERPETRATORS

The analysis of complaints reported to WPL1090 between 2017 and 2019 clearly suggests the modus operandi used by offenders involves one or more of the following ways:

- Hacking of ID (Facebook/Instagram/Email/WhatsApp etc.)
- Faking/impersonating of ID (Facebook/Instagram/Email/WhatsApp etc.)
- Tagging someone in objectionable messages/post/images on Facebook/Instagram/Twitter.
- Threatening/abusive/objectionable messages/emails/photos/video links.
- Blackmailing with personal information.
- Posting personal phone numbers with objectionable messages in public and private forums.
- Forcefully making someone a member of whatsapp/FB groups and embarrassing her.
- Posting objectionable videos about a girl on you tube, tik tok, vigo live, hike, share chat, aloo, badoo or other such platforms.
- Net calling (few digit numbers or proxy numbers).
- WhatsApp calls or messages from proxy numbers.



2.1 PRACTICAL EXAMPLES OF CYBERBULLYING

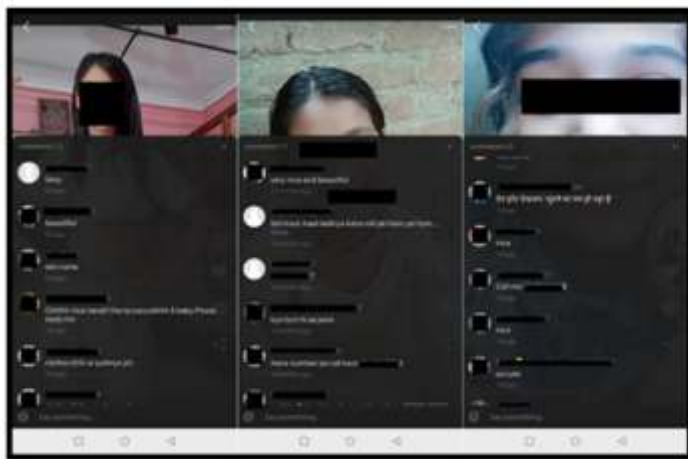
Some practical examples of cyberbullying are discussed below to help identify such phenomenon quickly.

Creating fake/impersonated profiles : Creating profiles using a girl's name and photo without her permission. Here, a Facebook account was created using the name and photos of a girl without her permission.



Obscene Comments on Live Streaming Applications : Bullying with mean, objectionable or lewd comments.

In the picture shown, a girl shared her videos on a live streaming application and which attracted many obscene and vulgar comments.



Blackmailing to Leak Private Information and Pictures : Threatening to disclose private and personal information and images. These screenshots are from a real conversation, where a man threatened to leak the photos of a girl if she did not do what he asked her to do.



Sending Lewd Messages : Sending dirty, indecent, filthy messages on WhatsApp or any social media or messaging platform.

Any message which appears dirty or indecent is a form of cyber bullying. An example is shown here:

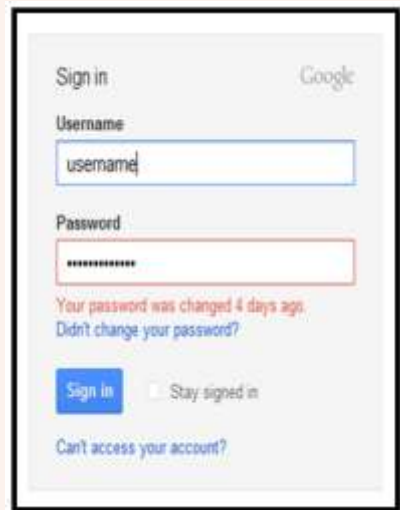


Sharing Someone's Private Information : Sharing personal information online without consent. As shown in the image, a group photo of girls was shared without their knowledge and by people unknown to them. They also made vulgar comments on the photos.



Hacking Profiles: When somebody tries to gain unauthorized access to a girl's account.

In the image, when a girl tried to log into her Gmail account, it said "your password changed 4 days ago". This meant that someone had, through hacking, changed her password and got access to her account.



Harassing Audio and Video calls through apps like WhatsApp:

If someone is making video and/or voice calls from an unknown number and trying to harass a girl.



2.2 IS CYBERBULLYING PUNISHABLE IN INDIA?

There is no generic definition of Cyberbullying in Indian laws. However, many activities involving a case of Cyberbullying are punishable under the Indian Penal Code (IPC), Information and Technology (IT) Act and POCSO Act (in case of minors). Some such activities and penal provisions are enumerated in the Table below:

Offence (Activities)	Provisions of the Law
Creating Fake/Impersonated Profiles/Identity Theft	Sections 66C, 66D IT Act and Section 419 IPC
Hacking profiles	Section 66 IT Act
Abusive and Obscene Messages, Comments and Other Content	Sections 354A, 354D, 499, 500 and 509 IPC, Sections 67, 67A IT Act, Section 11 POCSO Act
Blackmailing/Threatening	Sections 383, 503, 506 IPC
Posting, Sharing, Clicking images of private parts	Section 66E IT Act, Section 354C IPC
Repeatedly trying to contact despite clear denial	Section 354D IPC, Section 11 POCSO Act

2.3 CAN PERPETRATOR BE TRACED, TRACKED AND CAUGHT?

Yes they can be traced, tracked and caught by law enforcement agencies (police) even if it appears difficult to you. There are techniques, tools and tradecrafts which are used by law enforcement to do it.

Following is a brief list of instances that may have made you feel that tracing, tracking and catching an offender is not possible. But, in fact, it is possible in each of these cases (and many other) to identify, locate and catch an offender:

- a. Objectionable messages which come from anonymous email IDs
- b. Messages/calls from international numbers (phone or internet calls)
- c. Fake/Impersonated Profiles
- d. Social Media Profile/Email ID getting hacked
- e. Threatening messages and calls from someone who lives far away
- f. Photos/videos uploaded or shared without her permission.

In pursuit of helping victims, the law enforcement also works with various social media companies like Google, Facebook, WhatsApp, Twitter, Instagram, YouTube, etc. and with different mobile service providers such as Airtel, Vodafone, Idea, Jio, BSNL etc. In some cases, it may take a little longer to trace an offender, but with persistent efforts, they all can be traced, tracked and located.



3. DEALING WITH CYBERBULLYING

The complaints of cyberbullying can be reported to law enforcement and also to the platforms. In UP, apart from district police, WPL 1090 is a specialized agency which deals with complaints of cyberbullying in which victims don't wish to be identified publically and don't wish to report to platforms. You have to decide what works best for you.

3.1 APPROACHING LAW ENFORCEMENT

a. Registering a formal complaint with local Police Station

As a first step, it is useful to discuss it with someone more experienced in the family or school/college before you decide to approach local police station with a formal complaint. You have a right to register an FIR and police has a duty to help you do that and give you a copy of it. You need to carry screenshots or some electronic evidence to support the FIR and cooperate in the investigation by police.

Steps:-

- You need to visit your local Police Station and register an FIR.
- Co-operate with the investigation.
- Wait for the identification and legal action against the offender.
- Give your testimony in court, whenever the case comes up for trial.

b. Registering a formal complaint with UP Police Women Power Line 1090

Steps:-

- Call 1090
- The operator will register complaint and you will get automatic reference number
- The operator will put you in touch with a female operator of Cyber Forensic Unit, who would take your screenshots on a separate whatsapp number
- The 1090 team will get the content removed and identify the offender as soon as possible
- The offender will be warned.
- The operators will make feedback calls to the victims till she is satisfied.

3.2 REPORTING TO PLATFORMS

If you do not wish to approach the law enforcement, but only want to prevent an offender from contacting you and/or want to report him to the platform and/or remove the undesirable content, you can use the REPORT feature made available on most social media and content sharing platforms.

Doing this is very simple, as explained below:

Step 1: Look out for three dots at the corner of the post/comment/ video/account that you wish to Report. Once you locate this, click on it.

Step 2: You will find the Report feature here.

Step 3: When you click on the Report, you will be presented with a list of reasons including harassment/spam/obscenity, etc.

Step 4: Go through the reasons and choose the one that addresses your concern the best.

Once you have reported the objectionable content or account, the platform will show you a message acknowledging your Report. Thereafter, the platform will take necessary action such as deleting the objectionable material or blocking/disabling accounts.

Pro tip: Reporting accounts will ensure that the bully stops troubling you and also other people he may be harassing. So don't just block bullies, report their accounts too.

What all can you Report?

- Report a user/account to the platform for objectionable behavior or any behavior that you have a problem with.
- Report specific posts/comments/other activity to the platform to review
- Unfollow/Block a user to prevent him from contacting you
- Reporting may also help delete objectionable content and accounts

How does reporting actually work?

Just like a school has rules, every social media and content sharing platform also has certain standards (rules/norms) that the users are advised to follow. When you

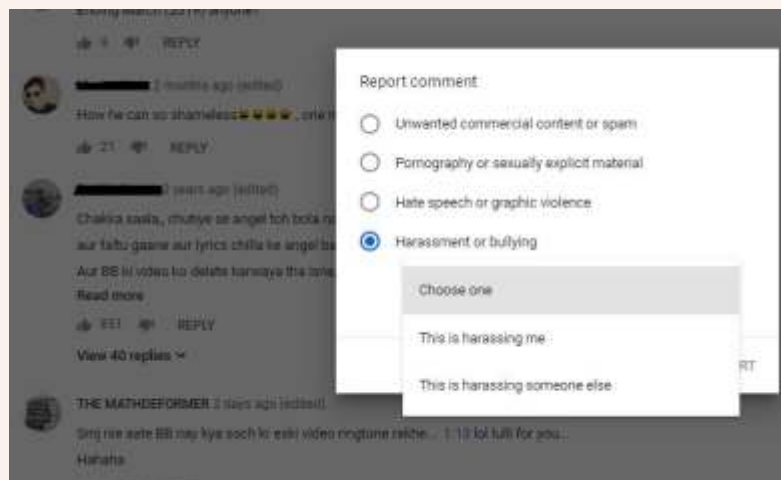
report something, the platform is notified of the same. It will then go through the reported content and delete/remove the content if it violates the standards of the platform. This is why when you report content, the platform asks you to state your reason.

REPORTING COMMENTS ON YOUTUBE:

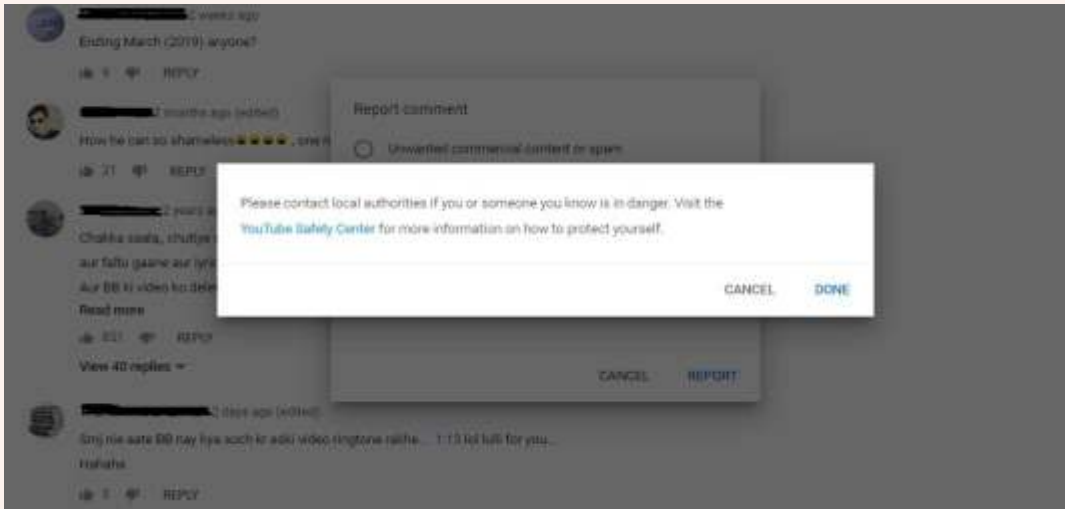
Step 1: Go to the Three dots. You will find the Report feature there.



Step 2: You will be presented with a list of reasons as to why you want to report the content.



Step 3: YouTube will show a message saying they have received your report



REPORTING POSTS ON INSTAGRAM:

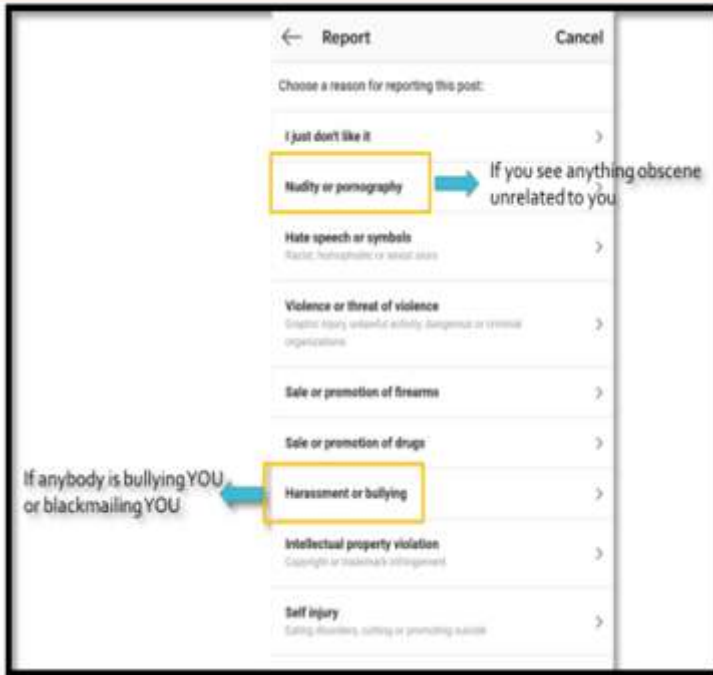
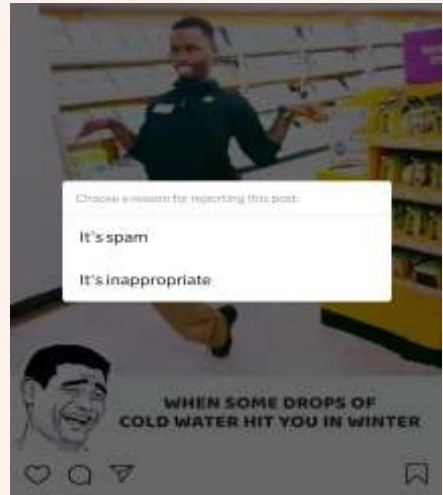
Step 1: Go to the top right corner of the post and click on the three dots.



Step 2: You will find the Report feature at the bottom of the list.

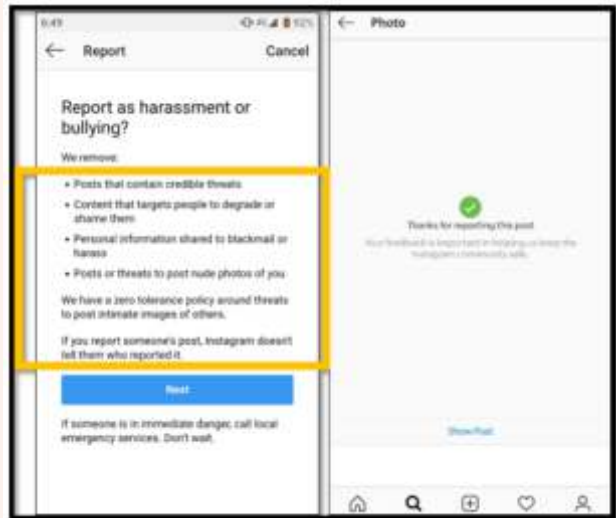


Step 3: When you click on Report, you will be given two options. Remember, that "It's spam" is generally used to report repetitive ads. For cases of cyberbullying, you can choose "It's inappropriate".



Step 4: Once you choose "It's inappropriate", you will be given a list of reasons to choose from. Choose the appropriate reason for reporting the content.

Step 5: Confirm your report by clicking on “Next” and Instagram will show you an acknowledgment message.

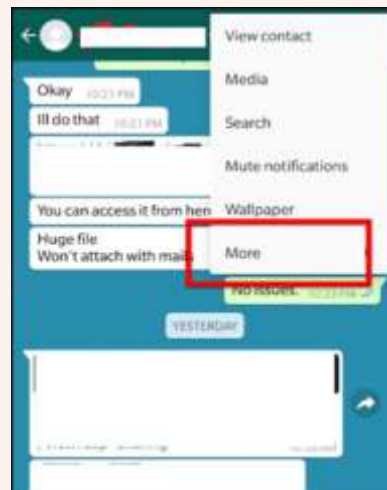


REPORTING ACCOUNTS ON WHATSAPP :

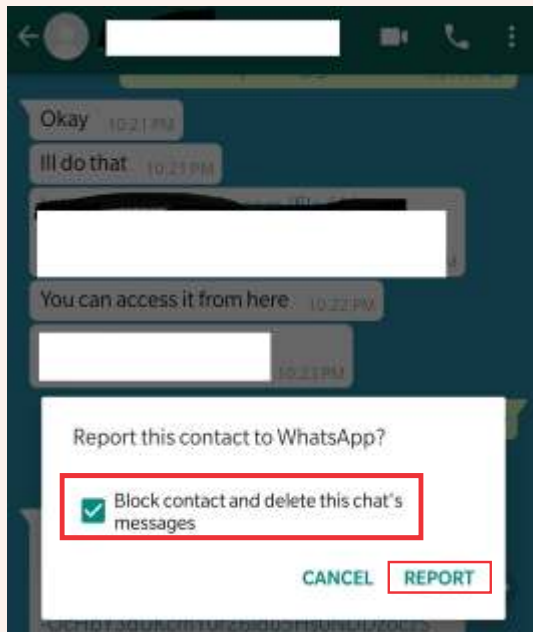
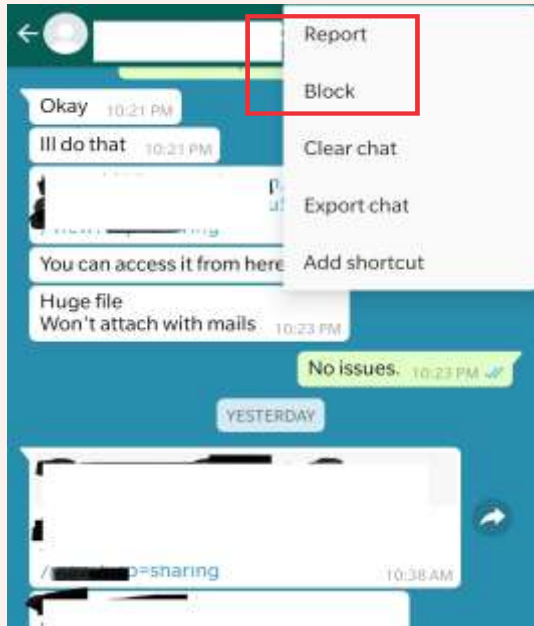
Step 1: Open the chat with the number you wish to report, and click on the three dots at the top right corner.



Step 2: Click on last option “More”.



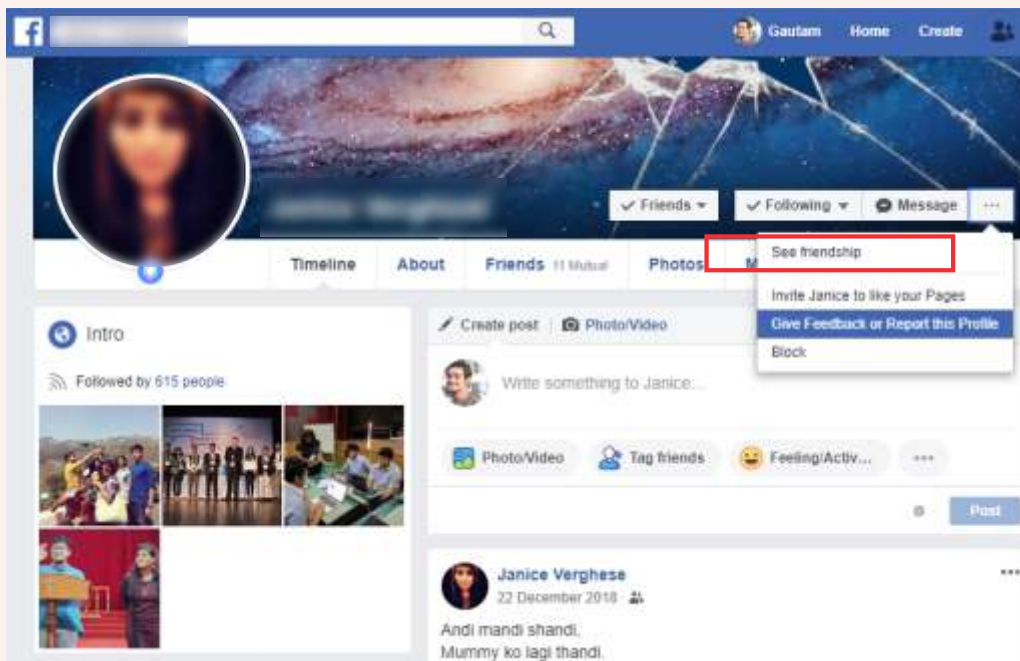
Step 3: You can find the Report and Block features.



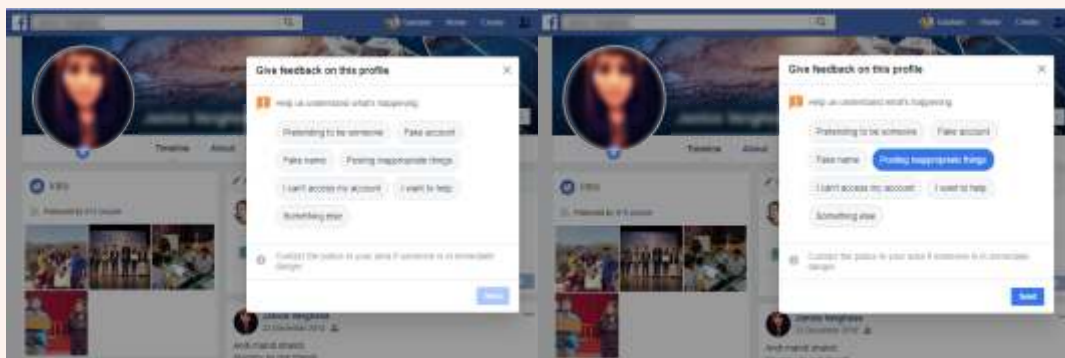
Step 4: After you click on Report, you will be given to option of blocking the contact too. Finally click on the "Report" feature at the bottom of the pop-up as in the picture.

REPORTING ACCOUNTS ON FACEBOOK:

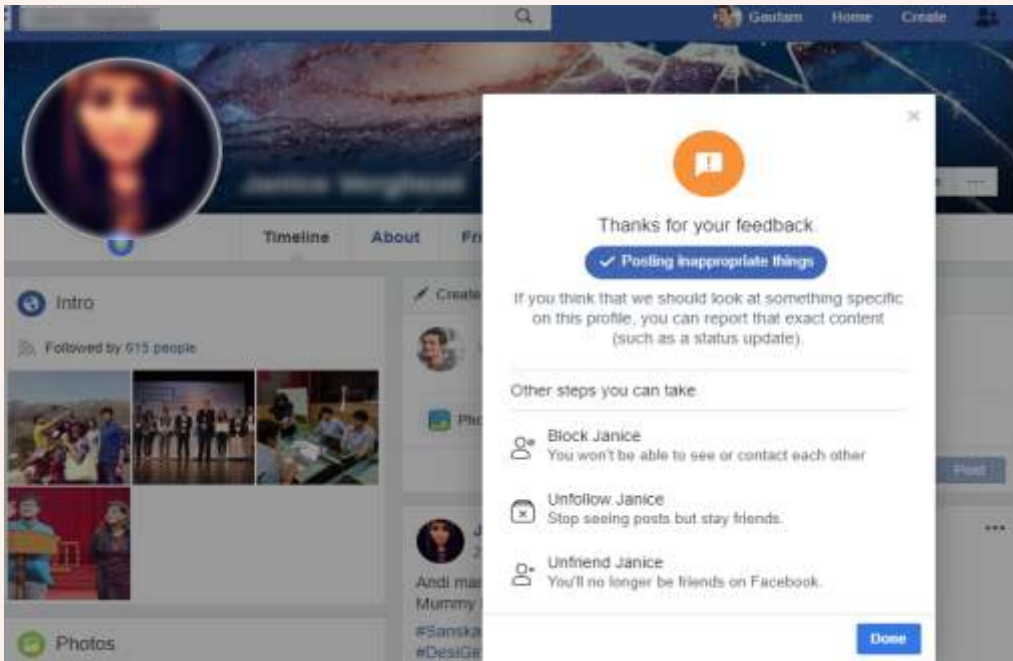
Step 1: Open the account that you wish to report and click on the three dots at the right side.



Step 2: Once you click on the option to “Report or Give Feedback” you will find a list of reasons to choose from.



Step 3: After you have selected the appropriate reason, confirm your report by clicking on “Done”.



3.3 SUPPORTING THE AUTHORITIES CATCH CYBER BULLIES

By pointing authorities in the right direction, you can make sure that the offenders are caught and action is taken against them swiftly. This is what you can do:

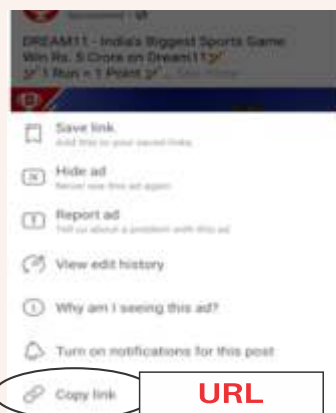
A. Saving URLS (Uniform Resource Locator is the address of a resource on the internet.)



Just like every house has an address, everything online has a web address. You can find this web address at the top of the screen on laptops or desktops as shown below:



If you are using an App, then you can click on the post and copy its URL as shown



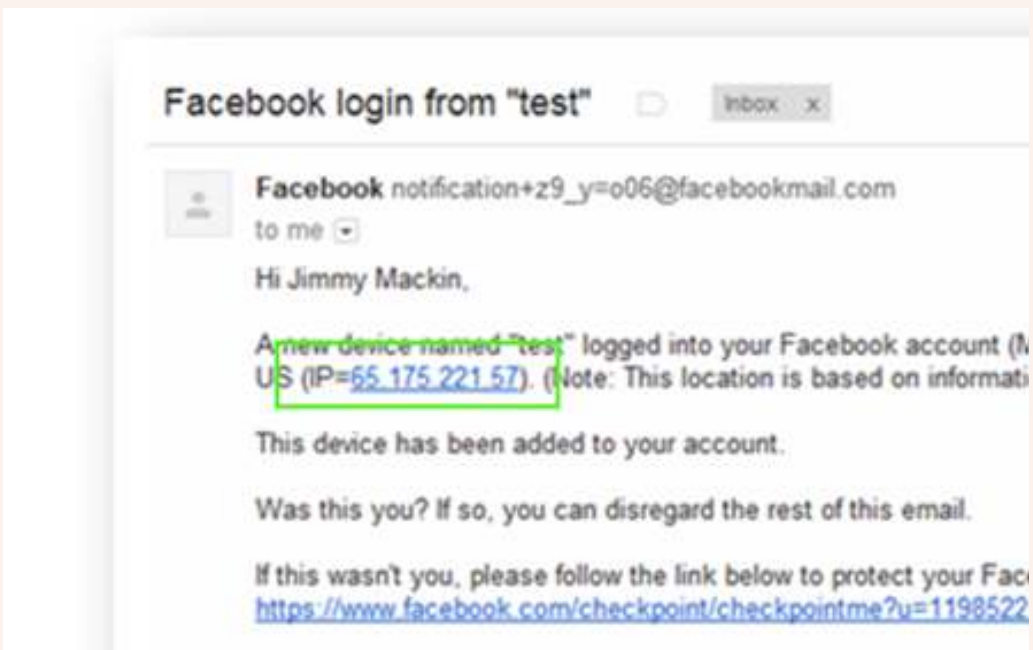
Once you have copied the URL, you can share it with the police in the form of evidence.

But how will it help?

Let's say, a user creates a fake account and troubles you. And before you can report it, he deletes the account. Using the URL, the details of the account can still be found out. This will help identify the user. Not just this, users running fake accounts can also be identified using URLs.

B. IP Addresses (IP Address is a unique string of numbers separated by full stops that identifies each computer or a unique address of computer on the Internet.)

Sometimes, when a new device or browser accesses your social media account, you may get a mail. This login alert sometimes also has an IP Address (shown below). Similar to your house address, the IP address helps identify the locations and details of a device. Save this IP address if you receive such a mail. The message may also contain information like the location and the name of the device accessing your account. Save all this information too.

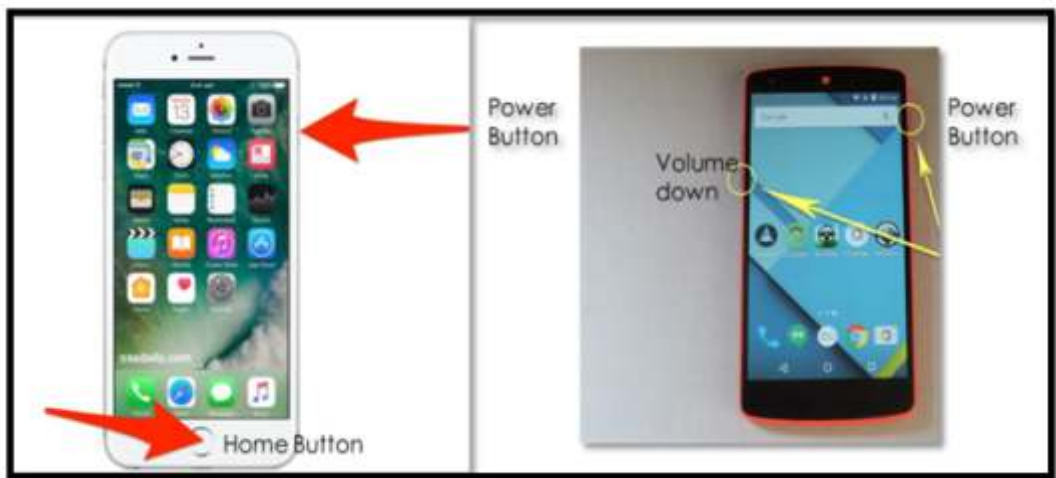


But how will it help?

If your account ever gets hacked/compromised, the IP address can help identify who gained access to your account and also when and where.

C. Taking Screenshots

Photos are the easiest form of evidence you can collect. You can take screenshots by simply pressing two buttons on your phones.



You can do this on your laptop or desktop too. Simply press the "Windows" Key and "Print Screen" Key simultaneously, to take a screenshot.



The minute someone bullies you online, take a screenshot of the photo/comment/account, save the URL and file a complaint.

Pro tip: Taking screenshots on laptops and desktops is advised because they also have the date and time at the bottom right of the screen. Phone screenshots only show the time.

After properly collecting the evidence as suggested above, one can send them to 1090 WPL team through a WhatsApp number (provided to you once you have filed your complaint with the 1090 WPL team). In case of an FIR at the local police station, one can take the information to the police station.

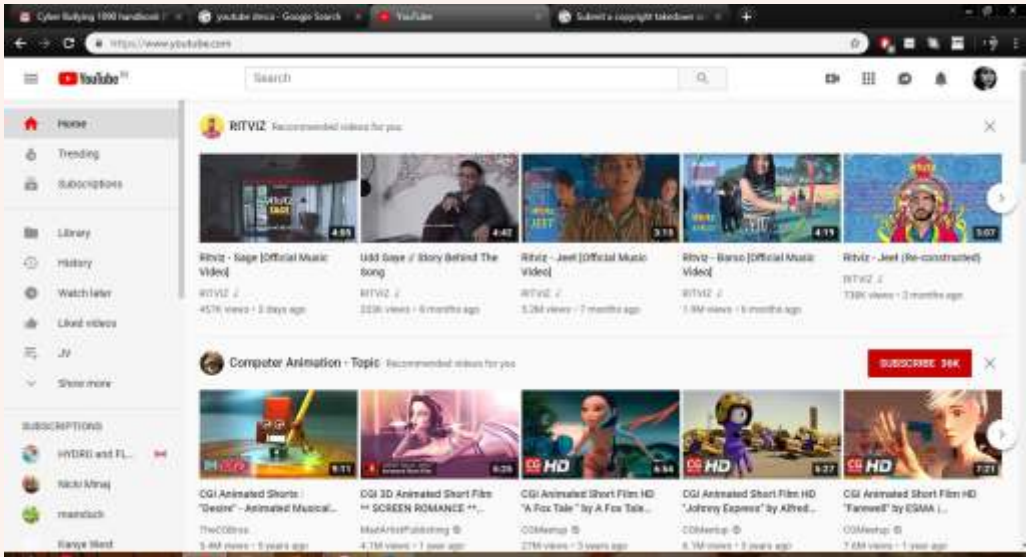
3.4 GETTING CONTENT REMOVED

If you ever find that your photos or videos are shared online without your knowledge or consent, do not worry. This is a violation of your copyright. There are laws in most countries to protect your intellectual property. India has the Copyright Act of 1957. The US has a similar law which is called the Digital Millennium Copyright Act (DMCA) 1988 of the United States. This law has a very interesting clause under which you can get your photos and videos removed from platforms, if shared without your consent. Since most social media platforms such as WhatsApp, Facebook, YouTube are American companies, they are subject to DMCA. You can get such content removed very easily by simply sending a mail or content takedown notice to the platform where they have appeared.

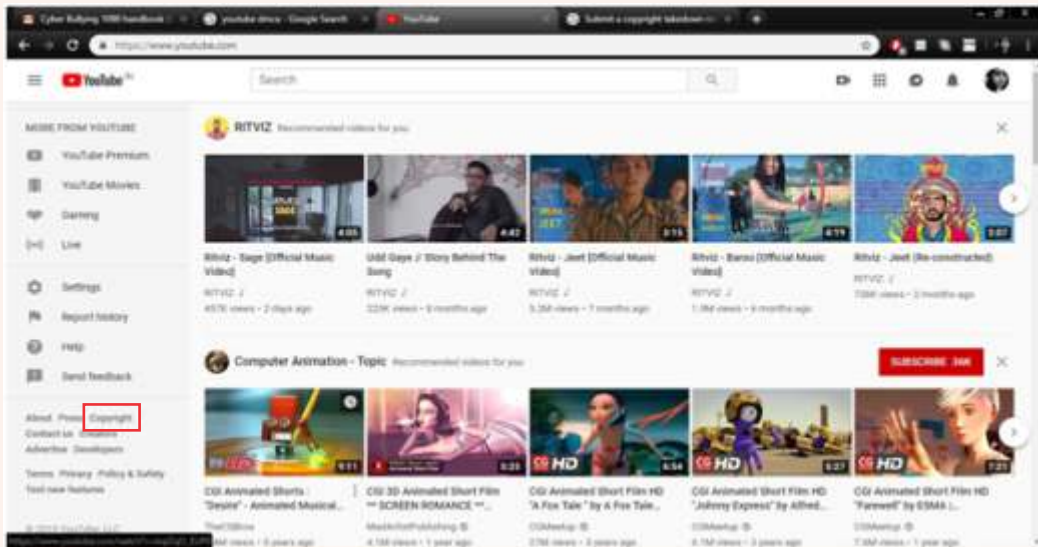
Some platforms like YouTube and Facebook provide the option to file a **copyright infringement report**, using which you can get content removed. For other platforms, you can send a **DMCA content take down notice** to get content removed.

You can go through the following steps on Youtube to understand how a **copyright infringement report** can be looked up and sent.

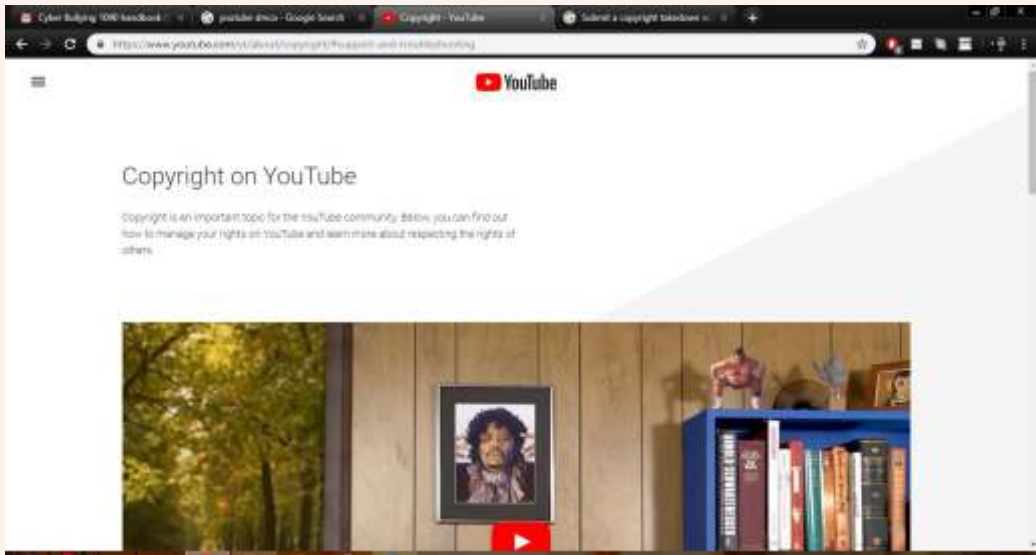
1. Open the platform.



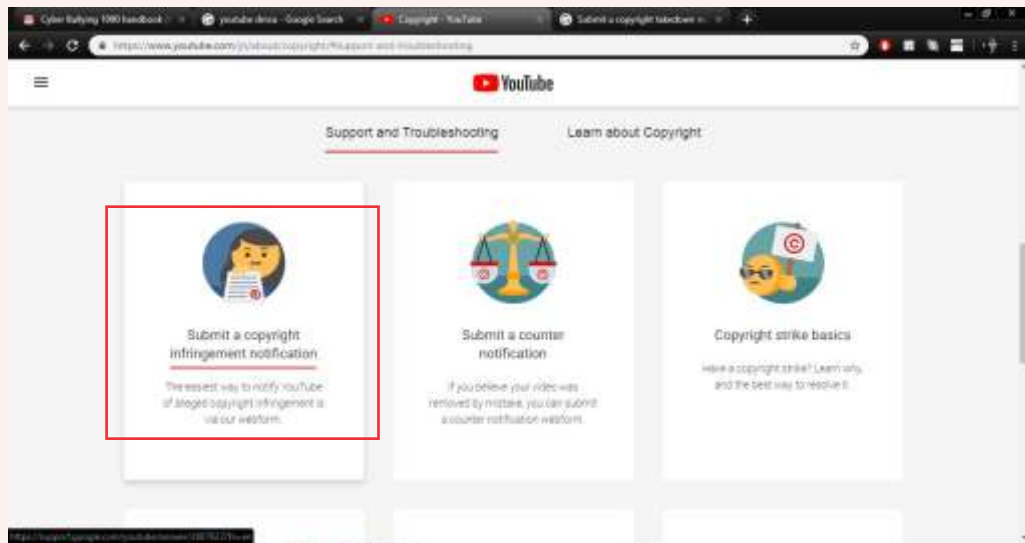
2. Go to the bottom of the webpage. Look for DMCA notice or Copyright as shown in the screenshot



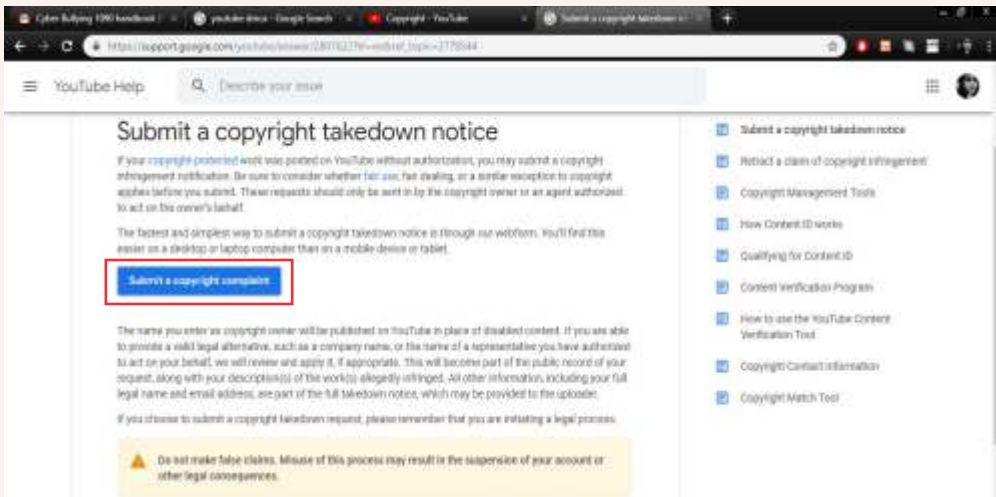
3. Click on Copyright and you will be taken to a new screen.



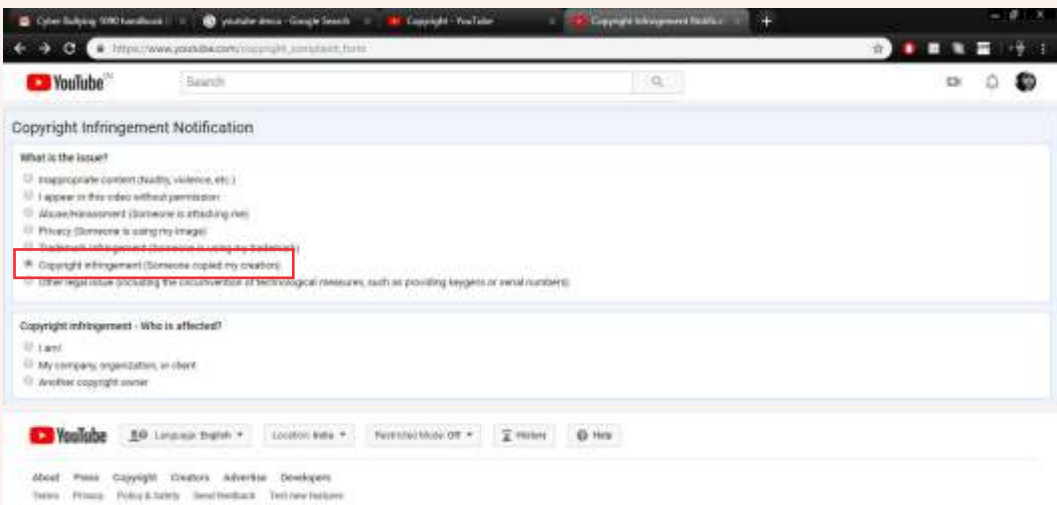
4. Scroll down and you will find the option to Submit a copyright infringement notification



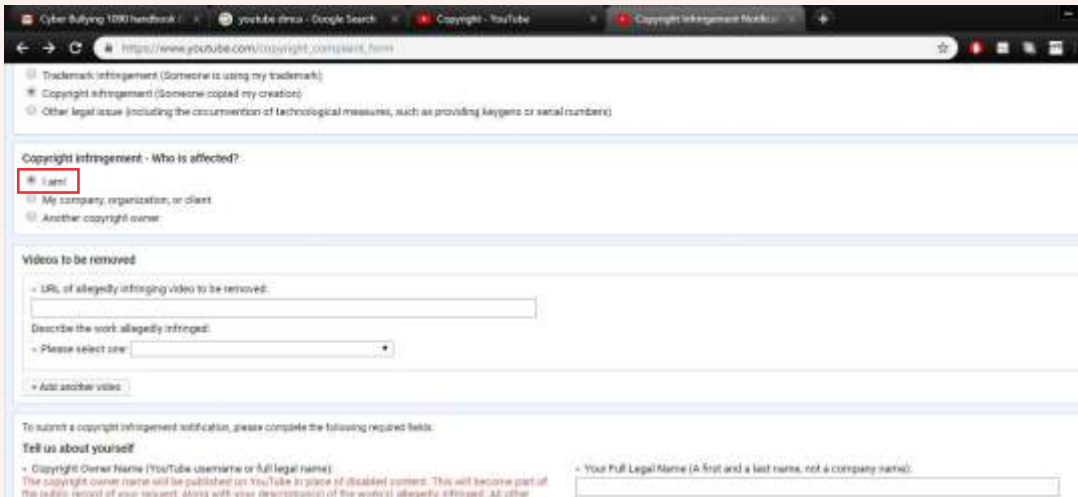
5. When you click on this, you will find the option to send the copyright infringement report.



6. Once you click this option, you will find the form. Enter your details correctly. Remember, that this is a complaint for copyright infringement, so choose this as the issue.



7. After choosing this, you will find more fields to fill regarding your issue.



The screenshot shows the 'Copyright Infringement - Who is affected?' section of the YouTube form. The 'I am:' dropdown is set to 'I am', which is highlighted with a red box. Below this, there are fields for 'Videos to be removed' and a section titled 'Tell us about yourself' with fields for 'Copyright Owner Name' and 'Your Full Legal Name'.

Copyright Infringement - Who is affected?:

- ☒ I am
- ☐ My company, organization, or client
- ☐ Another copyright owner

Videos to be removed

URL of allegedly infringing video to be removed:

Describe the work allegedly infringed:

Please select one:

+ Add another video

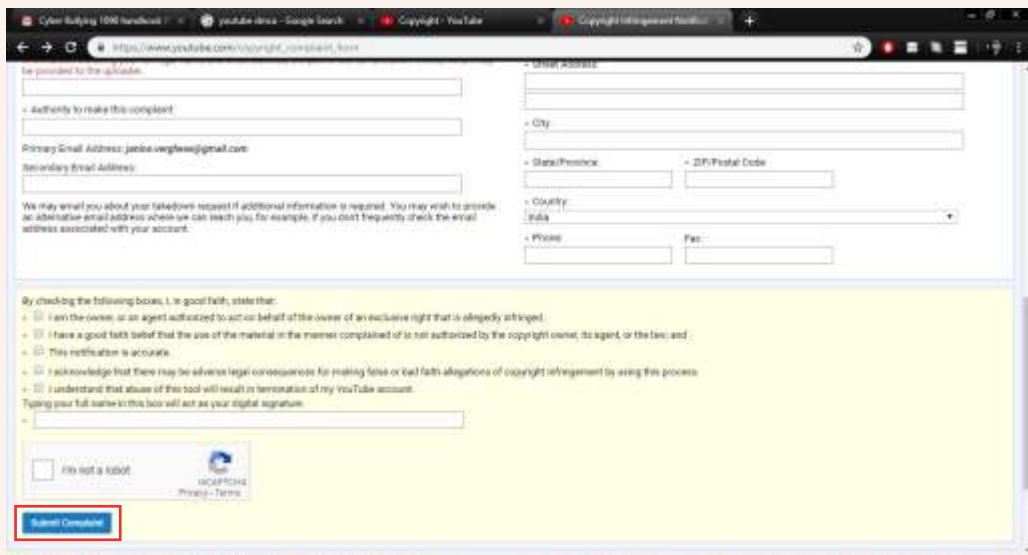
To submit a copyright infringement notification, please complete the following required fields:

Tell us about yourself

+ Copyright Owner Name (YouTube username or full legal name)

+ Your Full Legal Name (A first and a last name, not a company name):

8. After filling the details, click on Submit Complaint and appropriate action will be taken by the platform, in this case, YouTube.



The screenshot shows the 'Contact information and signature' section of the YouTube form. It includes fields for 'Email Address', 'City', 'State/Province', 'ZIP/Postal Code', 'Country', 'Phone', and 'Fax'. There is also a section for 'By checking the following boxes, I, in good faith, state that:' with several checkboxes. The 'Submit Complaint' button is highlighted with a red box.

Be prepared to the uploader:

+ Authority to make this complaint

Primary Email Address: janice.ueglew@gmail.com

Secondary Email Address:

We may email you about your takedown request if additional information is required. You may wish to provide an alternative email address where we can reach you, for example, if you don't frequently check the email address associated with your account.

+ Email Address:

+ City:

+ State/Province:

+ ZIP/Postal Code:

+ Country:

+ Phone:

+ Fax:

By checking the following boxes, I, in good faith, state that:

- ☒ I am the owner, or an agent authorized to act on behalf of the owner, of an exclusive right that is allegedly infringed.
- ☒ I have a good faith belief that the use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law; and
- ☒ This notification is accurate.
- ☒ I acknowledge that there may be adverse legal consequences for making false or bad faith allegations of copyright infringement by using this process.
- ☒ I understand that abuse of this tool will result in termination of my YouTube account.

Typing your full name in this box will act as your digital signature:

☐ I'm not a robot

RECAPTCHA

Privacy - Terms

Submit Complaint

How to send a content take down notice?

1. Look for the email address of the platform where your photo/video has been shared. You can find this in the Contact section.

2. Once you find the email address, you need to compose a mail as follows:

To: (email address of the platform).

Subject: Notice Under DMCA for Content Removal

Main body : This is a notice under the DMCA. My photo/video has been uploaded on to your platform without my consent. This is the link to the content: (copy the URL to your photo or video)

3. Attach a copy of a **government approved identity proof** such as your AADHAR card or PAN card etc and send the mail.

Within the next 72 hours the content should be removed.



4. ONLINE SAFETY AND PREVENTION

4.1 THE THREE PILLARS OF ONLINE SAFETY

To stay safe online, you need to know

- I. **Threats** you may face
- II. **Tools** available that can help keep you safe
- III. **Processes** of using these safety tools

In concrete terms, few simple things may help you such as described below :

A. Choosing Passwords

A very simple step to ensure your safety online, by taking care of your passwords. So, remember that:

- Sharing your passwords is not safe.
- Meaningless and non-guessable passwords are best.
- Different passwords should be used for different accounts.

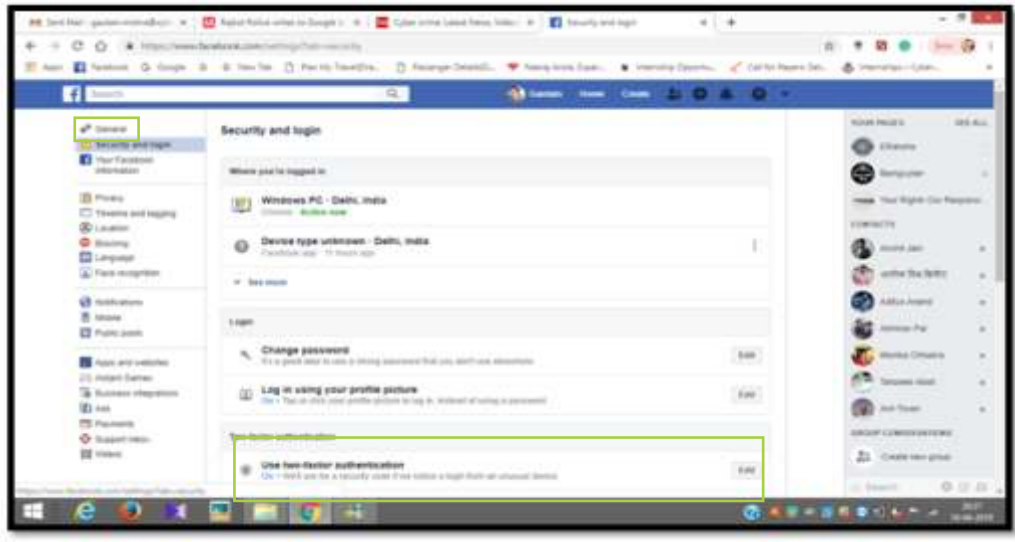
Remember, your password is the soul of your account. Your accounts are safe only as long as your passwords are. If you are finding it difficult to remember multiple passwords, you can use password managers to save your passwords. These apps use highest level of encryption and are difficult to crack into. If you have already shared your passwords with anyone, make sure you change them right away.

B. Using Two Factor Authentication (2FA) or Two Step Verification

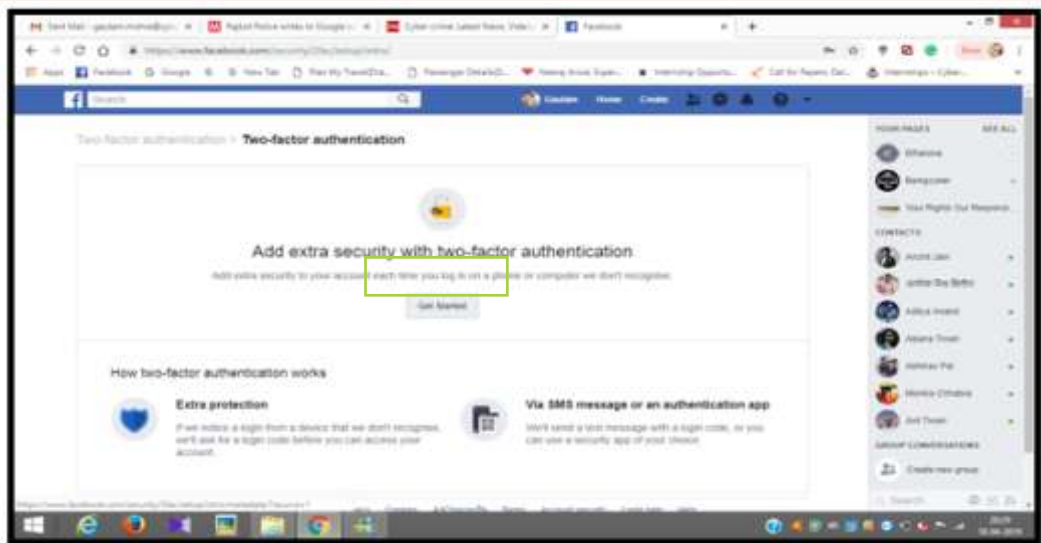
Use of this feature adds an extra layer of security to your online accounts. When you activate 2FA, you will receive an OTP on your registered mobile number. Only by using this OTP, can you log into your account. On some platforms, 2FA works a little differently. You can use dedicated applications to verify your login each time, such as on Facebook and Google Authenticator. This will make it more difficult to hack into your account. You can activate this feature by going to “Settings”.

2FA ON FACEBOOK:

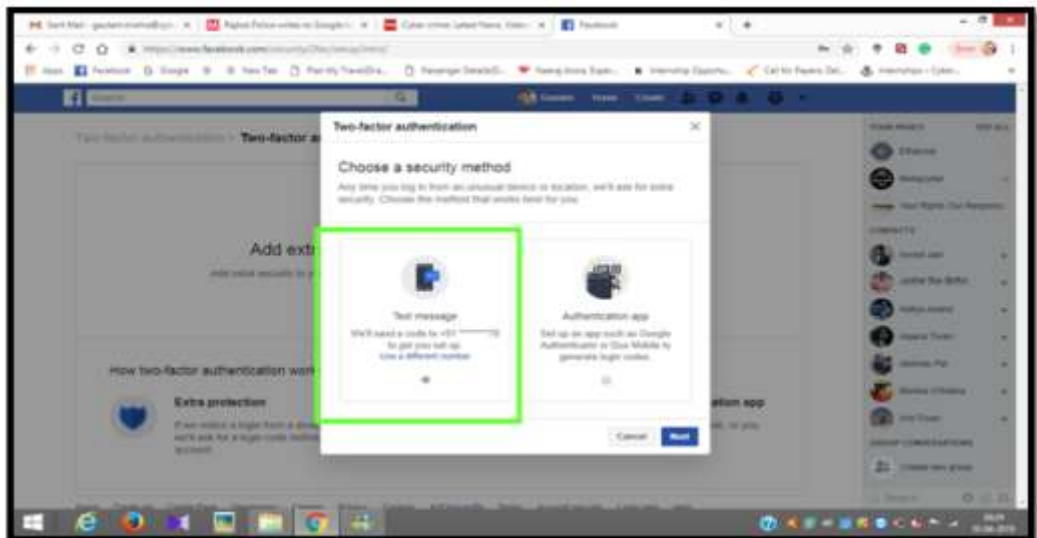
Step 1: Go to “Security and Login” in Settings.



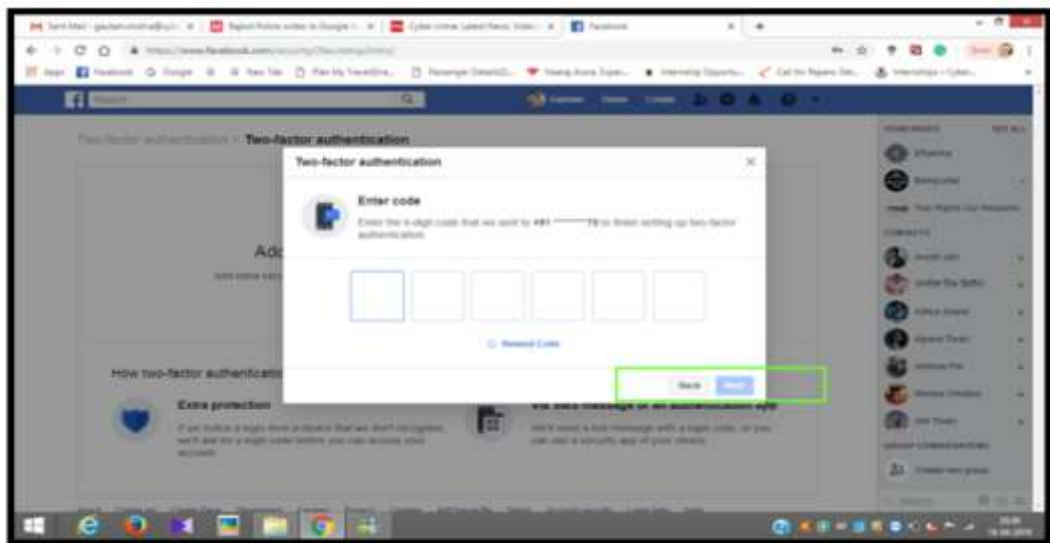
Step 2: Click on the “2 Factor Authentication” setting



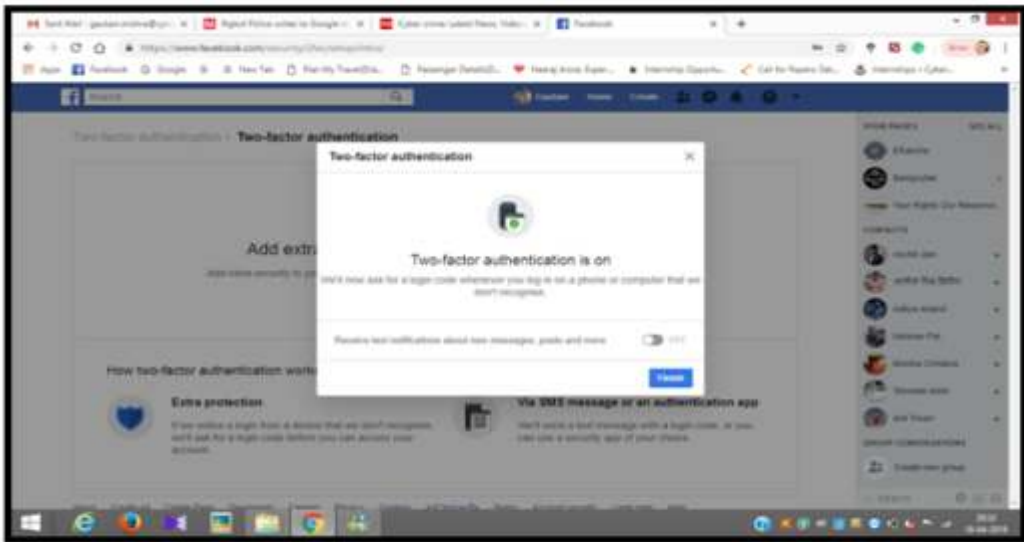
Step 3: Choose the first option to receive OTPs on your phone.



Step 4: Click on the “2 Factor Authentication” setting



Step 5: You will receive a message confirming that two factor authentication has been activated.

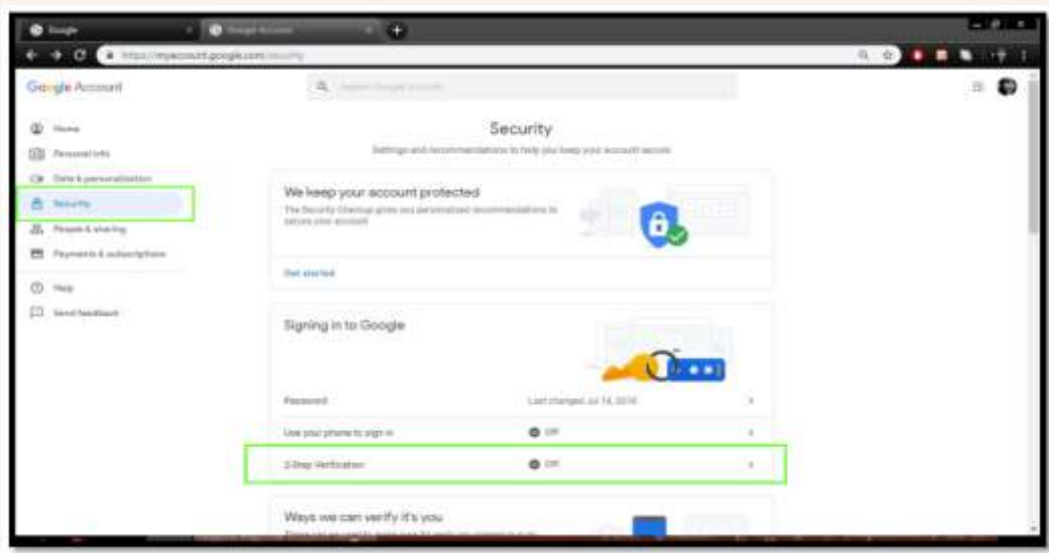


TWO STEP VERIFICATION ON GMAIL

Step 1 : Go to you Gmail Account and open "Google Account"



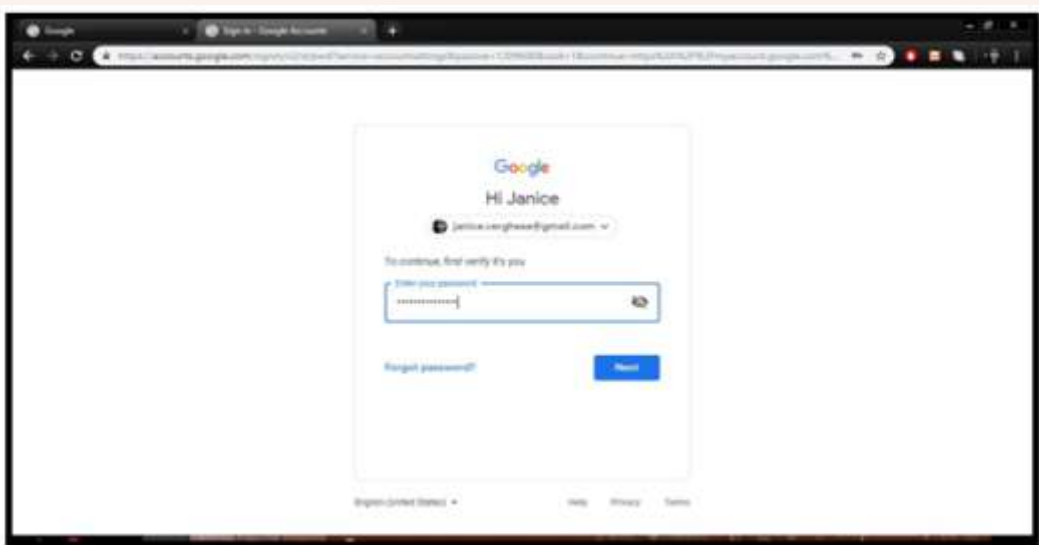
Step 2 : Go to “Security”, and click on two step verification.



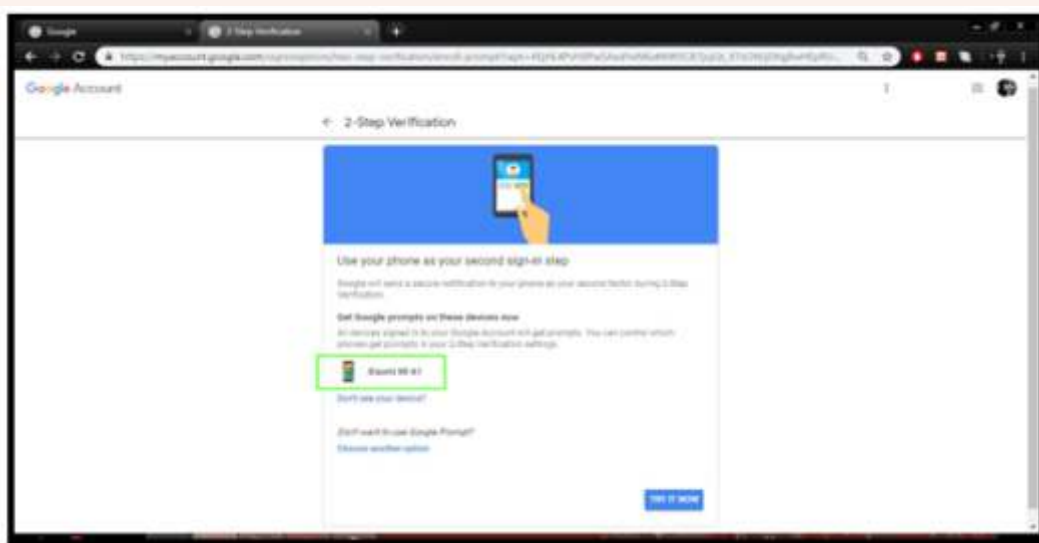
Step 3 : Click on “Get Started”.



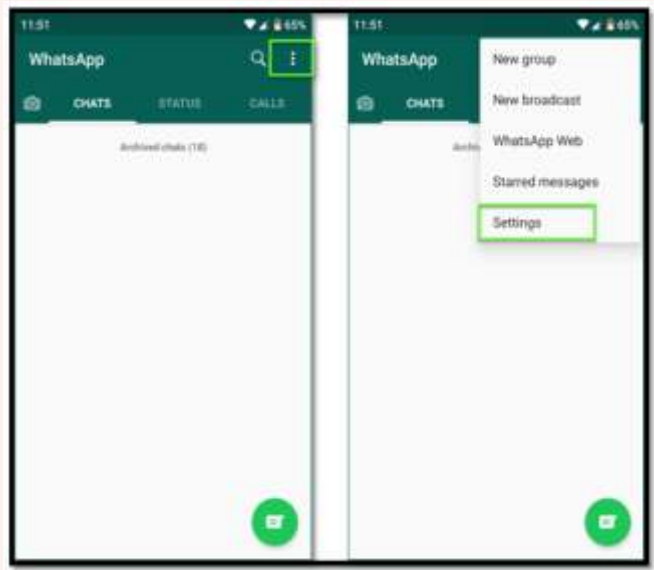
Step 4 : Enter your Gmail password.



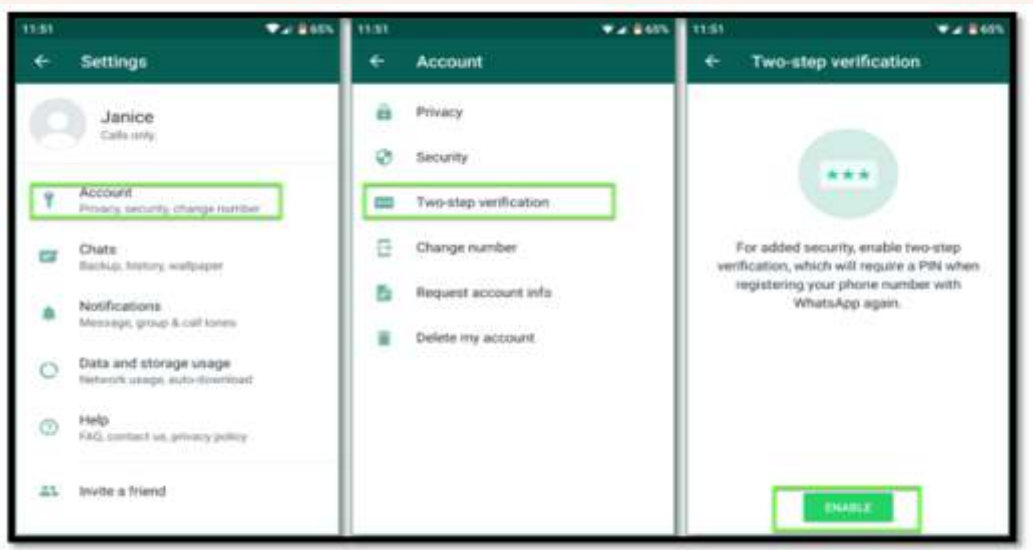
Step 5 : Enter your mobile number, verify by entering the OTP and you have successfully activated Two Step Verification.



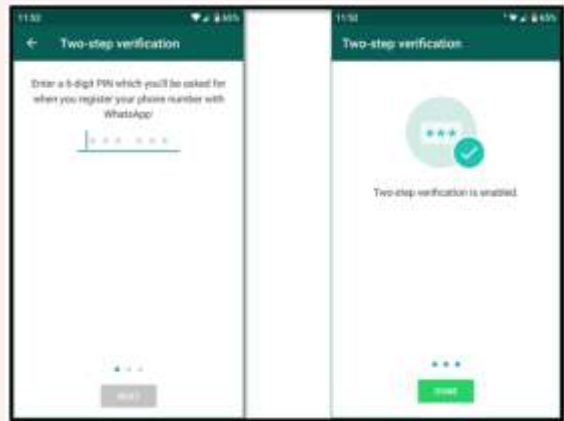
Step 1 : open WhatsApp, click the three dots at the right top corner, and go to “Settings”.



Step 2 : Go to “Account”, choose “Two Step Verification” and clickon “Enable”.



Step 3: Set up a 6 digit pin, and finally click on "Done".



C. Checking Security of Websites

a. Before logging into your accounts or sharing information on any website, check the URL and make sure the link begins with "https". HTTPS* links are secure, whereas HTTP links may be fraudulent and can be used to steal your information.



* **Https:** It stands for Hypertext Transfer Protocol Secure and is used for secure communication over the internet, such as <https://www.google.co.in/>

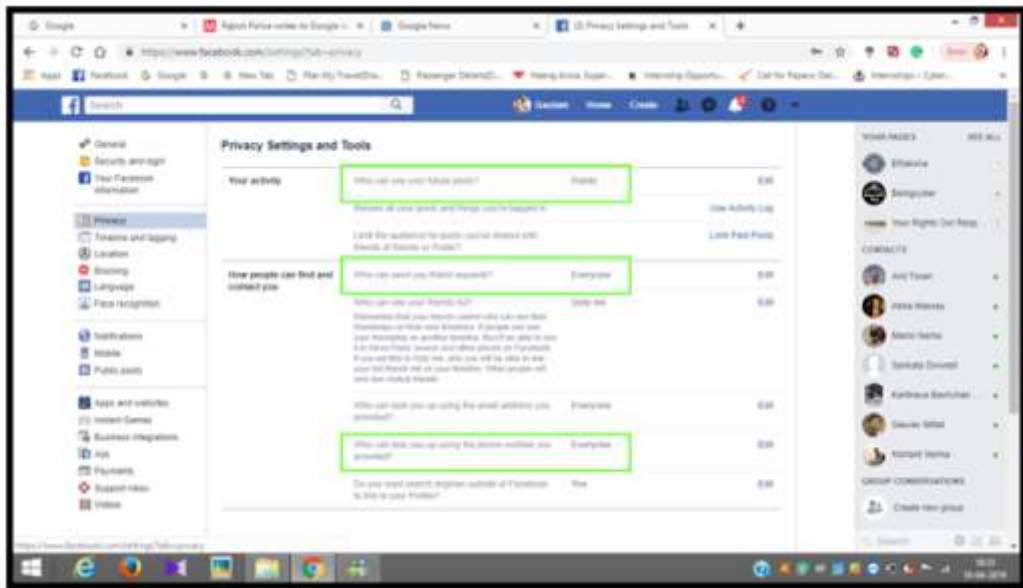
b. Websites can be spoofed very easily. The spoofed version looks very much like the real website and it becomes difficult to identify which is the real website. Looking out for URLs helps identify if websites are legitimate and whether you should share information on them or not.

Before logging into a website, check the URL closely with a slight change a fake URL may look like a real one. In the example, a real and a fake facebook account.

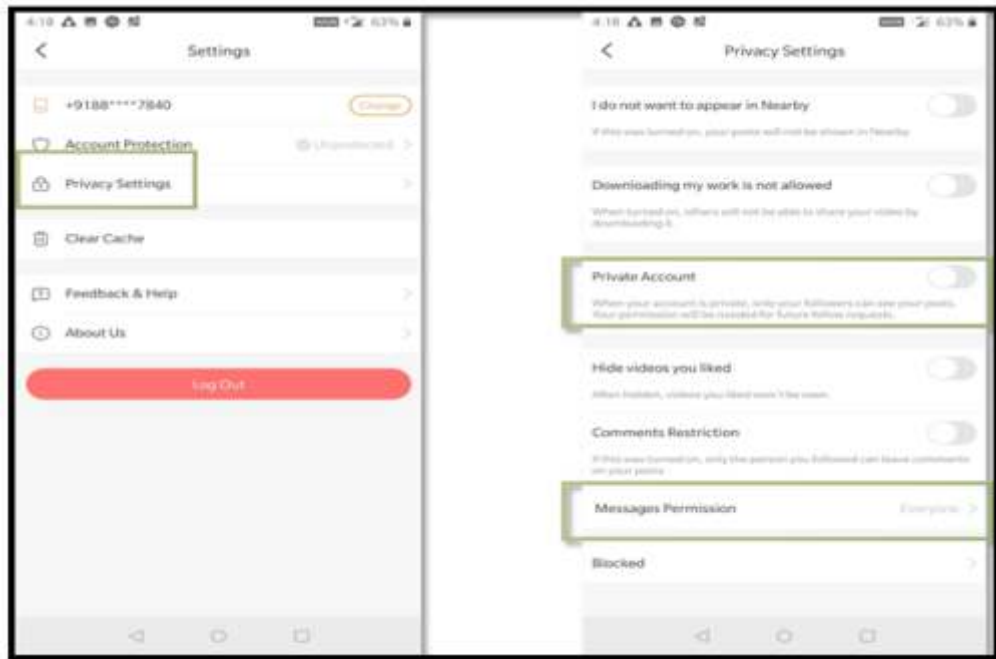


D. Making use of Privacy settings

Other than this, all platforms provide privacy settings that you can use to control your accounts and the audience accessing your posts. Using these, you can control who can see your account, who can approach you, and also who can search for you online. For example, on Facebook, you can choose if people can search for your account using your mobile number. By turning this feature off, you can ensure that even if someone finds your number, they will not be able to find your account using it.



You can also use privacy settings to keep your account private. This will ensure that nobody can see your posts and photos unless you authorize them.



4.2 Minimize Risks by Adopting Responsible Cyber Social Behavior

As we all know that responsible social behaviour keeps us safe and insulated from unnecessary conflicts and violence. Similarly we need to learn responsible cyber social behavior. Some key points include the following:

- Sharing private information like your password, daily life events or your location may not be such a good idea. This information can be used for cyberbullying.
- It is good to try and identify the person behind unknown accounts that may show deep interest in you. Even if you may have mutual friends, the person may not be the one who he claims to be. Ask your mutual connections about such accounts that are unknown or may look suspicious.
- Avoid doing things online that you wouldn't do offline. Your actions leave behind digital footprints and may be used against you even after you have rectified them.
- Avoid downloading free music/movies/games from untrusted sources. In the process of downloading free content, you may end up getting your devices infected by malware which can steal and misuse your data. Only download using trusted sources like PlayStore and AppStore, and always check ratings and reviews.
- If you feel your device is infected, you can reset your phone by using the process called bit-erasing. Before doing so, make sure you have taken a backup of your essential data like contacts, gallery, etc. Avoid taking a backup of your apps, as this may create a backup of the malware as well.
- If you ever feel like things are not right online, pause, and try to understand what is happening. You can reach out to your parents, teachers and friends and find a solution to your problem.

CYBER SECURITY TIPS

01

While logging into someone else's computer system or in cybercafé, don't save password and do delete your browsing history.

02

Never save your password and login credential on your web browser.

03

Avoid connecting to open source wifi or network. Through this, a hacker can easily hack into your electronic devices.

04

Use antivirus in your electronic gazette, which reduces your risk of data theft and removes harmful things from your electronic device.

05

While downloading an APP, it asks permission such as contact, photo, camera, etc. Check before giving it, whether or not it is necessary.

06

Off auto syncing on your mobile or computer system. In case of an attack by hacker, you will lose less data.

07

Don't click on unknown link/Url you get through mail, Whatsapp, messages, even if it looked genuine. This can be a hacking trick.

08

Check your privacy settings and decide whether such as your Whatsapp DP is visible to your contacts or to all. Photographs can be used for blackmailing and creating fake ID.

09

Be careful! You are being watched during video chats. Don't get carried away!

10

Do not believe and forward anything that you read on social media, without verifying it from a trusted source.

11

Never leave your account unattended after login, log out immediately whenever you are not using it.



📍 Address : Jiyamau, 1090 Circle, Lohia Path, Lucknow - 226001

☎ Contact : 0522-2205790

✉ Email : 1090police@gmail.com

🌐 Website : www.wpl1090up.in

🐦 Twitter: @WPL1090

January, 2020