FOREWORD

I am pleased to release the Hand Book on Cyber Crime which will be very relevant and pertinent in the field of Cyber Crime .It will be very useful for all the general public.

Cyber Crime effects all of us but it is children and women who are disproportionately affected by Cyber Crime. Cyber Crimes perpetrated against women and children not only violate their privacy and put their digital identities at risk but also can effect their mental health adversely and in some cases drive them to take extreme steps like suicide. Interestingly various malwares, botnets, hacking services etc. along with many tools are now freely available in various fishy markets, thereby criminals who don't have any technology know-how are also entering into Cyber Crime arena and are building syndicates across the country.

The menace of cyber-crime must be dealt at all levels and in a holistic manner by civil society, law enforcement agencies and individuals. Victims of Cyber Crimes should also come out openly and complain. The burden of shame has to be carried by the perpetrator and not the victim. There is an urgent need for greater awareness and sensitisation on this important issue among all stakeholders.

I commend Mr. Sanjay Mishra, Cyber Expert for this endeavor which will go a long way in sensitising people about the menace of cyber-crime and equip them with the right information to fight with this social ill.

I anticipate that all readers will be benefited by this Hand Book.

Ambar Kishor Jha, IPS

CDTI, Ghaziabad.

ABOUT HANDBOOK

This handbook is reference material to understand cyber-crimes against women and online cyber-crime safety for children. Online abuse against women is a serious issue in India, affecting more than half of survey respondents, yet women and other targets lack support and understanding to respond effectively. Thirty-six percent of respondents who had experienced harassment online took no action at all. Twenty-eight percent reported that they had intentionally reduced their online presence after suffering online abuse. Only a third of respondents had reported harassment to law enforcement; among them, 38 percent characterized the response as "not at all helpful. Some respondents found it hard to think of online harassment on par with violence, even though 30 percent of those who had experienced it found it "extremely upsetting" and lead to mental health issues like depression, stress, and insomnia. Though avid users of social media, respondents lose trust in popular platforms because of harassment against them or someone they know. Mechanisms to report abuse on social media platforms fall short. Victims are more likely to block abuse than to report it, yet blocking is ineffective against organized, sustained campaigns using multiple accounts. Assailants readily exploit mechanisms to report abuse, alleging their victims have violated platform guidelines to disable their accounts.

The purpose of this handbook is to improve the cybercrime against women and to assure online safety for children, prevention & expertise skills for the women and children in order to ensure that they are capable of efficiently preventing and solving cyber-crimes targeted at and benefiting from the cyber and online crime operating environment.

Sanjay Mishra

Cyber Crime Expert

CONTENTS

CYBER CRIMES AGAINST WOMEN AND CHILDREN- OVERVIEW

Technology is successfully being used to support engaging, positive and effective learning, and to realize and increase the potential of personalized learning by making learning more flexible, creative and accessible. Explore safe ways of using technology with learners to support self-esteem, assertiveness, participation and to develop friendships. Promote and discuss 'netiquette', e-safety and digital literacy. Show learners that the adults understand the technologies they use – or get the women and children safe on internet.

The chatting friends allure their lady friends by using words such as **"beautiful figure"**, **"sexy"**, and **"attractive"** etc., which is actually the beginning of obscenity trap. Slowly the culprit takes their female friends into confidence and induces them to be victim of virtual world crime. Troll them on any issues they speak up & harass them by sending obscene e-mails, stalking women by using chat rooms, websites etc,

Even criminal threatens victim girl to circulate the MMS if she discusses any incident relating to sexual assault committed by the said criminal with anyone and in some case the victim lady could not bear the humiliation and jeering by society and killed herself.

Give reassurance that the woman has done the right thing by telling someone; refer to any existing pastoral support/procedures. Help the women and children to keep relevant evidence for any investigation (e.g. by not deleting messages they've received, and by taking screen capture shots and noting web addresses of online cyber bullying instances).

As the criminal is behind the screen and isn't in public, he enjoys the benefit of anonymity. So, everyone needs to be aware of the impact of cyber-crimes against women and the ways in which it differs from other forms of crimes. Law enforcement agencies and the parents should be made aware of women and children responsibilities in their use of Information and Communications Technology, and what the sanctions are for misuse. Women and Children should know that who can provide them with support if a cybercrime takes place.

INTRODUCTION

There always exists more than one way to solve the problem. The terms *Hacker* **and** *Hacking* **are being misinterpreted and misunderstood with negative side-lines. But, the quality and types of hackers depends on attitude to the technology and is concerned with hands on ways of knowing and learning.**

Hacking

The Art of exploring various security breaches is termed as ***Hacking.***

- *Hacking is exploring the details of programmable systems.*
- *Stretching the capabilities of computer system.*
- *Sharing their computer expertise.*
- *Can also mean breaking into computer system (cracking).*

Communities of Hackers

- ***Hackers***
- ***Crackers***
- ***Phreaks***
- ***Script Kiddies***

Hackers

Hackers are *Intelligent Computer Professionals* who create security awareness by sharing knowledge. It's a team to gain depth of a system, what's happening at the backend, behind the screen and also find possible security vulnerabilities in a system. Hacker's watch lets you report and share information that helps to identify combat and prevent the spread of Internet threats and unwanted network traffic.

Hacking behaviours can also be an alternative to the institution-based work in science and technology.

Computer Security is a continuous battle. As computer security gets tighter hackers are getting smarter.

Types of Hackers

There are three types of hackers and are categorized on the basis of their intensions and the hacking ethics.

- **White Hat Hacker:** Those who work to secure computer system without breaking into them. They work with software companies to resolve vulnerabilities; won't announce vulnerabilities until company is ready or found to be unresponsive. They work ethically and will only attack system when authorized by the owner and will show code to software maker but no one else to how exploit vulnerability.
- **Black Hat Hacker:** Those computer professionals who cares more about controlling systems and accessing protected information than about securing computers. They hack system for their own gain or for malicious reasons and keeps vulnerable information to trade with other black hats on closed lists.
- **Gray Hat Hacker:** Those computer professional who might break into computer system to heighten awareness of security flaws and announces vulnerability publicly without informing software or system developer company, or on the same day that software company is notified. They release exploit code that isn't easily modified for hacking security.

Shades of Gray:

Many security specialists classify hackers as white hats or black hats but in reality, most hackers fall somewhere in between.

*__Vulnerability:__ It is a weakness which allows an attacker to reduce a system's information assurance.

Crackers

An Individual who breaks into computers with malicious intent and can have unauthorized access into a system and cause damage, destroy or reveal confidential information.

Their motives are to compromise the system to deny services to legitimate users for troubling, harassing them or for taking revenge. They can cause financial losses &image/reputation damages, defamation in the society for individuals or organizations.

Phreaks

These are persons who use computer devices and software to break into phone networks. They find loopholes in security of phone networks and to make phone calls at free of cost.

They actually used your number for calling and you may have big amount of phone bills, for doing nothing!!!

Script Kiddies

These are persons who are not having technical skills to hack computers. They use the available information about known vulnerabilities to break into remote systems.

It's an act performed for a fun or out of curiosity in which no individuals or organization are harmed.

Hackers Motivation

- *Fun*
- *Profit*
- *Extortion*
- *Technical Reputation*
- *Revenge/maliciousness*
- *Intellectual Challenges*
- *Desire to embarrass*
- *Experimentation*
- *Problem Solving*
- *Exposing System Weakness*
- *Want to be Hero of Wild Internet*

HACKERS STRATEGIES

- *Reconnaissance*
- *Scanning*
- *Gaining Access*
- *Maintaining Access.*
- *Clearing Tracks.*
- Reconnaissance

Reconnaissance can be described as the pre-attack phase and is a systematic attempt to locate, gather, identify and record information about the target. The Hacker seeks to find out as much information about the target as possible.

- **Scanning and Enumeration**

  Scanning and enumeration is considered the second pre-attack phase. This phase involves taking the information discovered during reconnaissance and using it to examine the network. Scanning involves steps such as intelligent system port scanning which is used to determine open ports and vulnerable services. In this stage the attacker can use different automated tools to discover system vulnerabilities.

- **Gaining Access**

  This is the phase where the real hacking takes place. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access. The method of connection which Hacker uses for an exploit can be a local area network, local access to a PC, internet or offline. Gaining access is known in the Hacker's world as owning the system. During a real security breach it would be this stage where the Hacker can utilize simple techniques to cause irreparable damage to the target system.

- **Maintaining Access and Placing Backdoors**

  Once a Hacker has gained access, they want to keep that access for future exploitation and attacks. Sometimes, Hackers harden the system from other hackers or security personnel by securing their exclusive access with Backdoors, Root kits, and Trojans. The attacker can use automated scripts and automated tools for hiding attack evidence and also to create backdoors for further attack.

- **Clearing Tracks**

  In this phase, once Hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking or to avoid legal action. At present, many successful security breaches are made but never detected.

INTRUDER

An individual who gains or attempts to gain unauthorized access to a computer system is known as Intruder.

Types of Intruders:-

There are three classes of Intruders:

Masquerader: An individual who is not authorized to use the computer but penetrate a system and access to exploits legitimate user's account.

Misfeasor: An individual who is authorized for access but misuse his or her privileges.

Clandestine User: An individual who seizes supervisory control of the system and uses this control for access control.

An Intrusion Detection System (IDs) is used to detect unauthorized intrusion into computer systems and networks.

Phishing

The act of sending an Email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information and are used for identity theft. The Email directs the user to visit a Web site where they are asked to update personal information such as passwords, credit card details, social security and bank account numbers. The Web site however is Bogus and set up only to steal the User's information.

Phishing attacks are also used to steal your Money!!!

Phishing Scams Could Be-

- Emails inviting you to join a Social Group, asking you to Login using your Username and Password.
- Email saying that Your Bank Account is locked and Sign in to your account to unlock it.
- Emails containing some Information of your Interest and asking you to Login to Your Account. Any Email carrying a link to click and asking you to Login.
- A link for attractive events, news, photographs, videos and presentation asking for secure login.

NOTE: *Always locate the URL bar of the browser for the proper address (website) before entering any password or intimate details.*

AN OVERVIEW OF HACKING INTERNET PROTOCOL

Internet Protocol (IP) ADDRESS

Identity on the web is IP address. An *Internet Protocol address (IP address)* is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. Every system has its own IP address which is stored in web or to the service providers.

Internet Protocol (IP) addresses is usually of two types:

1. **Public.**
2. **Private**.

Public IP Addresses

A public IP address is assigned to every computer that connects to the Internet where each IP is unique. Hence, two computers can't exist with the same public IP address all over the Internet. This addressing scheme makes it possible for the computers to "find each other" online and exchange information. User has no control over the IP address (public) that is assigned to the computer. The public IP address is assigned to the computer by the Internet Service Provider (ISP) as soon as the computer is connected to the Internet gateway.

A public IP address can be either **static** or **dynamic**.

A *static public IP* address does not change and is used primarily for hosting Webpages or services on the Internet.

On the other hand a *dynamic public IP* address is chosen from a pool of available addresses and changes each time one connects to the Internet. Most Internet users will only have a dynamic IP assigned to their computer which goes off when the computer is disconnected from the Internet. Thus when it is re-connected it gets a new IP.

You can check your public IP by simply typing my IP on Google or by visiting www.whatismyip.com

Private IP Addresses

An IP address is considered private if the IP number falls within one of the IP address ranges reserved for private networks such as a Local Area Network (LAN). The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private networks (local networks):

10.0.0.0 – 10.255.255.255 (Total Addresses: 16,777,216)
172.16.0.0 – 172.31.255.255 (Total Addresses: 1,048,576)
192.168.0.0 – 192.168.255.255 (Total Addresses: 65,536)

Private IP addresses are used for numbering the computers in a private network including home, school and business LANs in airports and hotels which makes it possible for the computers in the network to communicate with each other.

For example, if a network X consists of 10 computers each of them can be given an IP starting from 192.168.1.1 to 192.168.1.10. Unlike the public IP, the administrator of the private network is free to assign an IP address of his own choice (provided the IP number falls in the private IP address range as mentioned above).

Devices with private IP addresses cannot connect directly to the Internet. Likewise, computers outside the local network cannot connect directly to a device with a private IP. It is possible to interconnect two private networks with the help of a router or a similar device that supports Network Address Translation.

If the private network is connected to the Internet (through an Internet connection via ISP* Provider) then each computer will have a private IP as well as a public IP. Private IP is used for communication within the network whereas the public IP is used for communication over the Internet.

NOTE: You can know your private IP by typing **ipconfig** command in the command prompt. The number that you see against "IPV4 Address:" is your private IP which in most cases will be 192.168.1.1 or 192.168.1.2 or similar to this.

Unlike the public IP, private IP addresses are always static in nature.

Unlike what most people assume, a private IP is neither the one which is impossible to trace (just like the private telephone number) nor the one reserved for stealth Internet usage. In reality there is no public as well as private IP address that is impossible to trace since the protocol itself is designed for transparency.

*ISP: Internet Service Provider

SECURITY AND THREATS

Security

Security is a continuous process of protecting an object from the attack.

Security is defined by:

1. **Confidentiality:** To prevent unauthorized disclosure of information to third parties. This includes the disclosure of information about resources.
2. **Integrity:** To prevent unauthorized modification of resources and maintain accuracy. The alteration of resources like information may be caused by a desire for personal goal, sometime for fun or a need for revenge.
3. **Availability:** To prevent unauthorized withholding of a system resources from those who need them and when they need them.

Security Threat

The generic name as the collection of tools designed to exploit resources which is used by crackers is **security threat or malicious programs.**

Malicious Programs are further divide into two types:

1. Need Host program.

2. Independent Program.

1. **Need Host Program**: These are the essentially fragmented programs that cannot exist independently of some actual application program, utility, or system programs.

- **Trap Doors:** A trap door is a secret entry point into a program that is aware of the trapdoor to gain access without going through the usual security access procedures.
  The trap door is code that recognizes some special sequence of input or is triggered by being run from a certain user ID or by an unlikely sequence of events.
  Trap doors become threats when they are used by unscrupulous programmers to gain unauthorized access.
- **Logic Bomb:** Logic bomb is a code embedded in some legitimate program that is set to explode when certain conditions are met.
  When triggered, a bomb may alter or delete data or entire files, cause a machine halt, or do some other damage.

- **Trojan horse:** A Trojan horse is a program or command procedure containing hidden code that, when invoked performs some unwanted or harmful function.

Example: To gain access to the files of another user on a shared system could create permission so that the files are readable by any user.

Trojan is Remote Administration tools that give an attacker remote controller to remote access the victims.

Some of the examples are:

These are software used to control the victim's system.

Girlfriend, Net bus, Backorrifice, WINBACKDOOR, SUB7..

- **Zombie:** A zombie is a program that secretly takes over another Internet connected computer and then uses that computer to launch attacks which creates difficulty in tracing the Zombie creator. Zombies are used in denial-of-service (DOS) attacks, against targeted web sites.

2. **Independent Program**: These are self-contained programs that can be scheduled and run by the operating system.

- **Virus:** A virus is a program that can infect other programs by modifying them. The modification includes a copy of the virus program which can move further to infect other programs.
- **Worms:** A worm is a program that can replicate itself and send copies from computer to computer across network connections.

PART I

DIFERENT TYPE OF CYBER CRIME AGAINST WOMEN

CYBER BULLYING: Cyber bullying is when the Internet and related technologies are used to bully other people, in a deliberate, repeated, and hostile manner. This could be done via text messages or images, personal remarks posted online, hate speeches, Instigating others to dislike and gang up on the target by making them the subject of ridicule in forums, and posting false statements in order to humiliate or embarrass another person.

Cyber bullies may also disclose victims' personal data (e.g. real name, address, or workplace/schools) on websites. Cases of piggy-backing on victim's identity are now common. This could be used to publish objectionable material in their name that defames or ridicules a subject.

Under the Indian law, cyber-bullying is covered by section 66 D of the Information Technology Act. This section is titled "Punishment for sending offensive messages through communication service, etc." This section provides for imprisonment up to 3 years and fine up to one lakh.

Section 66D penalizes the following being sent through email, sms etc.:

- Information that is grossly offensive or has menacing character; or
- False information sent for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will. This section also penalizes the sending of emails (this would include attachments in text, image, audio, video as well as any additional electronic record transmitted with the message.) for the following purposes:
- Causing annoyance, or
- Causing inconvenience, or
- To deceive or to mislead about the origin of the messages.

Cyber bullying can be carried out through Internet services such as e-Mail, chat rooms, discussion groups, instant messaging or web pages. It can also include bullying through mobile phone technologies such as SMS. Cyber bullying can include teasing and being made fun of, spreading rumours online, sending unwanted messages and defamation.

CYBER BULLYING CAN BE DONE IN THE FOLLOWING WAYS

FORWARDING A PRIVATE IM COMMUNICATION TO OTHERS

An anti-social element or criminal may create a screen name that is very similar to women name. The name may have an additional prefix or postfix and sometime original. They may use this name to say inappropriate things to other users while posing as the other person. They may forward the above private communication so others to spread their private communication.

IMPERSONATING TO SPREAD RUMOURS

Forwarding gossip mails or spoofed mails to spread rumours or hurt women are common these days. They may post a provocative message in a hate group's chat room posing as the victim, inviting an attack against the victim, often giving the name, address and telephone number of the victim to make the hate group's job easier.

POSTING EMBARRASSING PHOTOS OR VIDEO

A picture or video of someone in a locker room, bathroom or dressing room may be taken and posted online or sent to others on cell phones.

BY USING WEB SITES OR BLOGS

Women used to tease on porn Web sites these days. Sometimes create Web sites or blogs which may insult or endanger women. They create pages specifically designed to defame women.

HUMILIATING TEXT SENT OVER CELL PHONES

Text wars or text attacks are when someone gang up on the victim, sending thousands of text messages related to hatred or defame and messages to the victim’s cell phone or on other messaging application.

SENDING THREATENING E-MAILS AND PICTURES THROUGH E-MAIL OR MOBILE TO HURT ANOTHER

Sometime ex may send hateful or threatening messages to women, without realizing that while not said in real life, unkind or threatening messages are hurtful and very serious.

STEALING PASSWORDS

Attacker may steal women password and begin to chat with other people, pretending to be same or by changing actual user profile and impersonate her.

Facebook Fake Profile cases

Facebook is a very popular online community and social networking website. They can create and join a wide variety of online communities. The profiles of Facebook members are publicly viewable.

The scenarios

1. A fake profile of a woman is created on Facebook. The profile displays her correct name and contact information (such as address, mobile number etc.). Sometimes it even has her original photograph and sometimes it has morph photograph as nude one or showing private parts with defamatory information, alleged immoral character etc.

The problem is that the profile describes her as a prostitute or a woman of "loose character" who wants to have sexual relations with anyone. Other Facebook members see this profile and believed that the photograph is original and start calling her at all hours of the day asking for sexual favours. This leads to a lot of harassment for the victim and also defames her in society.

Section Imposed (The Law): Section 66 E, 67 of Information Technology Act and section 509 of the Indian Penal Code.

Who is liable : Those who created and updated the fake profile are liable for the same.

The motive: - Jealousy or revenge (e.g. the victim may have rejected the proposal made by the suspect).

Modus Operandi

1. The suspect would create a free Gmail account using a fictitious name.

2. The email ID chosen by him would be unrelated to his real identity.

3. The suspect would then signup to Facebook and creates the offensive profile.

Cyber Pornography

Now a day, Cyber pornography is believed to be one of the largest businesses on the Internet today. These days many videos are recorded at various places like changing room in garment showrooms, hotel etc. Now a day smart TV is also used to record private video remotely as TV is connected with internet. The millions of pornographic websites that flourish on the Internet are testimony to this. Sometime ex-boyfriend or anti-social element uploads some private video for defaming or taking revenge or circulate on social media, messaging App or uploading on pornographic website to defame and some illegal financial gain.

Cyber pornography includes pornographic websites, pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc.).

The suspect accepts online payments and allows paying customers to view / download pornographic pictures, videos etc. from his website and when it is for revenge, video is broadcasting on messaging app or circulating on other online platforms.

Section Imposed (The Law): Section 67, 67A of Information Technology Act.

Who is liable: The persons who create and maintain the pornographic video will be liable. The one who created pornographic websites may also be liable in case they knowingly allow their users to upload such video to defame someone and access the pornographic websites.

The motive: Illegal financial gain.

Modus Operandi

The suspect registers on pornographic websites using fictitious details and upload such video on it.

The suspect accepts online payments and allows paying customers to view / download pornographic pictures, videos etc. from his website.

PART II

CYBER CRIMES AGAINST WOMEN AND ITS HANDLING

HOW TO REPORT BULLYING OR ABUSE ON SOCIAL MEDIA

Social Media businesses are governed by the laws of the country in which they are head-quartered, but they are also expected to comply with local laws where they operate. Most Social Media sites have a reporting system in place aimed at flagging inappropriate content, however, they do come under a lot of criticism for not taking online safety seriously enough.

Take Action

If someone is harassing you online, or their posts are threatening or hurtful toward you, report them on social media. Reporting might not always be a guaranteed approach, but it is a good first step at dealing with harmful content online. When reported, they might have their post removed, or get their account suspended/deleted depending on the situation. Reporting won't block the person from reaching you again, so make sure you block them too.

Report Accounts

First off, the person you report online will NOT be told *who* reported them. They may be warned that their profile has been reported or deactivated – however, the identity of the reporter isn't revealed to them.

Sometimes, depending on the type of report you're making, social media websites might ask you to fill out a form and answer a few personal questions. For example, if you are reporting someone pretending to be you on a fake account, they might ask you to send a scanned piece of identification to confirm your identity.

FACEBOOK

Facebook do not tolerate bullying or abuse and say that once they are aware of it, they will remove bullying content and may disable the account of anyone who is bullying another. They adhere to a set of **Community Standards** (**https://www.facebook.com/communitystandards/**) which include:

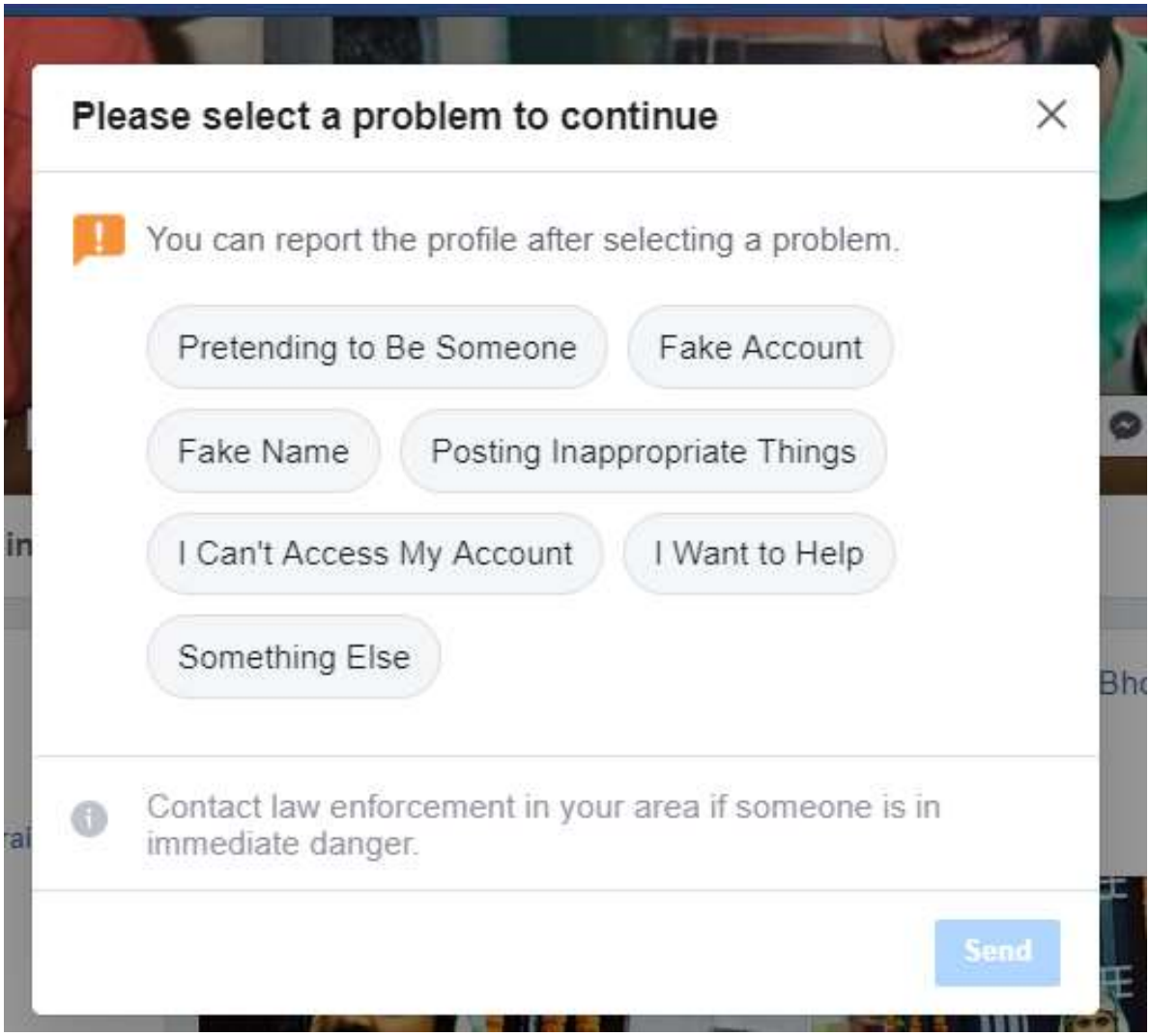
- Pages that identify and shame private individuals
- Images that have been altered to degrade private individuals
- Photos or videos of physical bullying posted to shame the victim
- Sharing personal information to blackmail or harass people
- Repeatedly targeting other people with unwanted friend requests or messages

Using the Report Links which appear on the page, you can report bullying to Facebook. A 'drop down arrow' should appear giving you a menu option to report the image, post or comment.

You can unfriend or block a person from Facebook. Click on their profile, on the message dropdown you will see the option to 'unfriend' and/or 'block'.

For reporting any profile you have to follow procedure

1. Go to the profile you wish to report.
2. In the bottom right of their cover photo, click the **"…"** icon and select **" Find Support or Report Profile".**

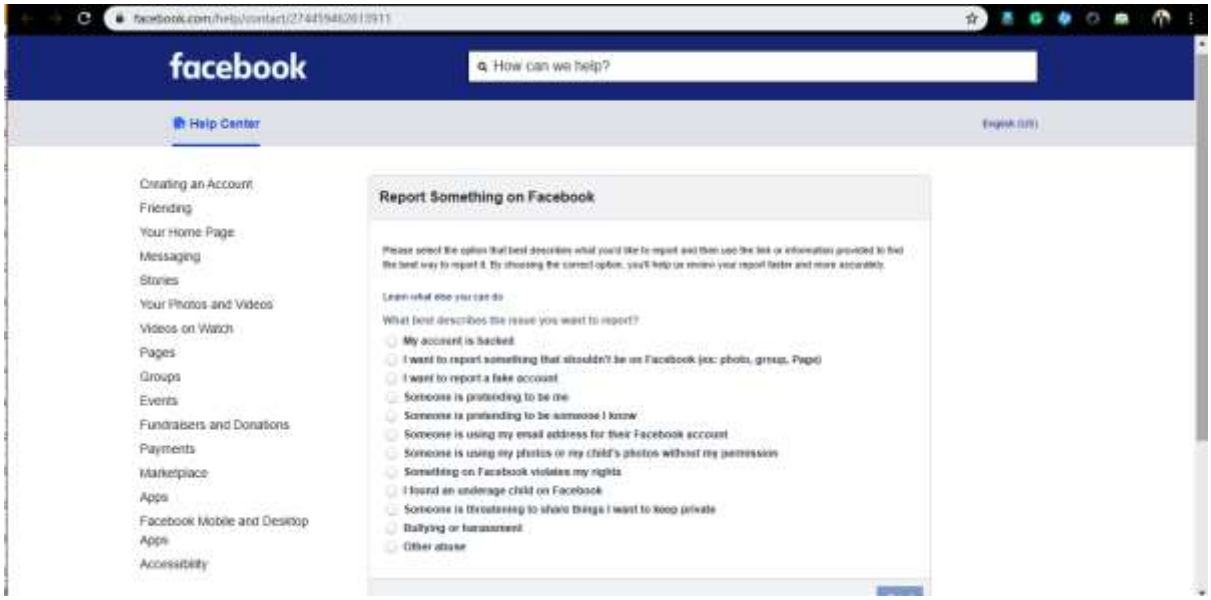


1. From there, just follow the on-screen instructions.

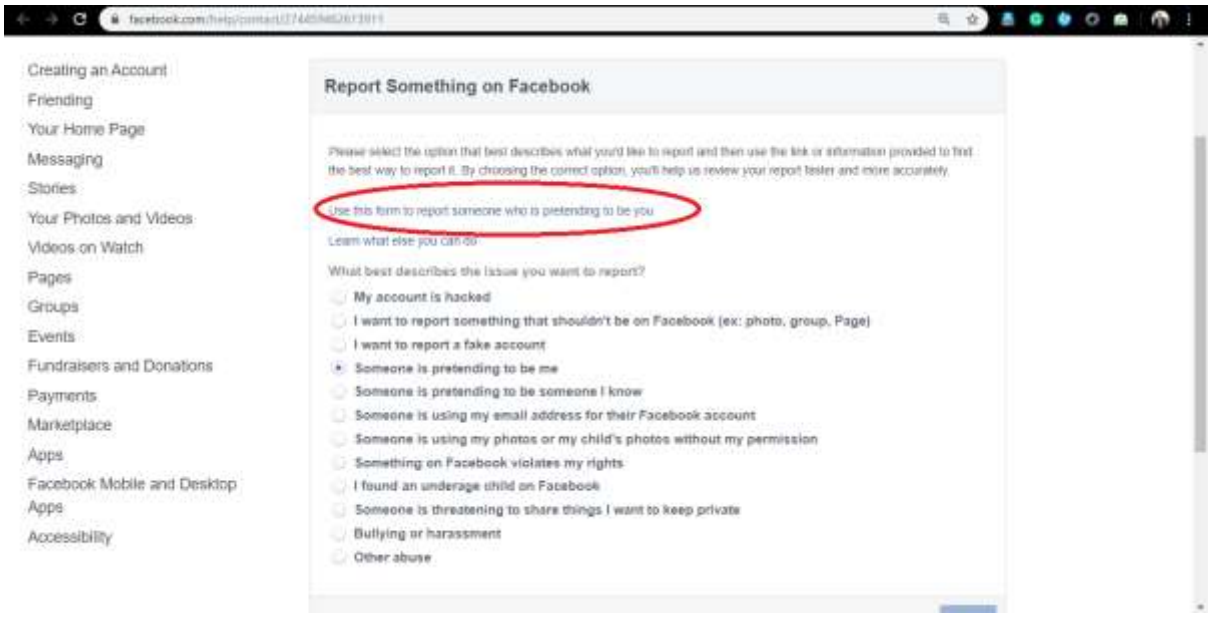
Sometimes women and children harass on social media because of fake profile using morph photograph which is sometimes nude photograph of individual that defame or mentally harass women and children's. In the case for deleting that account individuals can report on Facebook using following procedure which leads to delete the account within twenty four hours.

Note: - For any complaint and action, you must have to save URL (Uniform Resource Locator) link of profile or post.

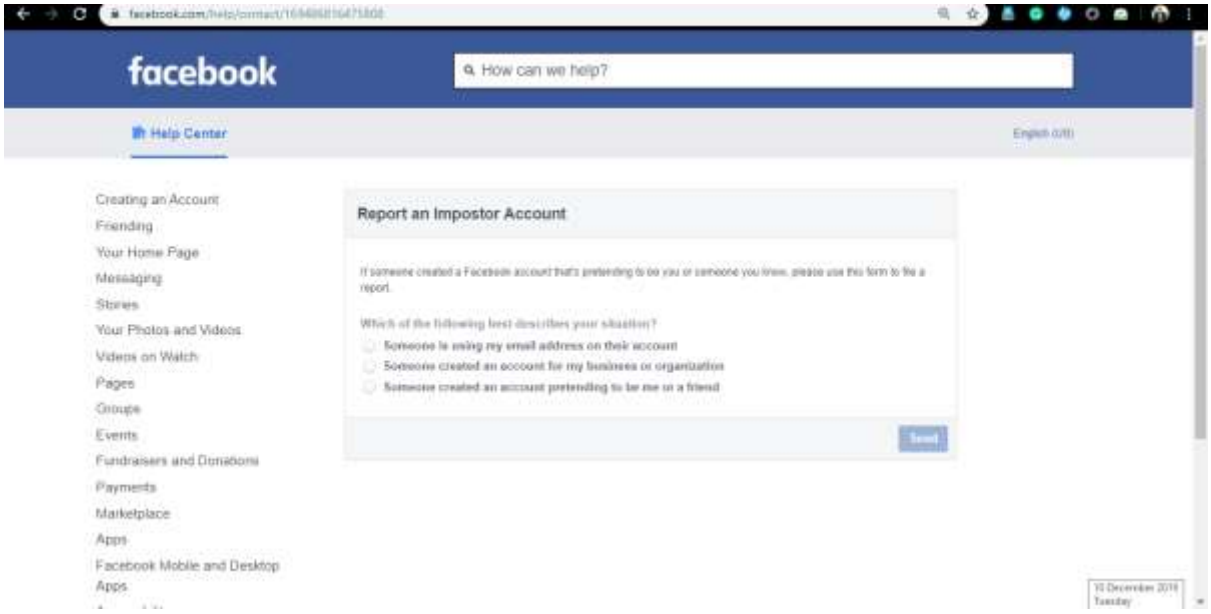
Step1. Open Google and search **"Report Something on Facebook"**



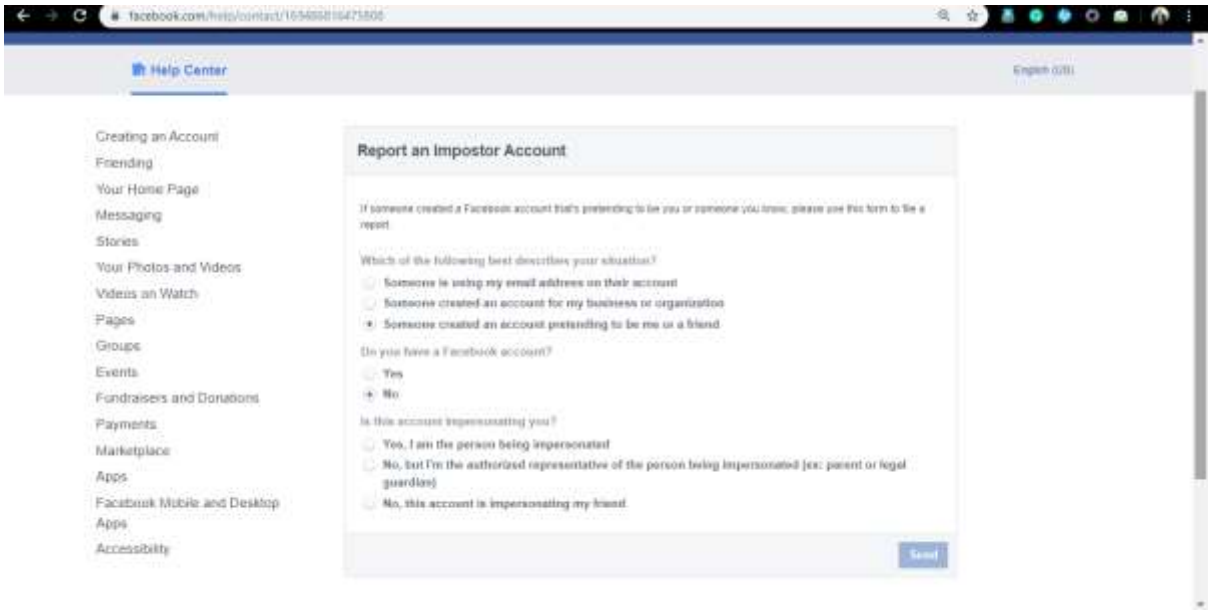
Step 2: There are number of option for number of reporting issues but for quick response, victim must select option **" Someone is pretending to be me"** then a link of form will appear.



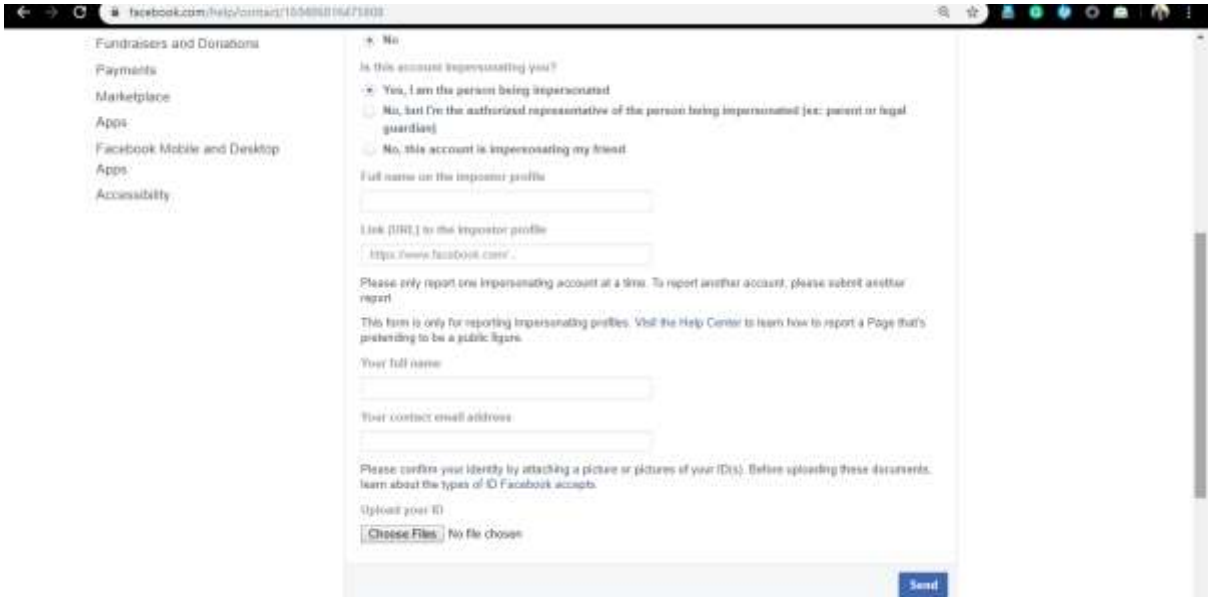
Step 3: Click on form link **"Use this form to report someone who is pretending to be you"**. Facebook provide three different option to report.



But, for removing the fake account, one should only click on last option "Someone created an account pretending to be me". Then Facebook give two options and ask that "Do you have Facebook account?". In the case even the victim is having account on Facebook then also they must select option of **"No"** because once you select yes Facebook ask to login your account and then report from their and once numbers of report facebook received about fake account then only it will be remove. So only select "**No**"option.



Step 4: Select the option **"Yes, I am the person being impersonated"** the a complete form will appear on screen to fill



Step 5 : Form Details is as follow

a) **Full name on the imposter profile:** - Type the name appear on fake profile.

   Note: Name must be same as on fake profile like language, title, symbol etc.

b) **Link (URL) to the impostor profile:** - Copy & paste Uniform Resource Locator of fake profile.

c) **Your Full Name:** Name of the victim as per identity proof document.

d) **Your contact email address:** - Victim must fill email address for receiving the action report on same mail. Meanwhile victim must assure that email id should not be registered with Facebook in any form because previously victim is already selected that he/she is not having account on Facebook, otherwise quick action not be taken or account may not be removed.

e) **Upload ID:** Victim must upload colour identity proof for taking action such as :

Group One

You can upload one of the items from group one to confirm your name or remove fake account. Anything that you send Facebook should contain either your name and date of birth or your name and photo.

- Adhar card
- Birth certificate
- Driver's license
- Passport
- Marriage certificate
- Official name change paperwork
- Personal or vehicle insurance card
- Non-driver's government ID (ex: disability, SNAP card, national ID card, pension card)
- Green card, residence permit or immigration papers
- Tribal identification or status card
- Voter ID card
- Family certificate
- Visa
- National age card
- Immigration registration card
- Tax identification card/

Group Two

If you don't have anything from group one, you can upload two different items from group two. The name on the items that you send Facebook should be the same name or date of birth or profile photo or some photo in any post that you want to claim that that account is fake using your identity.

This extra precaution is so that Facebook can make sure that the you are only the victim.

- Bank statement
- Transit card
- Check
- Credit card
- Employment verification
- Library card
- Magazine subscription stub
- Medical record
- Membership ID (ex: pension card, union membership, works ID, professional ID)
- Pay check stub
- Permit
- School ID card
- School record
- Social Security card
- Utility bill
- Yearbook photo (actual scan or photograph of the page in your yearbook)
- Company loyalty card
- Contract
- Family registry
- Diploma
- Religious documents
- Certificate of registration for accreditation or professional
- Professional license card
- Polling card
- Health insurance
- Address proof card
- Social welfare card

Step: 6 If a photograph of victim with identity proof holding in hand near face is consider on priority if upload so, make sure of it.

Step: 7 Click on Send icon, fake account will be removing shortly.

INSTAGRAM

Bullying or abuse on Instagram can take place in a number of ways:

- Negative Comments
- Fake Profiles
- Hacking Accounts

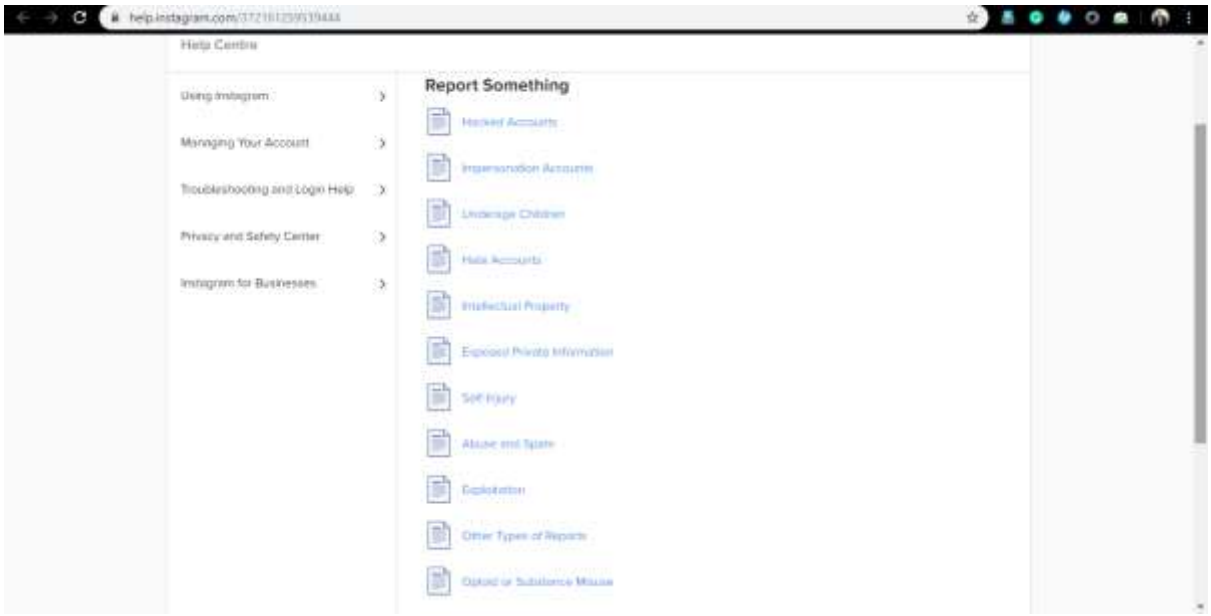
Instagram's advice is to block and unfollow the person who is being abusive. If it continues, you can report it here **https://help.instagram.com/ 165828726894770**

To block someone on Instagram

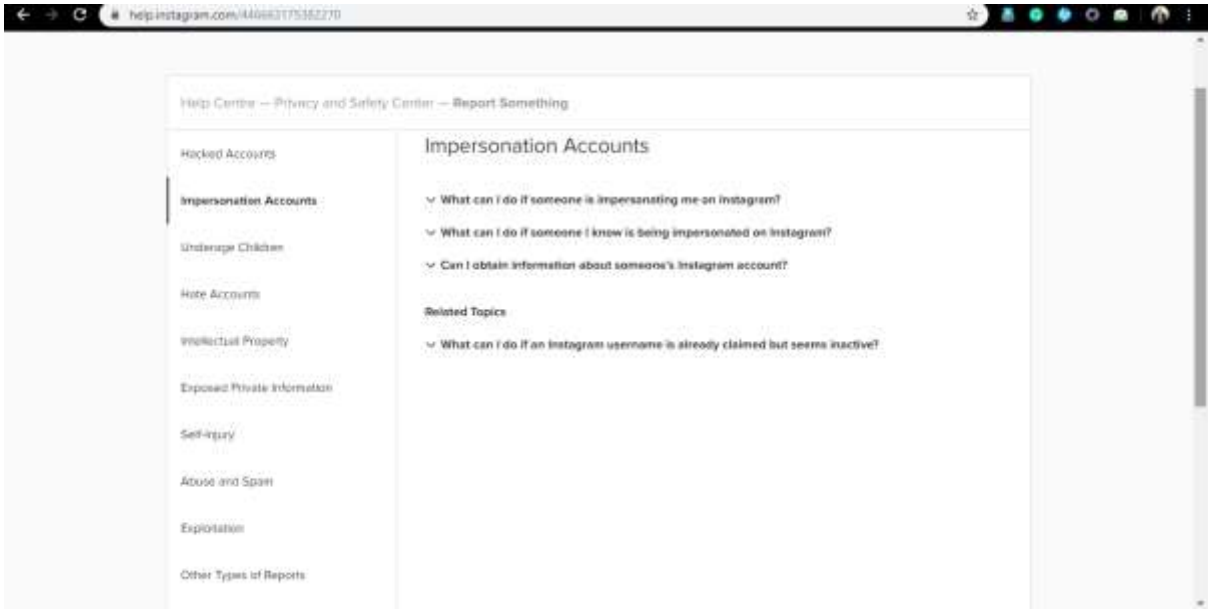
1. Tap the person's username to open their profile.
2. Tap the **"…"** icon that appears in the top right corner of the screen beside their name.
3. In the drop-down menu, tap **"Report".**
4. Select the reason why you're reporting this account and continue with the on-screen instructions.

Sometimes women and children harass on Instagram because of fake profile using morph photograph which is sometime nude photograph of women that can defame or mentally harass women and children's. In the case for deleting that account individuals can report on Instagram using following procedure which leads to delete the account within twenty four hours.

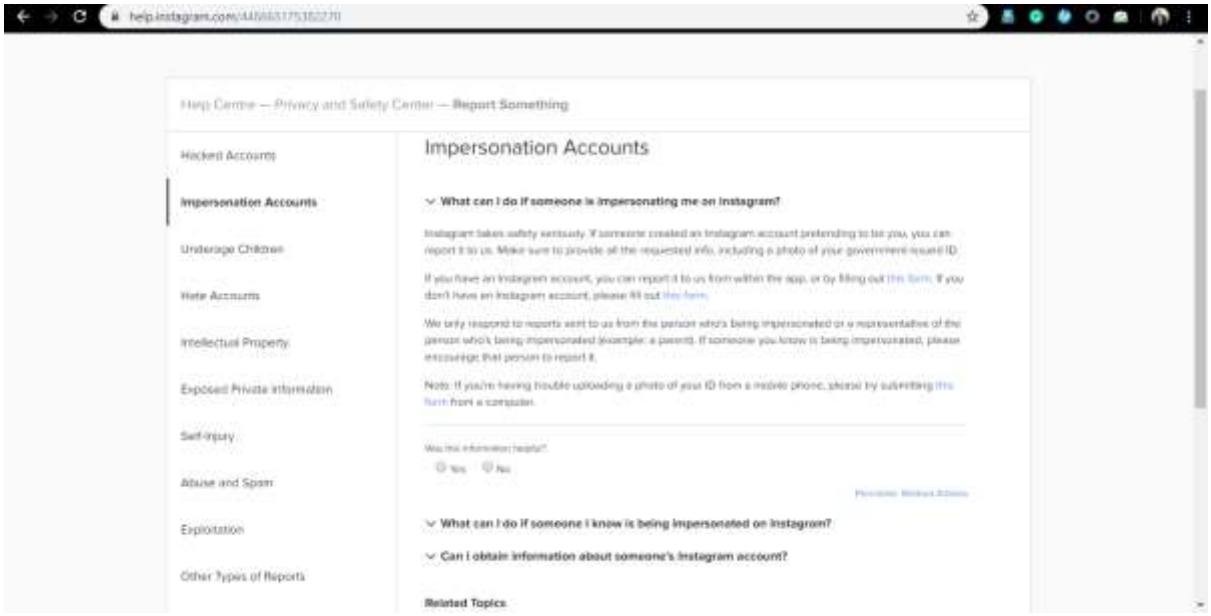
Step1. Open Google and search **“Report Something on Instagram”**



Step 2: - For removal of fake account one should click on option **“Impersonation Accounts”.** It open us various option for selecting best situation regarding problem.



Step 3: - For quick removal of impersonation or fake account one should must select an option **“What can I do if someone is impersonating me on Instagram?”**



After selecting above option its show Message Like

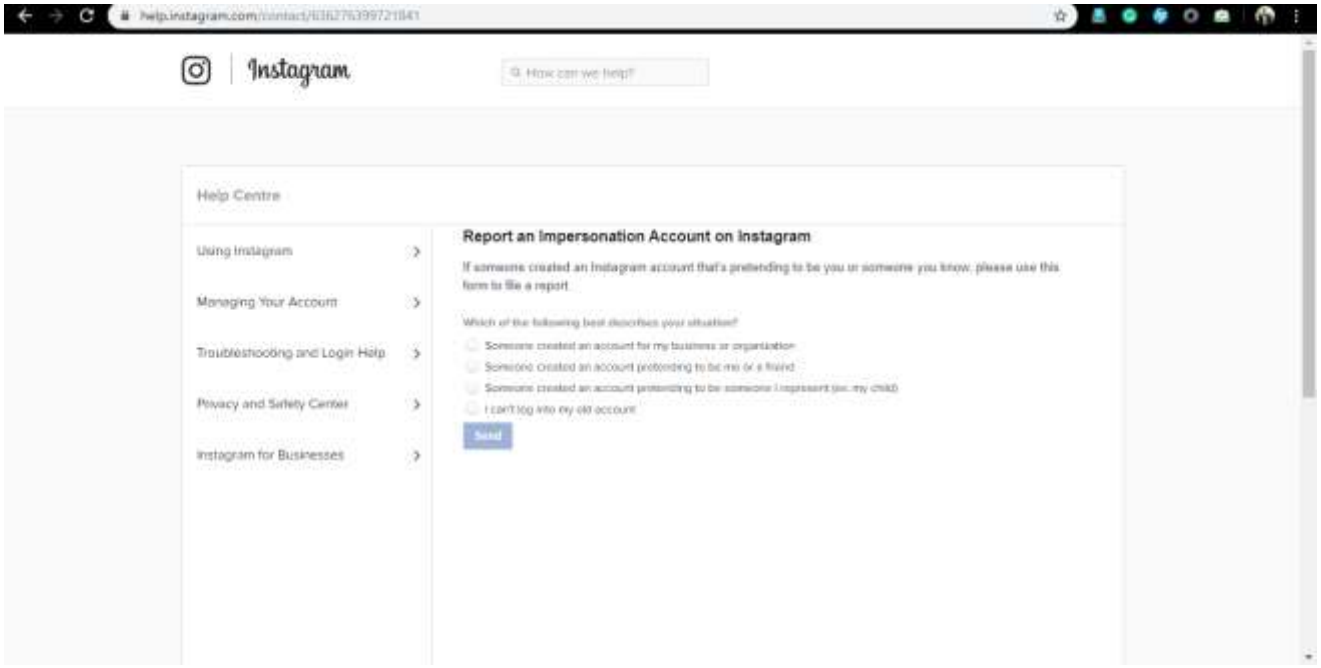
“Instagram” takes safety seriously. If someone created an Instagram account pretending to be you, you can report it to us. Make sure to provide all the requested info, including a photo of your government-issued ID.

If you have an Instagram account, you can report it to us from within the app, or by filling out this form. If you don't have an Instagram account, please fill out this form.

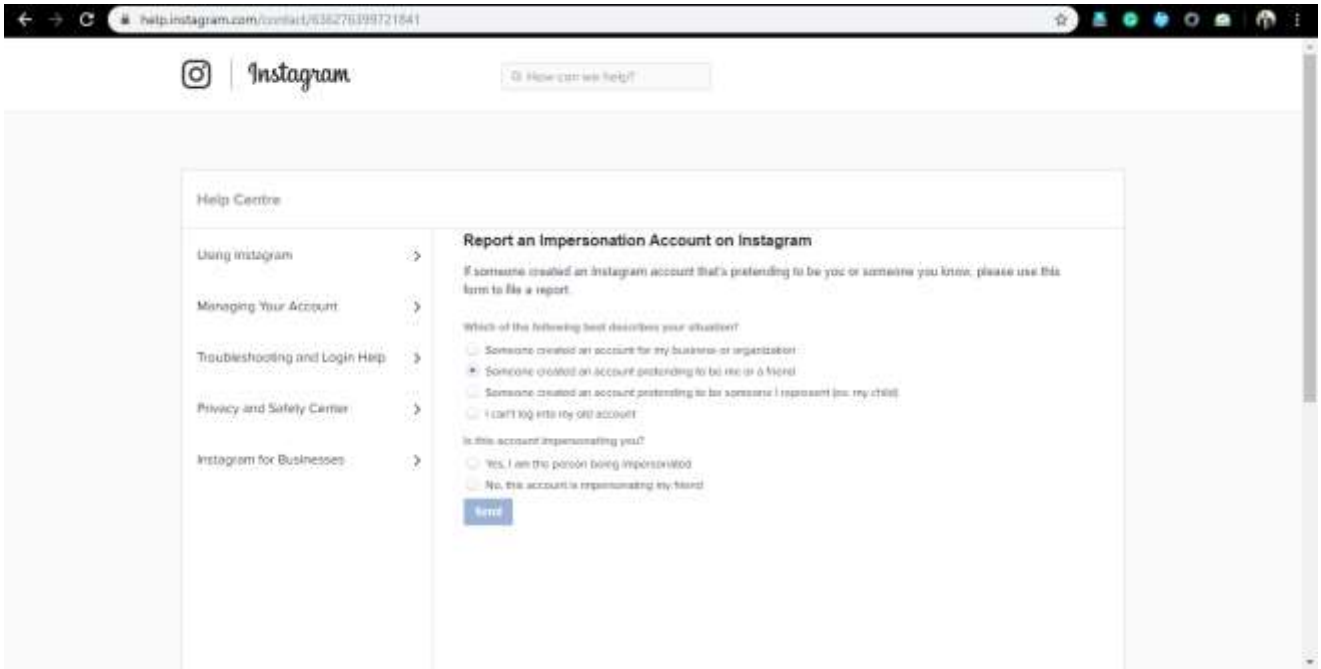
We only respond to reports sent to us from the person who's being impersonated or a representative of the person who's being impersonated (example: a parent). If someone you know is being impersonated, please encourage that person to report it.

If you're having trouble uploading a photo of your ID from a mobile phone, please try submitting this form from a computer.”

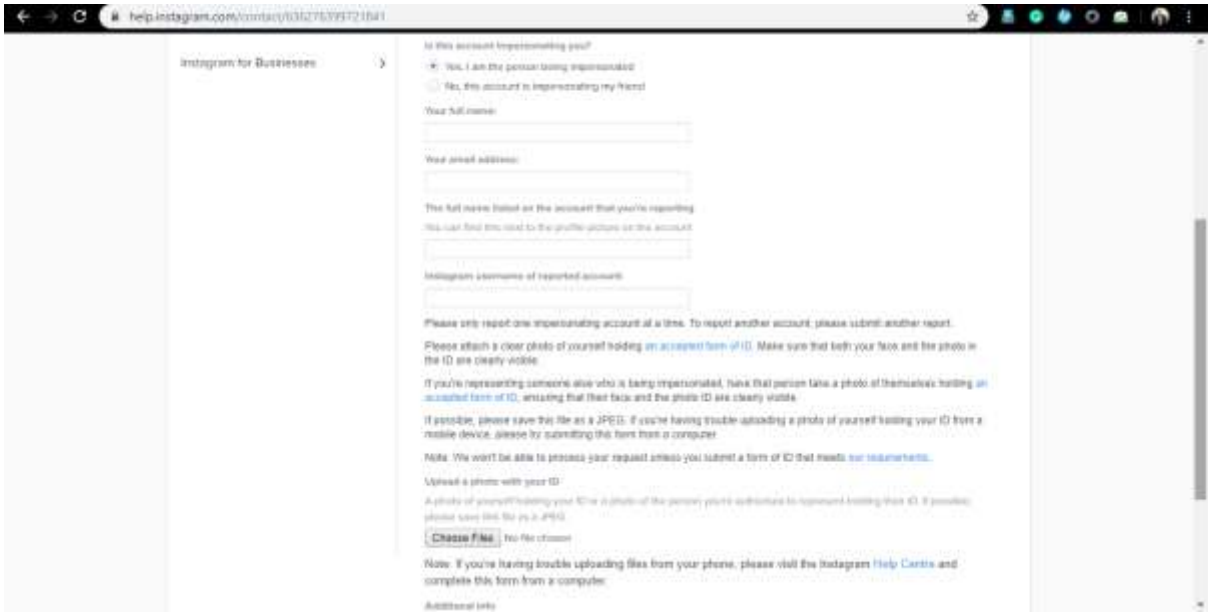
NOTE: ALWAYS CLICK ON SECOND FORM i.e. if you don’t have Instagram account, please fills out this form.



Step 4: - Select second option of **"Someone created an account pretending to be me or a friend"**



Step 5: - Select first option **"Yes, I am the person being impersonated"** and the fill the below form



Note: - Please only report one impersonating account at a time. To report another account, please submit another report.

Please attach a clear photo of yourself holding **an accepted form of ID.** Make sure that both your face and the photo in the ID are clearly visible.

If you're representing someone else who is being impersonated, have that person take a photo of themselves holding an accepted form of ID, ensuring that their face and the photo ID are clearly visible.

If possible, please save this file as a JPEG. If you're having trouble uploading a photo of yourself holding your ID from a mobile device, please try submitting this form from a computer.

Note: Instagram won't be able to process your request unless you submit a form of ID that meets Instagram requirements.

Step 6:- Click on Send Option, fake account will be deleted.

TWITTER

If a person sends you a tweet or replies to a tweet with a comment that you don't like, you can unfollow that person. To stop them from further contacting you, you can block them. If you receive unwanted replies or abuse or threats from someone on Twitter, you can report them direct to twitter **https://support.twitter.com/forms/abusiveuser**
You can protect your tweets so that people can only follow you if you approve them first. Do this by going into the 'settings' menu, then 'security and privacy' and ticking the 'protect my tweets' box.

To remove or block someone on Twitter, click on the button with a head icon on it next to the 'Follow' button on a user's profile. When you click on this you will see a menu with the options to 'block' the user to prevent them from seeing your profile and you can also 'report for spam', which will alert Twitter to any users who are abusing the service.

1. Go to the profile of the user you wish to report.
2. Select the  **gear icon.**
3. Select **Report** and then choose the type of issue you would want to report.
4. You can provide Twitter with more information about the issue you are reporting by selecting **"They're being abusive or harmful".**
5. Twitter will provide you with further recommendations once you've submitted your report.

SNAPCHAT

Bullying through Snapchat takes place in a number of different ways, including:

- Taking Screenshots of images without permission
- Sending pictures without permission
- Negative comments

If this happens to you, you can block a 'friend'.

- Tap the Menu icon
- Select 'My Friends'
- Locate their name in the list and swipe right across their name
- To delete them, press Delete

To block someone who added you on Snapchat:

- Tap **'added me'** on the Profile Screen
- Tap their name and tap the 'Wheel Icon' next to their name
- Press 'block'

This will prevent them from sending you Snaps or Chats or from viewing your content.

If a person is bullying or harassing you or you receive an inappropriate image, report it by completing their online form **https://support.snapchat.com/en-US/i-need-help**

To report something on Snapchat "Report a safety or Abuse issue."

1. Select the Snapchat icon at the top of the screen.
2. Select the **gear icon.**
3. Scroll down to "More Information" and select **Support.**
4. In the **search bar** type "Report"
5. In the drop down list, select **"Report a safety or Abuse issue."**
6. Under **"What can we help you with?"**, select **"I have a safety concern."**
7. Choose the type of issue you want to report.

YOUTUBE

If you feel a video you have seen on YouTube is inappropriate, you can 'flag' this by clicking on the little flag at the bottom right of the video. YouTube will then look at it to see if it breaks their terms of use. If it does, they will remove it.

YouTube state that videos with hate content, graphic violence or nudity cannot be uploaded so if you see one, report it as inappropriate.

To remove someone from your YouTube page, go to your account page and click on 'all contacts' in the 'Friends and Contacts' section. Choose which person you wish to unfriend and click on the 'remove contact'. Once you have done this, the person will no longer be on your 'share video' list.

If you receive abusive, bullying or threatening comments on YouTube, you can report them and they will investigate **https://www.youtube.com/reportabuse**

WHATSAPP

Legally, you have to be over 16 to use WhatsApp. As this is a messaging service, bullying can happen in many ways via WhatsApp. Once you install the App, it checks your address book and connects you automatically to anyone else you know who is using the App. You can block and delete a contact who may be bullying you through WhatsApp:

- Click on their name
- Using the dropdown menu, choose to 'block' the person.
- You can find out more by emailing WhatsApp at **support@whatsapp.com**
- Some Safety Information
- Keep it Private – don't post anything on a social networking site that identifies your real name, address, phone number, school etc. as this will enable a stranger to contact you in real life. Be careful you don't identify your friends too.

- Never upload anything that might embarrass you at a later date. Things you post on the Internet stay there and can come back and cause problems for you later on, for instance, when you go for an interview for college or university or apply for a job. If you're happy for the world to see the photo or comment, hit send. If you're not, don't upload it!!! Once you've hit send, you have lost control of that image or comment forever.
- With today's technology, many of us have a camera available at all times. Never feel pressurised into taking pictures of yourself that you wouldn't want others to see. Always trust your gut instinct over this. As before, once you hit send, you have lost control over that image and this can cause immense anxiety and stress.
- If you ever use a shared computer, whether it be at home, at school, a library or Internet café, never forget to log off once you have finished your session or when you close the browser. If you don't, the next user may be able to access the sites you have been using under your name.
- Many sites enable you to 'check in' or post your location each time you post a status update. Whilst this can let your friends know where you are, places you're visiting and things you might be doing, it can also mean that people you don't know can also view this information – especially if your profile is public. Go into the 'Settings' menu of the social networking site or app, scroll to the 'Security and Privacy' section and turn off or uncheck the 'location' box.

Keep yourself safe

- If someone makes you feel uncomfortable, embarrassed or afraid online, you need to tell someone immediately. If someone suggests meeting up with you in real life, again, tell someone immediately. This is a huge concern, especially if they have suggested you keep it a secret. No matter how much a person tells you about themselves, if you don't know them really well in the 'real world, they are still a stranger and may not be telling you the truth.

- There have been a number of cases of adults pretending to be young people online and trying to engage other young people in inappropriate activities. This is called 'Grooming' and is a criminal offence.
- Don't get into an argument or post offensive, bullying or abusive material online. Never post anything which promotes physical harm or make threats to anyone. Don't spread rumours or make up false information about a person and don't encourage others to harass someone. It is defamatory if you say untrue things about a person which can give them a bad reputation and it can also be seen as harassment – which is a criminal offence in the India.
- You are not allowed to upload a picture or video of anyone without their permission. Never set up a social networking site in someone else's name or upload false information about them.

Of course, all sites have a responsibility to keep their users safe and to ensure that all reports of cyber-bullying and abuse are dealt with effectively, however, we, as users of such sites, also have a responsibility to make sure we are using them in a safe, respectful and appropriate manner.

We have to increase sensitivity and awareness on gender stereotypes and sexisms online and changed attitudes towards prevention and elimination of cyber-crimes. And also improve knowledge of women and children on the prevention and protection of cyber-crimes.

Better capacity of women and children for prevention, protection and prosecution and for sensitive and appropriate reporting on cyber-crimes.

Improved knowledge and increased awareness of women and children, (potential) victims, groups at risk, parents, (potential) perpetrators and witnesses about cyber-crimes about the topic, risks, rights, available reporting and support services.

PART III

DIGITAL EVIDENCE

COLLECTION, PRESERVATION

AND HANDLING

Source of Digital Evidence

Storage medium - the disk, tape, CD, DVD, paper, or other substance that contains data

Storage device - mechanical apparatus that records and retrieves data from a storage medium

Removable Storage Media - floppy disk drives, external hard disk drives, CD drives, DVD drives, tape drives etc.

Smartphone and smart watch, pagers, digital devices like camera, GPS etc.

Characteristics of Digital Evidence

- It is often latent like fingerprints or DNA.
- It can transcend borders with ease and speed.
- It is fragile and can be easily altered, damaged or destroyed.
- Sometimes, it is time-sensitive.
- Many electronic devices contain memory that requires continuous power to maintain information, such as a battery or AC power.
- Data can be easily lost if the power source is unplugged or the battery is allowed to discharged.

Cyber Forensic Process Encompasses five Key Elements

1. Identification and acquiring of digital evidence.
2. Preservation of digital evidence.
3. Analysis of digital evidence.
4. Reporting the findings.
5. Presentation of digital evidence.

1. **The identification and acquiring of digital evidence:** Knowing what evidence is present, where it is stored and how it is stored is vital in determining which processes are to be employed to facilitate its recovery. In addition, the cyber forensic examiner must be able to identify the type of information stored in a format in which it is stored so that the appropriate technology can be used to extract it. After the evidence is identified the cyber forensic examiner/ investigator should image/ clone the Hard-disk or the storage media.

2. **The preservation of Digital evidence:** Is a critical element in the forensic process. Any examination of the electronically stored data can be carried out in the last intrusive manner. Alteration to data that is of evidentiary value must be accounted for and justified.
3. **The analysis of digital evidence** the extraction, processing and interpretation of digital data- is generally regarded as the main element of cyber forensics. Extraction produces a binary junk, which should be processed, to make it readable by a human being.
4. **Report the Findings** means giving the findings in the simple lucid manner so that any person can understand. The report should be in a simple terms, giving the description of the items, process adopted for analysis & chain of custody, the hard & soft copies of the findings, glossary of terms etc.
5. **The presentation of digital evidence** involves disposing evidence in the court of law regarding the findings and the credibility of the process employed during analysis.

Precautions while collecting Digital Evidence

Before collecting digital evidence, ensure that

- ❖ You have legal authority to proceed with the seizure.
- ❖ Scene of offence/ place of seizure is secured physically and electronically.
- ❖ Proper documentation is done.
- ❖ Appropriate personal protective equipment is used.

Collection of Digital Evidence

Procedure for Gathering Evidences from Switched-off Systems

- ❖ Secure and take control of the scene of crime, both physically and electronically.
- ❖ Make sure that the computer is switched OFF. Some screen saver may give the appearance that the computer is switched OFF, but the hard drive and monitor lights may indicate that the machine is switched ON. Some laptop computers may power ON by opening the lid.
- ❖ Remove the battery from laptop computers.

- Unplug the power and other devices from sockets
- Never switch ON the computer, in any circumstances.
- Label and photograph (or video graph) all the components in-situ and if no camera is available, draw a sketch plan of the system.
- Label the ports and (in and out) cables so that the computer may be reconstructed at a later date, if necessary.
- Open the side casing of CPU of laptop or desktop.
- Identify the Hard disk and detach it from power cables & motherboard.
- Record unique identifiers like make, model and serial number.
- Take signature of the accused and witness on the Hard disk
- Gather non-electronic evidence like diaries, notebooks or pieces of paper with passwords.

Procedure for Gathering Evidences from Live (Switched-on) Systems

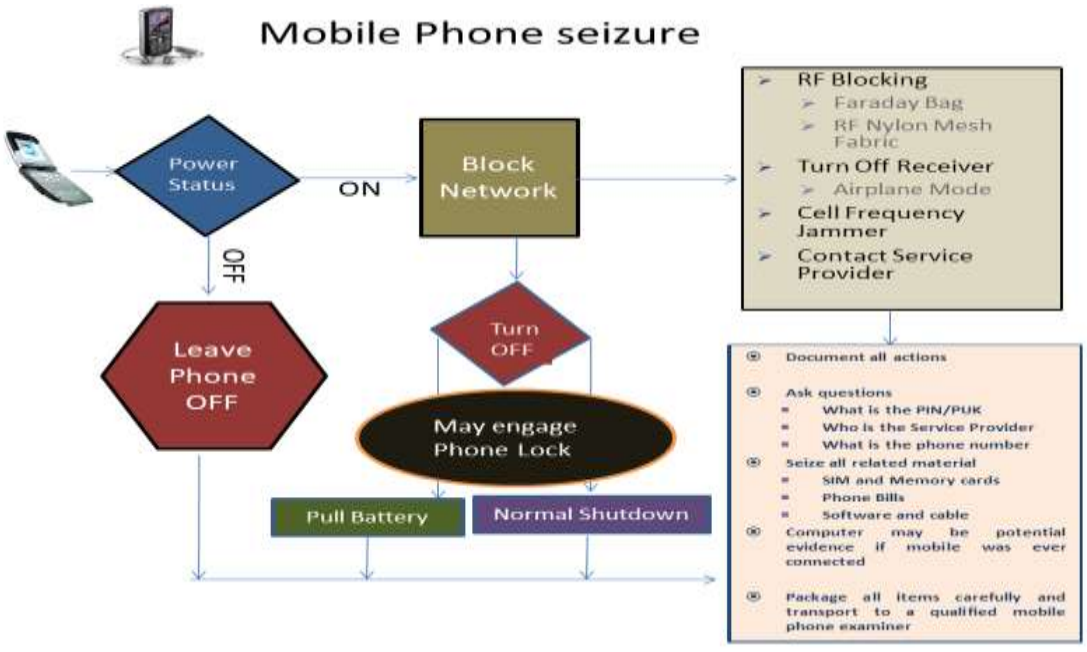
- Record what is on the screen by the photograph and by making a written note of the content of the screen.
- Do not touch the keyboard or click the mouse and if the screen is blank or a screen saver is present, the case officer should be asked to decide if they wish to restore the screen. If so, then a short movement of the mouse will restore the screen or reveal that the screen saver is password protected. If the screen restores, then photograph/videography and note its content. If password protected is shown, then continuous as below without further disturbing the mouse. Record the time and the activity of the use of mouse in these circumstances.
- Take the help of technical expert to use live forensic tool to extract the information that is present in the temporary storage memory like RAM.
- If no specialist advice is available, then remove the power supply from the back of the computer, without closing down any program. When removing the power supply cable, always remove the end attached to the computer and not the one attached to the socket. This will prevent any data being written to the hard drive if an uninterruptible power protection device is fitted.

Gathering Evidences from Mobile Phones

- If the device is "OFF", do not turn it "ON".
- If PDA or cell phone device may enable password, thus preventing access to the evidence.
- Photograph device and screen display (if available).
- Label and collect all cables (including power supply) and transport it with device.
- Keep the device charged.
- If device cannot be kept charged, then analysis by a specialist must be completed prior to battery discharge or data may be lost.
- Seize additional storage media (memory sticks, company flash, etc).
- Document all steps involved in seizure of device and components.

Benefits and uses of Faraday Bag while seizing mobile phones investigator:

- Potentially avoids the problem of the mobile phone becoming PIN/ PUK locked.
- Faraday Window enables the forensic examiner to view the phone in a "**faraday**" condition which gives an "immediate preview of evidence".
- Re-usable
- Prevents data from networks communicating with the device, thus preventing any chance of evidence being tempered with.
- Prevents any chance of evidence being manipulated during covert acquisition.

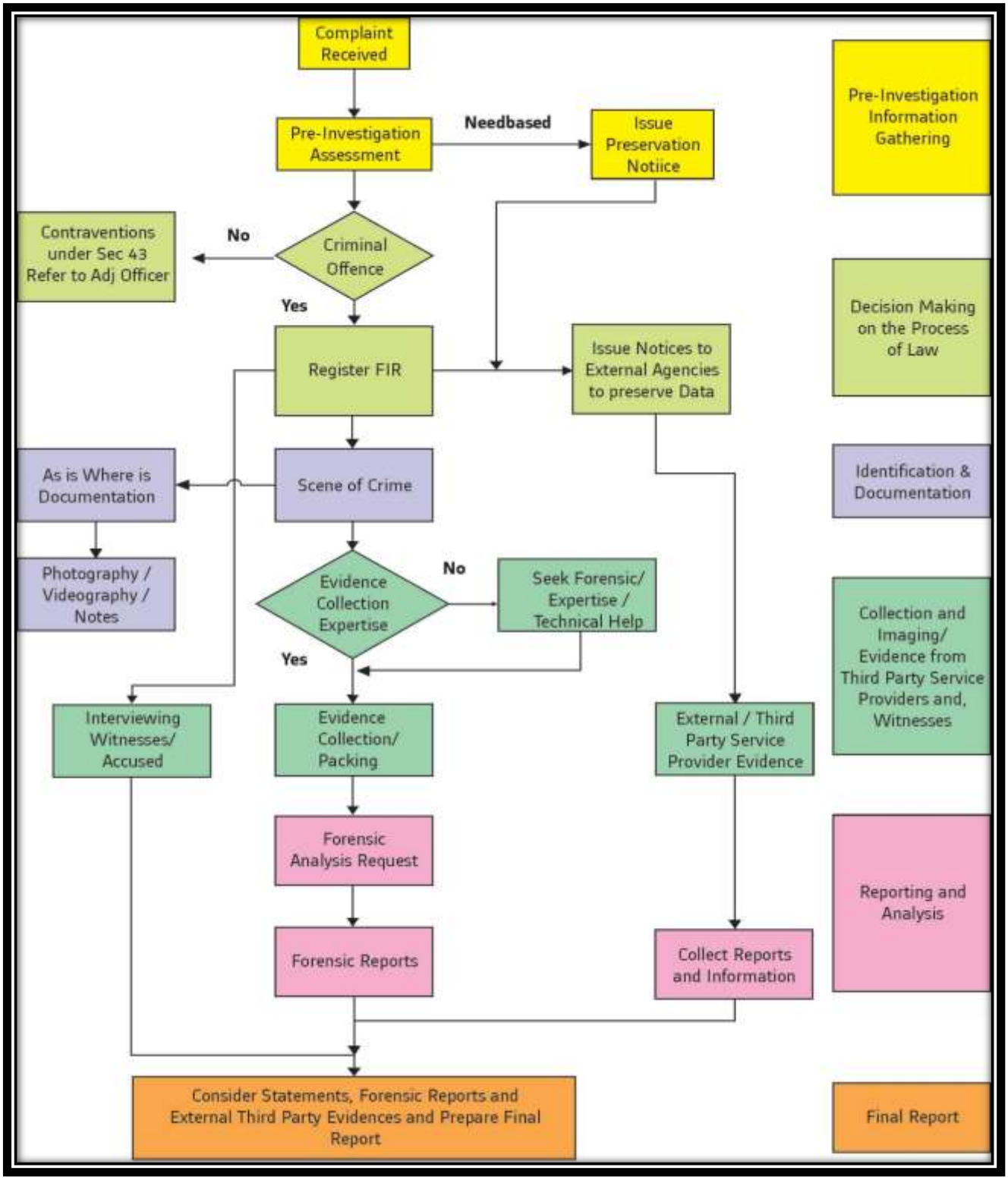


PART IV

STANDARD OPERATING PROCEDURE

FOR LAW ENFORCEMENT AGENCIES

Standard Operation Procedures - A Flow Chart



Flow Chart for Digital Crime Investigation Under ITAA 2008

Panchanama Seizure Memon & Proceedings

- Sec 80 of IT Act 2008 – Power of Police officer and other to enter search
- Ensure 2 Independent Witness and if possible technical person belonging to place of search to identify equipment correctly
- All equipment should be identified at scene of crime and mentioned in documentation
- Time/Zone Plays a crucial role. Make sure information is noted carefully from systems in ON mode and don't turn ON any device.
- Make sure Serial No is allotted to each device and noted in Panchanama, Chain of Custody and Digital Evidence form

Deposition of evidence in court

- IO should prepare well to exhibit the evidence in the court of law.
- All digital evidence should be presented as exhibits and introduce as evidence to establish the process used to identify, collect, preserve, transport, store, analyses, interpret, or reconstruct the information.

EVIDENCE PRESERVATION NOTICE

Date:

Crime Number:/Enquiry Reference: Sections of Law:

Police Station:

To,

Name
Address of the person to whom the notice is served.

Please refer to the case/enquiry mentioned above. The undersigned is investigating / enquiring in to the matter. As per the Complaint/ Investigations, it is learnt that/ established that, critical evidence in this matter exists in the form of electronic records contained in the computer systems of.....,

This is a notice to you and demand that such evidence identified must be immediately preserved and retained by you until further written notice undersigned. This request is essential, as a paper printout of text contained in a computer file does not completely reflect all information contained within the electronic file. This request is made as per the provisions of the section 91 Cr PC.

Additionally, the continued operation of the computer systems identified herein will likely result in the destruction of relevant evidence due to the fact that electronic evidence can be easily altered, deleted or otherwise modified. Failure to comply with the notice will make you liable for legal action as per IPC and other relevant laws.

- For purpose of the notice, "electronic record" has the same meaning as defined under ITAA and, shall include, but not be limited to, all text files (including word processing documents), spread sheets, e-mail files and information concerning email (including logs of e-mail history and uses, header information and "deleted" files), internet history

files and references, graphical image format (GIF) files, databases, calendar and scheduling information, computer systems activity logs, and or file fragments and backup files containing electronic data.

- Please preserve and retain all electronic records generated or received (relating to the enquiry) (give details).

- Please preserve and retain all electronic records containing any information about (the enquiry) (give details).

- You must refrain from operating (or removing or altering fixed or external drives and media attached thereto) standalone personal computers, network workstations, notebook and/ or laptop computers operated by (accused) (give details).

- You must retain and preserve all backup taps or other storage media, whether online or offline, and refrain from overwriting or deleting information contained thereon, which may contain electronic records identified above.

Please contact the undersigned if you have any questions regarding this notice.

(To be signed by the enquiry officer/ IO with official seal)

LOGO OF DEPARTMEMT

NOTICE: CRPC 91

OFFICE OF THE …….

CYBER CRIME CELL

ADDRESS ……

Letter No : ……./ …../……. Dated: - ……/……/20 XX

To,
COMPANY NAME
ADDRESS
PIN

Sub: - Request u/s 91 Cr.P.C for IP and relevant details.

Dear Sir,

……. Police station… …… India is investigating into a **Crime No. …...** under **Section …… of Information Technology Act**,

FULL CONTACT INFORMATION OF INFORMATION SEEKER	
Title and Badge Number	**Police Inspector, Cyber Crime Cell.**
Telephone Number & Extension	
Name	
Physical Address	
Email address	

SEEKING DETAILS OF:

PROFILE DETAILS	
Profile Name	
User ID Number	
Vanity Name (If applicable)	
Full URL to profile	

Known email address	
Period of activity From	

We hereby request to furnish information on following points:

1) Details provided at the time of creation the profile, including the email address including DEVICE INORMATION (IMEI NO, MAC) If Any
2) Full Details of Mode by which the account was activated. (If by SMS provide the Mobile number or if email link provide the email address, if other please specify in Detail).
3) IP addresses details (with ports) at the time of profile creation.
4) IP address details (with ports) for all the active sessions for period mentioned Aforementioned.
5) Changes made in Profile Id Details like Email, Phone Number etc.

Code of Criminal Procedure 1973

91- Summons to produce document or other thing

(1) Whenever any court or any officer in charge of Police Station consider that the any production of any document or other things is necessary or desirable for the purpose of any investigation, inquiry, trial or other proceedings under this Code by or before such court may issue a summons, or such officer or written order, to the person in whose possession or power such documents or thing is believed to be requiring him to attend and produce it, or to produce it at the time and place stated in the summons or order.

(2) Any person required under this Section merely to produce the document or other thing shall be deemed to have complied with the requisition, if he causes such documents or thing to produce instead of attending personally to produce the same.

(3) Nothing in this section shall be deemed

(a) To affect section 123 and 124 of the Indian Evidence Act 1872 (1 of 1872) or the bankers books Evidence Act, 1989 (13 of 1891), or

(b) To apply to a letter, postcard, telegram or other document or any parcel or thing in the custody of the postal or the telegraphic authority.

Your early reply in this matter will be highly appreciated.

Sincerely,

……
Police Inspector
……. Police Station
…….
INDIA

Digital Evidence CollectionFrom			
CrimeNumber:		Date:	
PS/Circle/SDPO:		Time:	
IO Name:		Item Number:	
Location:		Custodian/ Suspect: Name:	

Computer Information			
Laptop	Desktop	Manufacture	
HDD Only	External HDD	Model Number	
Others		Serial Number	
Time Zone		Asset tag	
BIOS Date and Time		Actual Date and Time	

Evidence Drive			
Acquired By		Date of Acquisition	
SignatureofI.O		Time of Acquisition	

Acquisition Information			
IDE	SCSI	Manufacture	
SATA	Other	Model Number	
		Serial Number	
		HDD Size	

Collection Details		Destination Drive Details	
Software used		Manufacture	
Version		Model Number	
Write Protect Device Used		Serial Number	
Verified By		HDD Size	
Image File Name			
Notes			

Forwarding Note

(In all cases where examination of any material is required at the laboratory, a copy of this form duly fi led in should accompany the exhibits.)

I. Nature of Crime

Case No...../ …….	Police Station -
Section of Law -	District -
Date - ...../...../	State -

Nature of Crime

.....

.....

Brief History.....

.....

Any Other relevant details

…….....

.

II. List Of Exhibits For Examination

Sr. No./ Barcode	Description of Exhibits	How, When and By, Whom Found	Source of Exhibits	Remarks

III. Nature Of Examination Required

Sr. No./ Barcode	Description of Exhibits	Nature Of Examinatio n Required	Date or any Key word or Filter	Remarks

IOs are advised to pay additional attention to this section, as this plays a critical component in the investigation. Apart from requesting the information required for the investigation like files, deleted information, etc., from the digital evidence, lot of other information, which can be developed as supporting (secondary) evidence in the investigations like login time, users list, various applications installed, IP address, printers connected, etc.

IOs are suggested to contact the forensic lab professionals to understand what kind of information can be retrieved from these digital media which can be vital evidence.

Sr. No.	Full Name	Occupation	Sex	Date and Time of Arrest	Whether bailed, Court or Police Custody

Seal	Rank and Sign. of I. O.
O/W No.	Date.....
Forwarded to the Director.....	
Specimen Seal/s/Impression/s On exhibits or Parcel/s	Sign and Designation Of Forwarding Officer

Certificate Of Authority

Certified that the Director.....

has the authority to examine the exhibits sent to him in connection with

Case No. ..... u/s.....

Pol. Stn ..... ……Date..... Of .....
State versus.....

Date:	
Place:	Sign and Designation of Forwarding Authority:

PART V

CASE STUDY OF CYBER CRIME AGAINST WOMEN

Avnish Bajaj vs. State (DPS MMS Scandal Case)

Avnish Bajaj vs. State

(2005) 3 CompLJ 364 Del

Key Words: Internet Service Providers (ISPs), Cyber Space, Criminal Liability, Director's Liability, Listing

FACTS:

The case involved an IIT Kharagpur student Ravi Raj, who placed on the baazee.com a listing offering an obscene MMS video clip for sale with the username alice-elec. Despite the fact that baazee.com have a filter for posting of objectionable content, the listing nevertheless took place with the description, "Item 27877408 – DPS Girls having fun!!! full video + Baazee points." The item was listed online around 8.30 pm in the evening of November 27th 2004 and was deactivated, around 10 am on 29th November 2004. The Crime Branch of Delhi police took cognizance of the matter and registered an FIR. Upon investigation, a charge sheet was filed showing Ravi Raj, Avnish Bajaj, the owner of the website and Sharat Digumarti, the person responsible for handling the content, as accused. Since, Ravi Raj absconded; the petition was filed by Avnish Bajaj, seeking the quashing of the criminal proceedings.

CONTENTIONS:

Petitioner

1. Since the MMS was transferred directly between the seller and buyer without the intervention of the website, they can at most be responsible for the listing placed on the website which by itself was not obscene and did not attract the offence under Section 292/294 IPC or Section 67 of the Information Technology (IT) Act.
2. Due diligence was taken by the website to immediately remove the video clip once it was brought to its knowledge that it was objectionable.

3. The scope of Section 67 of the IT Act is only restricted to publication of obscene material and does not cover transmission of such material.

State

1. Offence under Section 292 of Indian Penal Code (IPC) includes not only overt acts but illegal omissions within the meaning of Sections 32, 35 and 36 IPC.
2. The failure to have adequate filter in a system which is entirely automated entails serious consequences and a website cannot escape such legal consequences.
3. The fact that payment was made to the seller even as on 27th December 2004 shows that no attempt was made to prevent or stop the commission of the illegality by the website.

HELD (Delhi High Court)

The court observed that a prima facie case for the offence under Section 292 (2) (a) and 292 (2) (d) IPC is made out against the website both in respect of the listing and the video clip respectively. The court observed that "*[b]y not having appropriate filters that could have detected the words in the listing or the pornographic content of what was being offered for sale, the website ran a risk of having imputed to it the knowledge that such an object was in fact obscene*", and thus it held that as per the strict liability imposed by Section 292, knowledge of the listing can be imputed to the company.

However, as far as Avnish Bajaj is concerned, the court held that since the Indian Penal Code does not recognize the concept of an automatic criminal liability attaching to the director where the company is an accused, the petitioner can be discharged under Sections 292 and 294 of IPC, but not the other accused.

As regards S. 67, read with Section 85 of the IT Act, the Court however, observed that a prima facie case was made out against the petitioner Avnish Bajaj, since the law recognizes the deemed criminal liability of the directors even where the company is not arraigned as an accused. The judgement however did not declare Avnish Bajaj guilty.

IT ACT	Information Technology Act 2000/2008 (Amendment)	PUNISHMENT
65	Tampering with Computer Source Code	3 year &/or fine upto 2 lakh
65 B	Admissibility of Electronic Records	Indian Evidence Act
66	Hacking	5 lakh/ 3 year
66 B	Stolen Computers etc.	3 year & or fine upto 1 lakh
66 C	Identity Theft and Personation	3 year & fine upto 1 lakh
66 D	Punishment for cheating by personation by using computer resource	3 year & fine upto 1 lakh
66 E	Violation of Privacy	3 year &/or fine upto 2 lakh
66 F	Cyber Terrorism	Life time
67	Publishing Obscene Material	1. 3 year & 5 lakh 2. 5 year & 10 lakh
67 A	Publishing Sexually Explicit Act	1. 5 year & fine upto 10 lakh 2. 7 year & fine upto 10 lakh
67 B	Publishing Child Pornography	1. 5 year & fne upto 10 lakh 2. 7 year & fine upto 10 lakh
67 C	Prevention and retention of information by intermediaries	3 year/fine
68	Non-compliance with Controller's Order	2 year & or 1 lakh
69	Failure to Decrypt Information	
69 A	Blocking and Interception of Information	7 year & fine
69 B	Power to authorized to monitor & collect traffic data or information through any computer resources for cyber security	3 year/fine
70	Accessing Protected System	10 year and fine
70 B	Service provider fail to provide data	1 year/fine

71	suppresses any material fact Penalty for Misrepresentation or	2 year & 1 lakh
72	Breach of Privacy and Confidentiality	2 year &/or fine upto 1 lakh
72 A	Punishment for disclosure of information in breach of lawful contract	3 year/fine
73	False Certificates	2 year &/or fine upto 1 lakh
74	Publication for Fraudulent Use	2 year &/or fine upto 1 lakh

PART VI

WOMEN SAFETY APPLICATION

WOMEN SAFETY APPLICATIONS

Technology has reduced the complexities of life and has given immense power to people by allowing everything within the reach of their hand. Connecting with people is just a click away bringing the other person near to you, virtually. Your peers can reach out to you easily from anywhere around the world. In accordance to this, our government is working constantly to provide every service to the people easily within their reach using different platforms. The Digital India initiative fuelled this approach further.

In addition, technology, too, has got our backs, with several apps released for women to protect themselves. Here are some of the best safety apps for women in India.

App	**Download**	**Rating**
Life360-Family Locator	50,000,000+	4.5
bSafe	500,000+	3.7
Watch.Me	100,000+	3.8
Shake2Safety	100,000+	3.7
Himmat Plus	50,000+	4.4
My SafetyPin	50,000+	3.9
Smart24x7	50,000+	3.0
Raksha	10,000+	4.4
Chilla	10,000+	4.2
Rescuer	5,000+	4.4

1. **Life360**-Family Locator

With Life360 you can Create your own private groups, called “Circles,” of loved ones, teammates -- whoever matters most and chat with them in Family Locator for FREE.

View the real-time location of Circle Members on a private family map that’s only visible to your Circle. Receive real-time alerts when Circle Members arrive at or leave destinations (Eliminate disruptive “Where are you?” texts)

Works on both Android Phones and iPhones

Real-Time Location Sharing Stay connected and in sync with your entire family and eliminate the multiple texts needed to coordinate your family events and daily life. Family Locator alerts you when your family members have checked in at a location and thanks to GPS sensors in your phone, family locator can also advise if someone is running late.

Life360 Family Locator app on your phone, and invite your family. Once registered, each member appears as a unique icon on the navigational map so you’ll know exactly where they are. No need to send annoying “Where are your?” or “What’s your ETA?” texts, the Life360 Family Locator puts this information at your fingertips. And to make life super easy, app send you alerts the moment your family arrives at an appointed location!

Location - Life360 locates you on a shared, private map. This setting allows us to show location accurately and quickly.

Phone permission - Life360 has a feature called Driver Care Support that, with a single push of a button, connects you to a live representative over the phone. Our live representative knows who you are and where you are to assist in roadside situations such as tows, jumps, and lockouts. This app also offer an immediate emergency response in the case of a vehicular collision. Phone permissions allow us to connect your phone to the live representative and authenticate that you are the one calling them.

Network - This connects you to the Internet and allows us to send and receive location information to and from family members on your private map.

2. **bSafe**

bSafe is an all-encompassing safety app for women. bSafe is the most advanced and reliable personal safety app that allow you to create your own security network and take care of each other.

Be a guardian to others: Receive SOS alarms when ones are in trouble. View location on the map when they need you to walk them safely home

Get help yourself: Send SOS signal to your guardians by pressing a button or saying a key phrase. This app is designs as it Stream and automatically record emergency video. You can ask friends to follow you on the map when you feel insecure and can also tell where to pick you up by sending your exact location

Get an excuse to leave an unpleasant companion by receiving a fake phone call, Personal Safety App / Emergency Alert / SOS app. Its works even on locked screen and also works even when there is no internet connection. Its provide facility that you can use without registration and root.

Himmat

This is a free safety app that is designed by the **Delhi Police**, primarily for women in the capital. To use the app, users need to register in, then a registration key (OTP) will be received that must be entered to complete the app configuration. The key to its operation is the ability to send your exact location along with audio-video of the surroundings to the Delhi Police Control Room expeditiously, when an SOS alert is raised by you. It is available in two languages- Hindi and English.

My Safetipin

My Safetipin app is an exceedingly useful map-based safety app that makes navigation safe and easy. It basically rates the safety of the location – red pin on the map indicates

'unsafe' area, green colour is for 'safe', and amber for 'less safe'. In addition, it tells you about the public transport availability in the area, whether there is a police station, pharmacy or ATM nearby, how crowded the location is, as well sharing your real-time location via GPS tracking, with your loved-ones. It also allows users to pin unsafe locations and help others. This app is available in three languages- English, Hindi and Spanish.

Smart24x7

Designed for the safety of the women and senior citizens, Smart24x7 is linked directly with several state's police. It's simple and easy to use. There is a PANIC button, which when pushed, instantly sends an alert to all the numbers you put on the emergency contact, as well as the police. The app also starts recording video and audio when you are in a panic situation and shares it with the police. The alerts are generated via GPRS. But in case GPRS stops functioning, location and alert message are sent via SMS. Another impressive feature, Smart24x7 offers call centre support that offers a range of emergency services, such as ambulance and fire service. It's a keeper!

Raksha

This is definitely the most important app that every woman in India must have. When you need real help, Raksha sends an alert message along with your location to your contacts at the press of one button. Another added advantage is that even if the app is not working or switched off, you can still send an alert by pressing the volume key for 3 seconds.

Shake2Safety

The simplest and easiest app for women is Shake2Safety that just requires you to shake your smartphone or simply press the power button four times, which will send an emergency SOS message or place a call instantly to the registered numbers. The best

part, it can work with no internet connection and locked screen on. Besides working as a safety app, it also allows you to report robbery, accident or any natural disaster.

Shake2Safety is a SOS app that lets you send text messages to emergency contacts, share picture with location and record audio in emergency situations. All this happens by just shaking the phone or pressing power button 4 times.

Alert your family members and friends in an emergency situation with this app. Some of the features are sending multiple text messages with location to different numbers saved as emergency contacts by shaking your phone or pressing power button 4 times. It can also sending picture of emergency situation with location to a contact using shareable media. It can Recording a 4 second audio in your device. You can know your current location by just clicking the button at top right corner of the app.

Siren button.

Go to preferences in settings to set the Sensitivity (between 10 to 25 for most phones) to avoid sending text message, call or share picture by mistake. Now you can send a Picture of the emergency situation with location to a contact.

You can also send picture to a contact using multimedia messaging or MMS via Hangout etc. Enable or disable photo sharing from preferences in the settings menu. Saves a 4 second audio recording during a SOS event. Enable or disable this feature from the preferences. Enable or disable power button or shake feature from the preferences.

Use this application in case of emergency like accident, harassment, robbery, abuse, natural calamity, bullying, terrorist attack, medical emergency, airplane mishap, domestic violence, natural disaster like earthquake, tsunami etc

Material design and easy to use interface.

* Manually restart the app after the phone is switched on from off position.

* Now you can activate the app in the settings menu

* Shake detection is ignored after 10 seconds.

* For call and text message/SMS standard carrier charges may apply. If you have unlimited text message then no charges may apply.For sharing picture your Data charges may apply if your phone is not in free WiFi range.

Note -> The sensitivity shown is in reverse order. This means 5 sensitivity is too high and by a little shake the app is activated and 100 is lower that means you have to shake too much to activate. In simple terms it is the other way round.

* For location please keep your GPS on. When there is no Wi-Fi, GPS or mobile data then no location goes with the message/picture. Also it gives your last location if GPS is off.

My Safetipin is a Personal Safety app that helps you make safer decisions about your mobility, based on the safety score of an area. Safetipin calculates the safety score of a place based on 9 parameters, and your contribution allows us to continuously update the data to reflect how people feel in a place. Do let us know how safe you feel by doing a safety audit or sharing your feeling.

Safetipin collects primary data on women's safety in public spaces at night, on the basis of 9 parameters.

Lighting – Availability of enough light to see all around you

Openness – Ability to see and move in all directions

Visibility – Vendors, shops, building entrances, windows and balconies from where you can be seen

People – Number of people around you

Security – Presence of police or security guards

Walk Path – Either a pavement or road with space to walk

Public Transport – Availability of public transport like metro, buses, autos, rickshaws

Gender Usage – Presence of women and children near you

Feeling – How safe do you feel

Planning to go out for the evening? Check how safe a neighbourhood is, by tapping the place on the map. You will see the safety score for that area.

You can share your location with a friend or family member and they will get notifications if you enter an area with a low safety score, if you divert from your intended route or if you are stationary for extended periods of time.

You can find the safest route from one place to another, based on the safety score. Once you select the route you prefer, the control will be transferred to Google maps so that you can reach your destination safely.

You can view the cafes, shops, markets, hospitals etc., near you and find a comfortable place to wait in case you are in an unsafe area. This feature is great when waiting for a cab or for someone to come get you.

Changing your home? Visiting a new city? My Safetipin will help you make the safest choice.

If you are in a place with no safety score and are interested in using My SafetiPin, do let us know. We will get back to you when we have data about your city.

Smart24x7 has introduced a personal safety & security app for personal & business use that alerts emergency contacts with your GPS location. This is a unique approach towards strengthening citizen security, You can now also help others by pressing the button on your mobile.Our app is currently supported by Gurgaon Police, Jalandhar Police,Chandigarh Police, Jammu Police, Mohali Police, UP Fire Services(Lucknow & Noida).

Smart24x7 enables the old cities to turn Smart City.

This application can also be used by Senior citizens to secure them when they are in distress by sending SOS signals to their loved ones.

See Our App in Work:

http://www.youtube.com/watch?v=a7PJuEBStgU

http://www.youtube.com/watch?v=C_b8zWXwAto

*Key Features

Panic Alerts will be sent to the loved ones whenever user presses PANIC Button during emergency.

If GPRS is not working alert will be generated via SMS.

You can get instant help from nearest Police, Hospitals, Fire.

Use Fake Call feature to walk out of any difficult situation.

Smart24x7 Application does voice recording, photographs during the panic Situation & transfers to the police.

24x7 Call center to assist you in emergency.

Tracking of Primary Contact while in emergency.

Share Travel alerts with your loved ones & Social Network.

Basic chat to communicate with Friends.

Tracking of Service Providers location Ambulance, Police and Fire.

Maid/Servant Registration with Police is simplified

Improve battery life

New features- On the way to Office/Home to inform your loved ones about your status.

Whenever you are in emergency Just follow three easy steps :-

1) Press the Panic button.

2) Select the type of services required.

3) Click Submit and you are done.

In today's trend, we are continuously worried about the security of our child, daughter, wife, and mother and of course complete family. If they go somewhere we are continuously thinking about them and we don't know if any problem suddenly comes up with them so in that case, we are unable to do any kind of action on it. But now RAKSHA is here for solving all your troubles.

In Raksha app, we completely understand the situation occurring with your dear ones. By using this application you can check where they are right now. We have used GPS tracking system in the application and if someone clicks on "Are you in trouble?" button it sends the message on registered no's with the current location of the user of the app.

★ "Chilla" is the most powerful personal safety app ever developed . It is the first app which can detect detect woman scream .

"Chilla" is a personal safety & security app that can be triggered by just a shrill scream It totally removes the hassles of unlocking the phone or opening the app. It has been found that in cases where someone follows a girl / women or eve-teases her , she generally doesn't calls out to parents or police and if they attack her , the app is of no use to her then. In that situation scream is a natural reaction and tapping that is the best possible way to bring her help.

The app can be triggered by:

Scream / loud shout (should also be shrill enough)

Pressing power Button 5 times

After Trigger, it does the following

Sends SMS with location

Automatically places a call

If a scream is detected the app automatically unlocks the phone and places a call to the guardian.

The power button feature works even if the app is not on.

It virtually acts as your personal guardian angel when you are in distress and goes a long way in ensuring your personal safety .Not just the safety of women, the safety mode can be additionally customized to cater to the safety of men too. Besides, the app can be used in case of emergencies too, for example during a heart attack, the victim's location and recording can be immediately sent without unlocking the phone (just by pressing the power button). It can also be used in case of any sudden attack or thug or when there threat to personal safety as one can just silently put his hand in pocket and press the power button to send out alerts .

The best part is, Chilla (safety app) is made for the sole motive of helping women lead freer and safer lives. A revolution in field of personal security, Chilla is your ultimate safety app, install it today and put your safety in your own hands.

Other functionalities

Can send SMS and place automatic call even in no Internet Zone

Automatic dial number can be of police for immediate police contact

Remembers last location

No need to even unlock the phone in case any emergency

Its is helpful with Eve teasing , rape, Medical Emergency , Panic attack , sudden attack, unknown Threat (vithu). It can even call ambulance in emergency (with automatic call set to ambulance)

Does not track you when you are not in danger

Extremely small size app : 2 Mb

auto call ambulance , call police

★ The app is listed on Ministry of Communication and IT website , India ★

https://apps.mgov.gov.in/descp.do?appid=1065&param=citizenapps

Find the latest news about the app on its facebook page :

https://www.facebook.com/ScreamAlertapp/

The app was also showcased in Indian national tv new channel IBN7, shabaash India show as best safety app for women ever developed (this app has triggered news a lot)

https://www.youtube.com/watch?v=xTqRY0cSMas

We wish there will be no rape news after this app. This is the best app in category of apps for women.Feel safer with this app in your pocket . This safety app can be used along with some other women safety apps like Vithu (v gumrah) , my Safetypin (personal safety app) , ridesafe - (Travel safety app), himmat , safety razor.

We believe that apps are better way to prevent rape , molestation and crime against women in comparison to safety devices like pepper spray ,safety shoes , safety boots etc. bcz device like these can be used against the women (safety) and phone is always withu.

Just download this savior personal security app and don't forget to tell your relatives and friends about this wonderful app and help fight against rape and molestation.

Ever felt unsafe on your way from work? Wanted to let a friend know you're uneasy without anyone around you noticing? Ever tried to call for help without having to reach for your phone?

With personal safety assistant Rescuer, those days are over. Rescuer makes it easy for you to feel safe and connected no matter where you are — without even having to touch your phone. Your loved ones can contact Rescuer any time to make sure you're safe, and if there's an emergency, Rescuer will make sure they're the first to know. Rescuer has four life-saving features:

1. Voice recognition: Say your customized key phrase, and Rescuer will hear it, even your phone is locked away in another room. Rescuer then immediately sends out emergency messages with your GPS coordinates and pictures of the crime scene to your pre-set emergency contacts.
2. Volume button toggle: Silently call for help by pressing your phone's volume buttons to send emergency messages to your contacts. Rescuer will send them your coordinates and photos of the emergency without you having to utter a word.

3. Remote Location Tracking: Allow your worried loved ones to send a quick text to Rescuer to find out your location and safety status -- no more forgetting to let your friends know you got home safe. Rescuer does the job for you!
4. Quick access help widget: Already have your phone open? Just press the giant red help button on your home screen and emergency messages and pictures of the crime scene will be sent in no time.

When it comes to your safety, you should never have to settle. Whether you're in a life-threatening emergency and can't reach your phone or just don't feel safe, Rescuer has your back. Rescuer is FREE for a limited time, so start living safer today!

For any inquiries, questions, comments, or concerns, please email curlybraceapp@gmail.com. We love hearing from you!

Rescuer Website: https://sites.google.com/view/rescuer/home

Rescuer Privacy Policy: https://sites.google.com/view/rescuerprivacypolicy/home

By installing Rescuer, you agree to the Terms and Conditions: https://sites.google.com/view/rescuertermsandconditions/home

Rescuer, and all of its corresponding functionalities, are patent pending and 100% proprietary. All rights belong to the owner.

Rescuer has most recently been featured on Gadget Review (www.gadgetreview.com), mscareergirl (mscareergirl.com), and JohnnyJet (johnnyjet.com).

Keywords—Free, lifesaving, emergency response, 911, GPS, accurate location, friends, family, loved ones, parents, children, friend, kids, emergency assistant, personal tracking device, students, safely walk, campus, justice, parental safety, police, fire department, car accident, crash, signal, help, mother, father, 911, emergency response, alone, follow, alarm, alert, rescue, protect, safe, rescuer, rescue me, sos, button, signal, send friends, call, cell, cheap, communicate, respond, text message, contact, control, convenient, fast, coordinates, save lives, send, device, directions, distress, emergency, evidence, emergency texts easy, GPS, handheld, location, maps, google map connected,

no wifi, mobile, panic, locator, phone, official, voice, voice recognition, emergency alert system, speak to send, voice emergency, volume buttons, volume, emergency response volume buttons, volume button automation, widget, emergency family, automated, life-saving app, SMS response, parental, location send back, location text response, qualified contacts, call 911, distress signal, voice recognition 911, popular, protect, reliable, report, safety, track through text, sos, children, preschooler, kindergarten, elementary school, high school, children, emergency alert, college, men, women, security, smartphone, SMS, free family app, SOS, police signal, surveillance, GPS tracking, no wifi, TXT, usage, user-friendly, fast, easy, emergency phone locator, free, send location in emergency, walk, night, 2017, campus, sketchy, shady, sos button, jogging, safety, women