



# WHAT TO DO WHEN SOMEONE IS IMPERSONATING YOU ONLINE

LAST UPDATED JULY 2025

## AUTHOR'S NOTE

It's important to remember that this can happen to anyone and that you are not to blame for someone else's malicious intent.

This resource is intended to provide ways to navigate this situation and help you make decisions. It addresses actions that can be taken on Facebook, Instagram, Whatsapp and Bumble specifically.

Sometimes this can be a hard fight and can impact one's mental health as well. We recommend to reach out to people you trust and organisations which can help or support you if you are in such a situation.

You are not alone and there are people who care about you, including us.

# SECURE YOUR ACCOUNTS

Before you begin to take action against impersonation. It's important to secure your accounts.

- Please change your passwords on personal social media, communication and financial accounts to a stronger password. Here is an example of a how to create a stronger password -

<https://youtu.be/aEmF3lylvr4>

This will prevent further access to your accounts or information to your abuser incase they have any access to these.

- If you have lost access to your account , we recommend that you try recovery and if that fails, please check the section below on reaching out for additional support.
- Add more recovery options to your account and remove any potential recovery options that may be controlled by the abuser
- Add login notifications to your account to know if someone else has logged in.
- Add a two factor authentication (eg authenticator or passkeys) to your account

# CHECKING FOR COMPROMISED ACCOUNTS

To further secure yourself. Look at any accounts that may be compromised and secure them.

- To check for compromised accounts and emails this site is a useful resource:

<https://haveibeenpwned.com/>

- Looking for impersonating accounts on social media

<https://whatsmyname.app/>

# DOCUMENT ALL INSTANCES OF IMPERSONATION

Documentation of impersonation would be useful for taking legal action against someone. You can also get your friends to work with you on this since it might be hard to do it by yourself

- Screenshot all the instances of impersonator profiles with time stamps
- Screenshot and record any interactions that you can access with time stamps
- Record the profile links
- Note down any identifying information
- Screenshot stolen pictures and download videos

# REPORTING ON PLATFORMS

If you find an account impersonating you

## **Bumble:**

Users can report a matched profile as fake on Bumble. This also works if you unmatch them too -

<https://bumble.com/en/help/how-can-i-report-a-fake-profile>

## **Facebook:**

Facebook users can report fake profiles here -

<https://www.facebook.com/help/174210519303259>

Non Facebook users can report fake profiles here -

<https://www.facebook.com/help/contact/295309487309948/>

## **Instagram:**

Users can report scams here -

<https://help.instagram.com/165828726894770/>

In case Instagram and Facebook do not provide a satisfying resolution one can also appeal on Meta Oversight board -

<https://www.oversightboardappeals.com/>



**Whatsapp:**

Users can report here -

<https://faq.whatsapp.com/1142481766359885/>

Grievance Office Contact for escalating reports

[grievance\\_officer\\_wa@support.whatsapp.com](mailto:grievance_officer_wa@support.whatsapp.com)

Most platforms have trusted partners\* who can offer more support for such circumstance. It is recommend to find a trusted partner who can help you through the reporting process.

---

***\* trusted partner is a organisation chosen by platforms to support people resolve issues on platforms by providing access escalation and direct communication with platform policy teams.***

# GETTING VERIFIED

To further protect yourself from impersonation consider getting verified accounts on the platforms you use.

## **Verification - Instagram and Facebook**

<https://www.meta.com/en-gb/meta-verified/>

## **Verification - X ( Formerly Twitter)**

<https://help.x.com/en/managing-your-account/about-x-verified-accounts>

## WHAT DOES THE LAW SAY ?

Here are some of the provisions of law that would apply to impersonation. But we recommend consulting a lawyer to find provisions and tactics which better suit your case.

- Section 336 of the BNS concerns Forgery. This refers to the act of creating a false document or electronic record where there is intent to cause harm, deception or support fraudulent claims. Penalties include imprisonment for up to seven years and fines.
- Sections 318 and 319 of the BNS refer to cheating, and Section 318 includes dishonest concealment of facts as deception. Section 319 defines cheating by impersonation as the act of deceiving someone by pretending to be the identity of oneself or another person.

Knowingly substituting one person for another, or misrepresenting, fits under the category of impersonation. Penalties include **imprisonment for 5 years, or with fine, or with both.**

# CYBER CRIME PORTALS

National Cyber Crime Portal

[www.cybercrime.gov.in](http://www.cybercrime.gov.in)

Cyber Crime Helpline – 1930

If the police station refuse to register one can also call the cyber crimes department to report at state level

[https://cybercrime.gov.in/Webform/Crime\\_Nodal\\_GrivanceList.aspx](https://cybercrime.gov.in/Webform/Crime_Nodal_GrivanceList.aspx)



## CREDITS



**CC-BY-SA-NC 4.0.**

This was created by Chinmayi SK (2025) and is licensed under CC-BY-SA-NC 4.0.

For usage of this document, please contact - [theteam@thebachchaoproject.org](mailto:theteam@thebachchaoproject.org)

## ILLUSTRATION

@tactooncat

## CONTRIBUTORS

V - Editor and Reviewer  
Tania - Reviewer  
Meenakshi - Reviewer  
Gem - Reviewer  
M - Designer