



# IS THIS REAL?

## HOW TO IDENTIFY FRAUD ONLINE 101

LAST UPDATED JULY 2025

## AUTHOR'S NOTE

Identifying fraud is always tricky because the methods of fraud keeps evolving.

If you have been a victim of fraud, remember to be kind to yourself as the frauds are increasingly becoming hard to detect. In **2024**, over **740,000** complaints of scams were registered through **the national cybercrime platform**.

This document will help you with some basic guidelines and tools to detect fraud, but is not a comprehensive list. Do reach out to an expert if your needs require it.

# COMMON FRAUD ONLINE

- **Financial Fraud:**  
Where a person resorts to coercion or blackmail to extort money.
- **Identity Fraud:**  
Where a person/ group resorts to various means to obtain personal information with an intention to use their identity for other purposes. This includes usage for impersonation and other crimes.



01

**WHAT CAN BE  
DONE TO PREVENT  
FRAUD ?**

# VERIFICATION OF IDENTITY OF THE CONTACT

- If you suspect a fraud consider checking the identity details on suspect registry of National Cyber Crime Reporting Portal. Though limited to registered complaints it could still be useful in checking for reported fraud accounts and numbers.

[https://cybercrime.gov.in/Webform/suspect\\_search\\_repository.aspx](https://cybercrime.gov.in/Webform/suspect_search_repository.aspx)

- Check for similar frauds online through a broad search on search engine and specific portals like Reddit.
- Verify identity using platform verification methods. Note: Platform verification methods can be biased and could be potentially infringe on a person's privacy. This is the one means to verify a potential fraud.

a. Bumble's platform verification:

<https://bumble.com/the-buzz/request-verification>

- Verify the identity of the contact offline
  - a. Check to see if there are any mutual acquaintances and obtain their verification and if there is a network of trust.
  - b. If it is on a dating website request to meet in person in a public space and/or with trusted people around
- If there is an image of the contact consider using [Google Image Search](#) or [Tineye](#) to do a reverse image search.

# PROTECTING YOUR INFORMATION

- Don't share your account details (including passwords, phone number and even account ids ) with strangers!
- Ensure security of your accounts
  - a. Change password frequently and use strong passwords.  
**Here is an example of a stronger password**  
<https://youtu.be/aEmF3lylvr4>
  - b. Add recovery email and phone numbers to your account and check them on regular basis. Download recovery keys (where available)
  - c. Download recovery keys if that is an option provided by your platform.
  - d. Turn on login alerts for your account
  - e. Enable two factor authentication and use passkeys where possible.

# IDENTIFYING A PHISHING ATTEMPT

- Carefully check the sender of the message: if there are spelling mistakes or unknown website links or phone numbers sending you the messages. Do not open any links.
- If the phishing email is pretending to be a friend or a known organisation, then contact them another way (e.g. phone) to verify that the email came from them.
- Most phishing emails are impersonal and usually have a sense of urgency. Any messages which uses a tone of urgency or alarm should be carefully examined.
- Here is a quiz you can take to help you learn to identify phishing - <https://shira.app/>

**Disclaimer:** Phishing is getting complicated these days, so in case you can't determine if something is legitimate, it is safest to not click on suspicious links. Also consider contacting organisations or individuals who are digital security experts.

# IDENTIFYING A PHISHING ATTEMPT



## Instagram

- **Phishing:** This page lists of suspicious email domains you can check before clicking links: <https://help.instagram.com/670309656726033/>
- **List of common scams on Instagram** (this is also similar to scams on facebook): <https://help.instagram.com/514187739359208/>
- **Phishing can be reported on instagram by writing to:** [phish@fb.com](mailto:phish@fb.com)
- **Reporting a person for fraud on instagram :** <https://help.instagram.com/192435014247952>



## Facebook

- **Where to report if your account is compromised:** <https://www.facebook.com/hacked>
- **Reporting content on facebook:** <https://www.facebook.com/help/reportlinks>



## Whatsapp

- **Reporting and blocking a number:** <https://faq.whatsapp.com/414631957536067/>



## Bumble

- **Reporting someone on Bumble:** <https://bumble.com/en/help/how-can-i-report-someone>

# WHAT IS THE LAW ON HOW TO REPORT FRAUD?

## Legal Provisions

- Any forgery or false documents can be reported under section 340 and section 336 of BNS (Bharatiya Nyaya Sanhita- India's Criminal Code)
- **Sections 318** and **319** of BNS can be used to report some forms of cheating. **Section 318** also includes dishonest concealment of facts as deception. **Section 319** defines cheating by personation as the act of deceiving someone by pretending to the identity of oneself or another person.

## Cyber Crime Reporting Portal

- Financial scams or frauds can be reported on this portal: <https://cybercrime.gov.in/Webform/Index.aspx>
- Cyber Crime Helpline – 1930
- File a FIR with cyber cell or help desk at the police station most accessible to you.
- 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\\_NodalGrivanceList.aspx](https://cybercrime.gov.in/Webform/Crime_NodalGrivanceList.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