

WhatsApp, SMS & Fake-KYC Fraud: Spot the Message Before You Tap

Fake KYC warnings, SMS links, files that install malware, fake bills and fines, and WhatsApp takeovers: how to read who really sent a message, and what to do before you tap anything.

30 min read · Content last verified 18 September 2026 · Reviewed by Shravya M

Free awareness guide. Not legal or financial advice. <https://www.shravyadigital.com/guides/whatsapp-sms-kyc-fraud>

CONTENTS

1. Before you start
2. Chapter 1: "Your KYC expires today"
3. Chapter 2: Read who sent it
4. Chapter 3: Links and files that install something
5. Chapter 4: Keeping your WhatsApp yours
6. Chapter 5: Fake bills, fines and deliveries
7. Chapter 6: Report it, even if you didn't lose anything
8. Quick reference card

Before you start

This guide is the reading for **Course 3** of the Digital Safety Pathway. It takes about 30 minutes to read and covers the messages that arrive on your phone: fake KYC warnings, SMS with links, files that install malware, and tricks that take over your WhatsApp.

All names, numbers and messages here are made up.

Keep this number: 1930 is the national cybercrime helpline. If money has already gone, call it first, then your bank.

Chapter 1: "Your KYC expires today"

What it looks like

"Dear customer, your bank account will be BLOCKED today due to pending KYC. Update now: [short link]." Anita taps the link. It opens a page that looks like her bank's, asking for her customer ID, password and the OTP that has just arrived.

Why it works

The Reserve Bank of India has warned, repeatedly, about frauds in the name of KYC updation. RBI describes the pattern: unsolicited calls, SMS or emails that manipulate people into revealing personal information or login details, or into **installing unverified apps through links in the message**, using **false urgency** and threats that the account will be **frozen, blocked or closed**. Once you share your details, fraudsters get into your account.

The check

RBI's advice:

- If you receive **any** request to update KYC, **contact your bank directly** to confirm it.
- Get your bank's number **only from its official website or official sources**, never from the message.
- **Ask your bank branch** what ways are available to update KYC.
- **Never share** login details, card information, PINs, passwords or OTPs with anyone, and don't send copies of your KYC documents to people you don't know.

The rule: A KYC warning with a link is a scam until your bank, contacted directly, says otherwise.

Chapter 2: Read who sent it

What it looks like

*Two messages about "your account" arrive a minute apart. One comes from a sender name ending in **-T**. The other comes from an ordinary 10-digit mobile number.*

Why it works

Most people read the message and never look at the sender, and fraudsters rely on that.

The check

Under TRAI's rules for commercial messages, registered senders' SMS headers carry a **suffix** that shows what kind of message it is:

Suffix	Type of message
-P	Promotional
-S	Service
-T	Transactional
-G	Government

For example, the Indian Cyber Crime Coordination Centre (I4C) sends alerts from the header **I4CMHA-G**. A message about your bank account from an **ordinary mobile number** should make you suspicious. Even from a proper header, **never follow a link to "update" anything**: open your bank's app or type its website address yourself.

The rule: Look at who sent it before you read what it says.

Chapter 3: Links and files that install something

What it looks like

*A WhatsApp message offers "Bank Reward Points worth ₹7,250, download the app to redeem", with a file ending in **.apk**. Another message has "0714 Statement of Account.zip".*

Why it works

A file you open can install software that reads your messages, including OTPs, or takes over your accounts. RBI names installing unverified apps from links as part of KYC frauds. In August 2026, I4C warned about **.zip files** named like "**Statement of Account**", "**RBI**" or "**MCA**", sent over WhatsApp, SMS and email, that install malware on Windows computers and hijack **WhatsApp Web**. I4C also notes that regulators such as the RBI **never** send software updates, security fixes or account statements as WhatsApp attachments.

The check

- Install apps **only from your phone's official app store**, never from a file someone sends.
- **Don't open .apk, .zip or .exe files** you weren't expecting, even from someone you know: their account may have been taken over.
- If you opened one, disconnect the device from the internet, tell your bank, and get the device checked. The government's **Cyber Swachhta Kendra** (csk.gov.in), run by CERT-In, offers free tools and advice for cleaning infected devices.

The rule: Never install anything from a message.

Chapter 4: Keeping your WhatsApp yours

What it looks like

"Hi, I sent a code to your number by mistake, please forward it to me." The message is from a friend's number. A minute ago, Rahul got an SMS with a WhatsApp code he didn't ask for.

Why it works

The code WhatsApp sends by SMS is what registers your number on a new phone. Whoever has it can move your WhatsApp to their phone and then message all your contacts as you, asking for money or sending the same trick on. The "friend" asking is often a friend whose account was taken first.

The check

- **Never share the WhatsApp registration code**, with anyone, for any reason.
- **Turn on two-step verification** in WhatsApp's settings. It adds a PIN of your own that is needed to register your number again, so a stolen code isn't enough.
- **Check Linked Devices** (Settings, then Linked Devices) and log out of any computer you don't recognise. This is I4C's advice too.
- **If your account is taken over**, I4C advises logging out of all linked devices, warning your contacts not to open anything sent from your account, and getting your computer scanned.

The rule: Your WhatsApp code is your account. Never pass it on.

Chapter 5: Fake bills, fines and deliveries

What it looks like

"Your electricity will be disconnected tonight at 9:30. Call this officer: 98XXXXXXX." "Unpaid traffic challan: pay the fine here to avoid court." "Your parcel could not be delivered, pay ₹25 to reschedule."

Why it works

Each message is small, urgent and believable, and the amount is often tiny, so paying feels harmless. The link or number leads to a fake payment page or to a caller who asks you to install a screen-sharing app. Sanchar Saathi's awareness pages list fake traffic challans and "undeliverable parcel" messages among common scams.

The check

- **Check the bill, fine or delivery yourself**, in the provider's own app or on a website whose address you typed.
- A **personal mobile number** for an electricity officer, a courier or the police is a warning sign.
- Never install a screen-sharing app because someone asked you to.

The rule: Pay bills and fines only where you found the address yourself.

Chapter 6: Report it, even if you didn't lose anything

- **Chakshu** on **Sanchar Saathi** (sancharsaathi.gov.in): report suspected fraud calls, SMS and WhatsApp messages. **Report within 30 days** for action.
- **TRAI DND app**: TRAI's advisory also suggests flagging suspicious numbers here.
- **1930** or **cybercrime.gov.in**: if you have lost money, or had an account taken over.
- **Your bank, the same day**: if your bank details, card, or banking app might have been exposed. Use the number on your card, passbook or the bank's official app.

The same number usually messages thousands of people. Your report can get it blocked before it reaches someone who believes it.

The rule: Report it on Chakshu, and on 1930 if money or an account is involved.

Quick reference card

1. **KYC warning with a link?** Contact your bank directly, using its official number.
2. **Look at the sender:** -P, -S, -T or -G, or just a mobile number?
3. **Never follow a link** to "update" anything. Open the app yourself.
4. **Never install** an .apk, or open a .zip or .exe, from a message.
5. **Never share your WhatsApp code.** Turn on two-step verification.
6. **Check Linked Devices** in WhatsApp now and then.
7. **Bills, fines, deliveries:** check in the official app or a website you typed.
8. **Report** on Chakshu; call **1930** and your bank if money is involved.

Take the course for what you just read

Take the free 10-question assessment and pass with 8 or more. Every course you pass counts towards a Pathway Certificate issued by Shravya Digital, earned when you pass all five courses in the pathway: <https://digital.shravyaworld.org/courses/whatsapp-sms-kyc-fraud>

Sources

Checked against these primary sources on 18 September 2026. Rules change: if something here looks out of date, trust the source.

- RBI, "RBI cautions against frauds in the name of KYC updation" (https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=57244)
- TRAI amendments to TCCCPR, 2018: -P, -S, -T, -G header suffixes (PIB, Feb 2025) (<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2102413>)
- I4C caution on malicious .zip files and WhatsApp account takeover (PIB, 7 Aug 2026) (<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2295889>)
- TRAI advisory on fraudulent activities misusing TRAI's name (PIB, 6 Aug 2025) (<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2153153>)
- Chakshu: report suspected fraud communication (DoT) (<https://sancharsaathi.gov.in/sfc/>)
- Cyber Swachhta Kendra (CERT-In) (<https://www.csk.gov.in/>)