

Raju & The Forty Thieves



*A Booklet on Modus
Operandi of
Financial Fraudsters*

Office of the RBI Ombudsman (Mumbai-II)
Maharashtra And Goa





Foreword

As a part of the Reserve Bank of India's customer awareness initiatives, in July 2021 this office had published a booklet 'Be(A)ware' on the modus operandi of financial fraudsters. Encouraged by the positive response received from members of the public as well as different institutions, we take forward the idea of financial education, to be more accessible to those who have just begun their journey into digital financial world and are not so well-versed with the nuances of online financial transactions. This includes people from different ages and education levels such as school children, young adults, semi-literates and senior citizens, irrespective of whether they live in urban, rural or semi urban areas.

Continuing the 'Be(A)ware' series, this booklet 'Raju and the Forty Thieves' is a manifestation of our efforts. The booklet is an easily understandable pictorial depiction of incidents happening around us and helps us to learn how to keep hard-earned money and ourselves safe from fraudsters.

As the name suggests, 'Raju and the Forty Thieves' contains forty such stories providing glimpses of fraudulent events being reported to us and provides simple tips about DOs and DON'Ts. Raju is a typical gullible citizen, and, in these stories, he appears in different characters, some time as a senior citizen, some time as a farmer, sometimes as a happy-go-lucky guy, etc., although with same curly hair always to identify with different walks of life.

Let us make ourselves aware of such modus operandi used by fraudsters and educate those around us to be aware of such financial frauds. The tireless efforts put by the team of RBI Ombudsman, Mumbai-II, Maharashtra and Goa, to spread financial literacy by preparing such booklets during covid period, is gratefully acknowledged.

The readers are requested to share their feedback and suggestions, if any, to bomumbai2@rbi.org.in.

Be Aware and Beware!



INDEX

SL. No.	Topic Name	Page Number
1	FRAUD THROUGH PHISHING LINKS	1
2	VISHING CALLS	3
3	FRAUD USING ONLINE MARKETPLACES	5
4	CREDIT CARD ANNUAL FEE WAIVER- FAKE OFFER	7
5	ATM CARD SKIMMING FRAUD	9
6	FRAUD USING SCREEN SHARING APP/REMOTE ACCESS	11
7	SIM SWAP/ SIM CLONING	13
8	FRAUDS BY COMPROMISING CREDENTIALS THROUGH SEARCH ENGINES	15
9	SCAM THROUGH QR CODE SCAN	17
10	IMPERSONATION THROUGH SOCIAL MEDIA	19
11	JUICE JACKING – STEALING OF DATA THROUGH CHARGING CABLE	21
12	LOTTERY FRAUD	23
13	ONLINE JOB FRAUD	25
14	FAKE ACCOUNT NUMBER	27
15	FRAUD THROUGH EMAIL	29
16	MESSAGE APP BANKING FRAUD	31
17	FRAUDULENT LOANS WITH STOLEN DOCUMENTS	33
18	BETTING SCAM	35
19	FAKE VACCINATION CALL	37
20	COVID TESTING- FAKE ONLINE SITE	39



SL. No.	Topic Name	Page Number
21	FRAUDSTERS IN THE PRETEXT OF RECOVERY AGENTS	41
22	SOCIAL WELFARE SCHEME FRAUD	43
23	MULTI-LEVEL MARKETING (MLM) SCAMS	45
24	WORK FROM HOME SCAM	47
25	ONLINE SHOPPING FRAUD	49
26	FRAUD USING PUBLIC WI-FI	51
27	FAKE ADVERTISEMENTS/OFFERS	53
28	FAKE LOAN OFFER	55
29	CREDIT CARD ACTIVATION FRAUD	57
30	CREDIT CARD LIMIT UPGRADATION FRAUD	59
31	SAFE GUARDING YOUR AADHAAR CARD	61
32	ONLINE FRAUD USING CASHBACK OFFERS	63
33	DISCOUNT FRAUD	65
34	CHARITY FRAUDS	67
35	OVERDRAFT AGAINST FD	69
36	FRAUDS USING MALICIOUS APPLICATION	71
37	ILLEGAL LOAN FINANCING APPS WITH EXORBITANT INTEREST RATES AND HARASSMENT TACTICS	73
38	CARD CLONING AT MERCHANT OUTLETS	75
39	FRAUD THROUGH DETAILS SHARED WITH KNOWN PERSON/FAMILY/RELATIVES	77
40	PAYMENT SPOOFING APPLICATIONS.	79



1. FRAUD THROUGH PHISHING LINKS

One day, Raju received message on his phone: 'Dear customer, if your KYC details are not updated within two days, your account will be blocked. Use the below link to update the details at <http://updateKYC.XYZbank.com>'

Raju: "Oh! All my money will be blocked; I need to update my KYC details."



Raju clicked on the link, but the link to update KYC details did not work. Soon, he gets a call.



Fraudster: "Hello Sir, I am calling from XYZ bank. Are you facing any issues in updating your KYC details?"

Raju: "Yes, the link is not working."



Fraudster: "The website load might be high; I will update the details manually. Please share your username, password and OTP."



Do's:

- ✓ Always cross-check the KYC status with your home branch or through your relationship manager when you receive calls, links or SMS from unknown sources requesting you to update KYC.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



After some time, Raju received SMS alerts on his phone stating that Rs 50,000 was debited from his account.



Raju immediately called the other person, but he didn't answer the calls. Raju realized that the person was a fraudster and he should not have shared any personal details with him.



Don'ts:

- x Don't click on unknown/unsolicited links received on the phone/email without verifying it.
 - x Don't share your confidential details with strangers.



2. VISHING CALLS

One day, Raju received a call.

Fraudster: "Hello Sir, I am calling from XYZ Bank."

Raju: "Hi, what is the matter?"

Fraudster: "This is regarding your insurance policy. Your policy is activated, and you need to pay Rs18000 as a premium."

Raju: "No! I don't have any insurance with XYZ bank."

(scratches head)

Fraudster: "Sir, it got activated as a promotional offer at a very low fee. But if you don't need it, I will deactivate it."

Raju: "I don't understand how you activated the policy without my consent, and why should I trust you?"

Fraudster: "Sir, I am calling you directly from the XYZ Bank customer care. I have all your details like Name, Address, Card details, DOB, Company Name and Designation."

Raju: "Okay, so tell me how to deactivate the policy?"

Do's:

- ✓ Always cross-check with your relationship manager or bank branch about any issue before trusting anyone.
- ✓ OTP is like a key to your safe wealth, so always keep it away from fraudsters.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



Fraudster: "I will deactivate it online from here. Please share the OTP which you will receive now."

Raju: "Yes, I got the OTP. It is 859623."

MONEY TRN
ENTER OTP BELOW TO
AUTHORISE TRANSFER OF
15,000/- TO MR. UZO KING
859623

VERIFY

CLICK!

Fraudster: "I have deactivated the policy, Sir."

Raju: "Thank you!"

A few minutes later, Raju received a message alert.
"Rs-15000/- is debited from your account."

Raju immediately visited the nearby XYZ branch and enquired about the transaction.

Raju realized his mistake: the call was from a fraudster;
he should not have believed a stranger.

Don'ts:

- ✗ Don't trust unknown callers claiming to be speaking on behalf of banks asking for confidential information / details. Banks don't seek such details over phone.
- ✗ Never trust strangers in the digital world easily, and be cautious while answering calls from unknown numbers.

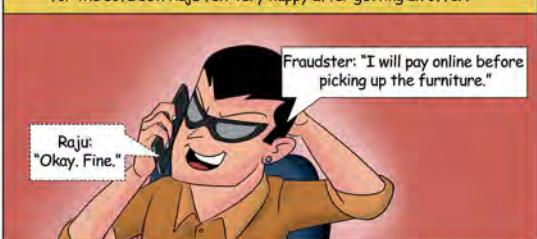


3. FRAUD USING ONLINE MARKETPLACES

Raju wanted to dispose of sofa set. He posted the advertisement on the website which is an online marketplace for second-hand goods.



Immediately after posting the advertisement, there was an enquiry from a fraudster offering to pay Rs 15,000/- for the sofa set. Raju felt very happy after getting an offer.



Fraudster: "Please share your account number."

Raju: "My account number is 123xxx67."

Fraudster: "I will first send Rs 10/- before making the final payment to verify the account."



The fraudster sent Rs10/- to Raju's account and asked for confirmation for the final payment.

Raju: "Okay, I got it."



Do's:

- ✓ Always remember, UPI PIN is required only to make a payment and is not required to receive any payment.
- ✓ Always verify the mobile number in the UPI application before initiating a payment.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



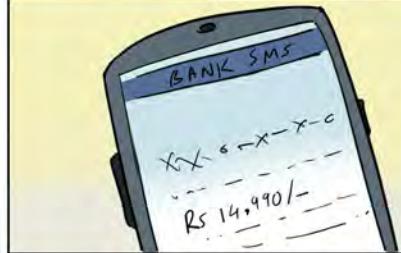
Then the fraudster sent a UPI request for receiving a payment of Rs 14,990/- instead of paying Raju.



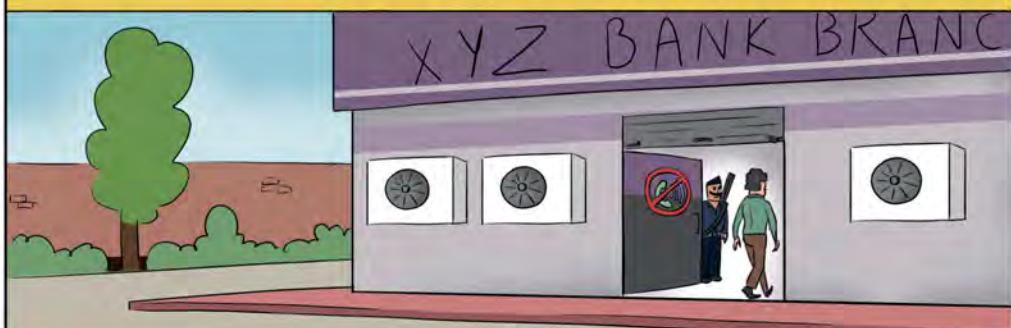
Fraudster: "As per bank rules, the PIN needs to be entered for high-value transactions."



Raju entered the pin immediately, and his account was debited for Rs14,990/-



Realizing that he was cheated, Raju quickly approaches the bank branch and registered a complaint on the same day.



Don'ts:

- ✗ Don't share OTP or confidential account details with strangers.
- ✗ Don't enter the UPI PIN to receive an amount from another person.



4. CREDIT CARD ANNUAL FEE WAIVER- FAKE OFFER

One day, Raju received a call from an unknown number.

Fraudster: "Good morning, Mr Raju! I am Rohit Kumar from your Bank customer care. We are happy to inform you that your credit card annual fee will be waived for this year as you are one of our most valuable customers."



Raju: "Oh!
That's great news."

Fraudster: "Mr Raju, Please confirm a few details before I can proceed further. Your card number is 42781234 XXXX, and your full name is Raju Deshpande, right?"



The fraudster had already gathered Raju's card details from illegitimate sources.

Raju: "Yes, these are correct."



Fraudster: "Mr Raju, now you will receive an OTP. Please share it with us so that we can waive the fee at our end."

Do's:

- ✓ Be cautious while responding to calls from unknown numbers claiming to be from your bank.
- ✓ Report to your Homebranch immediately on realizing the fraud.
- ✓ Block your card to prevent further financial loss.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



Raju reasoned that since the caller already knew his card details, the call must be genuine. He shared the OTP with the fraudster immediately.

Fraudster: "Thank you, Mr Raju. Your annual fee is waived off. Have a great day!"



The call was disconnected. Soon, Raju received an SMS stating that Rs12,000 was debited from his credit card account.



Raju immediately called the fraudster, but his phone was switched off.



Raju realized the person was a fraudster, and he should not have shared the OTP with him.



Don'ts:

- ✗ Don't share your OTP with anyone. Fraudsters might be able to collect your account details, but transactions can only happen if you share the confidential OTP sent to your phone.



5. ATM CARD SKIMMING FRAUD

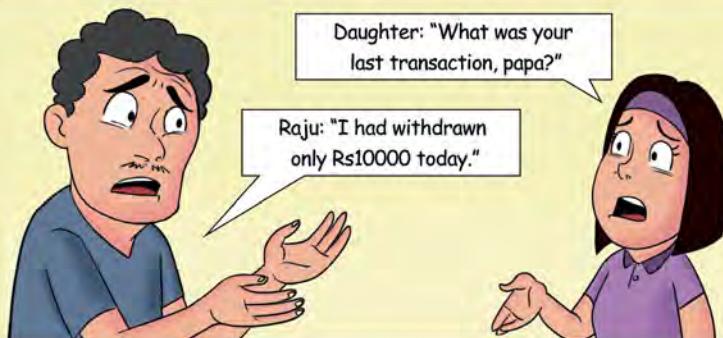
Raju receives his monthly salary in his account. He visits an ATM to withdraw money for his monthly expenses.



After a few hours, Raju gets SMS alerts for a few more debit transactions. (Rs 15,000/- is debited from your account. Rs 12000/- is debited from your account.)



Raju tells his daughter about the SMS alerts.

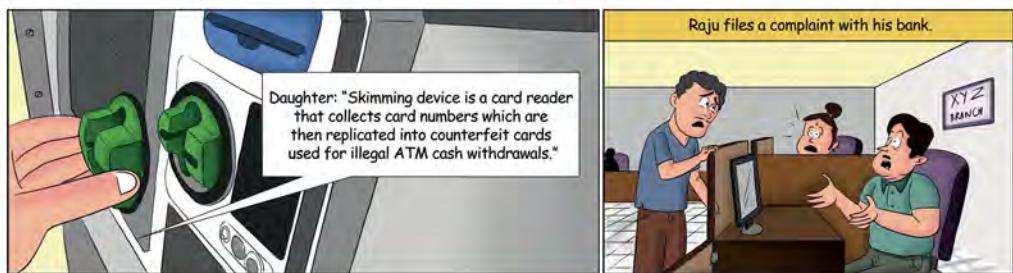
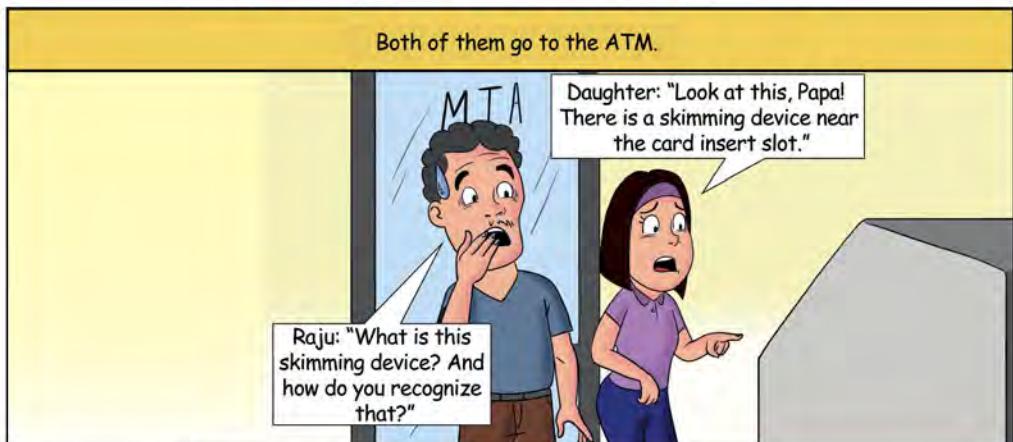


Daughter: "Let me first block your ATM card. We can easily block it through your Mobile Banking App."



Daughter: "Also, did you share any of your bank or ATM card details with anyone? Or did you share your OTP?"

- Do's:**
- ✓ Before initiating any transaction in the ATM machines, ensure that skimming devices are not present. Skimming devices are hidden by fraudsters by overlapping them with the card insertion slot.
 - ✓ Report the fraud to the bank within 3 days of the card cloning incident. Check your transaction history frequently to verify all transactions.
 - ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at (<https://cybercrime.gov.in>)



Don'ts:

- ✗ Don't give your ATM card to anyone on the ATM premises to transact on your behalf. This kind of social engineering is being used to target senior citizens/semi-educated persons who have difficulty operating ATMs.



6. FRAUD USING SCREEN SHARING APP/REMOTE ACCESS

Fraudster: "Hello Sir! Good Morning.
I am calling from ABC Gaming Corporation. We are delighted to offer you a cash reward for playing an online game."



At first, Raju doubted that the person might be a fraudster and remained silent.

Fraudster: "Sir, I am an employee of the company which makes online games, and this is a beta version of the new game we have developed. We need feedback from users before launching the game to the public. So, we are inviting gamers to download this app, play games and give us feedback for improvement. We will be giving you Rs 10,000/- for this."



Do's:

- ✓ Verify the authenticity of the offer on the official website of the entity concerned.
- ✓ Install antivirus/spam blocking software on your mobile phone.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



Fraudster: "Oh no! How can it be, Sir? You haven't shared your account/card details with us. This is just an entry code for the opening game."

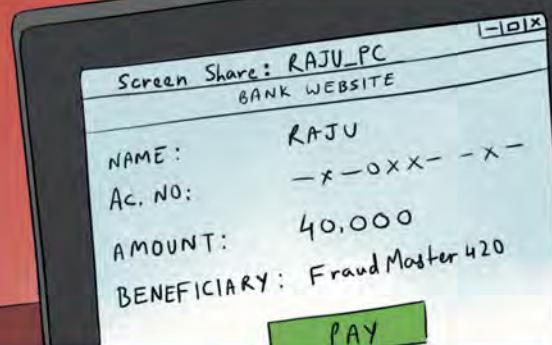
Raju: "Oh, that's right.
xxxxx is the entry code."

Fraudster successfully installed the screen-sharing app in Raju's mobile and gained access to his phone. He could read the messages on Raju's mobile and track his keypad.

Fraudster: "Sir! We would be giving you Rs 10000 for participation but before that please pay Rs 10 to the account 12345 through net banking to activate the account. Please call me once done."

Raju thinking that it was just a matter of Rs 10/- transferred the amount through Net Banking. Soon he received debit messages of Rs 35000, Rs 20000 and Rs 40000.

Raju: "Oh my God! How did this happen! I have not shared any OTP."



Once the screen-sharing application was installed, the fraudster had access to the net banking password entered by Raju for making the payment (of Rs 10).

Don'ts:

- ✗ Don't download any applications over links sent through SMS, Email or instant messaging applications.
- ✗ Don't download screen-sharing applications shared by any unknown persons.

Screen sharing codes generated by these apps should not be shared with unknown persons.



7. SIM SWAP/ SIM CLONING

Fraudster: "Hello Sir,
I am calling from ABC telecom company.
We are offering you a SIM card upgrade
for better internet connectivity
and more data."



Raju: "What should I
do to avail
this benefit?"

Fraudster: "You must share
with us basic details
like your Aadhaar Card number
and unique 20-digit SIM card
number. Thereafter, you will
get a text. Reply 'I'
to activate the offer."



Raju: "Okay."

**Do's:**

- ✓ Verify the status of the SIM card with your Telecom Service Provider when in doubt instead of believing unknown callers.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



Raju shares the details with the caller.



Raju: "What has happened to my mobile! There is no network, and I am not able to make calls, send messages, etc."



Fraudster uses the new SIM to retrieve the username for the banking application by using options like forgot username, reset password etc. and transfer all the money to his account.

After a few minutes, when Raju received emails showing cash debits from his bank account, he checked his bank account balance. He noticed that some unauthorized debits were made from his account for which no SMSs were received on his registered mobile number as the SIM was compromised to transfer funds, shop online, etc.



Don'ts:

- Don't share confidential details like Aadhaar number and SIM number with unknown callers.



8. FRAUDS BY COMPROMISING CREDENTIALS THROUGH SEARCH ENGINES

Raju is fond of watching cricket, and he was very excited about the upcoming cricket match. But as soon as he opened the Sports App, he realised that his subscription had expired.



Raju thinks: "What is the big deal!
The Internet has all the solutions."



Thinking this, he searched for a way to recharge the Sports App on the internet. After searching for a while, he found a phone number for the same. Raju dialled the number immediately.



Do's:

- ✓ Always obtain the contact details/customer service number, etc. from the official website of the service provider only.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



Fraudster: "You will get the payment link on your phone now. Please click and make the payment."

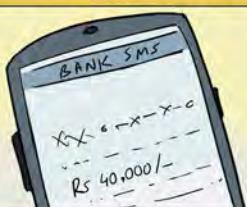


Raju - "Yes, I got the payment link. I will pay the amount now."



Raju clicked on the link.

Raju received an SMS stating that Rs 40,000 was debited from his account.



Instead of paying Rs 1000 to Sports App, Raju ended up transferring Rs 40000 to the fraudster.



Don'ts:

- Don't contact random phone numbers obtained from web search engines, especially for doing financial translation.



9. SCAM THROUGH QR CODE SCAN

Raju registered his old car on an online website to sell it.



Within hours, he was contacted by a person (a fraudster)

Fraudster: "Hi, I saw your car advertisement on the platform. I really liked it, and I am interested in buying your car."



Do's:

- ✓ Educate yourself about QR codes before using them.
- ✓ Report the transaction immediately to your bank.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



Raju: "Okay, I will send you my account details. Please send a token amount of Rs. 10,000/- to seal the deal. You can send the amount by NEFT/RTGS."

Fraudster: "I got your details. I will transfer the amount now. Thank you!"

Raju again receives a call from the Fraudster after 10 minutes.

Fraudster: "Hello, I called you earlier. I have been trying to transfer the amount for the last 10 minutes, but I'm unable to do so. Therefore, I will be sending you a QR code through email. Please scan the QR code so that I can send you the amount."

Raju: "Okay, no problem. I got the QR code; I will scan it."

I have scanned the QR code, but it is asking for my UPI PIN to proceed further.

Fraudster: "That is correct; you must enter your PIN to receive the money."

ONLINE BANKING

NAME: RAJU
Ac. NO: -x-0XX--x-
AMOUNT: 70,000
BENEFICIARY: Fraud Master 420

PAY

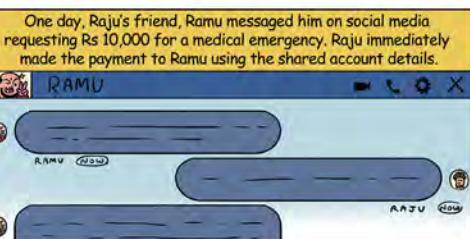
click! click!

Don'ts:

- Don't enter your UPI PIN to receive money from another person. UPI PIN is required only for sending a payment, not for receiving.
- Don't scan QR codes to receive any payment. QR code needs to be scanned for sending a payment, not for receiving Money.



10. IMPERSONATION THROUGH SOCIAL MEDIA

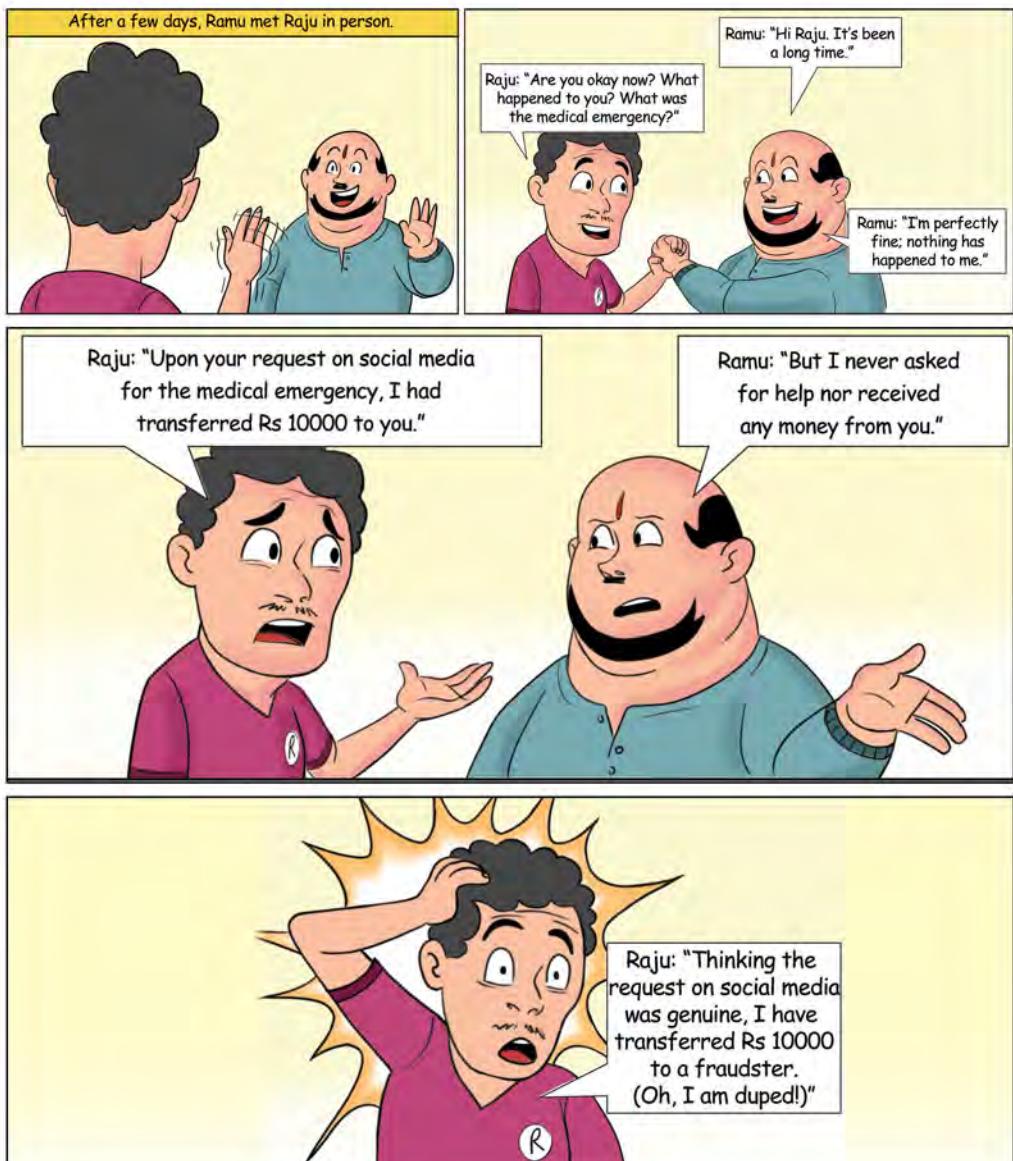


Soon Raju got accustomed to using social media: he started posting pictures, liking posts, sending friend requests and messages.

One day, Raju's friend, Ramu messaged him on social media requesting Rs 10,000 for a medical emergency. Raju immediately made the payment to Ramu using the shared account details.

Do's:

- ✓ Verify by calling/meeting the real person before making a payment.
- ✓ Always check the account details before making any payment.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



Don'ts:

- ✗ Don't keep your personal information like mobile number, email id and friend list open to the public.
- ✗ Don't accept friend requests/ follow requests from people you have never met in person.



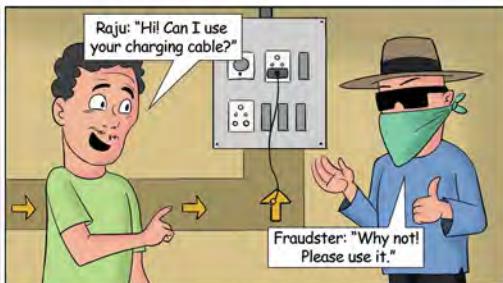
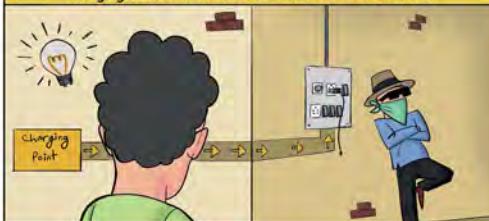
11. JUICE JACKING – STEALING OF DATA THROUGH CHARGING CABLE

Raju had to leave due to a medical emergency.
He realizes that his phone battery is low.



Raju: "Oh no! My battery got drained, and I don't have a charger."

A fraudster installs a charging cable with a virus and leaves it at the charging point in a public place. Raju notices the charging point with the charging cable and asks the fraudster if he can use it.



Do's

- ✓ Install anti-virus software on your mobile phone to protect it from unauthorized access.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



While charging, the charging cable injects the virus into Raju's mobile.



During the next few days, the fraudster captured all details entered by Raju on his mobile and got hold of vital bank details like username, password etc.



One day, Raju receives SMSs/emails indicating unauthorized debits in his savings account...



...and realizes that his account has been compromised somewhere.



Don'ts:
x Don't use charging adapters/cables from strangers.



12. LOTTERY FRAUD

Raju received an audio message stating that he had won an ABC jackpot.



Fraudster: "Hi... I'm Pankaj calling from ABC. Congratulations on winning the ABC jackpot of Rupees 10 Lakh. I have sent you the jackpot details. You may contact the number mentioned therein to claim the prize. Hurry up!"

Excited, Raju called the number in the jackpot message which featured a fake audio of a Superstar congratulating him on the prize.
He contacted the given number.

Raju: "Hi, this is Raju. I was asked to contact you for claiming the ABC Jackpot. How shall I claim my jackpot?"



Fraudster: "Congrats Rajul You must pay a delivery fee of Rs 1000 to be eligible to receive the prize. I have shared our account details on your Message App number. Please pay the amount immediately and call me back."



Unaware of this fraudulent activity, Raju paid the amount and called him back.

Raju: "Hi, I have paid the amount and sent you the details. When will I get my prize?"

Fraudster: "Excellent Rajul! We have only a few more steps to complete before you get the jackpot of Rupees 10 lakh. You will have to pay a tax fee of Rs 25000 to claim the prize amount."

Do's:

- ✓ Verify the message received from unknown numbers before trusting them as members of any company or management team.
- ✓ Always verify lottery offers with official websites of such events.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



Without thinking twice, Raju makes the payment.



Raju: "I have made the payment."

Fraudster: "Thank you, Sir!
You will receive your prize within
two days."

Raju waits for the jackpot for the next few days but receives no further updates...



...Later, he realizes that he was cheated.

Don'ts:

- ✗ Do not make payments without verification, expecting very high returns.



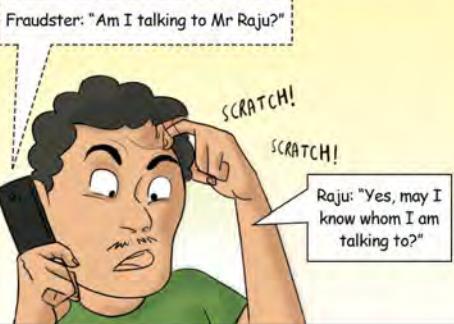
13. ONLINE JOB FRAUD

Raju had lost his job recently and was very worried. He started looking for jobs on online job portals. He updated his resume on various websites.



One day, he got a call from a fraudster, impersonating a person from XYZ Company.

Fraudster: "Hi, Raju. I am Rohit from the Human Resource department of XYZ Company. You are selected for a managerial job in our company based on your application."



Fraudster: "Your qualification has helped you in getting this job."

Raju: "Okay, that's nice. What is the next step?"



Do's:

- ✓ Verify the authenticity of the company or recruitment agencies before paying any money. Recruitment agencies generally do not charge candidates for hiring them.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



Despite waiting for several days, Raju did not receive any laptop. He tried calling on the number, but the number was always switched off. He searched the company name online but did not find anything. Raju eventually realized that he was defrauded of his hard-earned money.



Don'ts:

- ✗ Don't pay anyone under the pretext of a job. A legitimate company will never ask for payment from a potential candidate for a job offer.



14. FAKE ACCOUNT NUMBER

Raju was planning to buy a family insurance policy for himself and his family. On his way back home from the office, he saw a small stall in the name of ABC Insurance company.



Do's

- ✓ Cross-check an organization's credentials on a known database to see if they are genuine.
- ✓ Always approach registered offices for availing products.
- ✓ Funds are transferred solely based on account number.
- ✓ Fraudsters may give a genuine company name but give their own account number, always verify the account number with the company before making a payment.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



The next day Raju noticed that the outlet was gone. Even after 10 days, he did not receive any documents. Raju called the ABC insurance company.

"We don't have any such outlet. Also, we have a specific payment option on our official website. We do not entertain any other mode of transfer. Looks like you have been duped."



Don'ts:

- ✗ Do not pay anybody without verifying the authenticity of the company.



15. FRAUD THROUGH EMAIL

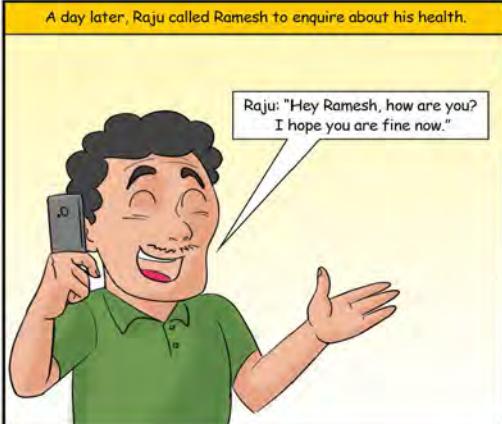
A fraudster sent an email to Raju, impersonating his friend Ramesh, asking for financial help for his medical emergency.



Raju pays the amount immediately without verifying the email ID or account details.



A day later, Raju called Ramesh to enquire about his health.



Ramesh: "Hello Raju. I am fine. How are you?
You've called me after a very long time."



Do's:

- ✓ Verify with the person concerned before making any payment based on the email received.
- ✓ Verify the email ID.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



(Raju was in shock after knowing this. His act of kindness made him a victim to a fraudster due to his negligence.
He should have verified the email ID.)



Don'ts:

- ✗ Don't make payments on receiving requests from random emails or similar-looking email ids.



16. MESSAGE APP BANKING FRAUD

One day, Raju received a call from an unknown number.

Fraudster: "Hello Sir. I am calling from the customer care centre of XYZ Bank. We are launching a new product, MessageApp. It's a banking facility that provides 24x7 banking services easily through your MessageApp. You will also receive a gift voucher when you use it for the first time. Please confirm whether 99*****99 is the mobile number registered with MessageApp."



Raju: "Wow! That's amazing.
Yes. This is my
MessageApp number."

Fraudster: "Okay Sir.
We have already sent
you a welcome message
on MessageApp. Please check."

Raju opens his MesageApp and sees a welcome message from a number with the poster of XYZ Bank as its profile picture and the bank's tagline as its status.



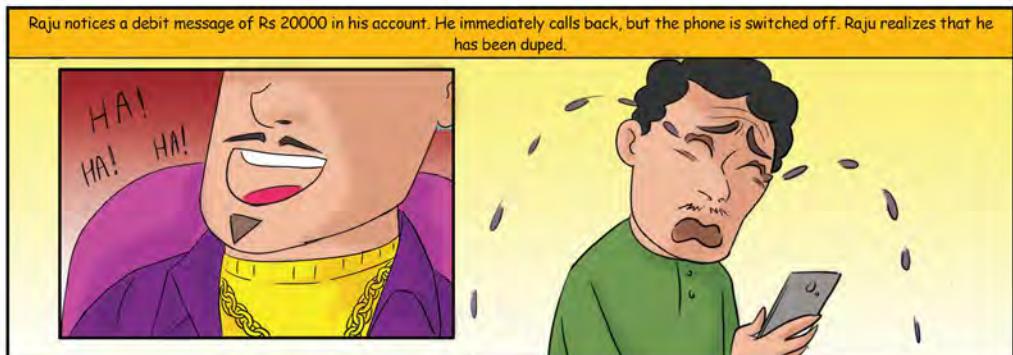
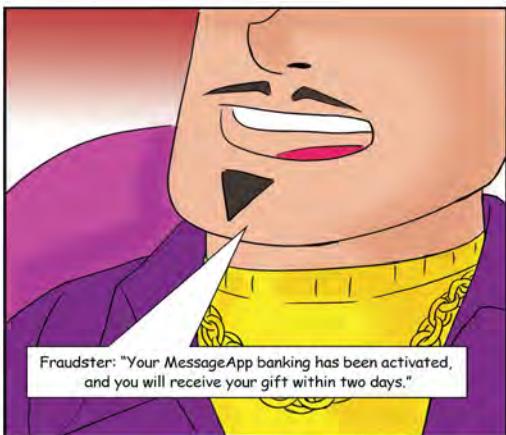
Fraudster: "Please enter the details of your debit card for verification. You do not have to share the details with me but enter it only on the official MessageApp number."

Raju: "I have entered it



Do's:

- ✓ Be cautious while responding to calls from unknown numbers seeking your account details.
 - ✓ Report to your home branch immediately on realizing the fraud. Block your account to prevent further financial loss.
 - ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.



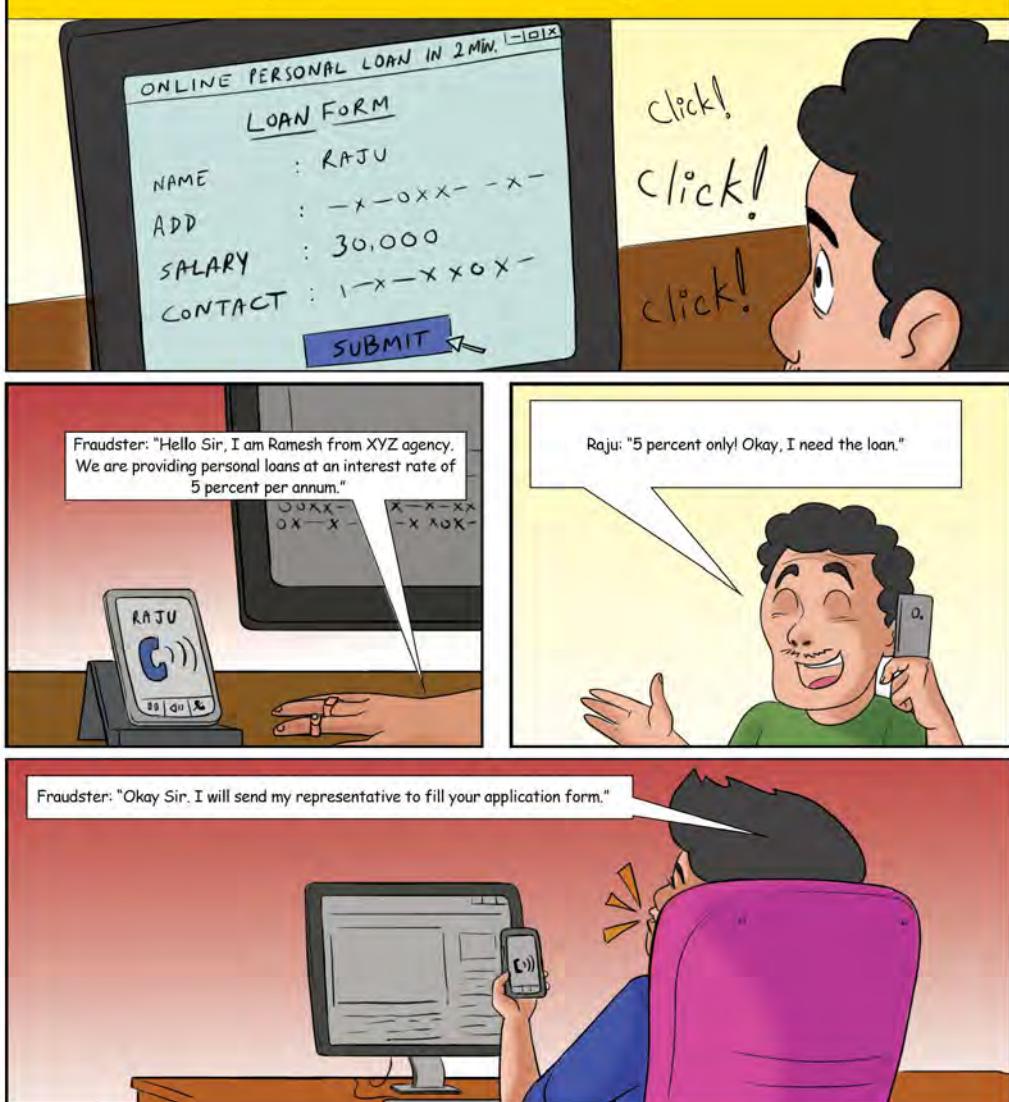
Don'ts:

- ✗ Don't trust unknown callers offering easy banking services and sending texts through Messaging Apps.
- ✗ Don't share card details and OTP.



17. FRAUDULENT LOANS WITH STOLEN DOCUMENTS

Raju fills up several forms on the internet for availing of a personal loan.



Do's:

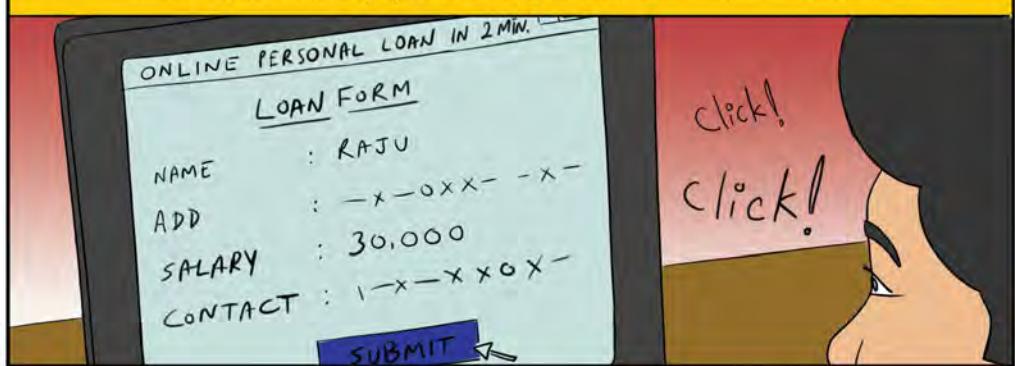
- ✓ Always monitor the end-use of the documents in the transactions.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



Raju fills the loan application form with all his details and provides a cancelled cheque to the representative.



The fraudster applies for a loan using Raju's documents but gives his own account number for the disbursal of the loan.



Raju: After a month, Raju receives a letter informing him Rs 10,000/- is due for the loan...

...Shocked, Raju calls the bank to inform them that he did not take any loan. But the bank shows the loan application form filled by him.



Don'ts:

- ✗ Never share your confidential details like the Aadhaar number, PAN number, cheque book or cheques with unknown persons.



18. BETTING SCAM

Raju was excited for the latest season of JKL cricket.

Raju searches for JKL betting groups on the internet.

The new JKL cricket season is here.
There are many stories of easy money through betting;
I must try it.



Welcome, Mr Raju.
We are glad you enquired about the betting.
How may I help you?"



"I want to place a bet for this JKL season."

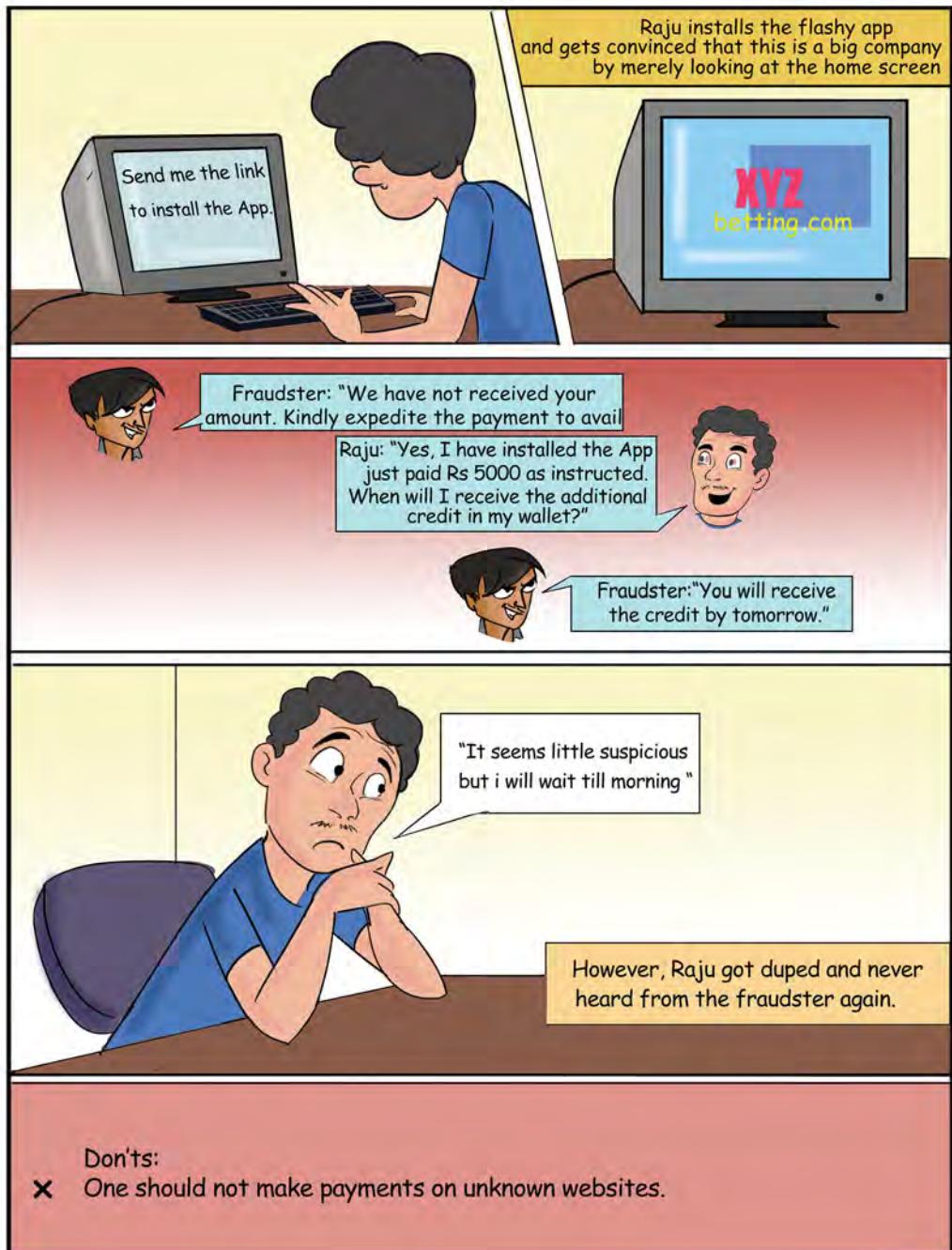


Fraudster: "First, you need to register on XYZ betting.com and as a welcome gift you will receive Rs 5000 on your first recharge of minimum Rs 5000."



Do's:

- ✓ In case scammed by a fake app/website, one should immediately call his/her bank to block the card/account/UPI service to prevent further transactions.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>





19. FAKE VACCINATION CALL

One day, Raju received a call from an unknown number.

"I am calling from the Local health Centre. We are calling to provide the vaccination facility at your home."



"Oh! Okay. But we can do it through the COWIN App only, right?"



"Yes Sir, but the home vaccination facility is not available on the App."



"No Sir, it is free of cost. I will verify your address and you will get registered for the vaccine. Please tell me your Aadhaar and PAN card details."



Do's:

- ✓ Read the entire SMS to read the purpose of OTP.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.



"My Aadhar number is 1234455, and my PAN card Number is adf1234."



"Thank you, Sir. Please wait. I am registering your Aadhar and PAN card, you will get a registration OTP code. Please share that."



(Raju received an SMS- your verification code is 1234)

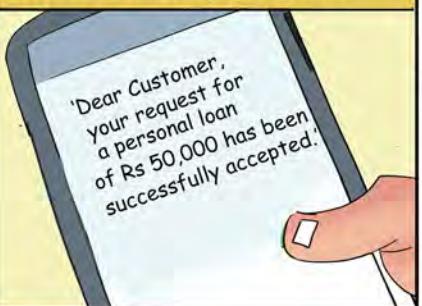


"Yes, it is 1234."

"Thank you, Sir. You have successfully registered for the vaccine, and you will get a confirmation soon. Please share the code when our health officials visit to vaccinate you."



The call got disconnected.
After some time, Raju got an SMS



The fraudster tricked Raju into sharing his PAN number and OTP for taking a loan of Rs-50,000 on behalf of Raju. Taking a loan based on Raju's PAN number makes Raju liable to pay back the loan to XYZ Company.



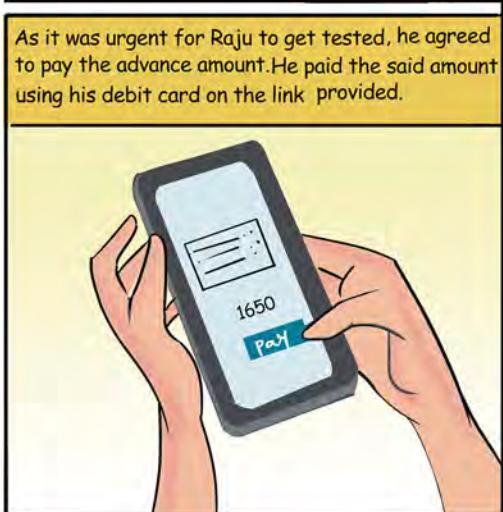
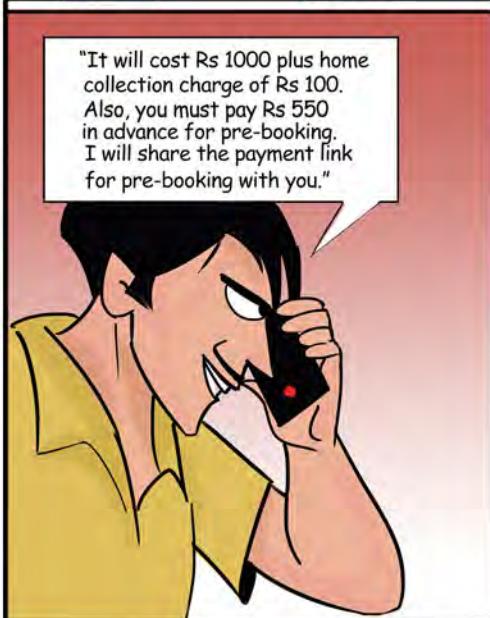
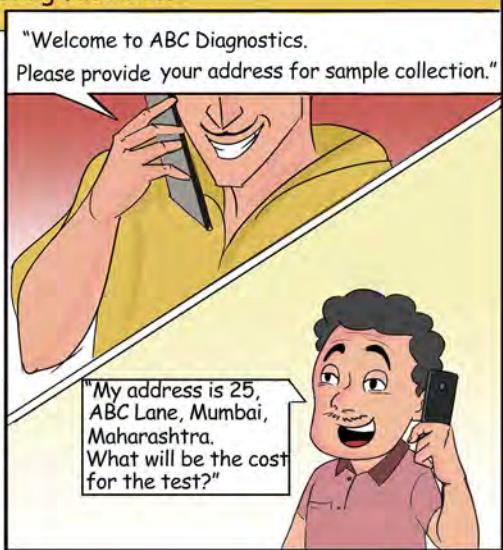
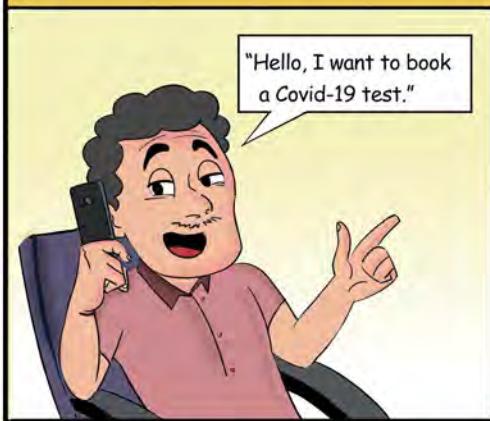
Don'ts:

- ✗ Don't share your Aadhaar, PAN card details and OTP with strangers. PAN card-based OTP is used for various financial services including cash withdrawal from bank accounts. Therefore, it is extremely important to protect your confidential details like Aadhar and PAN cards from fraudsters.



20. COVID TESTING- FAKE ONLINE SITE

Raju wanted to do the Covid-19 test at home. He searched on the internet for diagnostic centres that provide home testing facilities.

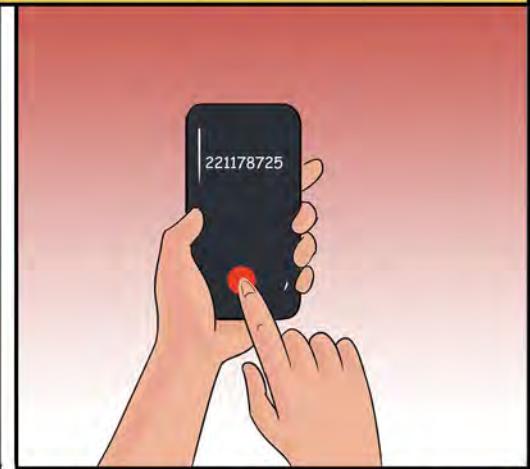


Do's:

- ✓ Always book any kind of test through registered pathology laboratories only.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.



Thereafter, the person disconnected the call and switched off his number.



Raju got tensed, and he searched the helpline number on the ABC Diagnostics site but couldn't find it.



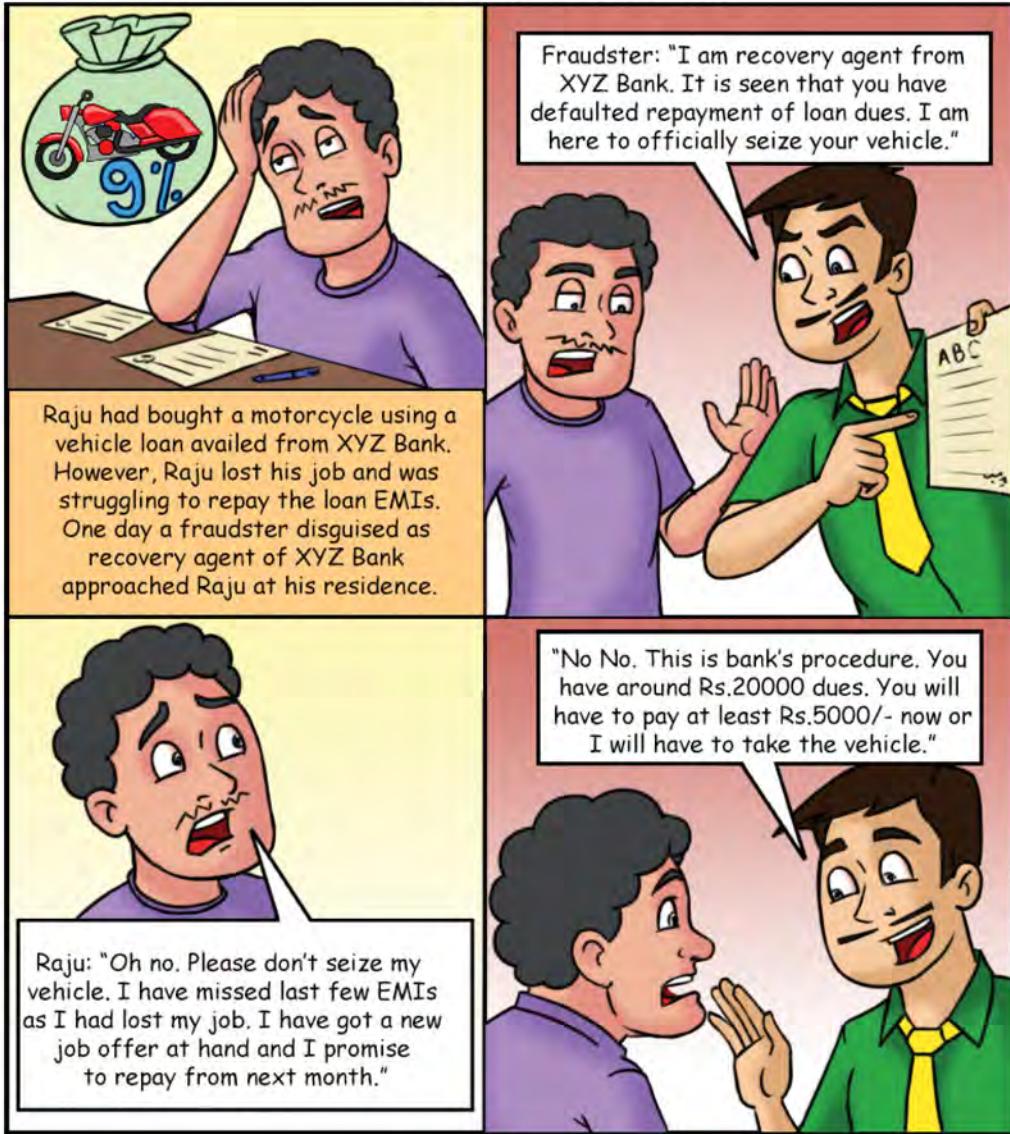
Raju eventually realized he was defrauded.

Don'ts:

- ✗ Do not make a payment in advance when you are doubtful. If anybody asks for an advance payment, it is a matter of caution and one should go ahead with those transactions with requisite precaution.



21. FRAUDSTERS IN THE PRETEXT OF RECOVERY AGENTS

**Do's:**

- ✓ Always ensure identification of Recovery Agents before making any payment / commitment. Check whether agent carries a copy of the recovery notice and the authorization letter from the bank along with the identity card issued to him by the bank or the agency firm. You can also cross verify with the home branch over phone.
- ✓ Report the incidence to the nearest Police Station and your home branch.



Fraudster collects money:

"Okay. I will pay Rs.5000/- now and remaining in next few months."



"Ok sir. I am doing this as a special favour. You can collect the receipt and pending dues position directly from the bank branch"

After few days another recovery agent approaches Raju at his residence:



"Good evening Sir. I am Ravi, Recovery Agent from XYZ Bank. Please see this recovery notice issued by bank stating that you have missed your last three EMIs and bank may go forward with seizure of vehicle. You may either pay directly at the bank or hand over to me against receipt."

"How come? I have already paid Rs.5000/-few days before to your agent"



"That is not possible sir. I am the authorised agent for XYZ bank in this area. Please see my ID Card and the authorization letter from the bank for recovering dues. Did you see his ID? Do you have any proof of making payment?"



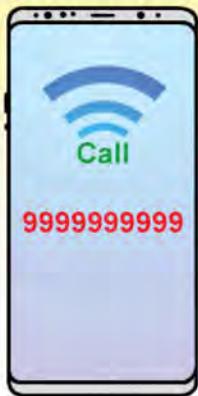
Don't's

- ✗ Never make any cash payments to bank/ recovery agents without proper acknowledgement of receipt.



22. SOCIAL WELFARE SCHEME FRAUD

One day, Raju got a call from an unknown number.



"I am calling from the agriculture department. Your account details have not been updated for the KISAN scheme, hence your subsidy funds around 12000 Rupees are lying unused with us."



"What should I do to update the account?"



"You can visit the website and update on your own, or else, I will update it if you provide me your details."



Do's:

- ✓ Verify the details of any government scheme from your Gram Panchayat or Tehsildar office before making any payment for getting the subsidy.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.





23. MULTI-LEVEL MARKETING (MLM) SCAMS

Raju's friend Krishna visited him to explain about a scheme with good earning potential.



"Hi Raju! I came across a fantastic opportunity to make money with minimal time and investment."



"Is it? Sounds exciting!!! Tell me more about it. I want to know everything."



"You must buy XYZ company products for Rs 20,000, and you will get a mobile phone of Rs 10,000/- for free. After you enrol three more people, you will get a commission of Rs 3,000 per person as you bring more and more people under the scheme."



Do's:

- ✓ Stay away from people trying to get you into these kinds of schemes.
- ✓ Verify the authenticity of the Multi Level Marketing scheme. Some of the network marketing schemes, like Ponzi scheme, Pyramid scheme etc., are illegal in India under the Direct Selling Guidelines, 2016 and the Prize Chits and Money Circulation Schemes (Banning) Act, 1978.
- ✓ Politely say no, even if the proposer of such a scheme is your friend or relative.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.



"This is a fantastic way to make money. I don't have to work every day as the agents recruited by me will be working on my behalf, and I will get commission on sales made by them."



"Yes, Raju. Therefore, I am visiting you. You may join my team as my agent."



Raju immediately filled up the form and agreed to become a direct selling agent of the multi-level marketing company.



However, sales were dismal and nonexistent. He could not accomplish the targets set by the company of recruiting 3 more agents, and he lost Rs 20000 as the products bought by him from the company also could not be sold. He did not get any mobile either.



Don't:
X Do not pay money to unknown companies and enrol in unknown schemes.



24. WORK FROM HOME SCAM

A fraudster advertises jobs over the internet and social media with attractive pay for working from home. (Earn Rs 1000 per day working from home).



Raju is very excited after coming across the advertisement and clicks on the link to register for work from home. Raju receives a call from a stranger.



"Sir, thank you for registering with our agency. We have gone through your CV, and you are selected for the work from home job. You need to provide your Aadhaar and PAN card details. You will also have to fill up some forms and sign some documents as per our company policy."



"Thank you. I will fill all the forms and send you my address proof and PAN card details."



Do's:

- ✓ Beware of short URLs, information requested on Google forms from unknown sources.
- ✓ Look for poor spelling, grammar in emails, SMS, and portals.
- ✓ Be cautious of the links/forms asking for personal information.
- ✓ Always check the header of emails for verifying the genuineness of the offer or entity.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.



"You can start working from tomorrow. You need to upload your work on the www.workfromhome.com portal. Here is your User ID and password. You also have to provide a security deposit of Rs 10000."

Raju makes the payment of Rs 10000 as a security deposit to the fraudster. The job progresses smoothly for a week. Raju kept receiving regular payments. He got 7000 Rs as remuneration.

In the next week, the agency started identifying mistakes; they consolidated the errors and produced a bill of Rs 1 lakh as compensation to the agency as per the terms and conditions of the contract signed by Raju initially.

Rs 1 lakh as compensation

Raju started receiving multiple harassment and recovery calls from different numbers in a single day.

He got calls from 'lawyers', 'police' threatening legal action and then, terrified with all this, Raju paid Rs 1 lakh to the fraudster.

Don'ts:

- ✗ Never send sensitive, personal, or proprietary information (Aadhaar or Pan card) via email to unknown people.
- ✗ Never sign any online agreement before consulting a lawyer.
- ✗ Never pay to get a job, genuine firms never ask for deposits



25. ONLINE SHOPPING FRAUD

One day, Raju received a message from an unknown number advertising mobile phones at a very cheap price. Out of curiosity, Raju clicks on the link and was surprised to see smartphones at a 50% discount. Raju contacted the number mentioned on the website.



Do's:

- ✓ Always shop from secured websites. It is recommended to make sure the websites show a tiny lock icon or 'https', in the checkout browser, indicating transactions are secure.
- ✓ Report the incident to the nearest Cyber Crime Police Station & National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.



Don'ts:

- ✗ Never do online shopping from unknown websites.
- ✗ Never buy anything from online sellers that accept payment only by gift cards, money transfers, etc., as such payments are nearly impossible to trace and reverse.
- ✗ Never pay in advance to unknown sites, as chances of getting a product are negligible after payment has been done.



26. FRAUD USING PUBLIC WI-FI

It was a Sunday. Raju and his family were in the shopping mall. Raju bought some clothes and groceries and went to the reception to make the payment.

"Your total bill is Rs 12000, Sir.
How would you like to pay, card
or cash?"

RECEPTION

"I will pay online."

Raju initiated the payment
but there was a network issue.

"I am facing connectivity
issues during the transaction.
Can you help me with this?"



"Sir, you can connect to the free
Wi-Fi if your network is
not working."

- Do's:**
- ✓ One should always use a secured Wi-Fi network.
 - ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.



Raju connected to the free Wi-Fi and completed the transaction."

"Thank you for shopping here, Sir!"



Raju was happy. His day was spent well.

After some time, he started receiving SMS alerts from his bank. Rs 14000/- and Rs 10000/- were debited from your account.' Raju was confused.

The last transaction he made was Rs 12000/- at the mall, and these transactions were different. He told his son about the messages.

"What was the last transaction, Dad, and where did you do that?"



"You used free Wi-Fi for the financial transaction? That is not safe, Dad. Hackers use this Wi-Fi to get access to users data and use it for illegal purposes."

"I made the last transaction at the shopping mall; I paid the bill online. My network was not working so I connected to free Wi-Fi and made the payment."



"Really? I was not aware of that, son."



"When you used the Wi-Fi network for the financial transaction, some hacker got access to your personal data and used it for unauthorized transactions from your bank account. That's why you are getting these messages."



"Oh God!! I made a big mistake. What can we do now?"



"We must immediately visit your bank and ask them to block your account."



(Raju became a victim of hackers by using public Wi-Fi for financial transactions.)

Don'ts:

- ✗ Do not use public Wi-Fi, especially while doing financial transactions. It is easy to hack into a laptop or mobile device that is on a public Wi-Fi connection with no protection. Hackers can read your emails, steal passwords and other credentials.



27. FAKE ADVERTISEMENTS/OFFERS

Poster:

DIWALI BUMPER OFFER -
THREE BRANDED
WATCHES WORTH RS
2500/- FREE FOR EVERY
SINGLE WATCH
BOUGHT!! HURRY UP!
LIMITED PERIOD OFFER!!

Please call
Ph: 90xxxxxxxx99
for more details!

"Wow!! This seems great!
I can buy one watch
and get 3 free! Anyways,
I wanted to give gifts to
my cousins this Diwali holiday
when I go home! I'd
better call before the offer ends."



"Hi. I came across your
Branded watch offer.
Where is your location?
I can come down to your
store for the purchase."



"Sir! You are lucky.
We are about to close the offer.
You need not come here,
Sir. We will deliver you
the product at your address."



Do's:

- ✓ In the case of branded products, verify the advertisements on official websites.
- ✓ For non-branded product advertisements, make a payment only after a personal visit to the shop or on delivery.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.



"That's great! Please send me pictures of the watches."



"Okay, I have shared my address.
I'll send the money right away."



"Sure, Sir. I have shared them already.

I have also shared account details
for transferring the amount.
You must pay Rs 3000 to confirm the order.

Once payment is successful,
we will deliver the watches
within 3 days. Hurry up, Sir.
The offer ends in
another 30 minutes.

Happy Diwali!!"



"Oh no! Why haven't they delivered yet!!? Their phones are switched off..How do I trace them now!!? I think I have lost the money!"

Raju indeed lost his money.

Don'ts:

- ✗ Don't be misled by tall claims made in advertisements. Check and verify before committing your hard-earned money.
- ✗ Do not pay any amount unless you receive the product.



28. FAKE LOAN OFFER

Raju is a humble farmer trying to make both ends meet.

One day, he received a call from a stranger.

"Hello, Mr Raju. We are calling from xyzzy Pvt Ltd. We have introduced a scheme for farmers in your region. You have been found eligible for availing a loan from our company at a subsidized rate."



"Oh! Okay. That would be helpful. What is the offer?"



"We offer special loans up to Rs 5 lakhs at an interest of just 3%! For availing this loan, you need to share your bank account and Aadhaar details for verification."



"Okay. I will think about the same and will let you know."



Do's:

- ✓ Always check the details of the lender (like their physical address/official website, etc.) before availing their loans.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.



"Sir, this offer is valid only for today. You need to send a processing fee of Rs 5000 immediately to avail of this offer. I have shared the account details for transferring the fee."



"Okay, Sir!! We will update you on the loan application within a week! Thank you."



"Oh! Is that so? Then I'll send the processing fee now. I will also send the rest of the details to your number soon."



Raju makes the payment. However, even after weeks, he does not receive any response from the company, and the number from which he received the call no longer exists.



Don't:

- ✗ Never make any upfront payment for sanctioning your loan. Banks and Financial Institutions never ask for advance fee for loan approval. Charges, if any, will be deducted from your loan money and balance amount will be transferred to your account.



29. CREDIT CARD ACTIVATION FRAUD

"Hello, Mr Raju. I am calling from XYZ Bank. Congratulations on your new credit card, Sir!"

"Yes, thanks; I received it."

(Raju recently got delivered a XYZ bank credit card):

Raju (believed the fraudster as he already had his credit card details):

"Okay. Please activate my card."

"Your name is Raju Deshpande. Your address is Lower Parel, Mumbai?"

"That's correct."

Do's:

- ✓ Call the bank to block the card/bank account/UPI services to prevent further monetary loss.
- ✓ Send an email /letter / visit your home branch to report the incidence.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.

A four-panel comic strip illustrating a scam. In the first panel, a man in a purple shirt asks for a card number. In the second panel, a woman in a purple shirt confirms it's 4500 1000 1000 1000. In the third panel, the man asks for expiry date and CVV. In the fourth panel, he asks for a code, and the woman provides it. A bottom panel explains that Raju received an SMS about a large debit from his credit card, which was defrauded under the pretext of activation.

"Your card number starts with 45. Kindly confirm the number."

"Sure. It's 4500 1000 1000 1000."

"Thanks for the confirmation. Kindly confirm the expiry date and card verification value (CVV) written behind the card."

"Yes, the expiry date is 01/25 and 111 is the CVV number."

"Yes, it's 123456."

"Thanks for the confirmation. Your card is activated now, and you will receive an SMS regarding this within the next hour. Have a nice day!"

"Thanks for the confirmation, Sir. You must have received an SMS for the final activation. Kindly confirm the code received on your phone."

Raju received an SMS from his bank, about debit of Rs 1.2 lakhs on his credit card. Here, Raju was defrauded under the pretext of credit card activation.

Don'ts:

- ✗ Never share your Card details and OTP to anyone.
- ✗ Don't trust unknown callers for your credit card activation. Credit cards can be activated from your mobile banking application.
- ✗ Don't share your card details/OTP with anyone, banks never ask for OTP.



30. CREDIT CARD LIMIT UPGRADATION FRAUD

Another day, Raju received a call from the bank.

Hello, Mr Raju.
I am calling from XYZ Bank.
Congratulations, Sir.
Your credit card is
eligible for a limit upgrade."



"Oh, thanks.
What will be the new limit?"



"The new limit will be
increased to Rs 5 lakh
from your current limit
of Rs 1 lakh."



"Oh, that's great!"



Do's:

- ✓ Immediately call the bank to block the card/account/UPI service to prevent further transactions.
- ✓ Send an email /letter / visit your home branch to report the incidence.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.



Sometime later, Raju received an SMS from his bank about debit of Rs 70000 on his credit card.
He was cheated by the fraudster.

Don'ts:

- ✗ Don't trust unknown callers for credit card activation / limit enhancements.
- ✗ Don't share your card details/OTP with anyone.



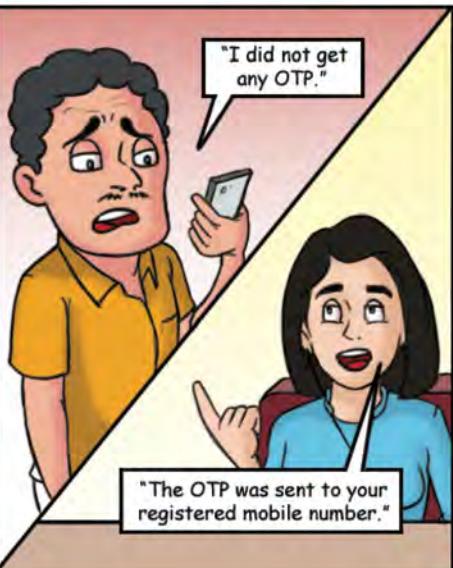
31. SAFE GUARDING YOUR AADHAAR CARD

One day, Raju went to his bank branch to get his Aadhaar card linked with his bank account.

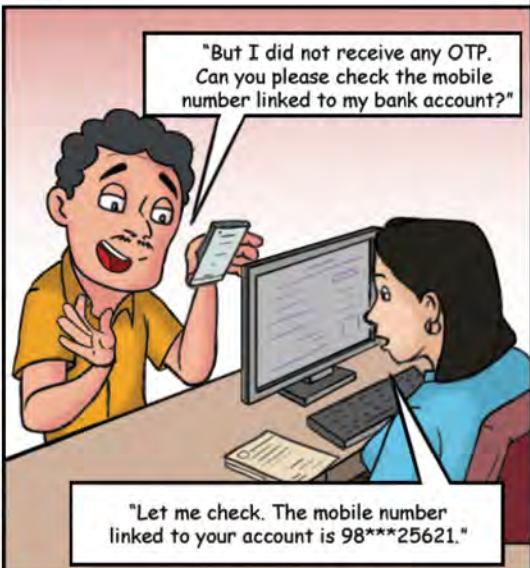


Raju submits the required documents.

"Please submit the Aadhaar linking form and photocopy of your Aadhaar card. Also, show me your original Aadhaar card."



"The OTP was sent to your registered mobile number."



"Let me check. The mobile number linked to your account is 98***25621."

Do's-

- ✓ Verify the mobile number linked with your bank account.
- ✓ Check your bank statements and passbook regularly to identify any suspicious activity.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.





32. ONLINE FRAUD USING CASHBACK OFFERS

Raju is very active on the internet and always prefers online shopping as E-commerce websites provide attractive offers on their products.

"Hello Sir! I am calling from ABC.com.
Sir, we are glad to inform you that we are providing you with a 50% cashback on your recent purchase from ABC.com."



"Oh really. 50% cashback is huge. Thank you so much...!"



"You are our valuable customer, Sir."



"Okay, so tell me. When will the cashback be credited to my account?"



"It won't take much time, Sir. You need to open the app, and there will be a pop-up message regarding the cashback."



Dos-

- ✓ Inform your home branch and block your account to prevent further financial loss.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.

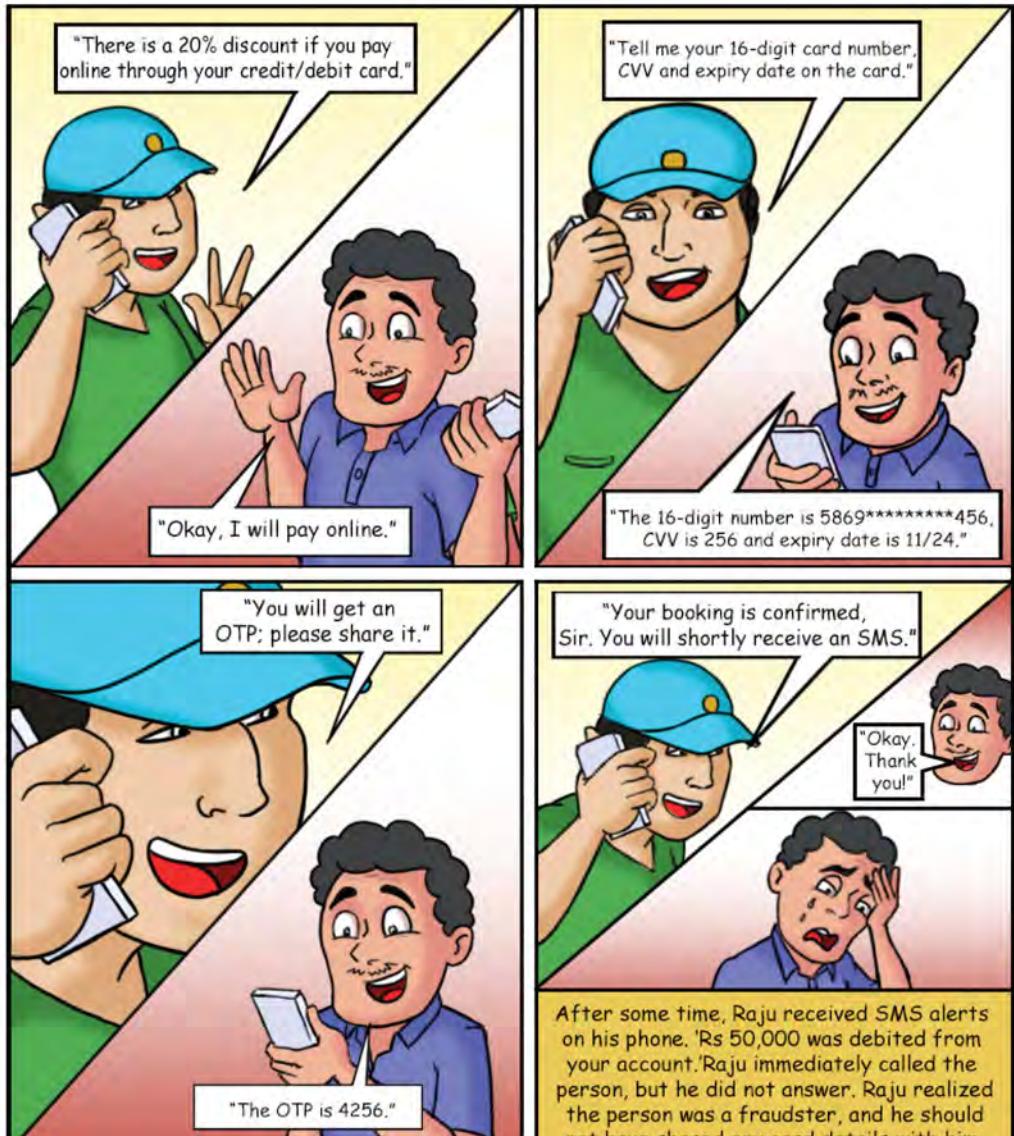




33. DISCOUNT FRAUD

**Dos-**

- ✓ Always verify the authenticity of a person/institution offering any deal or offer.
- ✓ OTP SMS will have other details like amount / merchant name / beneficiary name of intended transaction. Always read the OTP SMS alerts thoroughly before use.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.



Don'ts-

✗ Don't share your Credit/Debit card details and OTP with anyone.



34. CHARITY FRAUDS

Raju is a Government school teacher.

He came across a news report that Actor Monu was gifting smartphones to government school students.

NEWS REPORT

Actor Monu gifts 100 smartphones to Government school students

Raju searched on the internet about the actor's charity foundation and called up the number.

MONU charity Foundation

"Hello, Sir. Is this actor Monu's charity foundation??"



"Hi Sir. This is his office's number. I am his personal secretary. How may I help you?"



Do's-

- ✓ Always cross-check charity organizations' credentials on the Goverment website /database to see if they are genuine or fake.
- ✓ Always be vigilant because the fake website may look almost identical to a genuine charity site, changing only the details of where to send donations.
- ✓ Scammers often use high-pressure tactics, such as stressing the urgency and using highly emotive language. Always be cautious of anyone claiming that donations need to be immediate.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>



"Sir. I am Raju, calling from xxxx government school. I saw the news of your charity to the students. Sir, we have 100 poor students in our school who cannot afford laptops / smartphones. Can you please help us, Sir?"



"That would be great! Sir."



"Okay, Sir. I'll send you the registration fee right away. Please share your account details."



"Oh yes! Thank you so much for reaching out to us on behalf of poor children. I assure you of help."



"Okay. Please share your address. We will send you 100 smartphones. However, you will have to pay a token registration charge of Rs 50,000/- today itself for us to send the phones. The phones will be delivered in a week, and we will refund the registration fee after delivery."



Raju transferred the funds, but he later came to know that no such mobile phones were donated to government school students. Raju realised that he had been duped by fraudsters under the pretext of charity.

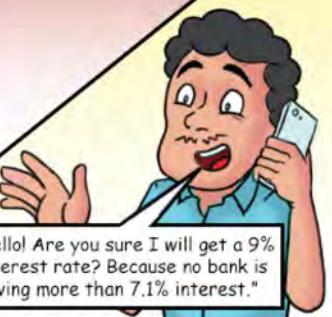
Don'ts-

- ✗ Don't call on a random number based on a google search without verification.
- ✗ Don't send money upfront without verifying the authenticity/genuineness of the claim.



35. OVERDRAFT AGAINST FD

Raju is a senior citizen, who had recently retired from his job and received a large sum of superannuation money, which he wanted to invest. One day Raju received a call from someone, pretending to be the employee/agent of a reputed bank, advertising a new scheme with a high interest rate.



"Hello! Are you sure I will get a 9% interest rate? Because no bank is giving more than 7.1% interest."

"Yes sir, this is a special scheme for a limited period only."



Raju: "Okay, I will visit the bank and open a Fixed deposit."

"Sir, our bank will send a representative to your home since you are a senior citizen."



Raju: "No, I can't hand over my money to an unknown person."



Do's:

- ✓ Check all documents before signing.
- ✓ Prefer visiting the bank branch or performing transactions over internet banking with the assistance of known person.
- ✓ Report the incident to the nearest Cyber Crime Police Station or National Cyber Crime Reporting Portal <https://cybercrime.gov.in> in case of cybercrimes.



"Sir, there is no need to hand over any money. You just need to give a crossed cheque. I will ensure that your money is not withdrawn by cash and deposited only in the fixed deposit account."



The fraudster visits Raju's home to collect the cheque and takes signatures on different forms, which Raju does not check before signing.



After a day, the fraudster visits the branch as a representative of Raju and deposits the cheque for creating a fixed deposit. However, he gave fake fixed deposit receipts to Raju and kept the original ones with himself.



The fraudster poses as a representative of Raju and uses the overdraft form signed by Raju, which has fraudster's account number for credit of the overdraft.



After a day, Raju got an SMS regarding an overdraft issued against the FD and upon visiting the branch, he was shocked to know that the FD receipt he had received was fake.

Don'ts:

- ✗ Do not hand over important documents/cheques to unknown person.



36. FRAUDS USING MALICIOUS APPLICATION

One day, Raju received a message seeking his willingness to do freelance work. As Raju was unemployed, he immediately dialled the number mentioned in the SMS.

"Hi, I received an SMS regarding freelance work. What is the work profile?"



(This is very easy, even my kid can do it.)
"Okay, I am interested."



After downloading the application, Raju started working. The work seemed genuine; however, he did not know that the fraudster was observing all his activities on his laptop.



Over time, the fraudster was able to get all the secure credentials from Raju's device through his application. Unaware of the malafide intention, Raju continues to use the application. The fraudster was also able to get the OTP sent on Raju's email since the fraudster got access to his email.

Do's:

- ✓ Verify the authenticity of the offer on the official website of the concerned entity offering jobs.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in.>"



After a few days, Raju received SMS alerts stating Rs 50,000 was debited from his account. Raju had no clue how his account was compromised or money was debited.



After investigation, it was found that his device contained a malicious application, observing all his activities and the passwords were being skimmed.



Don'ts:

- ✗ Do not download any application through links sent via SMS, email or instant messaging applications, especially from strangers, without verifying its authenticity.



37. ILLEGAL LOAN FINANCING APPS WITH EXORBITANT INTEREST RATES AND HARASSMENT TACTICS

Raju and Ramu were best friends. One day, Raju met Ramu and told him about his financial problems.



Do's-

- ✓ Be cautious while downloading any app and providing the app permission to access data from your mobile phone.
- ✓ Always check the registration status of the company/NBFC whose application is being used to provide loan and terms and conditions before availing loan from that NBFC at https://www.rbi.org.in/Scripts/BS_NBFCList.aspx.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in/>.



Within 7 days, Raju started receiving calls for repayment of Rs 7500/-.
Raju still had not arranged money to repay the old loan and gets shocked by the demand of Rs 7500/- as repayment for the Rs 5000/- loan.
Raju approached another friend, Laxman.



"I was under the impression that I will repay my loan amount along with nominal interest charges, but this app is charging exorbitant interest and many other charges. What shall I do now?"



Oh! Did you verify whether the entity is registered with RBI or have any other valid registration? Else, they would not be covered under any rules, and you are bound to pay as per the agreement only. Always check whether the finance company (NBFC) is registered / licensed by RBI



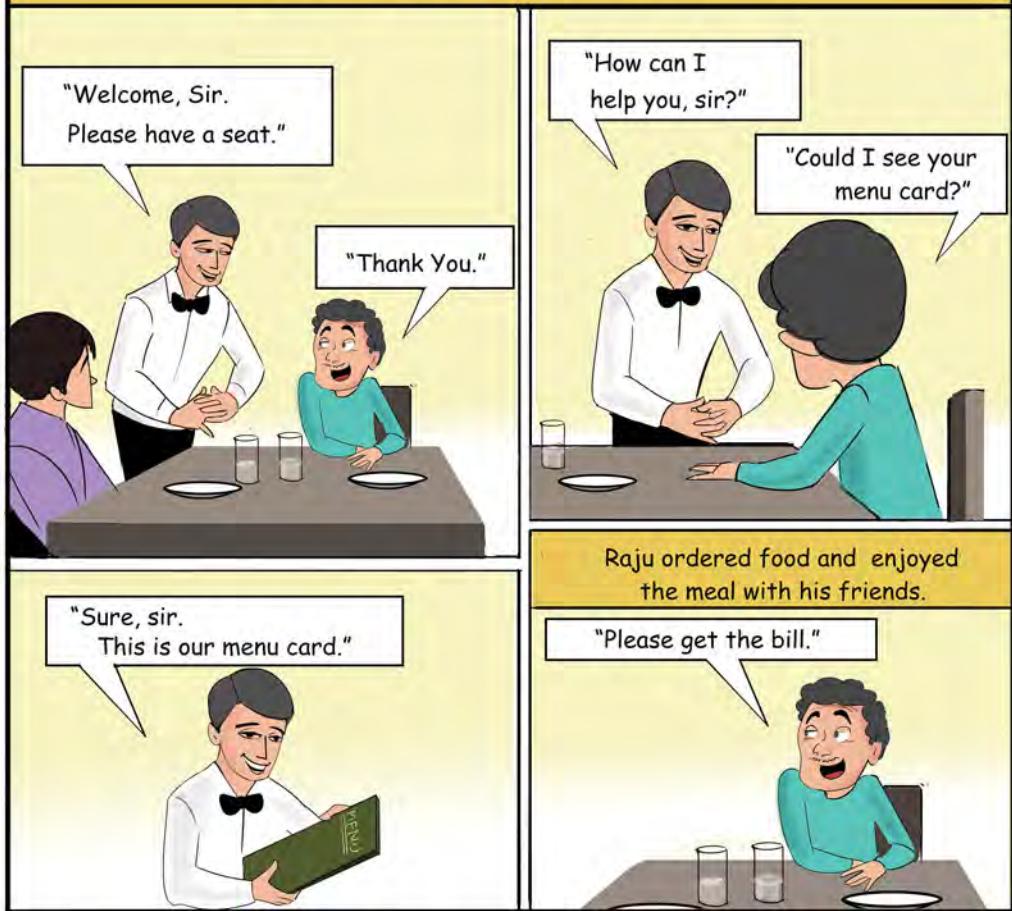
Don'ts:

- ✗ Be cautious and don't take loan if any mobile app is providing a quick loan without checking any document and credit score, and always check the interest rate charged.



38. CARD CLONING AT MERCHANT OUTLETS

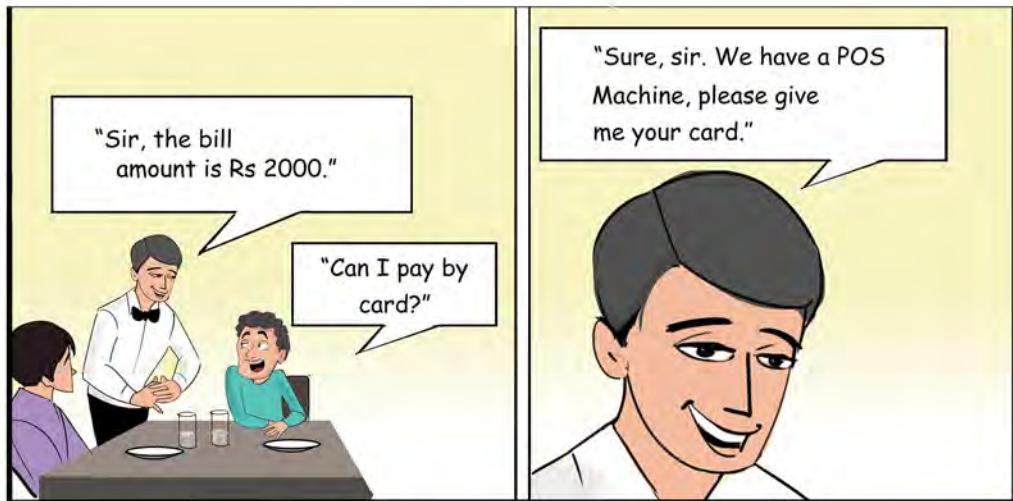
One day, Raju went to a restaurant along with his friend for lunch. He called the waiter.



Raju ordered food and enjoyed the meal with his friends.

Do's:

- ✓ Always hide your pin number while transacting through debit/credit card.
- ✓ Change the PIN at periodic intervals.
- ✓ Always ask merchants/dealers to swipe the card in your presence.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in.>"



(Waiter took the card, walked away from Raju and swiped the card in a skimmer when Raju was not paying attention.)



Later, the skimmed details of the card were given to a fraudster who cloned the card with all the card details and used those details to siphon off money from Raju's account.

Don't:

- ✗ Do not share your credit card/Debit card PIN with anyone.
- ✗ Do not let credit and debit cards out of your sight.

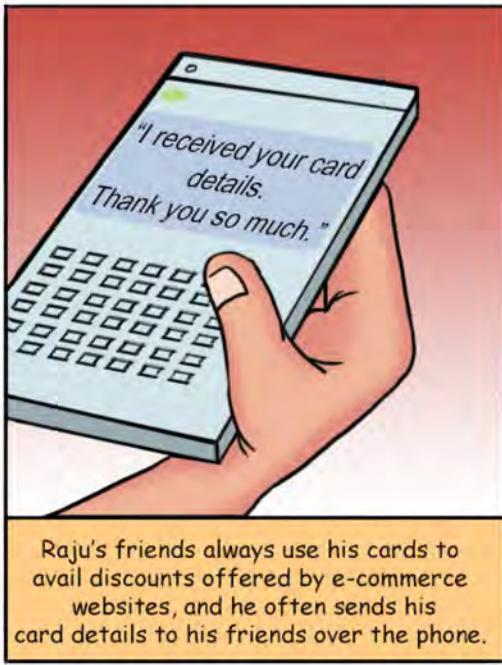


39. FRAUD THROUGH DETAILS SHARED WITH KNOWN PERSON/FAMILY/RELATIVES

Raju is a very friendly and helpful person, but he is ignorant when it comes to protecting his financial credentials or bank details. One day Raju received a call from his friend, Keshav.



"There is an exciting offer on xyz e-commerce website. It requires a creditcard issued by abc bank. You are using this card. Can you send me the details of your credit card over phone? I will pay you later."



Do's:

- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.
- ✓ Change the PIN at periodic intervals.



After a month, Raju received an SMS on his mobile number and was unable to figure out where the card was used.

Raju registered a complaint with the bank. The bank further informed him that the disputed transactions were done at an online merchant site.



Raju realised that he himself had never done any payment at the online site, but he had shared his card details with his friends. Raju immediately contacted all his friends, but everyone informed him that they did not do the transaction.



"Oh! Keshav, you should have told me about this incident, I would have blocked the card. I should not have shared my card details over the phone."



Don't:

- ✗ Do not share your card details over social media or messaging apps even if the recipient is your friend / relatives / family.

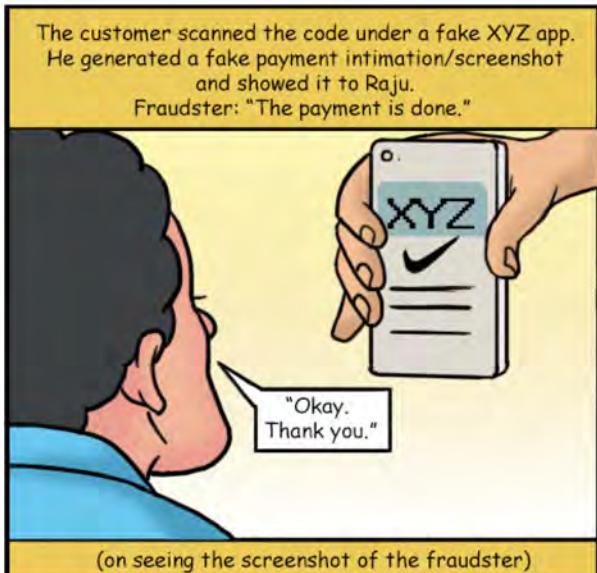


40. PAYMENT SPOOFING APPLICATIONS.

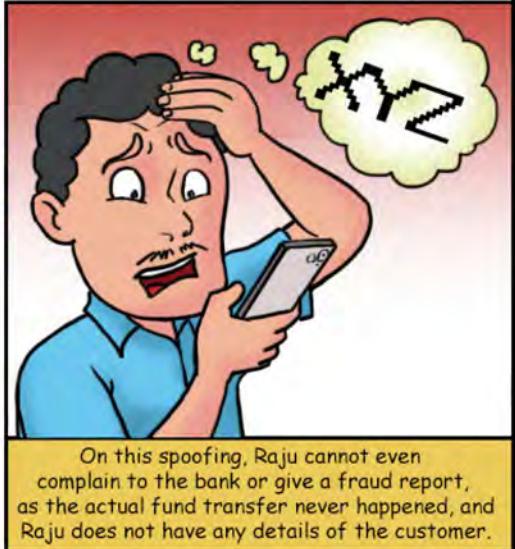
Raju is a friendly retail shop owner. He was sitting at his shop when a customer came and purchased something.

**Do's:**

- ✓ Always check/confirm transactions by checking your bank account whenever a transaction is done through UPI.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at <https://cybercrime.gov.in>.



At the end of the day, Raju cross-checked his shop account for reconciliation and found that one payment was not yet received in his account. Now he realized that he was duped by showing a fake screenshot.



Don't:

- ✗ Don't conclude financial transaction without actual receipt of fund.



Office of the RBI Ombudsman (Mumbai-II) Maharashtra And Goa

Design, content & execution: Raj Kumar, M Muralidhar, Forum Modi, Vishwas Krishna, P P Bhagat
Cover Design, Layout & Illustration by **StoryMirror**

