BE A CYBER JAGROOK CITIZEN

CYBER NETRA

COMIC BOOK ON CYBER INCIDENTS & PREVENTIVE MEASURES

BY CISO OFFICE

यूको बैंक UCO BANK

(भारत सरकार का उपक्रम) (A Govt. of India Undertaking)

सम्मान आपके विश्वास का Honours Your Trust

विज़न

सूचना की सुरक्षा हेतु बैंक के लिए
एक सुरक्षित साइबर स्पेस बनाना

Vision

To build a secure and resilient cyber space
for the Bank to protect information

मिशन

बैंक की बुनियादी संरचना, व्यक्ति, प्रक्रिया और प्रौद्योगिकी
के सम्मिलन से साइबर स्पेस में सूचना तथा बुनियादी संरचना
की सुरक्षा करना, साइबर के खतरों को रोकना एवं अनुक्रिया करना

Mission

To protect information and information infrastructure in cyber space, build capability to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of the Bank infrastructure, people, process and technology

TABLE OF CONTENTS

यूको बैंक
UCO BANK

From the Desk of MD & CEO

To all the UCOites & valued Customers,

In this age of technological marvels, where every click connects us to a world of possibilities, the digital realm unfolds both promise and peril. ***'Cyber Netra'*** emerges as our beacon in this digital expanse, a testament to our commitment toward fostering a cyber-secure society.

Within the vibrant pages of this comic book, we embark on a journey that transcends the boundaries of conventional wisdom. As we navigate these vividly illustrated narratives, we embrace not just stories, but invaluable lessons encapsulating the complexities of our digital ecosystem.

Today, as the custodians of this digital era, our responsibility extends beyond mere participation; it demands vigilant guardianship. ***'Cyber Netra'*** isn't just a compilation of narratives; it's an initiative, a call to action. It beckons each of us to become torchbearers of cyber awareness, equipped not just with information but fortified with the wisdom to discern and defend.

I invite you to immerse yourselves in these tales, to glean insights, and to heed the counsel of our Cyber Rakshak. Let us transform this knowledge into a shield that safeguards not just ourselves but our digital community.

Together, let us script a narrative where cyber awareness transcends from the pages of this book into the ethos of our daily lives.

Let 'Cyber Netrya' ignite the flames of cyber awareness, inspire a collective resolve, and empower each one of us to champion a safer digital world.

STAY AWARE. STAY SAFE.

With warm regards,

[Ashwani Kumar]

MD & CEO

From the Desk of Executive Director

Esteemed Readers,

In an era where our daily lives intertwine seamlessly with the digital landscape, the significance of cyber awareness cannot be overstated. 'Cyber Netrya' stands as a testament to our unwavering commitment to cultivating a community empowered with cyber literacy and resilience.

The vibrant tapestry of 'Cyber Netrya' unfurls within these pages, offering not just narratives but profound insights into the complexities of the digital sphere. As we immerse ourselves in these graphic stories, we embark on a journey of enlightenment, where each tale serves as a guiding light toward heightened cyber consciousness.

The aim of this initiative transcends mere storytelling; it aspires to cultivate a culture of proactive cyber vigilance. Each stroke of the artist's pen and every line of dialogue within this comic book serves a purpose - to enlighten, to inform, and to empower.

Dear Readers, I urge you to not merely read, but to absorb the wisdom encapsulated within these illustrated tales. Let the experiences of our Cyber Rakshak resonate as guiding principles, igniting within each of us a flame of awareness that illuminates our path through the digital labyrinth.

As we turn these pages, let us not confine the lessons learned within this book's confines but endeavor to transpose this knowledge into actionable steps. Let 'Cyber Netrya' be the catalyst that transforms passive knowledge into proactive guardianship, shaping a digital landscape fortified by our collective cyber awareness.

With unwavering determination and an open heart, let us embrace the insights offered within 'Cyber Netrya' and take steps towards a safer and more secure digital future.

With warm regards,

[Rajendra Kumar Saboo]

Executive Director

From the Desk of Executive Director

Dear UCOites, our valued Customers & beloved Citizens,

As we delve into the realm of *'Cyber Netra,'* we embark on a transformative journey into the heart of cyber consciousness. This unique comic book stands not just as a repository of stories but as a testament to our commitment in nurturing a digitally resilient community.

Within these vividly illustrated narratives lies a treasure trove of insights, a tapestry woven with threads of cyber wisdom. *'Cyber Netra'* endeavors to transcend the conventional boundaries of cyber education by presenting complex concepts in an engaging and accessible format.

This initiative isn't merely about flipping pages; it's about embracing a mindset shift. It beckons us to not only absorb the captivating narratives but to internalize the essence of cyber awareness embedded within each graphic depiction.

As the digital landscape evolves, so must our understanding and preparedness. I encourage you to traverse through the corridors of *'Cyber Netra,'* not as passive readers but as proactive ambassadors of cyber vigilance.

May this comic book kindle the flames of awareness, inspire conversations, and instigate a collective movement toward a safer digital ecosystem. Let us embrace this endeavor as a catalyst for change, fostering a community where cyber literacy becomes our collective strength.

With optimism and determination, let us embark on this journey together, poised to transform knowledge into action, and awareness into a shield for a secure digital tomorrow.

Best Wishes,

[Vijay N. Kamble]

Executive Director

From the Desk of Chief Vigilance Officer

To all my esteemed Colleagues and valued Customers,

In an era where the digital and physical worlds converge, vigilance becomes our foremost line of defense. As we step into Vigilance Awareness Week, the significance of proactive vigilance—both in cyberspace and in our everyday responsibilities—cannot be overstated. It is during such times that we reaffirm our commitment to integrity, transparency, and security.

I am proud to introduce ***'Cyber Netra,'*** not just as a comic book but as a dynamic tool for empowering each one of us to stay alert in this rapidly evolving digital landscape. This graphic narrative serves as a powerful reminder that cyber vigilance is an extension of our core values of honesty, responsibility, and protection.

'Cyber Netra' brings to life stories that highlight the real and present dangers of the cyber world, showcasing the vital role each of us plays in safeguarding not only our digital interactions but also the collective security of our institution and community. Through its engaging format, it reinforces the idea that cyber vigilance is a shared responsibility, one that is critical for maintaining trust and ensuring a safe digital environment.

Dear Colleagues and Citizens, let this comic serve as a guide to building your awareness and a reminder that vigilance must be constant, whether in identifying fraud, spotting misconduct, or defending against cyber threats. It is not only about avoiding risks but about cultivating a culture of awareness, integrity, and accountability in every aspect of our lives.

As we observe Vigilance Awareness Week, let us embrace the lessons within '***Cyber Netra'*** and renew our pledge to uphold the values of vigilance. Together, we can transform awareness into action, ensuring that we remain vigilant custodians of not only our digital world but also our ethical commitments.

With steadfast dedication,

[V. Anand]

Chief Vigilance Officer

From the Desk of
Chief Information Security Officer

To all my dear Colleagues & valued Customers,

In the digital symphony of our interconnected world, the melodies of innovation harmonize with the dissonance of emerging cyber threats. ***'Cyber Netra'*** emerges not just as a comic book but as a foundation in our shared mission to strengthen cyber preparedness.

Within the pages of '***Cyber Netra'***, we uncover not just narratives, but secrets to navigating the intricate labyrinth of cyberspace. The book aims not to overwhelm with jargon but to empower with practical wisdom, elevating cyber literacy to the forefront of our digital consciousness.

As the custodian of our Bank's cyber defenses, I implore you to embrace ***'Cyber Netra'*** as more than a book; it's a compendium of tools to fortify your cyber citadel. Let this book be a catalyst for transformation, propelling us from passive observers to proactive defenders of cyber sanctity. Together, let us heed the call for cyber awareness, not just within these pages but within our daily digital interactions.

May ***'Cyber Netra'*** resonate as a beacon of cyber consciousness, inspiring a movement where every click, every interaction, echoes the chorus of informed vigilance. Let the guidance from our Cyber Rakshak serve as pillars, anchoring us amidst the turbulence of evolving cyber threats.

With unwavering resolve, let us unite, armed with knowledge and pledge to amplify cyber awareness, transforming vulnerabilities into strengths and uncertainties into preparedness.

With warm regards,

[Mohammad Sabir]
Chief Information Security Officer

NAVIGATING EMERGENT CYBER TRENDS

In our rapidly evolving digital landscape, the surge of emergent cyber trends has reshaped the way we interact, transact, and navigate the virtual sphere. With technological advancements come new avenues for innovation and connectivity, but alongside these opportunities lurk evolving cyber threats and vulnerabilities.

Greetings and welcome to *'Cyber Netra,'* our initiative towards fostering cyber awareness through the power of storytelling and graphical representation. This comic book delves into the ever-evolving landscape of cyber trends, presented in an engaging and illustrative format to educate and empower our readers.

Within these pages, *'Cyber Netra'* unfolds stories that vividly portray emergent cyber scenarios. Through these graphical narratives, we aim to shed light on prevalent cyber threats, showcasing the importance of cyber vigilance and providing insights into safeguarding against evolving digital risks.

MEET OUR AVATAR OF CYBER AWARENESS
CYBER RAKSHAK

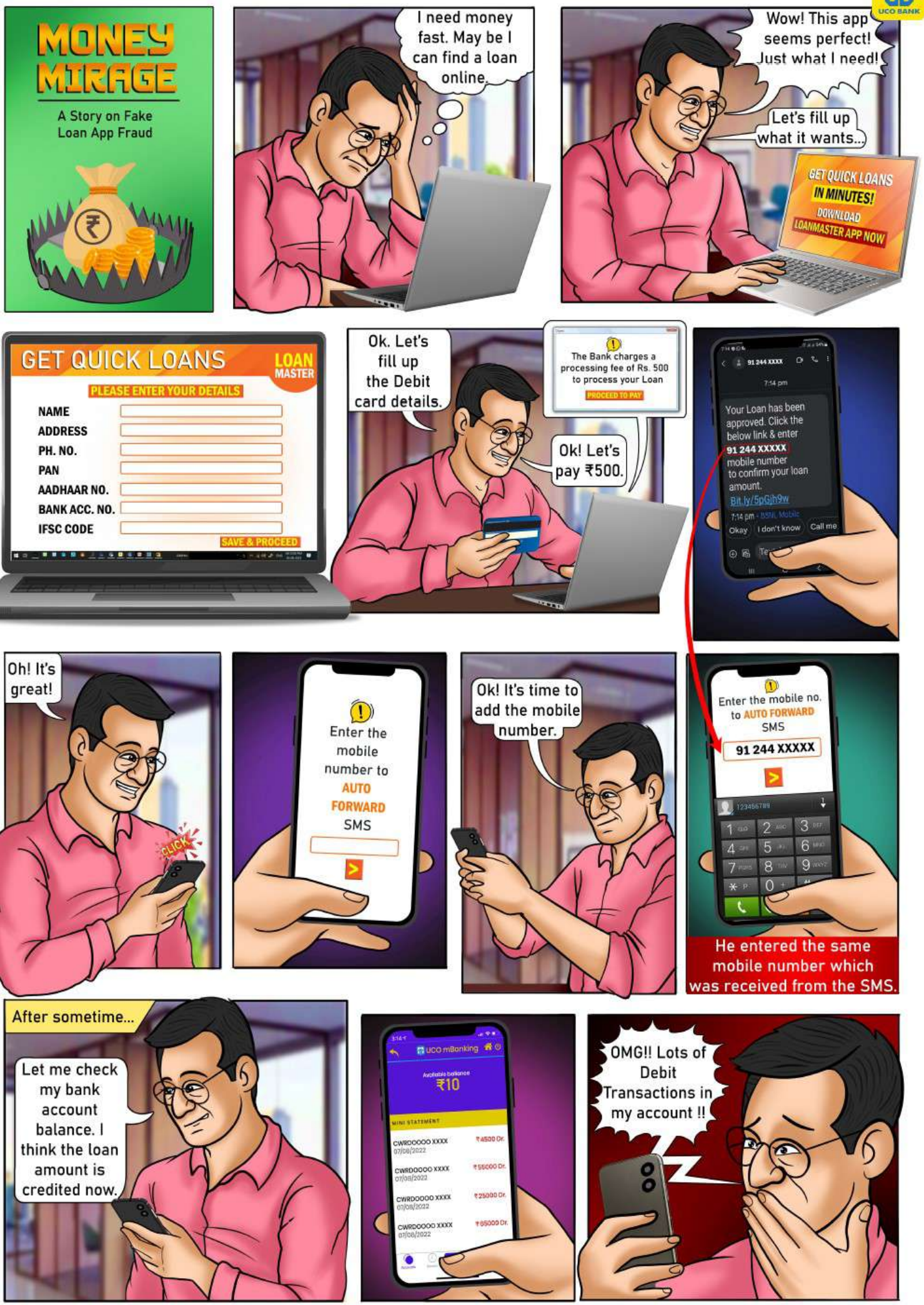
These two iconic mascots have been crafted to embody the essence of cyber awareness and best practices. As you journey through the tales in *'Cyber Netra,'* our Cyber Rakshak will stand as beacons of guidance, illustrating key cyber security practices at the conclusion of each story.

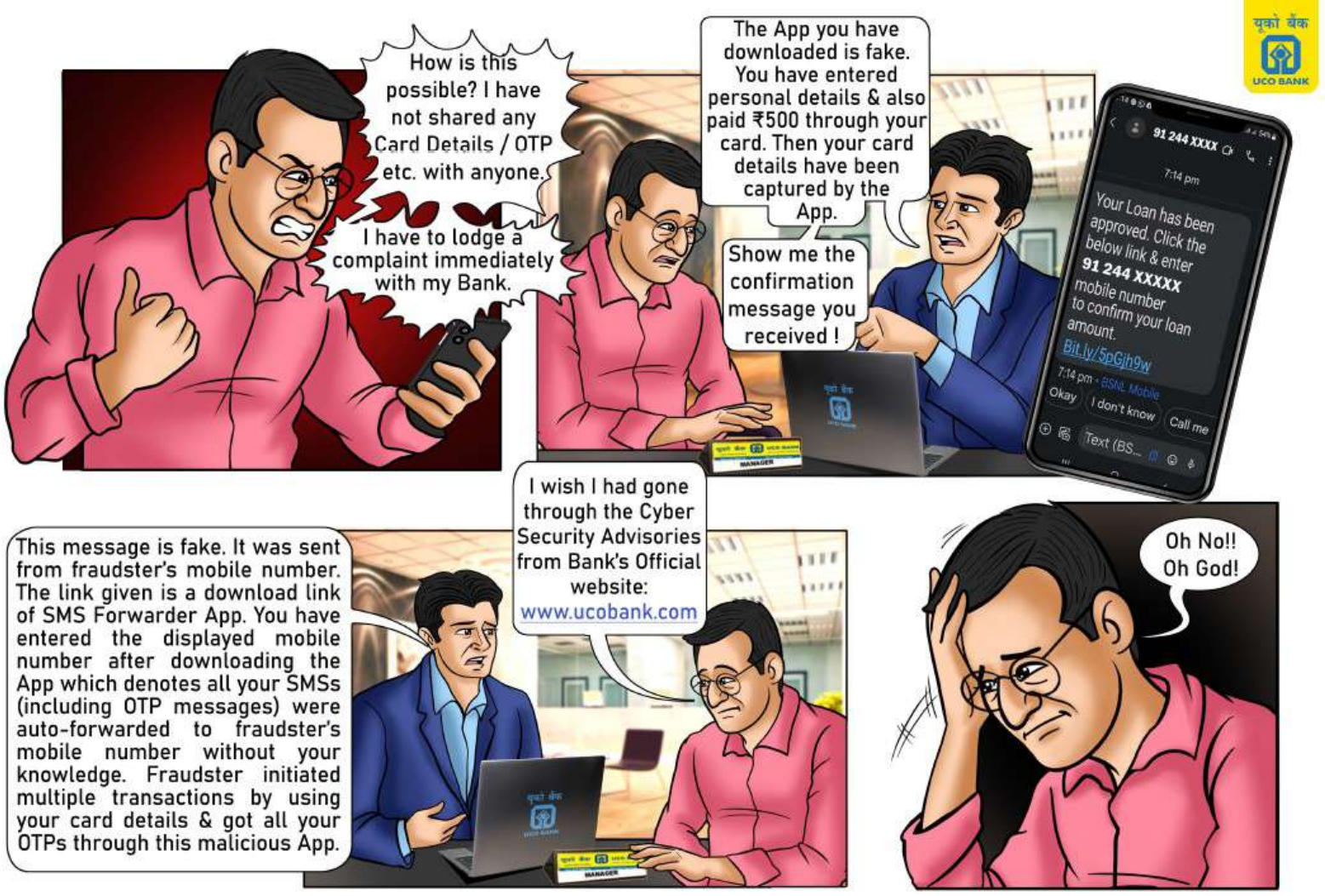
Join us in this insightful exploration as *'Cyber Netra'* unfolds the realms of cyber consciousness, with our Cyber Rakshak leading the way to a safer digital world.


DECEPTIVE DIALERS
A story on Fake Customer care hazard
Well. It's lunch time at the office. Let's book the tickets for the family vacation from IRCTC now.
Ohh! my IRCTC account Got Blocked!
Let's search something in the Internet.
Ahh!! here I got some helpline numbers in the Internet. Let's call, I hope it will solve the issue.
91 244 XXXX
Hello ! This is Raj. My IRCTC Account is blocked. Please activate my account.
I have to book some tickets urgently.
Sure Sir, We can help you unlock your account, but there's a small convenience fee of Rs. 10/-.
That's not a problem. Please quickly activate my account !
Dear customer, Please click he below link & pay the convenience fee for your IRCTC account.
CLICK
http://www.fakepayment.mysite/
Card Details
Enter your card information or use the camera
Name
Card Number
Expiration Date
CVV Code
Pay Rs. 10
Oh No!! It's showing payment error again!
PAYMENT ERROR !
Close
No problem Sir, It may occur due to server problem.
Give me few minutes to process the refund request on your behalf.

Beware! Fraudsters can't dupe you if you never rely on fake customer care numbers appearing in search engines

- Avoid searching customer care or helpline number related information in search engines because fraudster may display misleading information/ads to lure users.
- Always refer the official website or app of the organization to find legitimate customer care or helpline number related information.
- Never share sensitive, personal or financial information, such as card details, CVV, PIN, OTP, UPI PIN, financial credentials etc. with anyone under any circumstances.
- Most of the OTP messages mention the reason for generation of the OTP. Read every message carefully before taking any action.
- Immediately report cyber fraud incident at Cybercrime Helpline No. **1930** & lodge complaint at National Cybercrime Reporting Portal (**https://www.cybercrime.gov.in**).

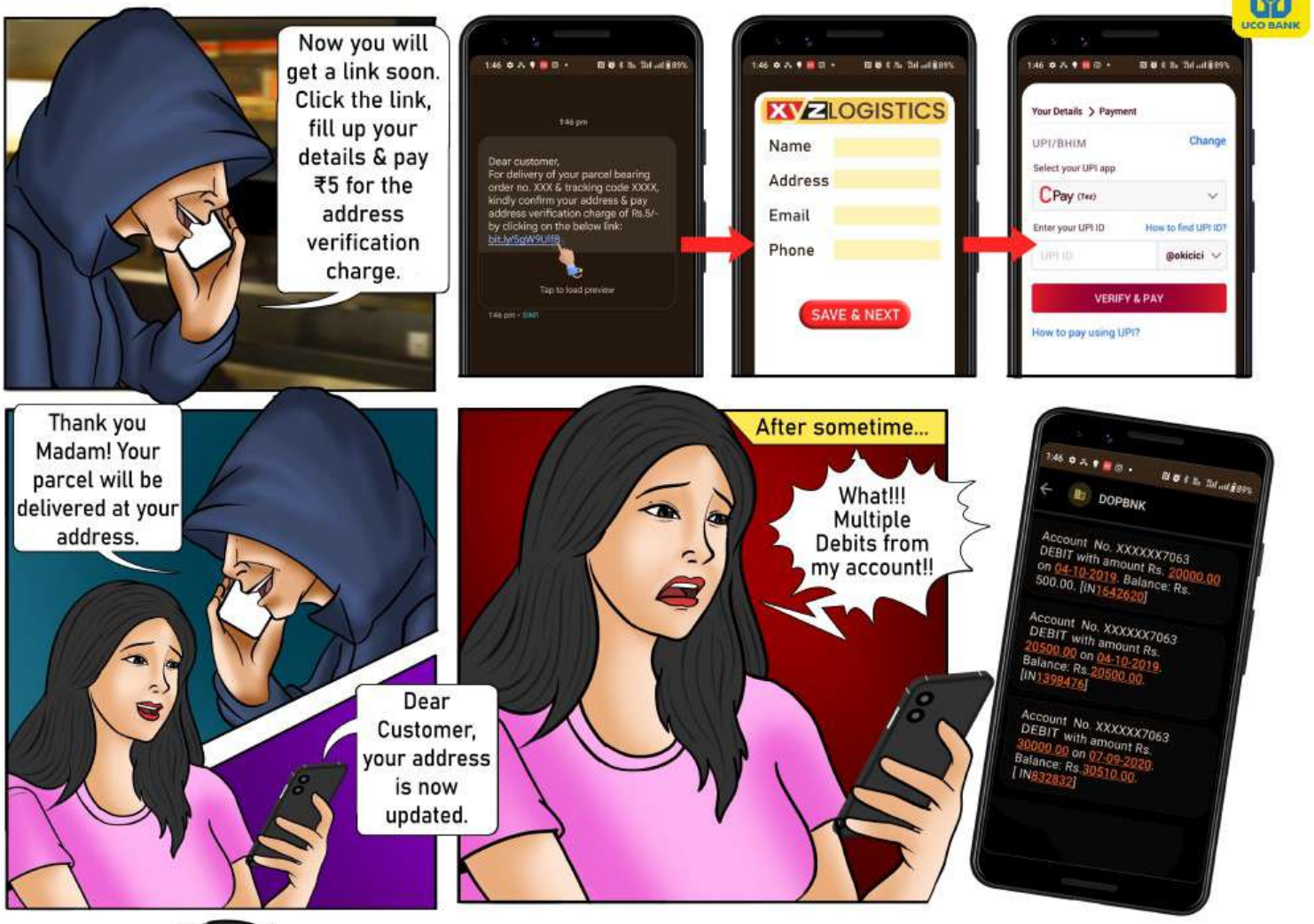

MONEY MIRAGE
A Story on Fake Loan App Fraud
I need money fast. May be I can find a loan online.
Wow! This app seems perfect! Just what I need!
Let's fill up what it wants...
GET QUICK LOANS IN MINUTES!
DOWNLOAD LOANMASTER APP NOW
GET QUICK LOANS
LOAN MASTER
PLEASE ENTER YOUR DETAILS
NAME
ADDRESS
PH. NO.
PAN
AADHAAR NO.
BANK ACC. NO.
IFSC CODE
SAVE & PROCEED
Ok. Let's fill up the Debit card details.
The Bank charges a processing fee of Rs. 500 to process your Loan
PROCEED TO PAY
Ok! Let's pay ₹500.
91 244 XXXX
7:14 pm
Your Loan has been approved. Click the below link & enter 91 244 XXXXX mobile number to confirm your loan amount.
Bit.ly/5pGjh9w
7:14 pm - BSNL Mobile
Okay
I don't know
Call me
Oh! It's great!
CLICK
Enter the mobile number to AUTO FORWARD SMS
Ok! It's time to add the mobile number.
Enter the mobile no. to AUTO FORWARD SMS
91 244 XXXXX
He entered the same mobile number which was received from the SMS.
After sometime...
Let me check my bank account balance. I think the loan amount is credited now.
UCO mBanking
Available Balance
₹10
MINI STATEMENT
CWRDOOOO XXXX 07/08/2022 ₹4500 Dr.
CWRDOOOO XXXX 07/08/2022 ₹55000 Dr.
CWRDOOOO XXXX 07/08/2022 ₹25000 Dr.
CWRDOOOO XXXX 07/08/2022 ₹65000 Dr.
OMG!! Lots of Debit Transactions in my account !!



Best Practices to avoid such scam

- Do not click on suspicious links received through Emails, SMS, WhatsApp, Social Media etc. for availing instant loan.
- Never share personal, sensitive or financial information with anyone.
- Avoid easy loan offers which are too good to be true.
- Stay away from lenders who ask for any advance payment in the name of sanctioning of loans.
- Never download any unknown Apps at the behest of any stranger. Always check the authenticity of an App, read reviews & ratings etc. before downloading it.
- Frequently review App Permissions and do not grant unnecessary permission to Apps.
- Always apply loan from RBI approved Banking & Financial Services Intitutions or Companies.
- Immediately report cyber fraud incident at Cybercrime Helpline No. **1930** & lodge complaint at National Cybercrime Reporting Portal (**https://www.cybercrime.gov.in**).


COURIER CONSPIRACY
Scam in the pretext of Parcel Delivery
I've been eagerly waiting for my parcel, expecting it through XYZ Logistics, but I haven't received any update on the delivery date.
+971 50 207 9849
RING RING
Call via SIM1 from
+971 50 207 9849
Message
RING RING
Hello!!!
Hi, this is Robin from XYZ Logistics. How can I help you?
Actually, could you please tell me the status of my parcel?
Sure Ma'am, please tell me your order number and tracking code?
My order number is TB 456 XXXX & my tracking code is T/3646/XXX.
Thank you madam.
We need to update your address urgently. Download the 'AnyDesk' App and share the unique code displayed.
AnyDesk
DOWNLOAD
AnyDesk
Your Address
257 191 945
Set password for unattended access...
Remote Address
AnyDesk
"AnyDesk" would like to access your Mobile Screen
Don't Allow
Allow
The user shared the unique code (Desk ID) with the hacker over call.
Madam, please accept the App permission displayed over the screen.
Don't Allow
Allow

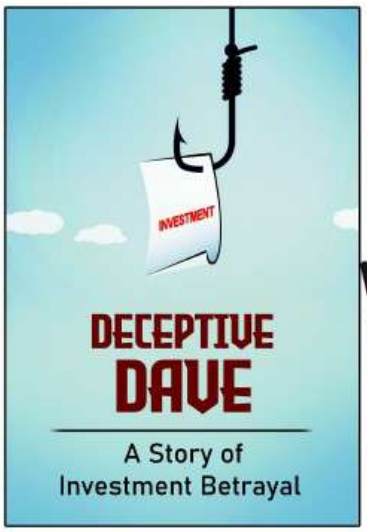


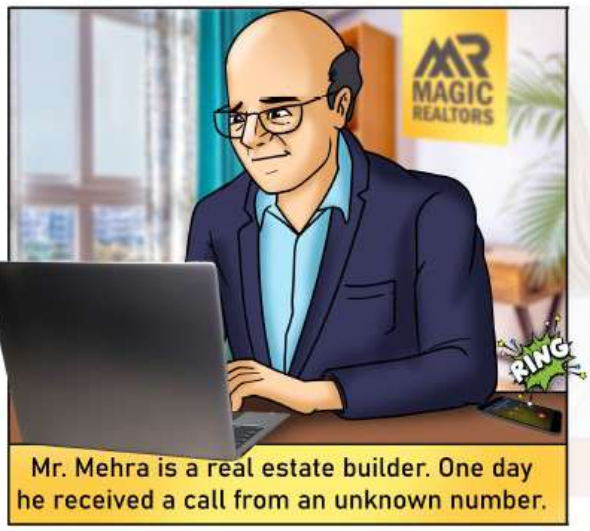
What happened here?

Nowadays, individuals awaiting parcels are defrauded by fraudsters through social engineering tactics. Fraudster manipulates the search engine results & displayed fake customer care number. If individual contacts that number, fraudster under the guise of a courier service company agent, cunningly gains the individual's trust and convinces to download fraudulent screen sharing App (remote access tool) & persuades for sharing the unique address code displayed within the App. Using deceptive techniques, fraudster coerces the individual into accepting App permissions and security warning notifications for gaining control of the device remotely. The google form link is shared for capturing the personal details as well as financial credentials like card details, UPI ID & PIN etc. Armed with this data and remote access to the victim's device, fraudster initiates unauthorized transactions and reads OTPs received during transactions, causing financial loss to the victim.

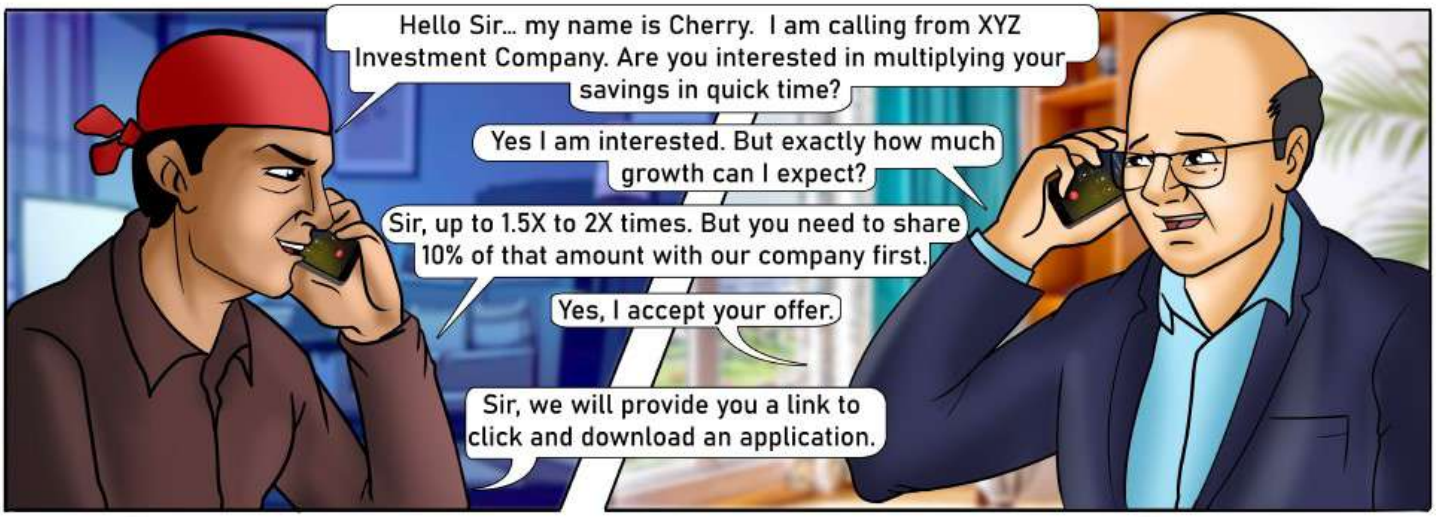
Best Practices to Avoid such Scam

- Avoid searching Customer Care or Helpline number on search engine because fraudster may display misleading information/ads under spoofed / fake website to lure individuals.
- Always refer the official website or App of the organization to find legitimate Customer Care or Helpline number related information.
- Do not download any unknown App and never carry out financial transaction on unknown / random website or at the behest of any stranger.
- Never share sensitive, personal or financial information, such as card details, financial credentials, OTP, PIN, UPI PIN with anyone or in any random forms / websites / social media platforms etc.
- Carefully review App permissions, notifications, security warnings etc. Do not grant unnecessary permissions to App which allow remote access.
- Immediately report cyber fraud incident at Cybercrime Helpline No. 1930 & lodge complaint at National Cybercrime Reporting Portal (https://www.cybercrime.gov.in).


INVESTMENT
DECEPTIVE
DAVE
A Story of
Investment Betrayal


MAGIC
REALTORS
RING
Mr. Mehra is a real estate builder. One day he received a call from an unknown number.


Hello, who's this?


Hello Sir... my name is Cherry. I am calling from XYZ Investment Company. Are you interested in multiplying your savings in quick time?
Yes I am interested. But exactly how much growth can I expect?
Sir, up to 1.5X to 2X times. But you need to share 10% of that amount with our company first.
Yes, I accept your offer.
Sir, we will provide you a link to click and download an application.


85945 XXXXX
Download XYZ Investment Company App from below link https://www.exnessbitly
RCS (Jio)


CLICK
Downloading the App from SMS link.


XYZ Investment Co.
Customer ID
Customer ID
Password
Password
Sign in


MY INVESTMENTS
Invested Balance
₹ 50,000
Current Balance
₹ 100,000
At first, he invested ₹50,000 which grew up to ₹100,000 within 7 days.
MY INVESTMENTS
Invested Balance
₹ 500,000
Current Balance
₹ 10,00,000
He again invested ₹500,000 which also grew up to ₹10,00,000 only in 4 days.
MY INVESTMENTS
Invested Balance
₹ 700,000
Current Balance
₹ 20,00,000
He again invested ₹700,000 which also grew up to ₹20,00,000 only in 3 days.


My amounts are now more than double. Now, let me withdraw the amount.

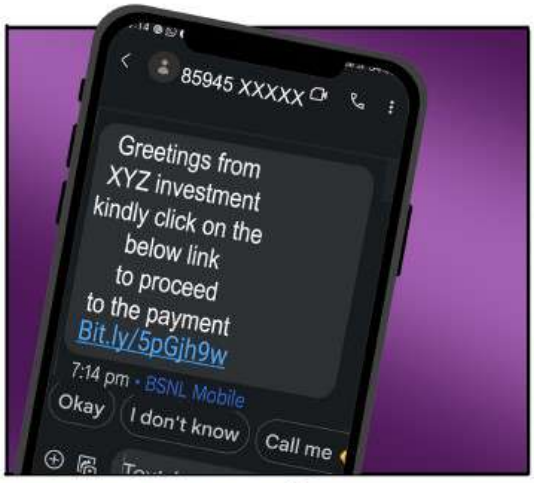
Now I want to redeem my amount.

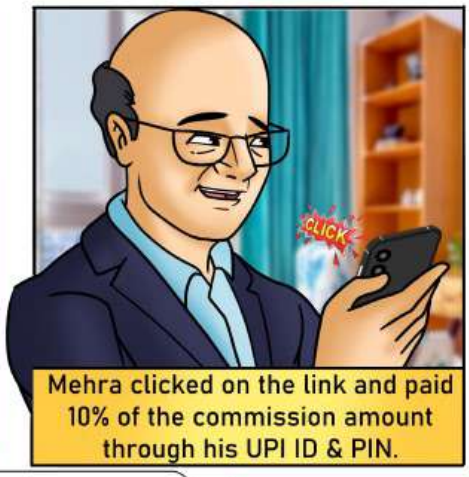
Sir, it is our company's policy that first you need to pay us the 10% commission then only we can redeem the whole amount into your account.

Sure, how can I pay the commission?

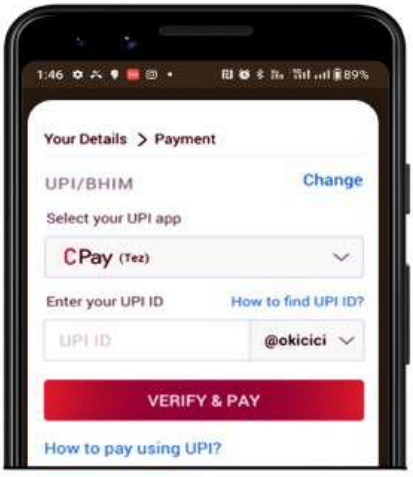
We will send you a link, please complete your payment by using your UPI ID & PIN.

OK! Please send.





Mehra clicked on the link and paid 10% of the commission amount through his UPI ID & PIN.



After some time...

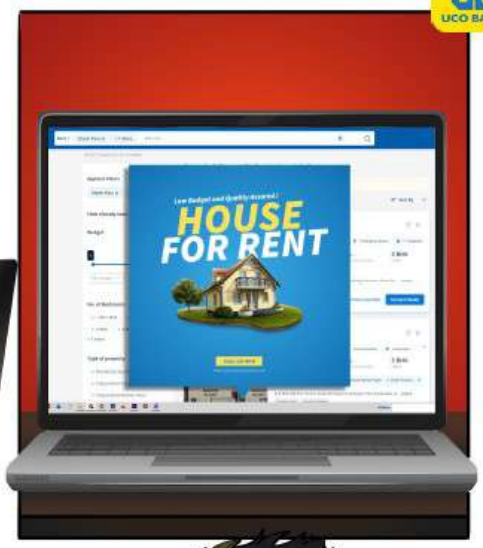
Safety Practices

- Be wary of investment opportunities that promise unusually high returns in less time.
- Don't let anyone pressurize you into making quick investment decisions.
- Conduct thorough research & read reviews, ratings etc. before downloading and using any investment App.
- Ensure to dealing with registered & reputable intermediaries/ investment companies.

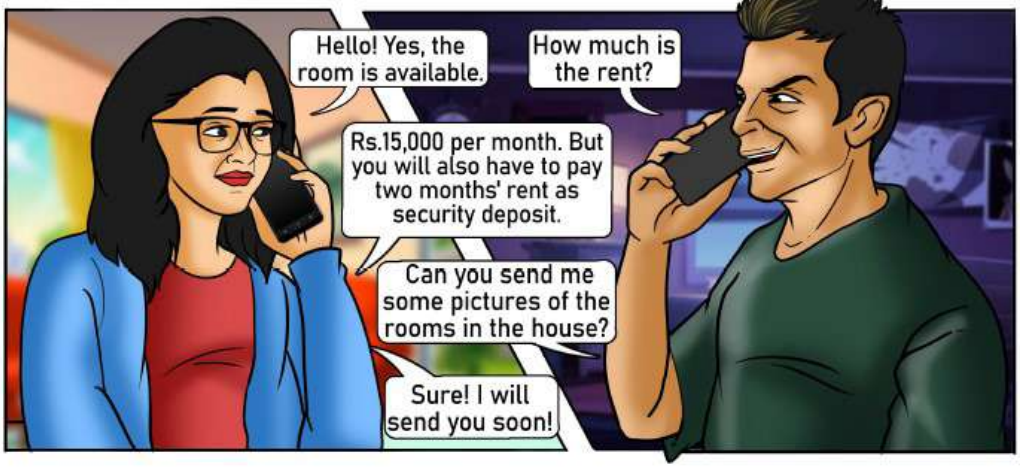
DIGITAL DECEPTION

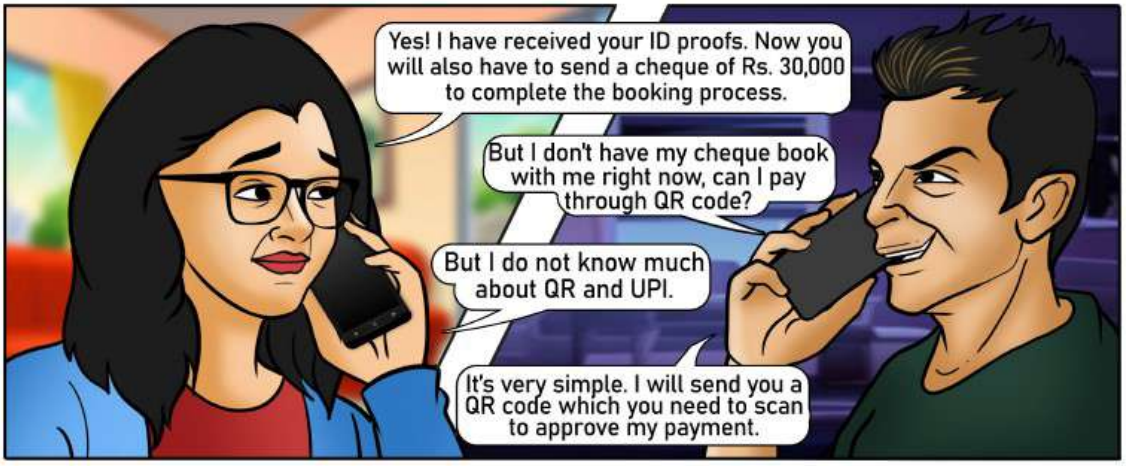
A story of Rental Scam through UPI & QR Code

Reena was looking for a tenant for her house. She put an advertisement of her house with her contact details on a real estate website.

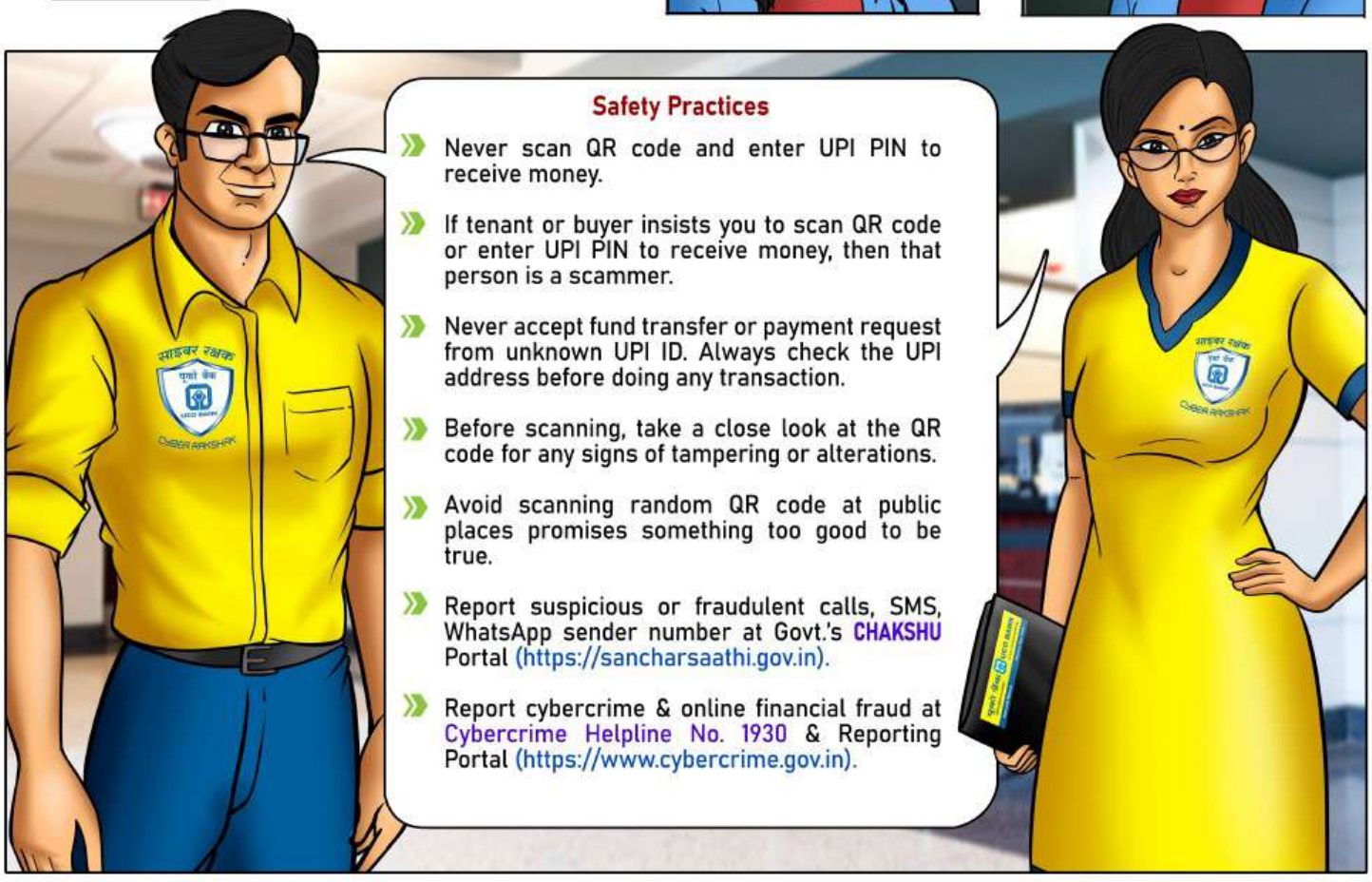


The very next day Reena received a WhatsApp message from an Unknown Number.






Ok! Let's do this accordingly.
CPay
9433458XXX
PAY
30000
PROCEED
CPay
ENTER UPI PIN
PAY
CANCEL
What! the amount got debited instead of crediting!
What you have sent me? The amount got debited instead of crediting !
Sorry! Looks like I sent you the wrong QR in hurry. Let me send you the right one for receiving Rs.60,000.
CPay
9433458XXX
PAY
60000
PROCEED
CPay
ENTER UPI PIN
PAY
CANCEL
Ok Ok ! Send me the correct QR immediately.
The number you are calling is currently unavailable.
Oh my God! I think I got robbed!!!

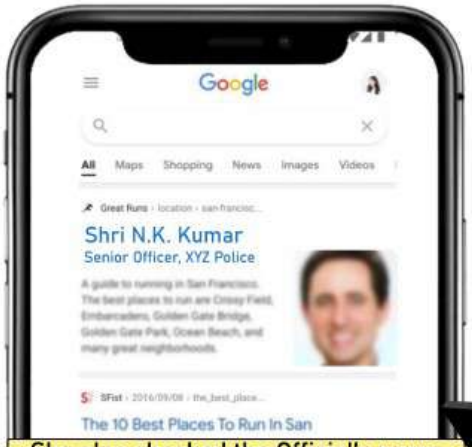

Safety Practices
Never scan QR code and enter UPI PIN to receive money.
If tenant or buyer insists you to scan QR code or enter UPI PIN to receive money, then that person is a scammer.
Never accept fund transfer or payment request from unknown UPI ID. Always check the UPI address before doing any transaction.
Before scanning, take a close look at the QR code for any signs of tampering or alterations.
Avoid scanning random QR code at public places promises something too good to be true.
Report suspicious or fraudulent calls, SMS, WhatsApp sender number at Govt.'s CHAKSHU Portal (https://sancharsaathi.gov.in).
Report cybercrime & online financial fraud at Cybercrime Helpline No. 1930 & Reporting Portal (https://www.cybercrime.gov.in).

FedEx SCAM

Unravelling the Drugs in the Parcel Deception

One day, Meenu got a call from unknown number.

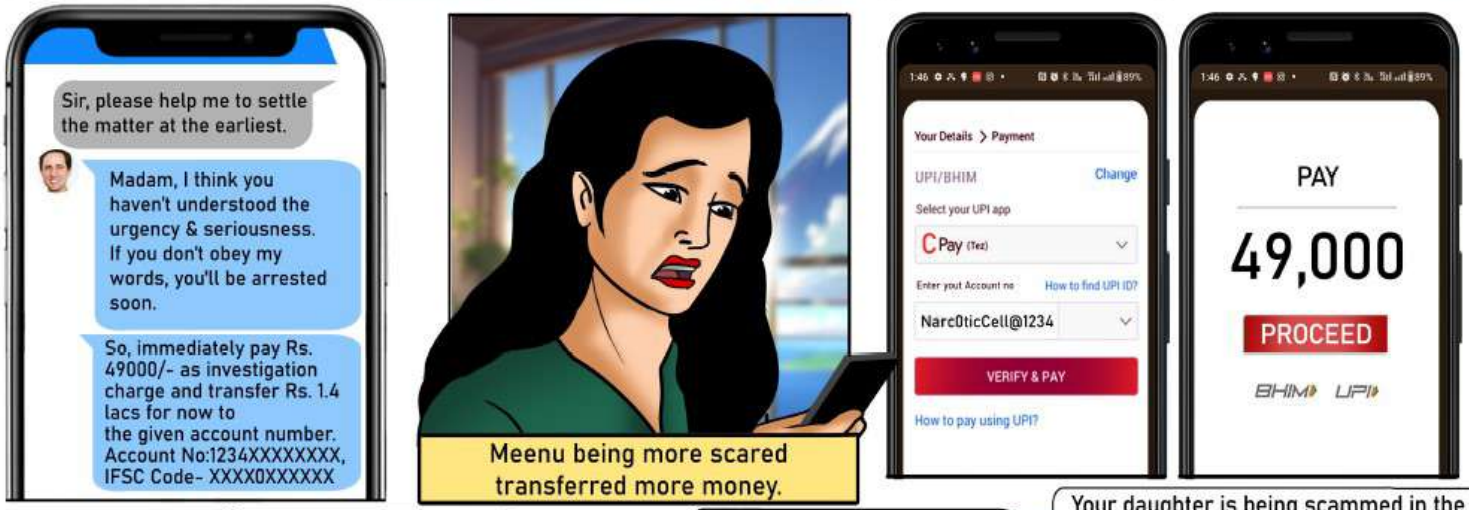
Meenu opened the Chat App & saw the name of a Senior Police Officer along with the Photo.

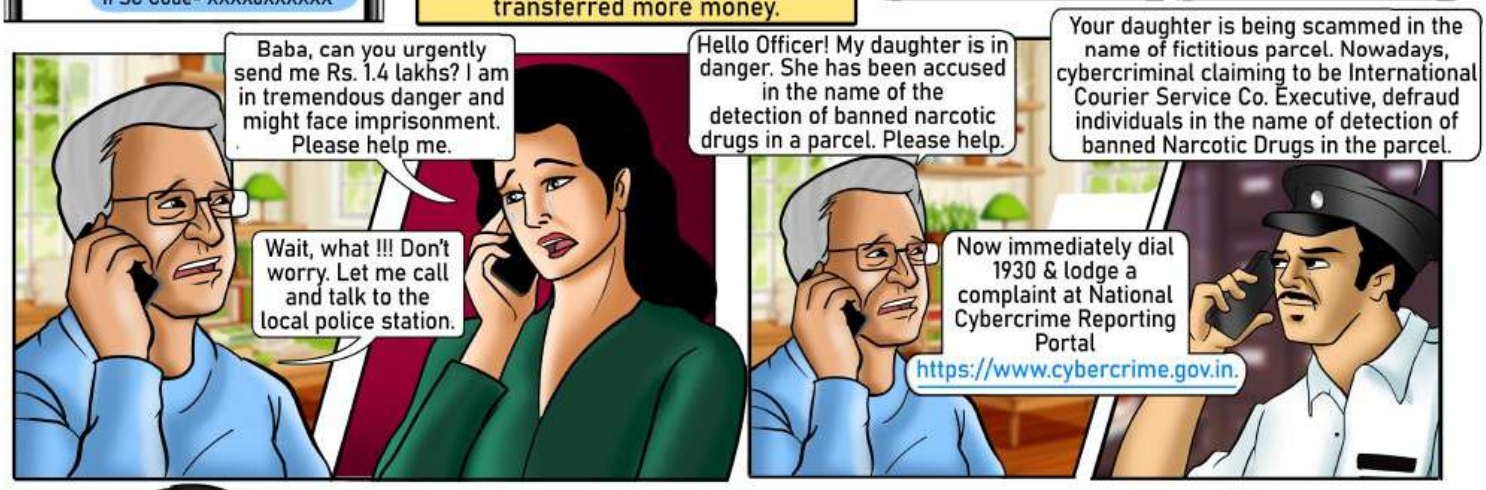


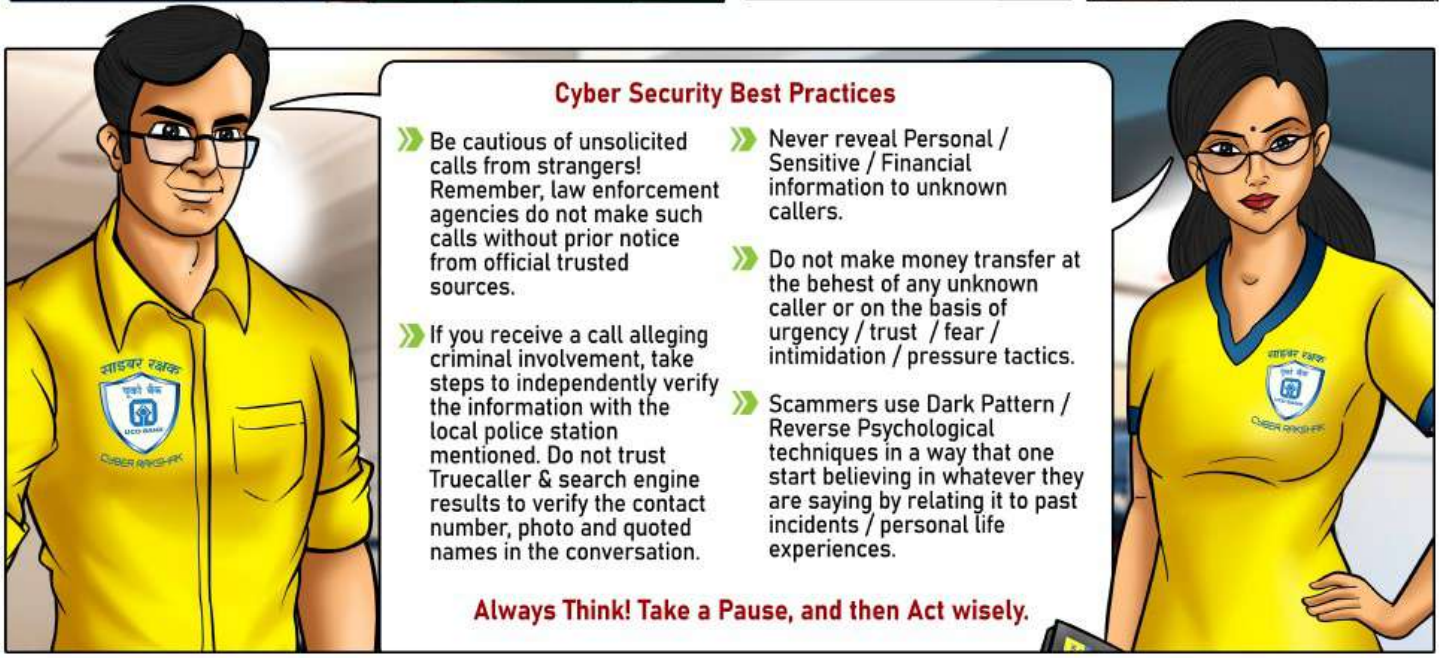
She also checked the Official's name & photo from the search engine & found it genuine.

She gave all the account details along with individual account balance.


Now, immediately you need to pay Rs. 49000/- for legal fees and Rs. 49000/- for customs clearance to the below UPI ID.
UPI ID - NarcOticCell@1234.
I don't want trouble with the police! Let's settle the matter internally.
Your Details > Payment
UPI/BHIM
Change
Select your UPI app
CPay (Tez)
Enter your UPI ID
How to find UPI ID?
NarcOticCell@1234
VERIFY & PAY
UPI ID - NarcOticCell@1234
PAY
98000
PROCEED
BHIM UPI


Sir, please help me to settle the matter at the earliest.
Madam, I think you haven't understood the urgency & seriousness. If you don't obey my words, you'll be arrested soon.
So, immediately pay Rs. 49000/- as investigation charge and transfer Rs. 1.4 lacs for now to the given account number. Account No:1234XXXXXXXX, IFSC Code- XXXX0XXXXXX
Meenu being more scared transferred more money.
Your Details > Payment
UPI/BHIM
Change
Select your UPI app
CPay (Tez)
Enter yout Account no
How to find UPI ID?
NarcOticCell@1234
VERIFY & PAY
How to pay using UPI?
PAY
49,000
PROCEED
BHIM UPI

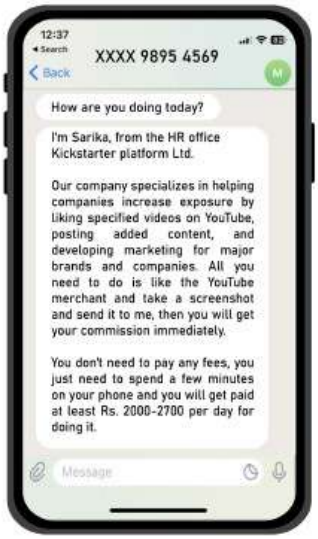

Baba, can you urgently send me Rs. 1.4 lakhs? I am in tremendous danger and might face imprisonment. Please help me.
Wait, what !!! Don't worry. Let me call and talk to the local police station.
Hello Officer! My daughter is in danger. She has been accused in the name of the detection of banned narcotic drugs in a parcel. Please help.
Your daughter is being scammed in the name of fictitious parcel. Nowadays, cybercriminal claiming to be International Courier Service Co. Executive, defraud individuals in the name of detection of banned Narcotic Drugs in the parcel.
Now immediately dial 1930 & lodge a complaint at National Cybercrime Reporting Portal
https://www.cybercrime.gov.in.

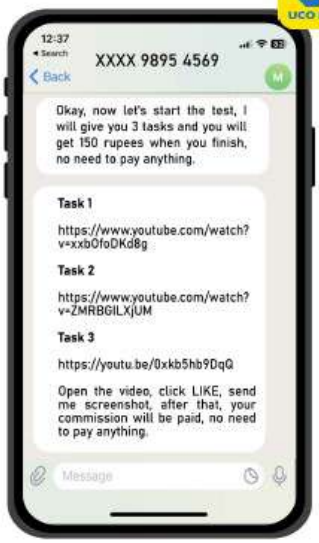

Cyber Security Best Practices
Be cautious of unsolicited calls from strangers! Remember, law enforcement agencies do not make such calls without prior notice from official trusted sources.
If you receive a call alleging criminal involvement, take steps to independently verify the information with the local police station mentioned. Do not trust Truecaller & search engine results to verify the contact number, photo and quoted names in the conversation.
Never reveal Personal / Sensitive / Financial information to unknown callers.
Do not make money transfer at the behest of any unknown caller or on the basis of urgency / trust / fear / intimidation / pressure tactics.
Scammers use Dark Pattern / Reverse Psychological techniques in a way that one start believing in whatever they are saying by relating it to past incidents / personal life experiences.
Always Think! Take a Pause, and then Act wisely.

Task trouble

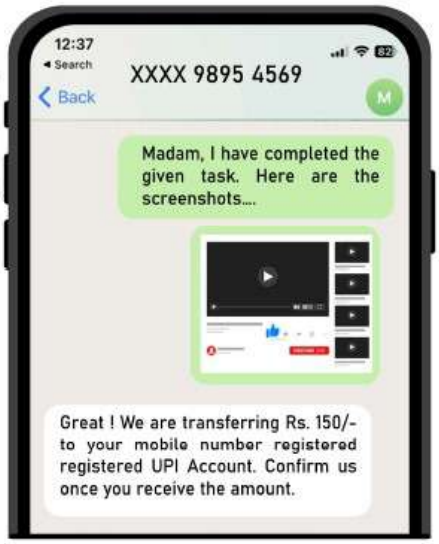
A story on Task Based Job Offer Trap

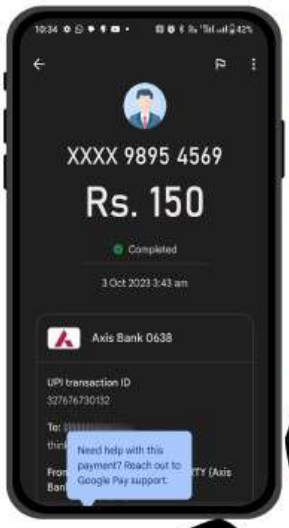
One day, Ronit received a message from an unknown number on Telegram Chat.

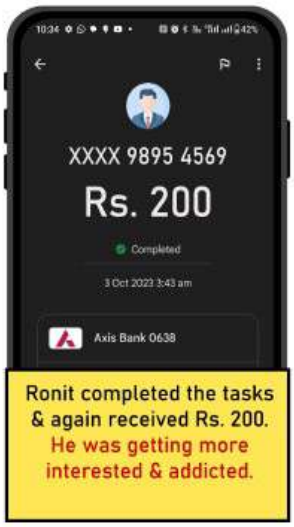




Ronit became so excited to see the message as it was very easy option to make quick & easy money sitting from home without giving any extra effort.

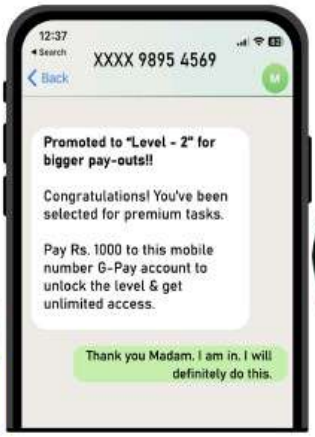




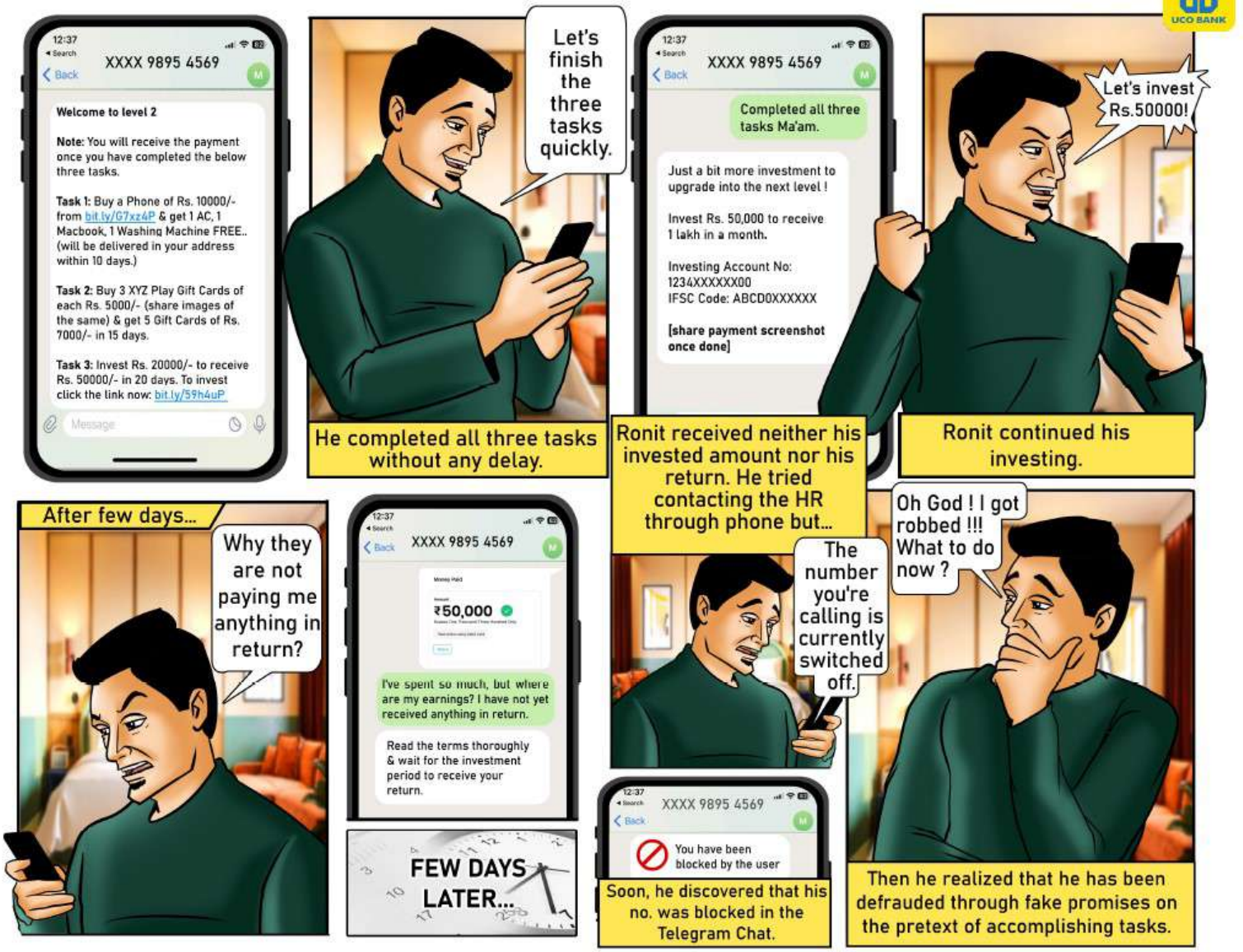


Ronit completed the tasks & again received Rs. 200. He was getting more interested & addicted.

The next day Ronit received another message.



Ronit immediately paid the fee and received some new tasks.



Best Practices to Avoid such Scam

- Be skeptical about unsolicited messages on social media / instant messaging platforms offering easy money after accomplishing online tasks.
- Never engage in user prompted tasks/actions at the behest of any stranger.
- Do not fall prey to alluring investment offers promising unrealistic returns.
- Refrain from sending money to anyone promising high-paying tasks.
- Verify legitimacy of job offers, investment opportunities etc. from official websites / Apps.
- Never share login credentials / personal / sensitive / financial information with unknown persons, especially on messaging apps.
- Do not download unknown files/Apps and avoid clicking on suspicious links.

DEEPFAKE DILLEMMA

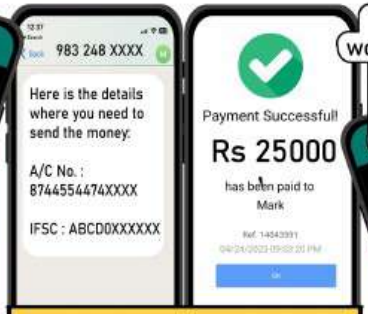
A story on Artificial Intelligence based Scam

One day, Sarah, a young professional, is at home, checking her phone.

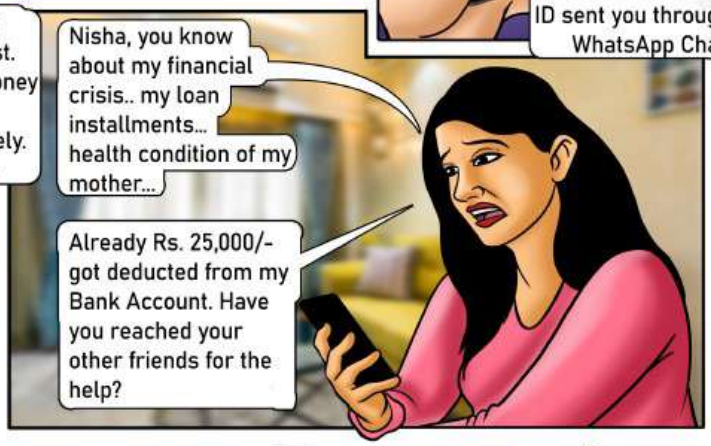
She sees her best friend, Nisha, calling through WhatsApp. It has a Photo of Nisha but the number is unknown.

Sarah is concerned but notices something strange about Nisha's appearance.

Nisha disconnected the call .



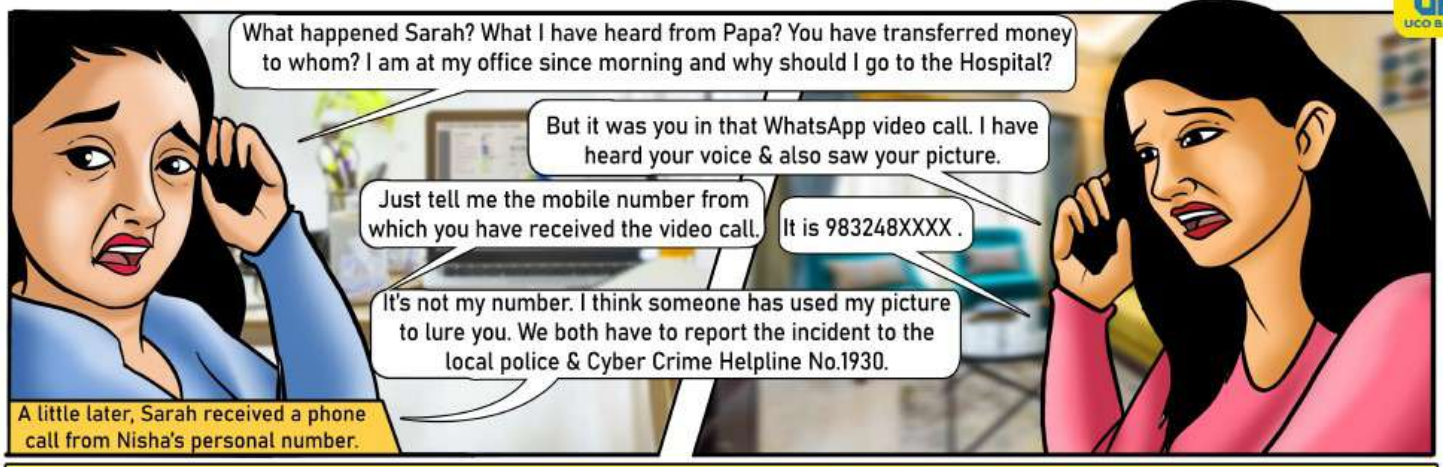
Upon receiving the Bank Account details, Sarah immediately initiated the money transfer.



This time "Nisha" in her response was behaving abnormally, repeating the same line!!

Now, Sarah, being more suspicious, disconnected the WhatsApp call.

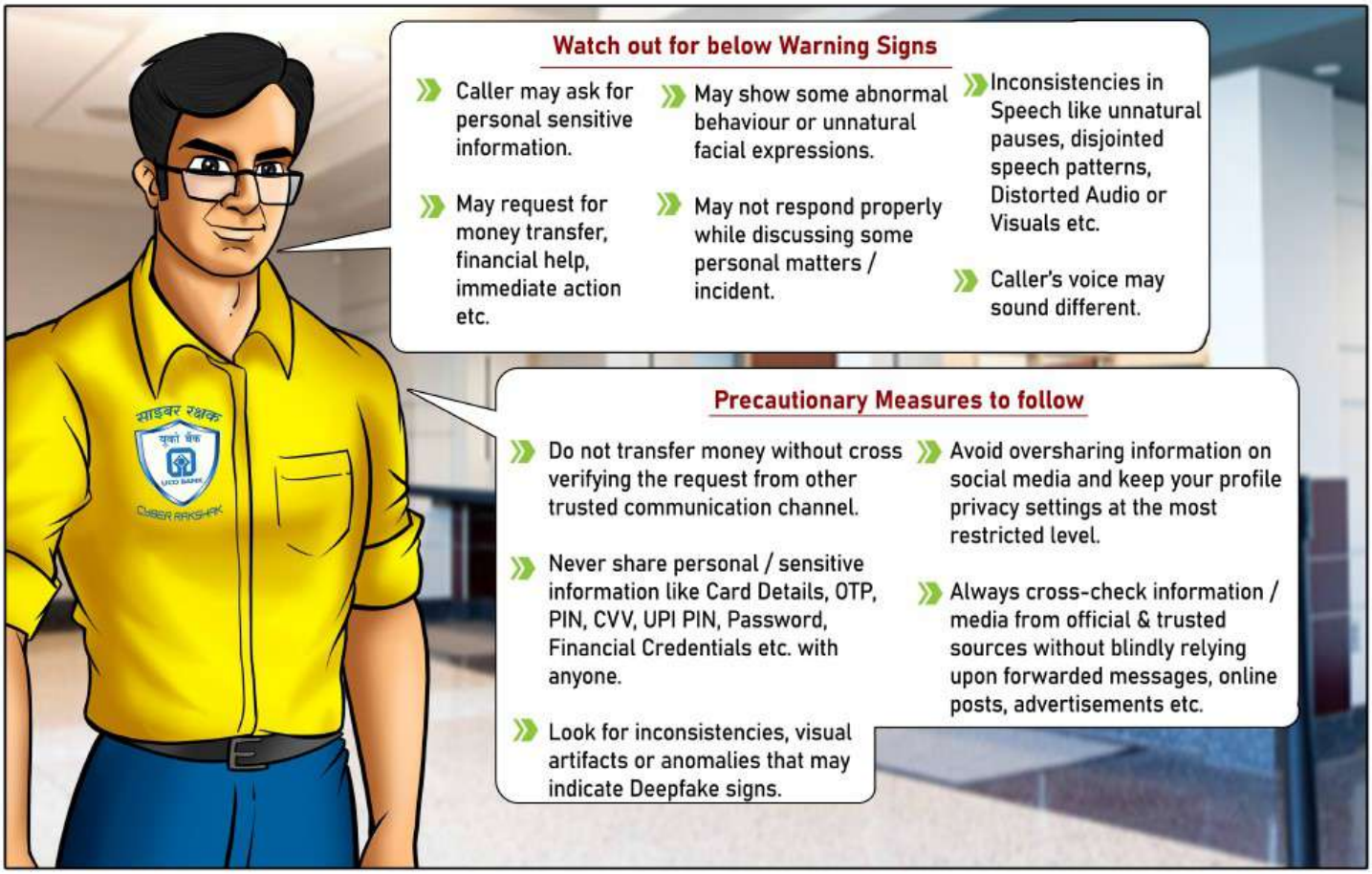
Immediately, she called Nisha's father, told the whole matter & asked for help.



After reporting the incident, both of them soon realized that this was a Deepfake Scam, where cyber-criminal, with the help of Artificial Intelligence (AI) creates fake audio, video, or text content that convincingly mimics real person's voice, appearance or communication style, making it challenging to distinguish between genuine and fake.

Let's understand How the Scam Operates?

- Scammers gather information about the target individuals eg: voice recordings, images, videos etc. to create a realistic digital replica.
- The collected data is then processed by AI algorithms to train AI models and replicate the target's voice, facial expressions, gestures, and communication patterns.
- Using the trained AI models, fraudster generates the Deepfake contents (such as videos, audios etc.) in which the target person's face or voice is manipulated or replaced with synthetic elements.
- The Deepfake contents are then delivered through various channels such as voice calls, text messages, video calls, social media etc. to deceive the known persons of the target individual.
- By exploiting human trust & emotion, scammer then tricks other persons for doing specific action like transferring money, making payments, sharing sensitive information etc.
- The consequences can range from financial loss to reputational damage, data breaches, and compromised personal or business information.



Watch out for below Warning Signs

- Caller may ask for personal sensitive information.
- May request for money transfer, financial help, immediate action etc.
- May show some abnormal behaviour or unnatural facial expressions.
- May not respond properly while discussing some personal matters / incident.
- Inconsistencies in Speech like unnatural pauses, disjointed speech patterns, Distorted Audio or Visuals etc.
- Caller's voice may sound different.

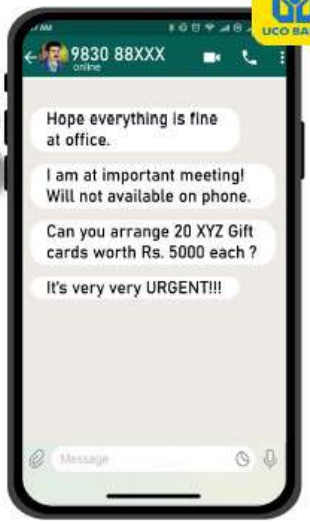
Precautionary Measures to follow

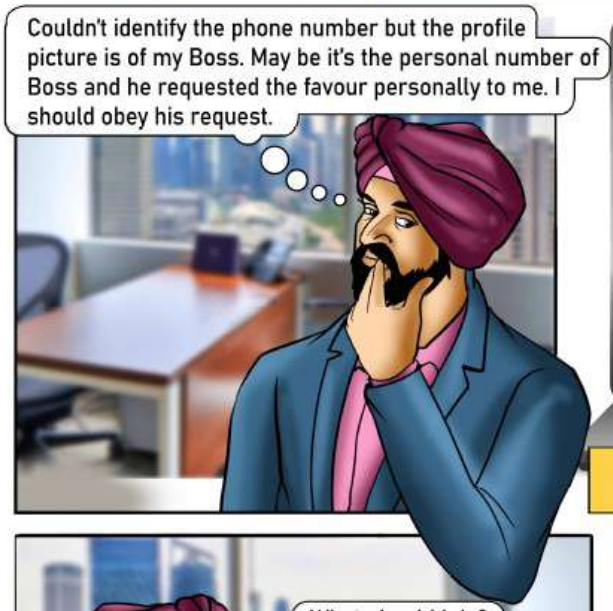
- Do not transfer money without cross verifying the request from other trusted communication channel.
- Never share personal / sensitive information like Card Details, OTP, PIN, CVV, UPI PIN, Password, Financial Credentials etc. with anyone.
- Look for inconsistencies, visual artifacts or anomalies that may indicate Deepfake signs.
- Avoid oversharing information on social media and keep your profile privacy settings at the most restricted level.
- Always cross-check information / media from official & trusted sources without blindly relying upon forwarded messages, online posts, advertisements etc.


BOSS BETRAYAL
Cyber scam that unfolds in the corridors of corporate deceit


What! Boss texted?
Mandeep Singh, an executive engineer, engrossed in his work.


THIINNNGGG
12:45 PM
New Message received
New Message received
New Message received
THIINNNGGG


9830 88XXX
online
Hope everything is fine at office.
I am at important meeting! Will not available on phone.
Can you arrange 20 XYZ Gift cards worth Rs. 5000 each ?
It's very very URGENT!!!
Message


Couldn't identify the phone number but the profile picture is of my Boss. May be it's the personal number of Boss and he requested the favour personally to me. I should obey his request.


THANK YOU!
XYZ eGift Card
1. Select a style for your Gift Card
XYZ gift card
₹1,000.00
2. Enter your Gift Card details
Add to cart
Buy Now
He bought the gift cards from the platform as said by the boss.


9830 88XXX
online
Sir, I have bought the gift cards as per your requirements.
THANK YOU!
Very good. Now please send Rs. 1.5 lakh to below account number.
Acc.: 1234XXXXXXXXX
IFSC: ABCD0XXXXXX
Keep it confidential !

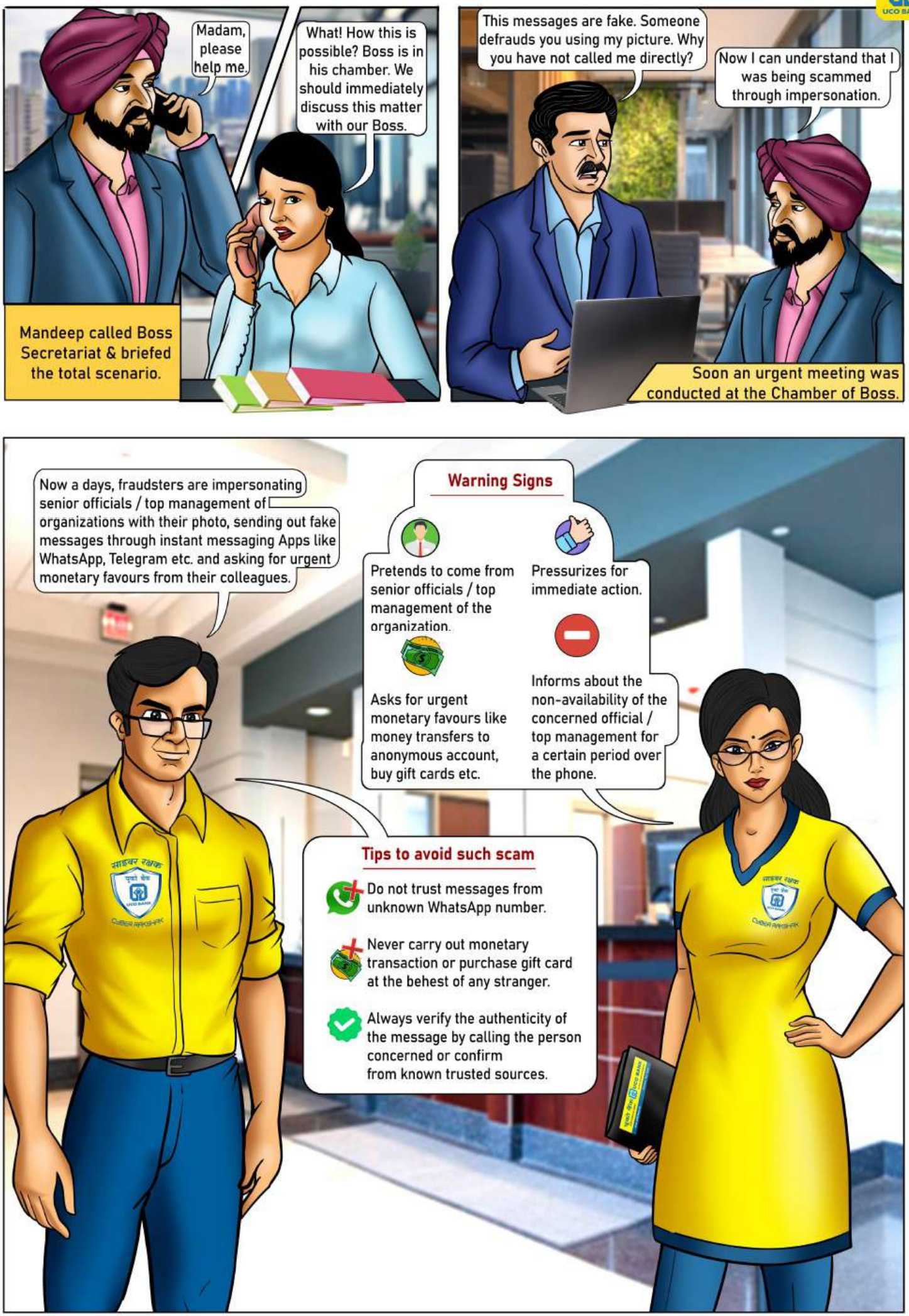

What should I do? Again he is asking for some money.


Payment Successful!
Rs 150000
Transfared to
ABC BANK XXXXXX
9830 88XXX
online
Sir, I have transferred the money to mentioned account.
Payment Successful!
Rs 150000
Very good.
Thank you.
Mandeep transferred Rs. 1.5 lakh to the given Acc no. & replied to his Boss.


THIINNNGGG
1:42 PM
New Message received
THIINNNGGG
After few minutes, Mandeep again received a WhatsApp message from another unknown number with the profile picture of his Boss.


4589 88XXX
online
There is some problem in my previous number.
I need Rs. 2 lakh immediately.
Here is the payment link.
bit.ly/kjgP5gd7
Pay Now. It's VERY URGENT.
Confidential !!
Message

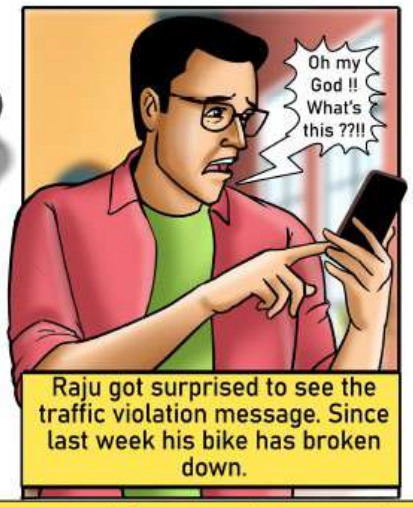

I don't have that much of amount right now. I should tell the matter immediately to Boss Secretary. May be I could get some help from her in this matter.


Madam, please help me.
What! How this is possible? Boss is in his chamber. We should immediately discuss this matter with our Boss.
Mandeep called Boss Secretariat & briefed the total scenario.
This messages are fake. Someone defrauds you using my picture. Why you have not called me directly?
Now I can understand that I was being scammed through impersonation.
Soon an urgent meeting was conducted at the Chamber of Boss.
Now a days, fraudsters are impersonating senior officials / top management of organizations with their photo, sending out fake messages through instant messaging Apps like WhatsApp, Telegram etc. and asking for urgent monetary favours from their colleagues.
Warning Signs
Pretends to come from senior officials / top management of the organization.
Pressurizes for immediate action.
Asks for urgent monetary favours like money transfers to anonymous account, buy gift cards etc.
Informs about the non-availability of the concerned official / top management for a certain period over the phone.
Tips to avoid such scam
Do not trust messages from unknown WhatsApp number.
Never carry out monetary transaction or purchase gift card at the behest of any stranger.
Always verify the authenticity of the message by calling the person concerned or confirm from known trusted sources.

FRAUDULENT FINES

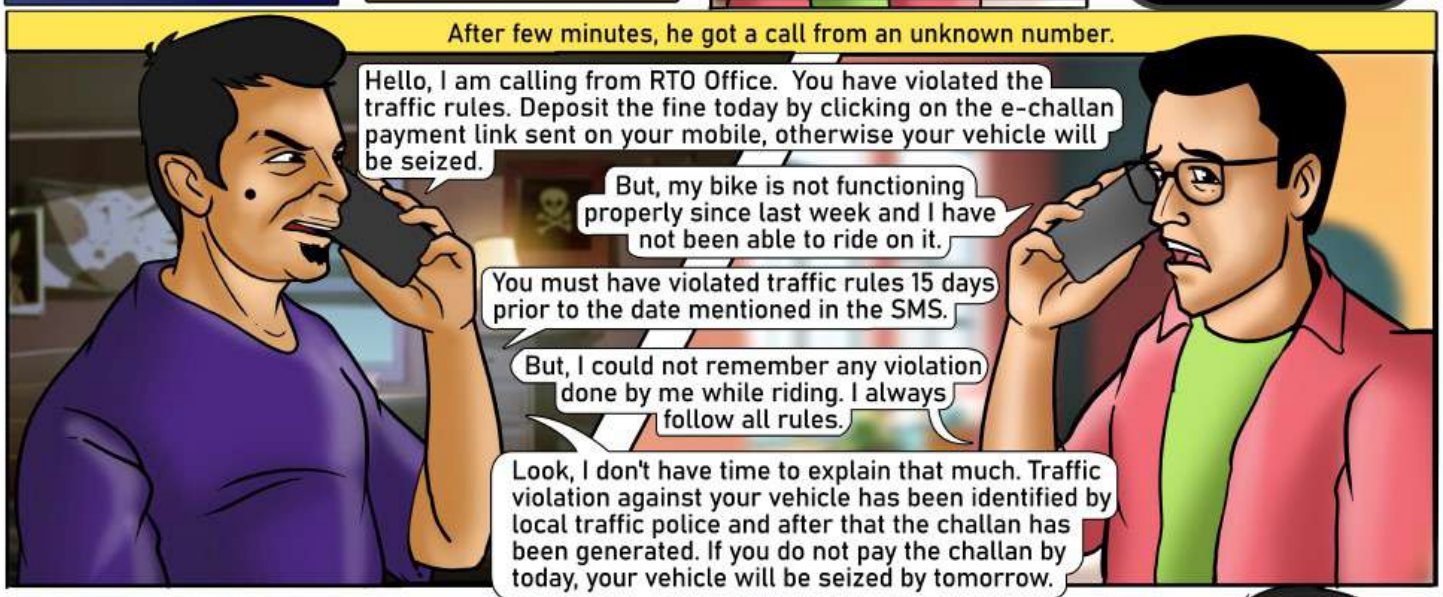
A story on E-Challan Scam through fake messages / calls

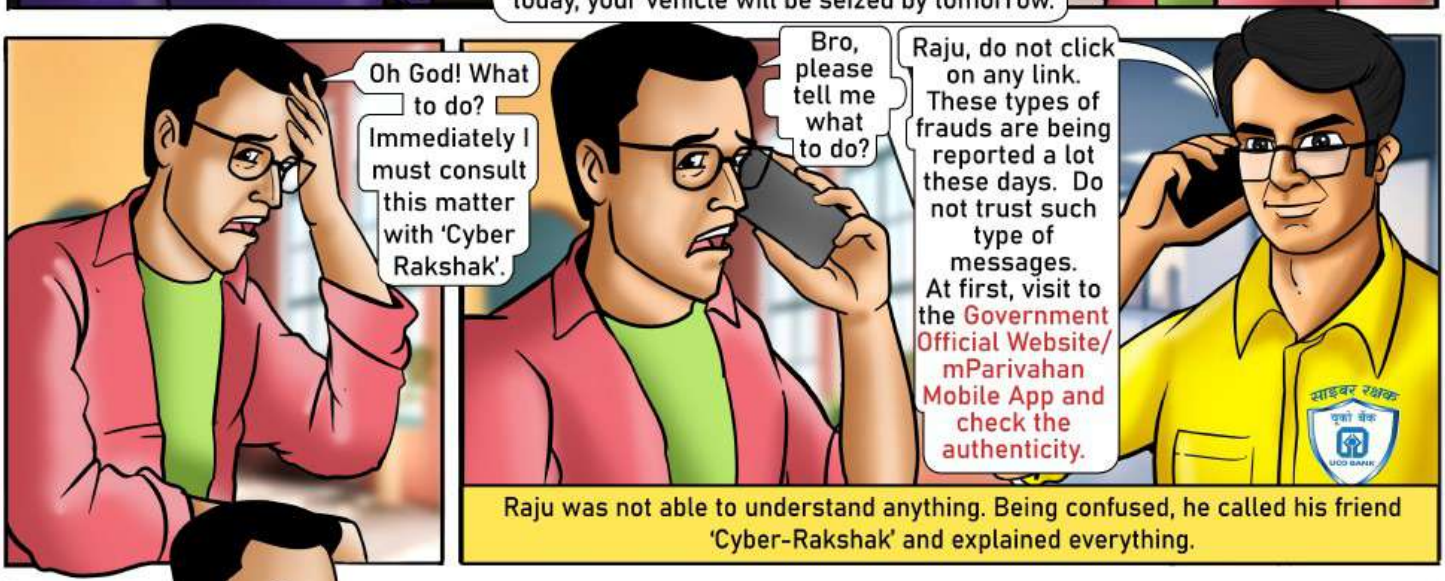
One day Raju got an SMS in his mobile.



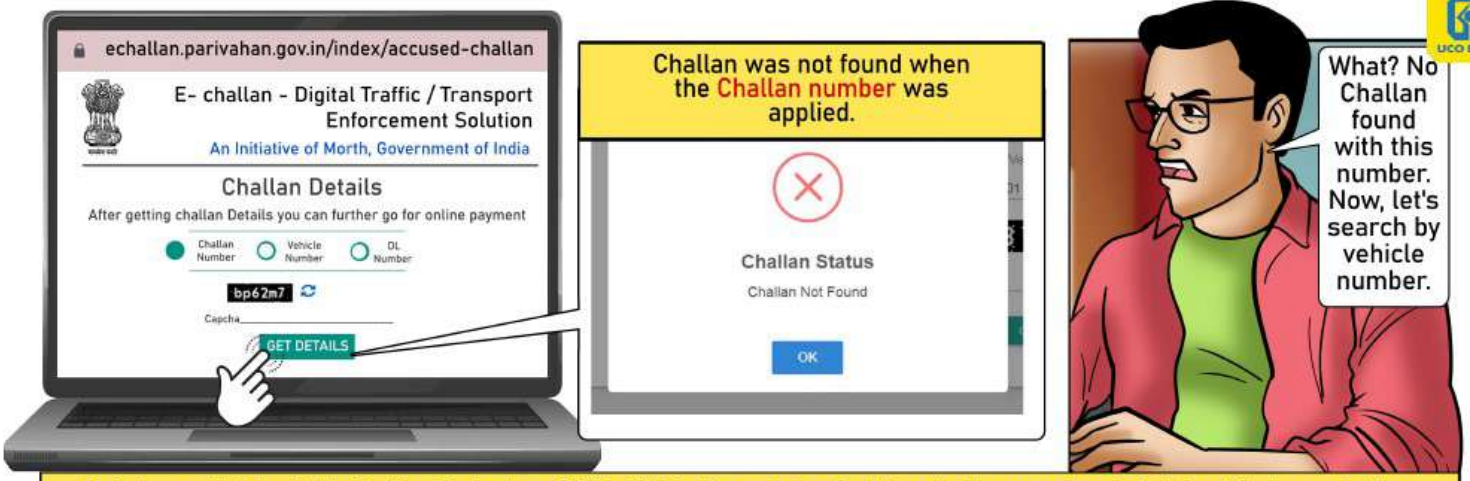
Raju got surprised to see the traffic violation message. Since last week his bike has broken down.

After few minutes, he got a call from an unknown number.

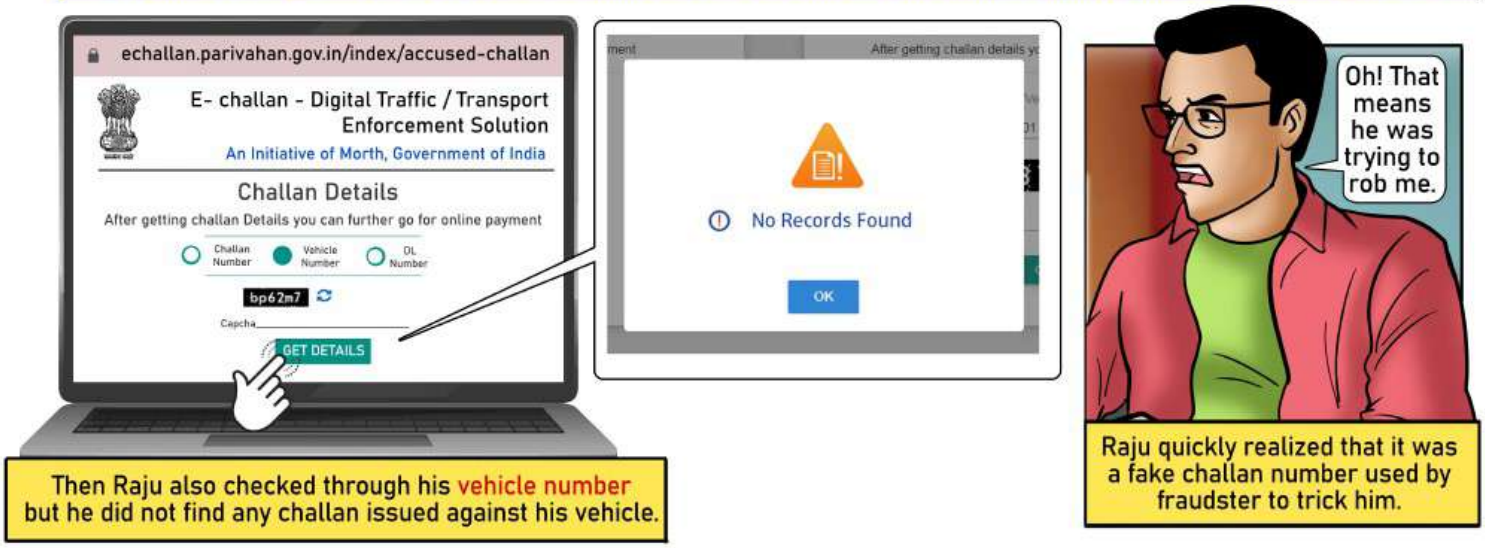




Raju was not able to understand anything. Being confused, he called his friend 'Cyber-Rakshak' and explained everything.

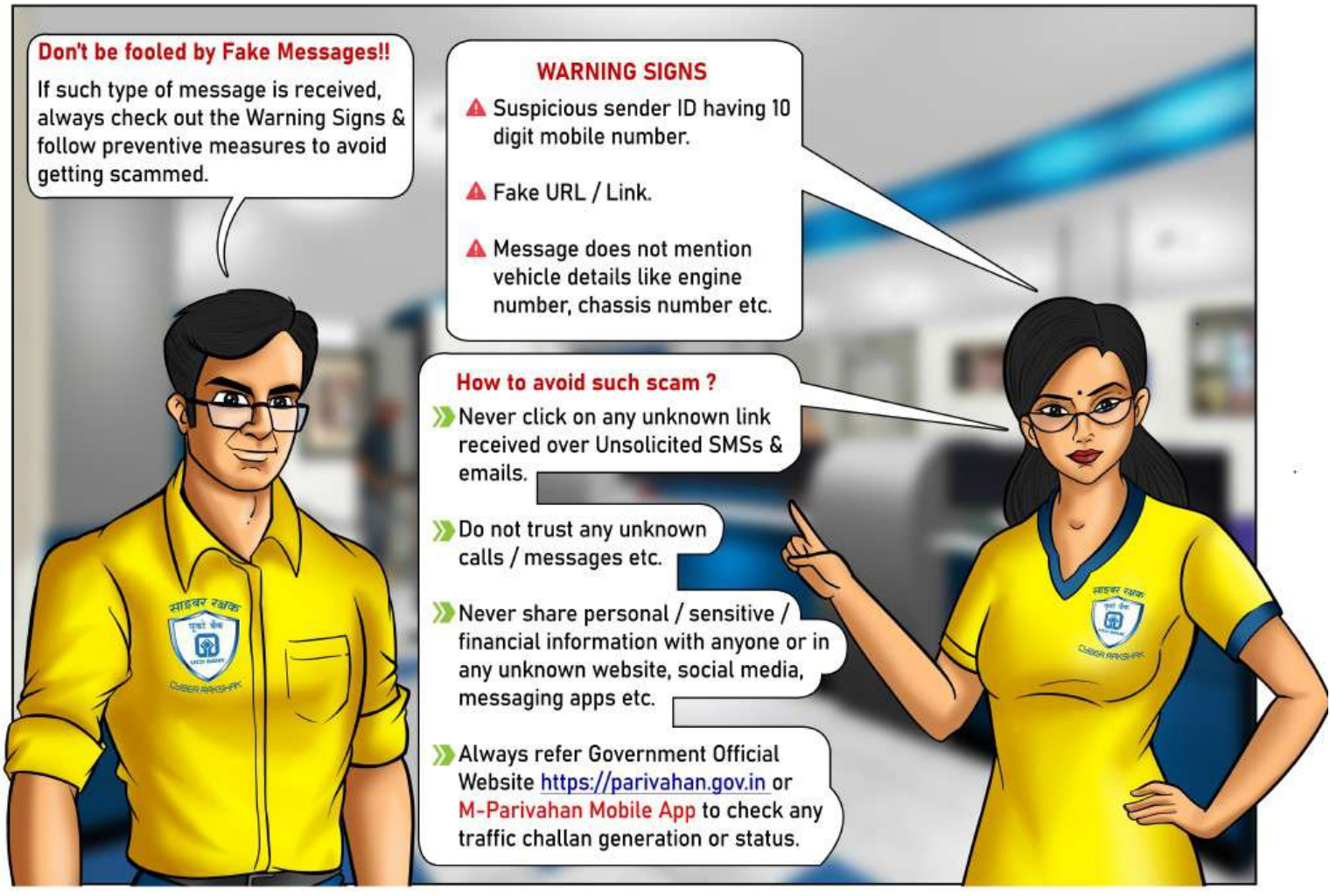


Raju immediately visited to the Parivahan Official Website and checked the challan number, but did not find any challan.



Then Raju also checked through his vehicle number but he did not find any challan issued against his vehicle.

Raju quickly realized that it was a fake challan number used by fraudster to trick him.



यूको बैंक
UCO BANK

Oh no !! I have been
ROBBED!!!

If you are a victim of
CYBER CRIME

Put the HAMMER in the right place at right time!

DIAL 1930 &

Register your complaint at

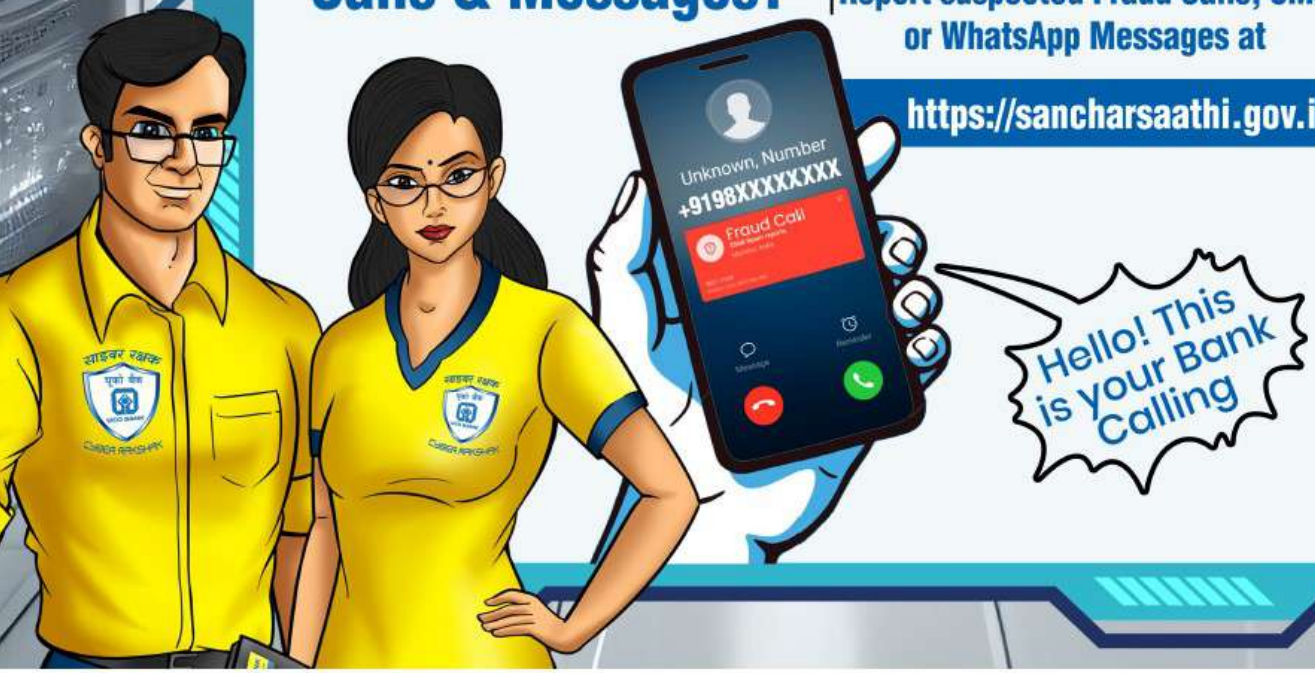
http//:cybercrime.gov.in

Tired of FRAUD Calls & Messages?

Go to **CHAKSHU Portal**

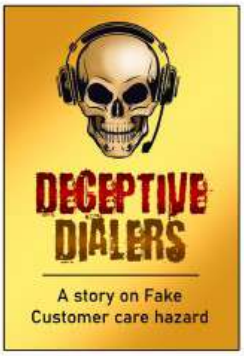
Report suspected Fraud Calls, SMS or WhatsApp Messages at

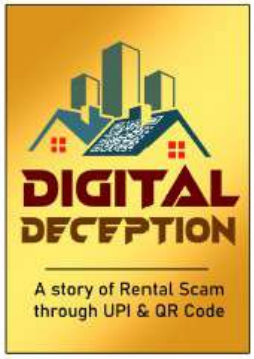
https://sancharsaathi.gov.in

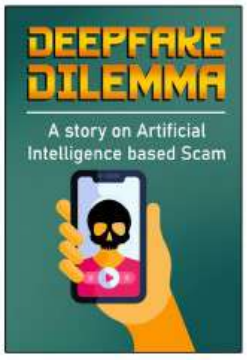


यूको बैंक
UCO BANK

APPENDIX







यूको बैंक
(भारत सरकार का उपक्रम)

UCO BANK
(A Govt. of India Undertaking)

सम्मान आपके विश्वास का

Honours Your Trust