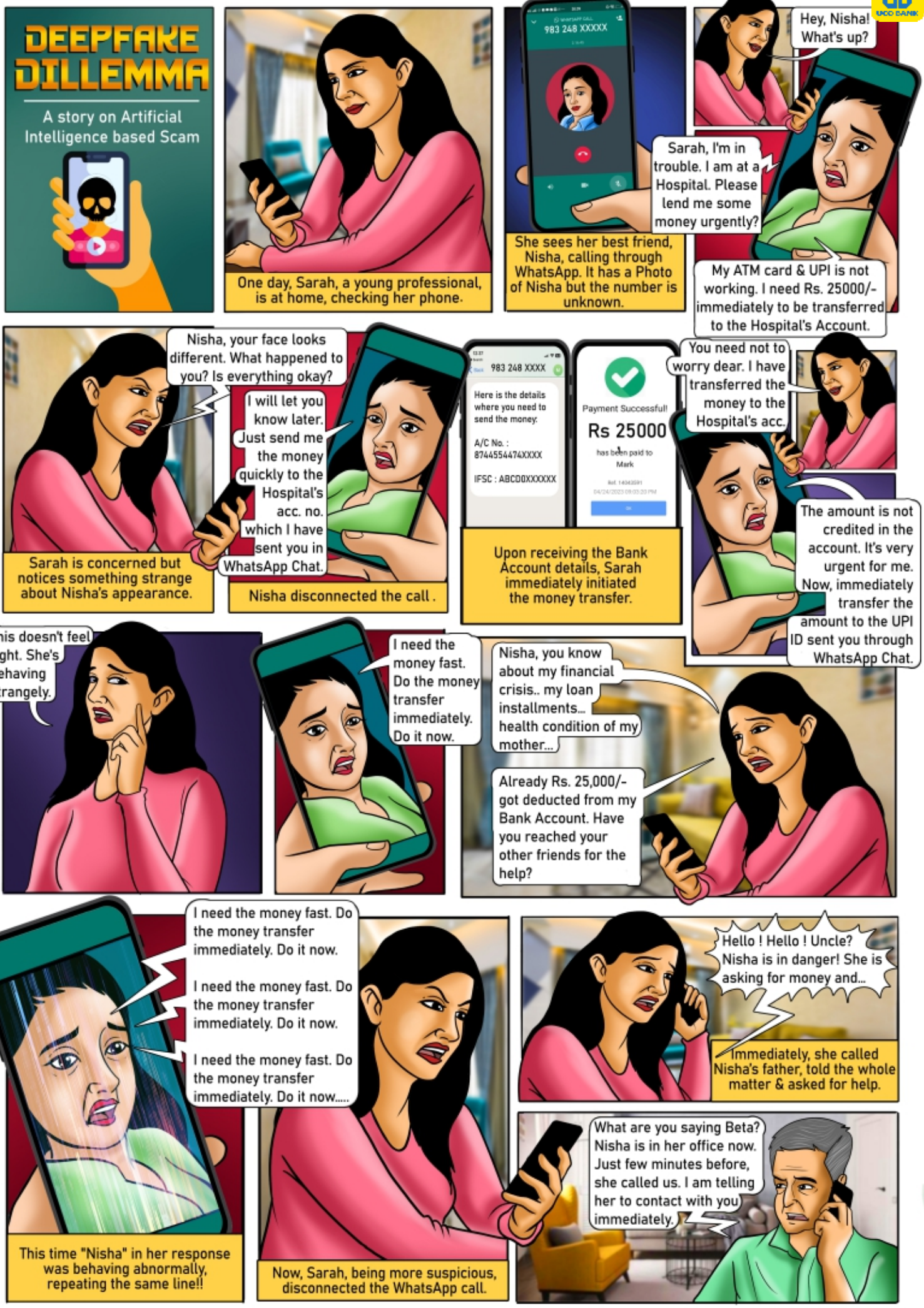
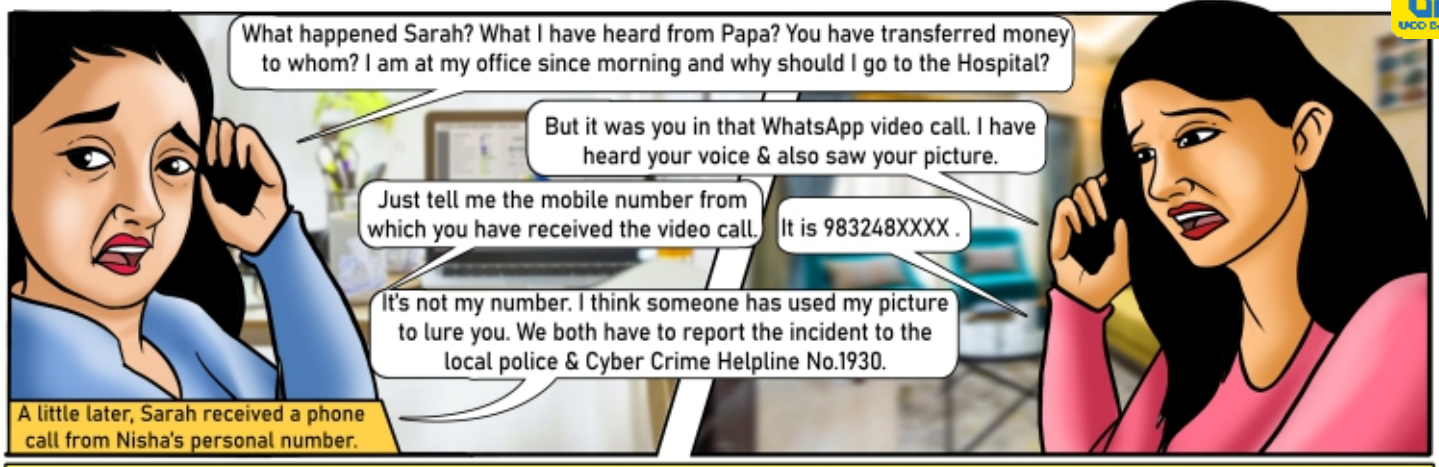

DEEPFAKE DILLEMMA
A story on Artificial Intelligence based Scam
One day, Sarah, a young professional, is at home, checking her phone.
983 248 XXXXX
She sees her best friend, Nisha, calling through WhatsApp. It has a Photo of Nisha but the number is unknown.
Hey, Nisha! What's up?
Sarah, I'm in trouble. I am at a Hospital. Please lend me some money urgently?
My ATM card & UPI is not working. I need Rs. 25000/- immediately to be transferred to the Hospital's Account.
Nisha, your face looks different. What happened to you? Is everything okay?
I will let you know later. Just send me the money quickly to the Hospital's acc. no. which I have sent you in WhatsApp Chat.
Sarah is concerned but notices something strange about Nisha's appearance.
Nisha disconnected the call .
983 248 XXXX
Here is the details where you need to send the money:
A/C No. : 8744554474XXXX
IFSC : ABCD0XXXXXX
Payment Successful!
Rs 25000
has been paid to Mark
Upon receiving the Bank Account details, Sarah immediately initiated the money transfer.
You need not to worry dear. I have transferred the money to the Hospital's acc.
The amount is not credited in the account. It's very urgent for me. Now, immediately transfer the amount to the UPI ID sent you through WhatsApp Chat.
This doesn't feel right. She's behaving strangely.
I need the money fast. Do the money transfer immediately. Do it now.
Nisha, you know about my financial crisis.. my loan installments... health condition of my mother...
Already Rs. 25,000/- got deducted from my Bank Account. Have you reached your other friends for the help?
I need the money fast. Do the money transfer immediately. Do it now.
I need the money fast. Do the money transfer immediately. Do it now.
I need the money fast. Do the money transfer immediately. Do it now.....
This time "Nisha" in her response was behaving abnormally, repeating the same line!!
Now, Sarah, being more suspicious, disconnected the WhatsApp call.
Hello ! Hello ! Uncle? Nisha is in danger! She is asking for money and...
Immediately, she called Nisha's father, told the whole matter & asked for help.
What are you saying Beta? Nisha is in her office now. Just few minutes before, she called us. I am telling her to contact with you immediately.



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.