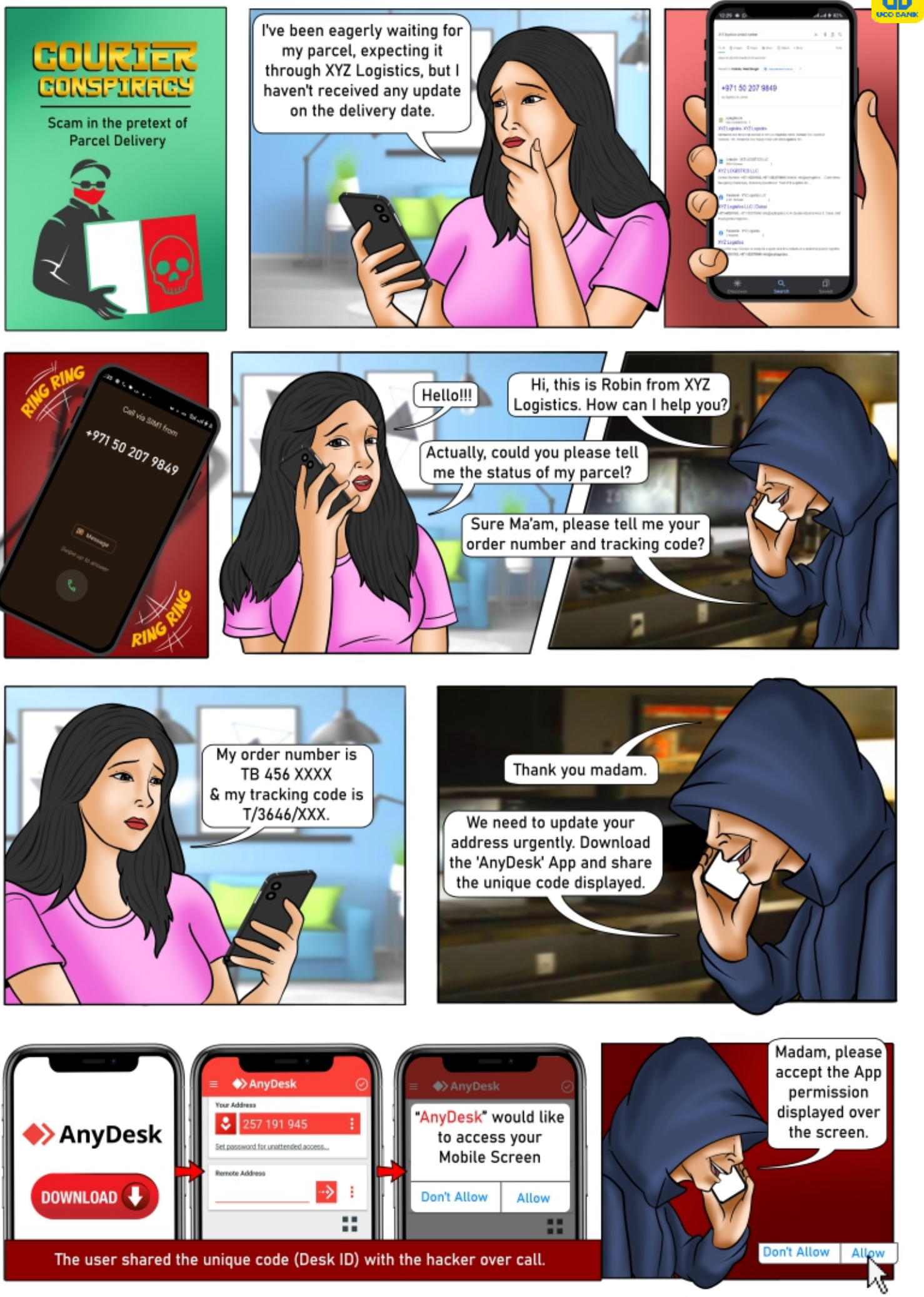
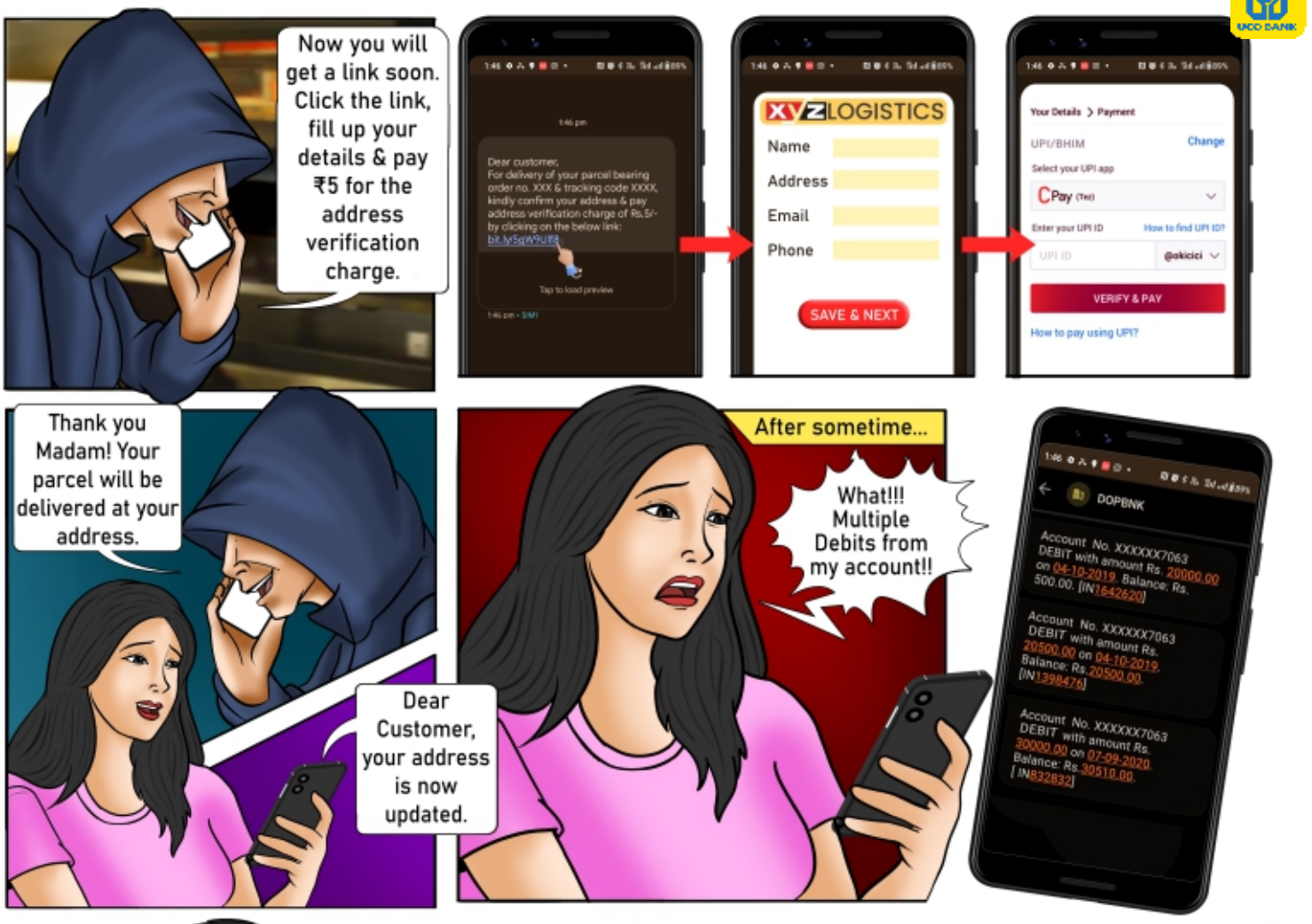

COURIER CONSPIRACY
Scam in the pretext of Parcel Delivery
I've been eagerly waiting for my parcel, expecting it through XYZ Logistics, but I haven't received any update on the delivery date.
+971 50 207 9849
RING RING
Call via SIM1 from
+971 50 207 9849
Message
RING RING
Hello!!!
Hi, this is Robin from 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).