CISO Office, UCO Bank

Cyber Tales by Tenali

– a fortnightly series

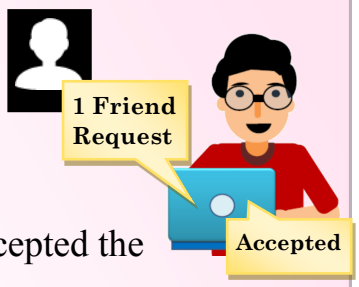
Vol I, Feb 2021

Online Scams

Cybercriminals are continuously adopting new techniques to dupe, blackmail and extort money from innocent users. In the latest instance, Tinku got scammed by new trick— 'Scam Video Call'.

How Tinku got tricked?

One day, Tinku received a friend request from an unknown girl in Facebook and he accepted the request.



Thereafter, Tinku began chatting frequently with the girl due to their common set of interest and also shared his Whatsapp number with the girl.

After a few days, they started talking over phone calls also.

One day, when Tinku was busy with his college project work, he got a video call from the girl via Whatsapp. Tinku picked up the video call.

To his utter surprise, there was some objectionable view on the other side of the video call. Tinku immediately disconnected the call.

After a while, the girl called Tinku and told him that she had recorded the video call conversation.

I have recorded the video call conversation. Pay Rs 1500 immediately or else I will send this video clip to all your Facebook friends.

What ? Why are you doing this?

The video conversation barely lasted for 5 to 6 minutes, but, since, Tinku's face was clearly visible in the video for few minutes, the girl started blackmailing Tinku and initially asked for Rs. 1,500. Tinku grew worried and since the amount was meagre, he paid it through online wallet.

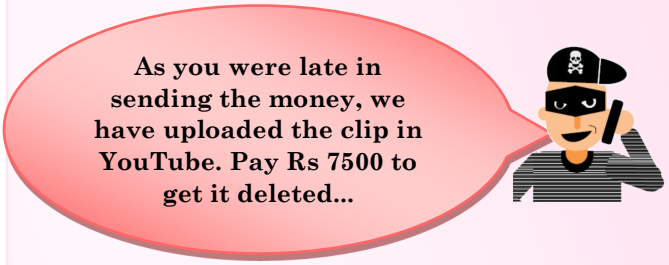
After a few hours, Tinku got another call...

We have a copy of your video clip. If you want us to delete that clip, send Rs 5000...Do it fast.

Don't try to act smart. We can easily make this clip VIRAL !!!

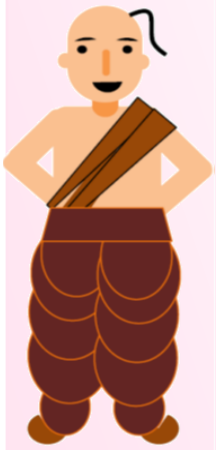
Please don't do that. I will send you the money.

Being worried about the consequences, Tinku again paid Rs 5,000 but the scammers were not happy and continued to blackmail him.



Finding no way out, Tinku called me.

What should Tinku do now?



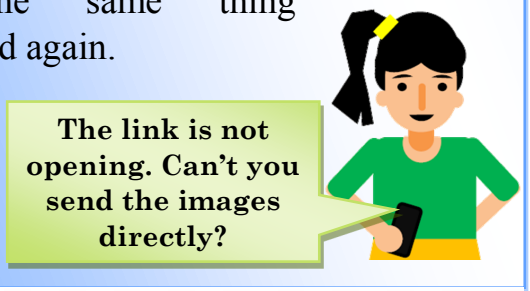
- Immediately Unfriend the girl in Facebook and report the profile to Facebook
- Block the scammer's numbers and block them in WhatsApp also
- Report the incident to the local cyber crime police station and the national cyber crime reporting portal.
- Aware his friends and family members not to fall prey to such scams

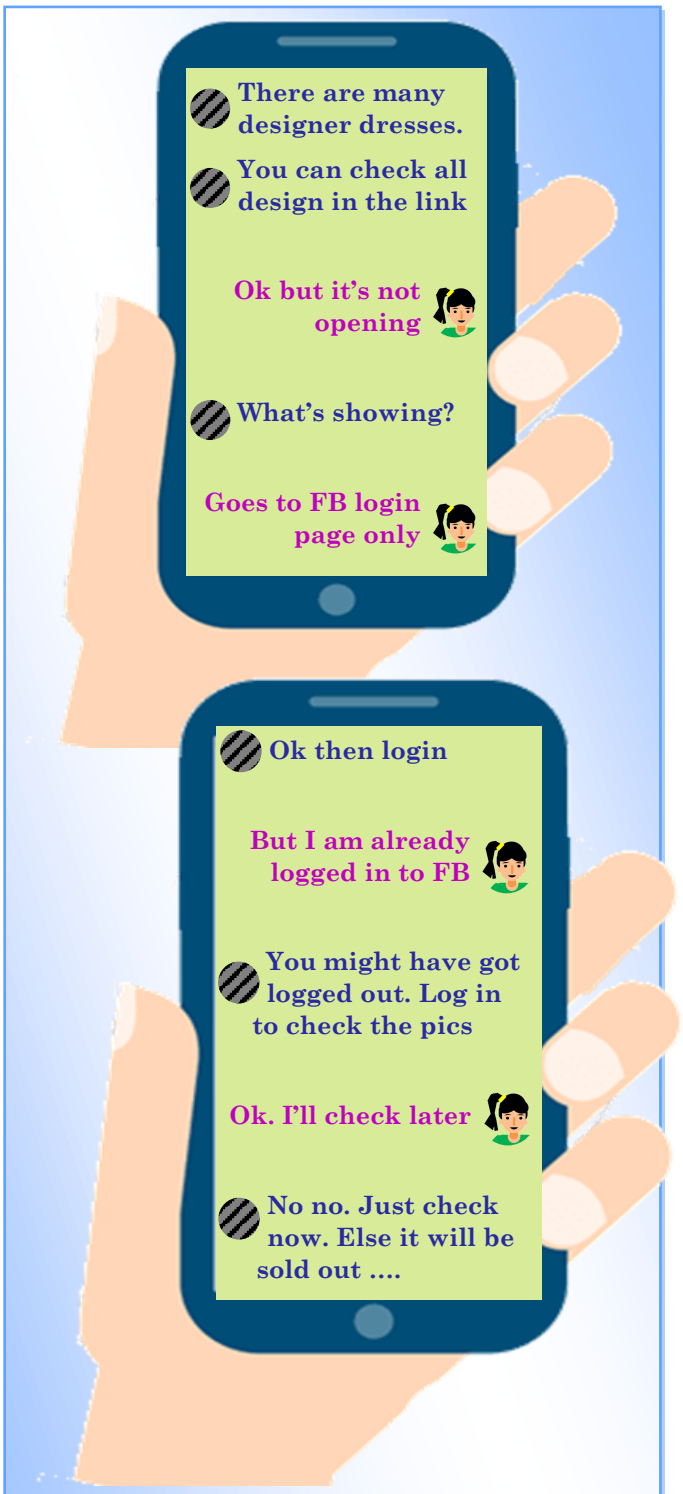
How Chutki's alertness saved her from identity theft?

A similar incident was faced by Chutki also. Being a regular customer of various items from Facebook groups & Online Marketplaces, she used to chat with unknown persons also.

One day she got a message from an unknown girl in Facebook and as usual, she responded without thinking much.

Chutki clicked the link also to check out the colour variants of the dress, which she though she might had asked to some random seller. On clicking the link, she was redirected to '**Facebook Login Page'.** She again went back and clicked the link and the same thing happened again.





The girl kept on insisting Chutki to check the items fast but as Chutki was busy in her online class, she did not respond.

After sometime, Chutki thought to check the items and clicked the link again. Suddenly she noticed that the URL does not appear similar to Facebook. On carefully inspecting the page, she observed that though the page resembles Facebook login page, but the URL in the address bar does not belong to Facebook. The URL in the address bar showed ***www.abcclickit.com/dwfs/3Rf6hy*** whereas actual URL of Facebook login page is ***www.facebook.com***.

Meanwhile the seller kept on messaging whether Chutki have checked the pictures of the kurtis. Chutki grew suspicious and blocked the seller in Facebook.

She immediately closed the browser and cleared the browsing history.

What Chutki should do now?

- Immediately block the fraudster and report the profile to Facebook.
- Report the incident to the local cyber crime police station and national cyber crime reporting portal.
- Upload a public post in her social media profile about the incident to aware her friends and family members.

Steps to Protect Ourselves

- Use internet and social media platforms cautiously.
- Apply strict privacy settings to secure personal details and photographs.
- Do not respond to WhatsApp / Telegram video calls coming from unidentified callers.
- Never share personal photos or videos with strangers over phone or online.
- Avoid accepting friend requests from unknown person online.

Facebook Security Guide

- Login to Facebook
- Open Settings > Privacy > Privacy Settings
  - Limit the audience of your posts & stories
  - Restrict who can send you Friend Request
  - Restrict who can see your friend list
  - Restrict who can view your birthday, birth year, contact information etc.

Basics of Instagram Account Security

- Open Instagram
- Go to Settings > Privacy
- Set 'Private Account'
  - This will disallow public audience from viewing all your pictures until they follow you
  - This will also ensure nobody can directly follow you. Instead, you will receive a follow request which you have to accept so that they may be able to follow you in Instagram.

Avoid accepting Friend Request / Video Calls from Unknown Accounts

Secure Your Telegram Account

- Open Telegram
- Go to Settings > Privacy and Security
- Set 'Calls' to 'My Contacts'
  - This will ensure only your known contacts can call you via Telegram app.
- Set 'Groups' to 'My Contacts'
  - This will allow only your known contacts to add you into groups.

WhatsApp Security Settings

- Open WhatsApp
- Go to Settings > Account > Privacy
- Set 'Groups' to 'My Contacts' -
  - This will not allow Admins of WhatsApp Groups to add you to random groups. Instead, Admins will have the option to invite you to the group.

If you have been a victim of online scams...

- Immediately report to the nearest Cyber Crime Police Station or in the website of National Cyber Crime Reporting Portal https://cybercrime.gov.in.
- Report fake profile to the respective online forum so that the authority may disable the fraud user.

Cyber Guru Tenali's Mantra

Use Internet and Social Media cautiously.

We welcome your valuable suggestions / feedback at ciso.office@ucobank.co.in