CISO Office, UCO Bank

Cyber Tales by Tenali

- a fortnightly series

Vol I, Jan 2021

UCO BANK
78
Years of
Honouring the Nation's Trust

In our glorious 78 years of "Honouring the Nation's Trust", we urge our readers to be extra vigilant and cautious in the ever-expanding horizon of cyber realm.

Let us follow few simple steps to protect ourselves in the upcoming journey:

- ***Never share Passwords, PINs or OTPs.***
- ***Do not click unknown links or download unknown apps.***
- ***Keep apps updated.***

CISO Office wishes

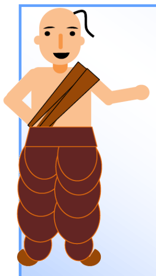
HAPPY AND CYBER SAFE NEW YEAR

to all our readers and thank them for their continuous support & compliments on our new fortnightly series '***Cyber Tales by Tenali***'.

We present one more modus operandi of a recent cyber incident with an illustrative graphic representation and best practices.

As always, looking forward for your feedback to keep our momentum alive in enriching this publication.

COVID-19 Vaccine Pre-Registration Scams

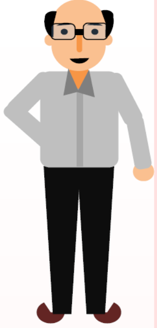


Amid the news surrounding the roll-out of COVID-19 vaccine in India, cybercriminals have come up with different ways to scam people in the name of COVID-19 vaccine registration.

Today, I will give you a walkthrough of some of the techniques being adopted by fraudsters in duping innocent people.

Meet the Characters...

Srinivas -

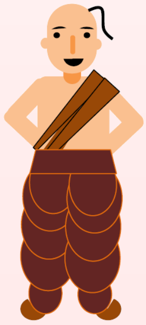


- A simple Internet user
- Acquainted with the know-hows of the digital world, but has tendency to overlook things in hurry.

Mogambo -

- Tapping latest developments, affecting people at large, to trick them.
- Loves playing with emotions of people.

Tenali -

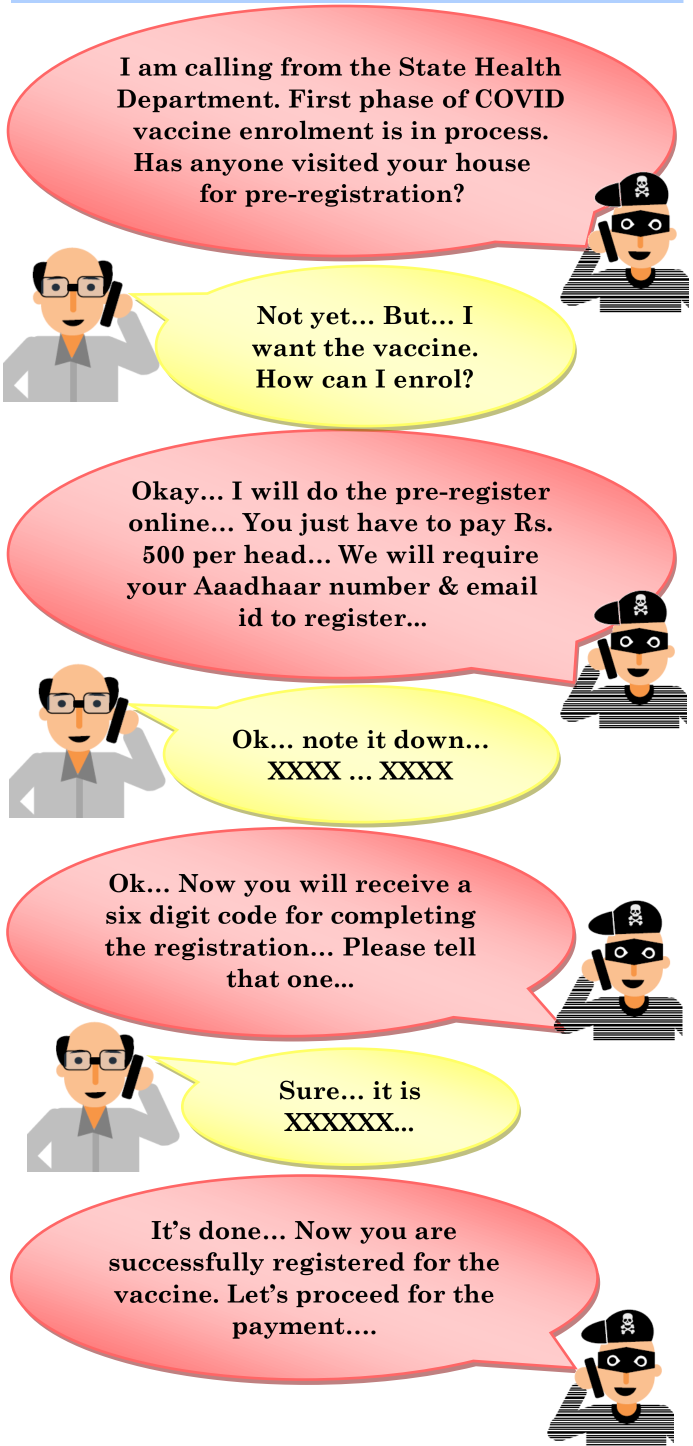


- Cyber Skill Expert & ***narrator of the story***
- Goal is to increase awareness on cyber safety and create safe, digital environment

Contd... COVID-19 Vaccine Pre-Registration Scams

Just a few days back, Srinivas's father has recovered from COVID-19 and is still under post recovery process.

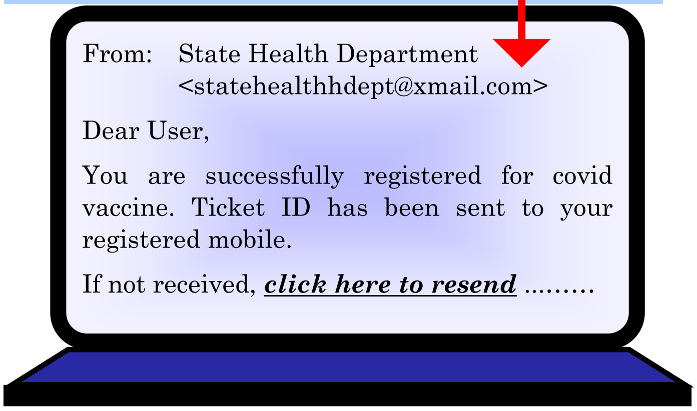
One day, Srinivas got a call from the State Health Department.


I am calling from the State Health Department. First phase of COVID vaccine enrolment is in process. Has anyone visited your house for pre-registration?
Not yet... But... I want the vaccine. How can I enrol?
Okay... I will do the pre-register online... You just have to pay Rs. 500 per head... We will require your Aadhaar number & email id to register...
Ok... note it down... XXXX ... XXXX
Ok... Now you will receive a six digit code for completing the registration... Please tell that one...
Sure... it is XXXXXX...
It's done... Now you are successfully registered for the vaccine. Let's proceed for the payment....

After completing the payment, Srinivas got a confirmation mail in his 'registered' email id.

The caller told Srinivas that he will receive a TOKEN ID in his mobile number which he has to share to the Health Workers during their visit to Srinivas's home and then disconnected the call…

After sometime, Srinivas noticed that the confirmation email looked a bit suspicious and the sender email id didn't looked like government's email id.



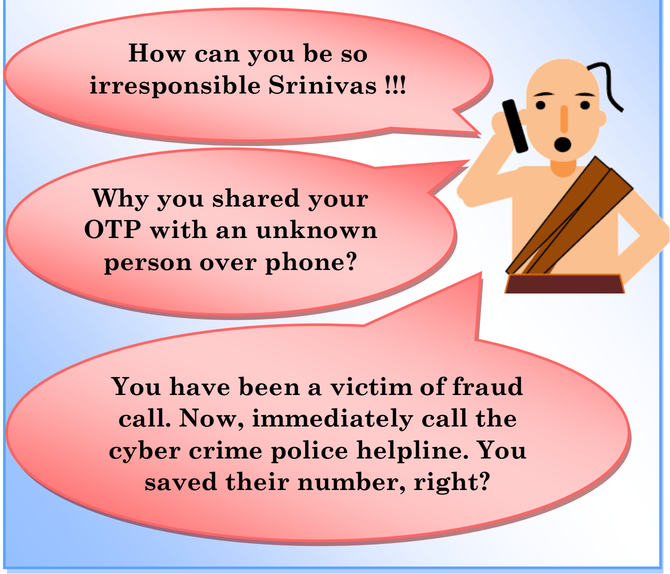
From: State Health Department <statehealthhdept@xmail.com>

Dear User,

You are successfully registered for covid vaccine. Ticket ID has been sent to your registered mobile.

If not received, ***click here to resend*** ....

Thankfully, Srinivas did not clicked the link and called me out of worry and explained the whole incident.


How can you be so irresponsible Srinivas !!!
Why you shared your OTP with an unknown person over phone?
You have been a victim of fraud call. Now, immediately call the cyber crime police helpline. You saved their number, right?

Contd... COVID-19 Vaccine Pre-Registration Scams

What has actually happened here?

Srinivas has been a victim of fake COVID-19 vaccine pre-registration fraud.

Mogambo, impersonating as State Health Department Official, calls random numbers and trick users for sharing sensitive information. In this instance, Mogambo has called Srinivas. Coincidentally, Srinivas was worried about his father's health, who had recently recovered from COVID-19. Mogambo, taking advantage of Srinivas's situation, conned him into divulging sensitive information in pretext of registering him for COVID-19 vaccine.

As Srinivas wanted to protect his family from the disease, he got tricked easily and thus shared sensitive information like Aadhaar number, email id, OTP and also sent pre-registration charges, without verifying the identity of the caller and giving a second thought.

What should Srinivas do now?

Srinivas should immediately report to the nearest Cyber Crime Police Station or in the website of National Cyber Crime Reporting Portal https://cybercrime.gov.in along with supporting documents like screenshot of caller number, copy of message received etc.

What that 'click here to resend' link might redirect to?

- Redirect to fake website looking similar to State health Departments website asking more sensitive personal / financial details of other family members.
- Download malicious software in Srinivas's device.

But, what Mogambo will do using Srinivas's Aadhaar number & OTP?

- *Open a mule account in the name of Srinivas and use it for fraudulent purposes* - Many wallets provide account opening with limited KYC details based on Aadhaar number and it's authentication with OTP sent on registered mobile number.
- *Change Srinivas's mobile number, name, address and other details linked to Srinivas's Aadhaar Card Number* - ***In UIDAI portal, any user can request for change in details by putting Aadhaar number and OTP received in mobile number registered with aadhaar card.*** If Mogambo changes Srinivas's registered mobile number in the Aadhaar database, then Mogambo will receive all the Aadhaar-based authentication OTPs instead of Srinivas.
- Take a print out of Srinivas's Aadhaar Card from online portal and use it for purposes like getting duplicate / new SIM Card, open Bank Account etc for fraudulent purposes.
- Perform any transaction requiring Aadhaar OTP authentication, i.e. Aadhaar number and OTP received in mobile number linked to Aadhaar.

What other methods may be adopted by Mogambo to trick users like Srinivas?

- Call user and ask to download remote access app in his mobile device
- Send fraudulent email with malicious attachment or message with fraudulent link

Contd... COVID-19 Vaccine Pre-Registration Scams

Keep Your Aadhaar Safe

The Unique Identification Authority of India (UIDAI) has a feature for locking and unlocking of Aadhaar number.

Once Aadhaar number is locked, then authentication of any service (like Income Tax filing, AEPS etc) which is using Aadhaar number as a authentication medium will not work unless Aadhaar number is unlocked. It is applicable for all mediums like , biometric, or OTP wherever authentication of Aadhaar number is required.

Before you lock your Aadhaar number, remember you must first generate your virtual ID. If the virtual ID is not generated by you then you will not be able to lock your Aadhaar number.

Generate VID in UIDAI Website

- In UIDAI website, open Resident portal
- Enter Aadhaar number & captcha
- Enter the OTP and submit. Now, your Virtual ID (VID) will be generated

How to lock / unlock Aadhaar using UIDAI website?

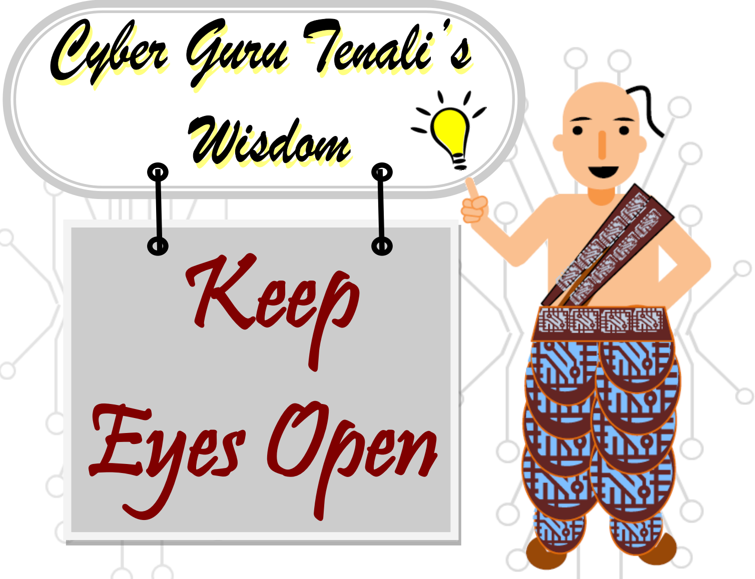
- In UIDAI website, open Resident portal
- Under Aadhaar Service, Click on Lock & Unlock.
- Select UID Lock Radio Button and enter Aadhaar Number, Full Name, and Pin Code as in the latest details and enter the security code.
- Click on Send OTP and then submit.
- Your UID will be locked successfully.

Locking Biometrics in Aadhaar in UIDAI Website

- In UIDAI website, go to 'My Aadhaar' then go to Aadhaar service
- Click on lock/ unlock biometrics.
- Next, enter your Aadhaar or VID number & captcha code and get OTP on your registered mobile number.
- Enter the OTP and submit. Now, your biometrics will be locked.
- Similarly, you can unlock your biometrics.
- This facility aims to strengthen the privacy and confidentiality of resident's biometrics data.

How to stay protected?

- Do not share sensitive personal / financial information like Aadhaar number, account number, card no, expiry date, CVV, password, PIN, OTP etc with anyone.
- Most of the OTP messages mention the reason for generation of the OTP. Read every message carefully before taking any action.
- Always update your latest mobile number with Aadhaar to receive OTP's pertaining to Aadhaar related transactions.



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