UCO Bank, CISO Office

Cyber Tales by Tenali – a fortnightly series

Volume No 9 Apr 2021/ I Issue

eSIM Frauds

eSIM is one of the new technologies that has become quite popular as various telecom operators such as Airtel, Jio and Vodafone have started providing people with the option to go for one.

However, the new trend is also prone to fraudulent activities that can steal your money. Today, I will narrate you what an eSIM fraud is and how you can remain safe from it. But before that, let us see what an eSIM is?

An eSIM is an embedded SIM that is built into a smartphone. It dismisses the need for a physical SIM though it works exactly like it, provided your network carrier supports eSIM.

(inbuilt in mobile slot)

Benefits

- Doesn't require a standalone slot in the smartphone, hence, saves space for battery or makes phone thinner.
- Works well for wearables such as a smartwatch.
- Can be enabled / disabled by the network carrier remotely.
- Eliminates the risk of damaged SIM cards etc.

Along with this, eSIM fraud has also started gaining popularity with increasing SIM swapping scams.

Today, I will narrate you how Sonu got tricked by Mogambo in the name of offering eKYC upgrade.

Sonu got tricked

One day Sonu receives a warning message.

55XX9

Dear customer, your SIM card will be blocked in 24 hours. Please update your eKYC.

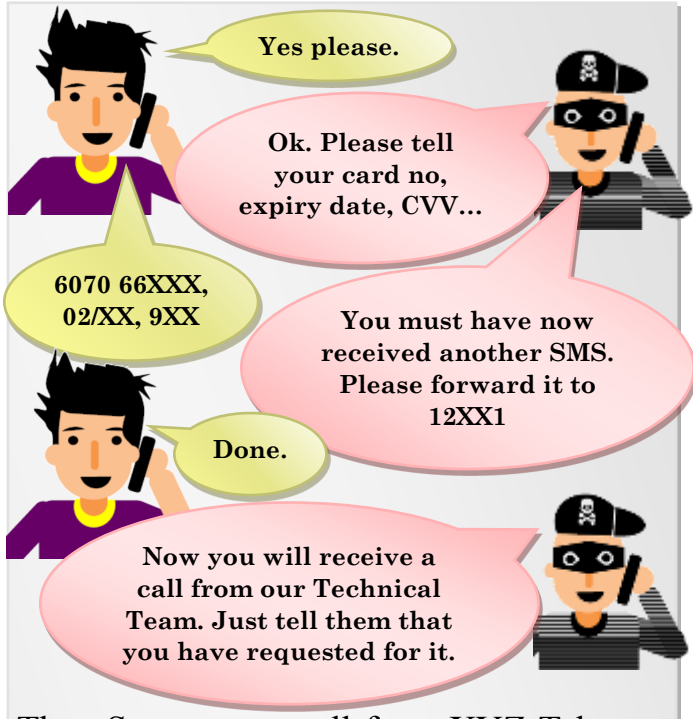
As Sonu got worried, suddenly he got a call from an unknown number...

Sir I am calling from XYZ Telecom. As your eKYC is pending since long, your SIM card will be blocked in 24hours.

But why? I have already submitted my ID while buying the SIM.

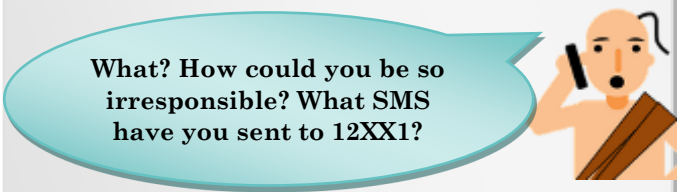
Sir, as per Govt rules we are updating eKYC. This process will cost you Rs50. And we will require your card details. Do you want to proceed?

Contd... eSIM Frauds



Then Sonu gets a call from XYZ Telecom asking whether he has requested for eSIM registration and Sonu confirms that.

After 2-3 hours, Sonu suddenly noticed that his mobile network is showing 'No Service'. Sensing something phishy, he got panicked and called me immediately from his mother's phone.



As Sonu explained the whole incident to me, I understood that this is a case of eSIM fraud and advised him to immediately report to Cyber Crime Police Station.

What has actually happened here?

- Mogambo called Sonu pretending to be XYZ telecom company's customer care executive.
- Mogambo, tactfully sends another SMS to Sonu containing the text to be sent to the official customer care number for registering Mogambo's email id with Sonu's mobile number & initiating the process of eSIM activation.
- As Sonu confirms his request to the actual customer care when they call Sonu, eSIM activating QR code is sent to Mogambo's mail id (which Sonu has sent himself to Customer Care 12XX1)
- After 2 hours, Sonu's physical SIM gets blocked as the corresponding eSIM has already been activated by Mogambo.

What should Sonu do now?

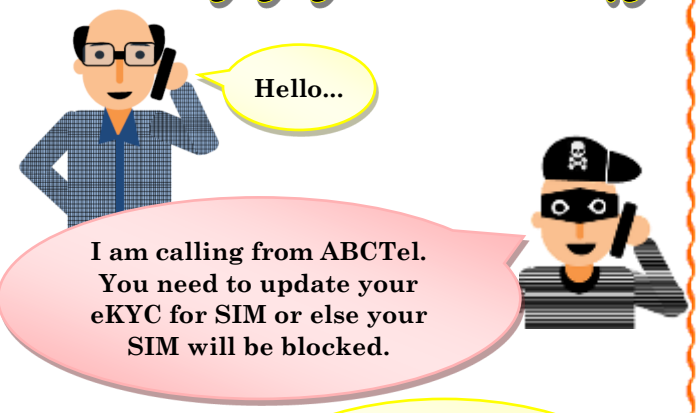
- Report to the nearest Cyber Crime Police Station & also in the National Cyber Crime Reporting Portal.
- Contact Customer Care of XYZ Telecom with request to block the eSIM.

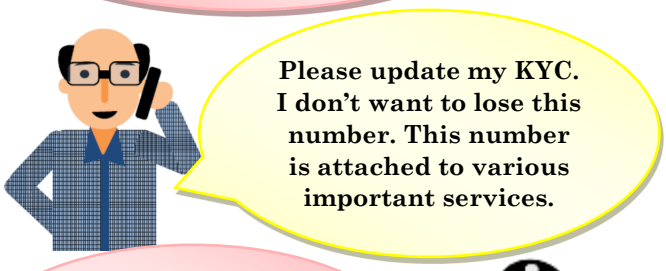
What could be Mogambo's intentions?

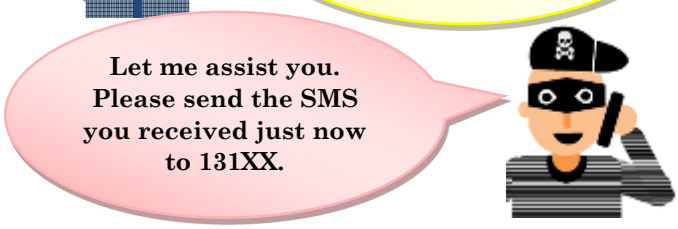
- Since Sonu's card details have also been compromised, financial transactions may be done as OTP will be received in Mogambo's mobile
- Perform USSD / SMS Banking / Phone Banking based transactions
- Register unscrupulous services using Sonu's number
- Register social media accounts
- Call Sonu's friend asking for financial help etc.

However, in another scenario, Srinivas saved himself from getting duped.

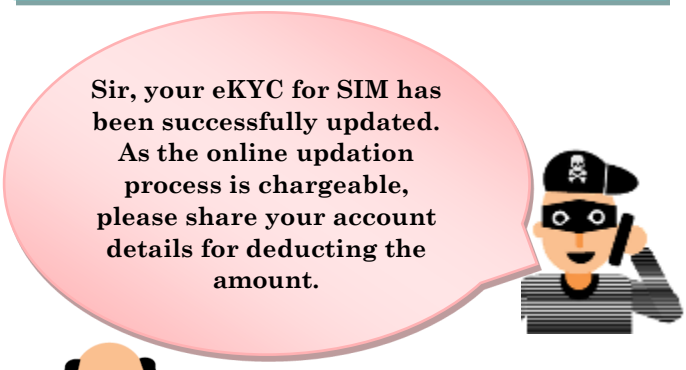
Srinivas's saved himself from getting tricked

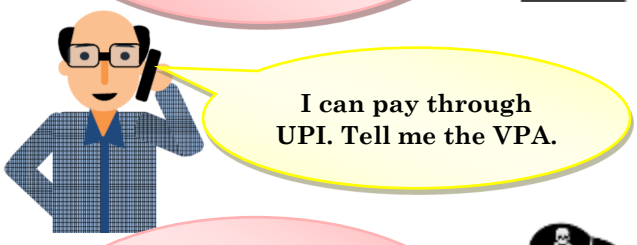


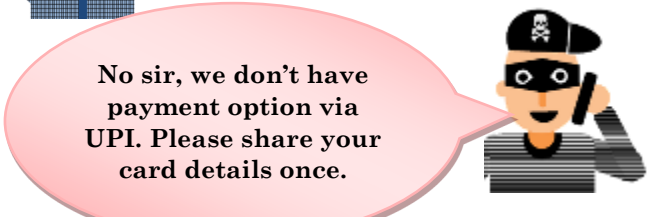


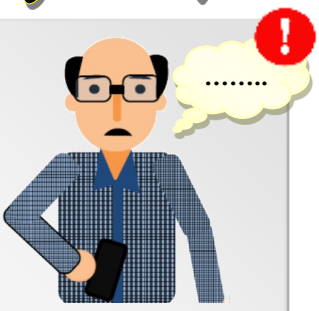


Srinivas followed all the steps as prompted by the ***Customer Care Executive***









As the person keeps on insisting to share card details, Srinivas feel suspicious and disconnect the call.

Within minutes, Srinivas realised that he may have been duped and sends 'NOSIM' message to 131XX.

He receives confirmation that his eSIM activation process has been cancelled.

Then he immediately calls me.

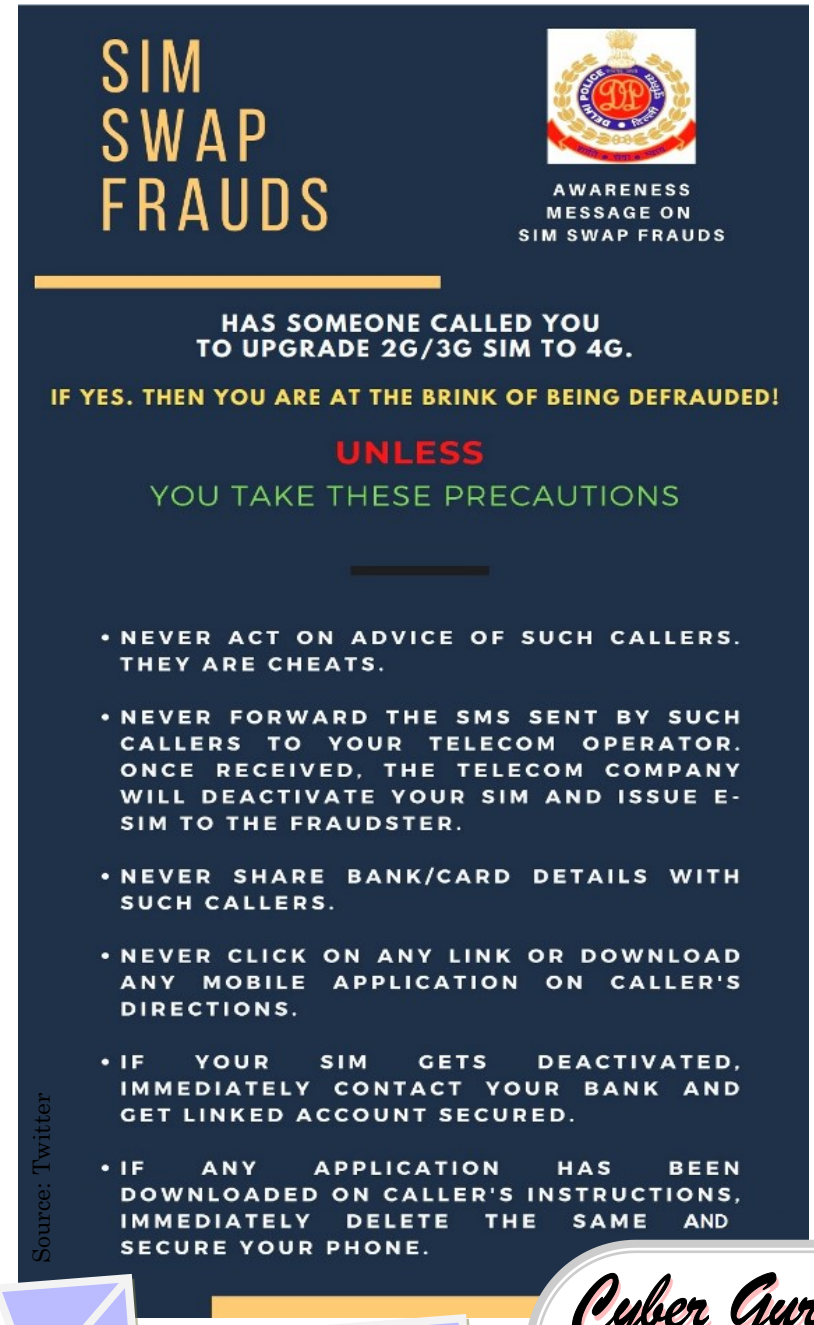
Protect Yourself

- Be cautious about unknown calls claiming to be from Customer Care Executives of Mobile Operators and asking for sending the SMS contents being told by them.
- Never reveal personal / financial details like Email id, Bank account no, card no, expiry date, PIN, password, CVV etc with anyone over phone call / email / SMS.
- For eSIM registration, always visit the verified website or authorised outlets of concerned telecom operators.

Watch out for OTPs you may not have requested.

Alert service provider in such events.

Contd... eSIM Frauds



Source: Twitter

Signs of Potential Fraud

- Usually starts with 'warning message'
- SMS received from random senders

Signs you may be a victim of SIM swap fraud

- Unable to place calls or texts.
- No network / service

In case you have fallen prey to eSIM Fraud, immediately -

- **Send "NOSIM" to 121 (Airtel)**
- **Call 199 (Vodafone-Idea)**
- **Call 198 (Jio)**

This will help you to stop the e-SIM initiation process.

Always double-check & verify message contents before sending any SMS.

Cyber Guru Tenali's Mantra

Keep Eyes Open

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