Cyber Tales by Tenali

- a fortnightly series

SIM CARD KYC VERIFICATION SCAM

यूको बैंक UCO BANK
(भारत सरकार का उपक्रम) (A Govt. of India Undertaking)
सम्मान आपके विश्वास का Honours Your Trust

Cyber tales by Tenali
Vol 18, August 2021, II Issue

Published by:
UCO Bank, CISO Office

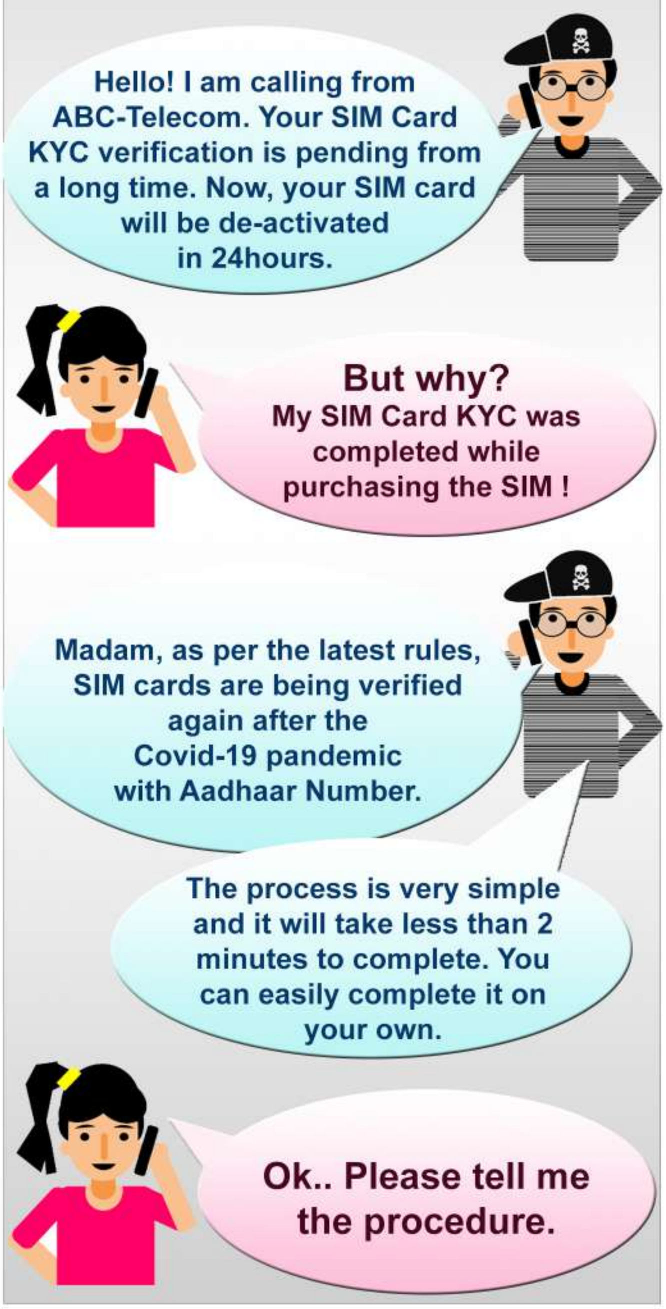
What's Inside:

India is on the path of digital transformation and there has been an increase in the adoption of technology & digital means of payments of all sizes. The number of online scams has also increased as more users have adopted the digital route of payments and verification in the backdrop of the pandemic. Cyber criminals are using public emotions like fear, lack of knowledge and various deceptive means to cheat vulnerable customers.

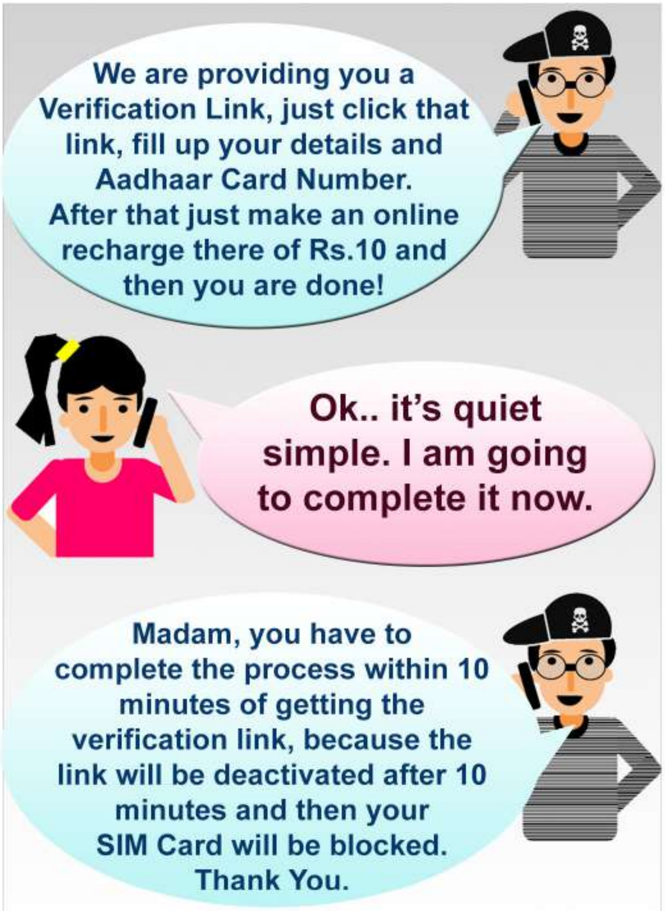
In this Edition, I will narrate you about a potential scam owing to mobile SIM Card KYC verification process.

How Munni was Tricked ?

One day Munni got a call from her Mobile Service Provider's Office.

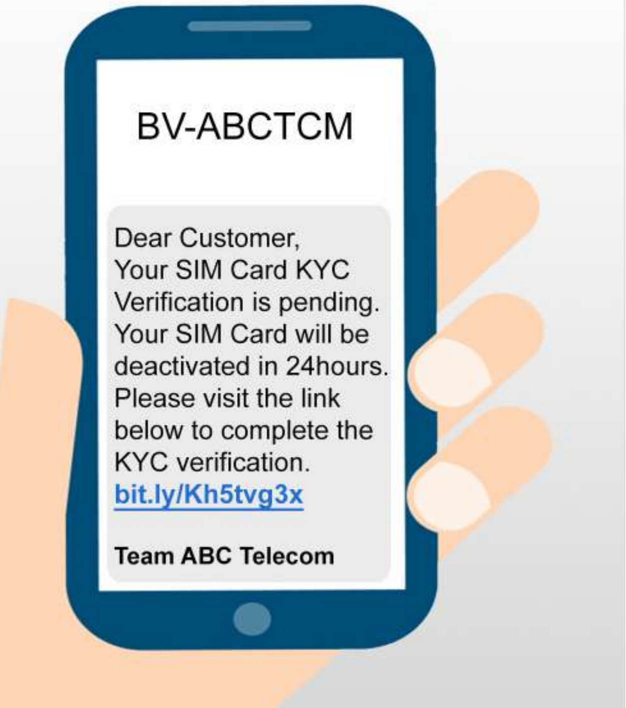

Hello! I am calling from ABC-Telecom. Your SIM Card KYC verification is pending from a long time. Now, your SIM card will be de-activated in 24hours.
But why? My SIM Card KYC was completed while purchasing the SIM !
Madam, as per the latest rules, SIM cards are being verified again after the Covid-19 pandemic with Aadhaar Number.
The process is very simple and it will take less than 2 minutes to complete. You can easily complete it on your own.
Ok.. Please tell me the procedure.

SIM CARD KYC VERIFICATION SCAM... Contd


We are providing you a Verification Link, just click that link, fill up your details and Aadhaar Card Number. After that just make an online recharge there of Rs.10 and then you are done!
Ok.. it's quiet simple. I am going to complete it now.
Madam, you have to complete the process within 10 minutes of getting the verification link, because the link will be deactivated after 10 minutes and then your SIM Card will be blocked. Thank You.

Call disconnected.

After that Munni received an SMS in her mobile.

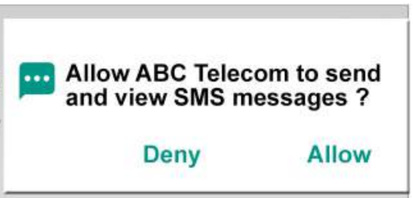


BV-ABCTCM

Dear Customer,
Your SIM Card KYC Verification is pending. Your SIM Card will be deactivated in 24hours. Please visit the link below to complete the KYC verification.
bit.ly/Kh5tvg3x

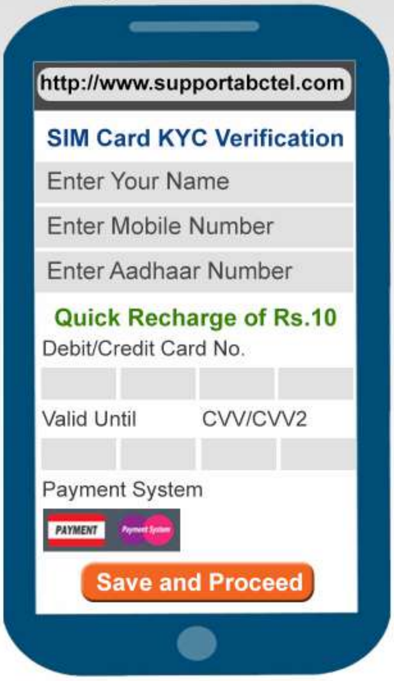
Team ABC Telecom

Munni immediately clicked on the link.



Allow ABC Telecom to send and view SMS messages ?

Then a pop-up window opened which asked for permission to view SMS messages. After allowing the permission, she was redirected to KYC Verification page.



http://www.supportabctel.com

SIM Card KYC Verification

Enter Your Name

Enter Mobile Number

Enter Aadhaar Number

Quick Recharge of Rs.10

Debit/Credit Card No.

Valid Until | CVV/CVV2

Payment System

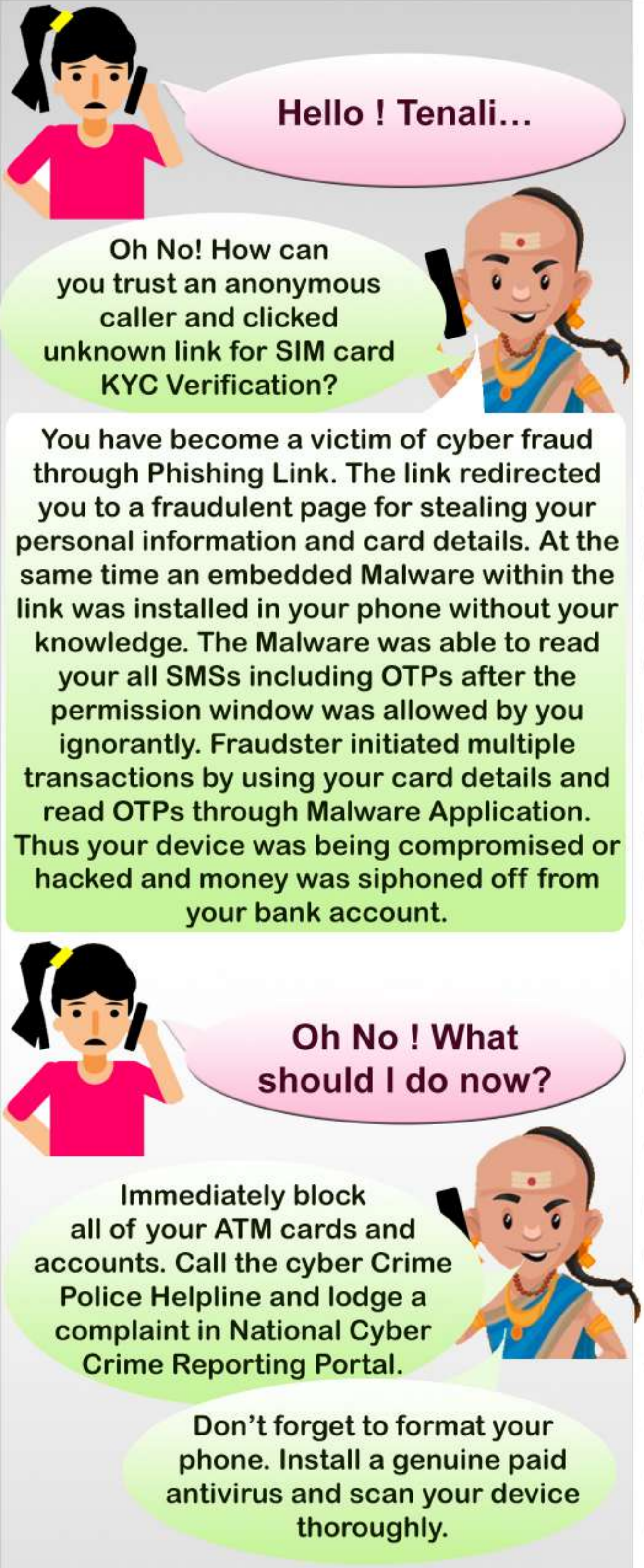
Munni filled up all her details and completed the payment for Recharge with her Debit Card and then got a confirmation message.

Dear Customer,

You have successfully completed the KYC Verification. We are always here to assist you. Enjoy our ABC-Telecom's hassle free, uninterrupted services.

After few moments Munni was surprised to see random messages were coming in her mobile regarding OTPs for different transactional amount along with their subsequent debit confirmation. Before she could understand anything, Rs.39996/- was deducted from her account by four transactions of Rs.9999/- each and her account balance became almost nil. Then she called Tenali and briefed the complete scenario.

SIM CARD KYC VERIFICATION SCAM... Contd


Hello ! Tenali…
Oh No! How can you trust an anonymous caller and clicked unknown link for SIM card KYC Verification?
You have become a victim of cyber fraud through Phishing Link. The link redirected you to a fraudulent page for stealing your personal information and card details. At the same time an embedded Malware within the link was installed in your phone without your knowledge. The Malware was able to read your all SMSs including OTPs after the permission window was allowed by you ignorantly. Fraudster initiated multiple transactions by using your card details and read OTPs through Malware Application. Thus your device was being compromised or hacked and money was siphoned off from your bank account.
Oh No ! What should I do now?
Immediately block all of your ATM cards and accounts. Call the cyber Crime Police Helpline and lodge a complaint in National Cyber Crime Reporting Portal.
Don't forget to format your phone. Install a genuine paid antivirus and scan your device thoroughly.

WHAT HAPPENED HERE?

Fraudsters are continuously developing innovative social engineering tactics to deceive victims into compromising themselves. Fraudster here posing as a customer care executive of telecom company convinced Munni with an easier process of KYC verification and sent her a malicious link. The link here performed multiple tasks. Atfirst, it asked for permission to read her SMS messages. Munni ignorantly allowed the permission and then Munni was redirected to a fraudulent website which captured her personal information and Card details. An embedded Malicious Code was being downloaded in her phone which created a passage for fraudster to compromise/hack her device. After the permission allowed by Munni for reading SMSs, the Malware was able to read all SMSs including OTPs. Thus Munni was deceived and money was being siphoned off from her bank account.

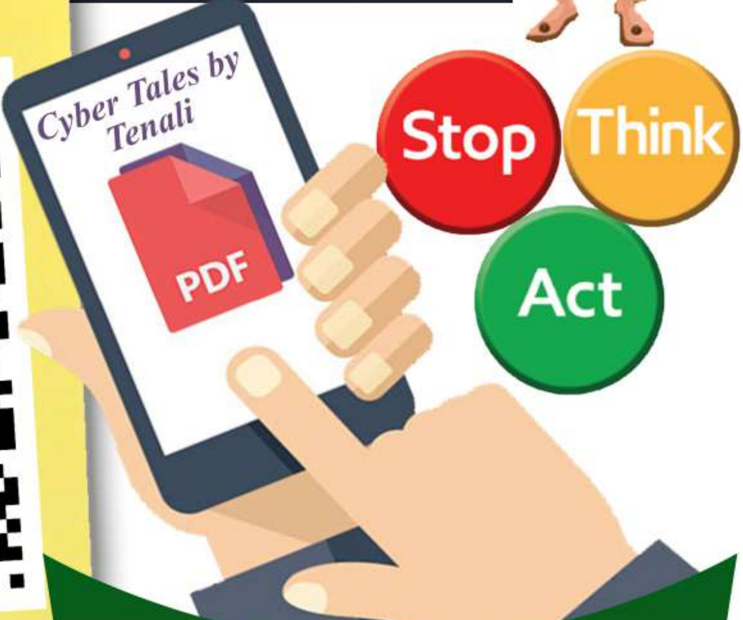
PREVENTIVE MEASURES

- ✓ *Be careful while allowing any App Permission. Do not grant 'SMS/Notification Access' to unknown Apps or Links.*
- ✓ *Do not Trust on any unknown caller.*
- ✓ *Do not click on any external link. If someone entices to click on any link, that person may be a scammer.*
- ✓ *Always check messages if they contain odd spelling, grammatical mistakes, and poor phrasing. These are all indicators of Fake messages.*
- ✓ *Do not make online payment on unverified websites as it captures debit / credit card details.*
- ✓ *Install a genuine paid antivirus and frequently scan your device.*

SIM CARD KYC VERIFICATION SCAM... Contd

Munni has lost Rs.39996 in SIM Card KYC Scam !
SMS
BEWARE OF FAKE SMSs OR CALLS !
KEEP EYES OPEN

Scan this QR Code to Download & know the whole story



In case you have fallen prey to any such fraud - **REPORT IMMEDIATELY TO THE NEAREST CYBER CRIME POLICE STATION & NATIONAL CYBER CRIME REPORTING PORTAL**

https://cybercrime.gov.in

IMPORTANT ADVISORY

In case of a Digital Payment fraud, report it to the Bank for blocking all the digital channels immediately to prevent more loss. All digital channels of our Bank like ATM card, UPI, E-Banking etc can also be blocked by UCO Digi Safe Corner under UCO M-Banking App and the same features of UCO Digi Safe are also available in UCO Secure App.

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