CISO Office, UCO Bank

Cyber Tales by Tenali

– a fortnightly series

Vol II, Dec 2020

CISO Office wishes to thank our readers for their overwhelming response and positive feedback on our new series '***Cyber Tales by Tenali***'. Keeping the trend forward, we present another modus operandi of recent cyber incident with an illustrative graphic along with the best practices.

Do give us your feedback to keep our momentum alive in enriching this publication.

Meet us...

Tinku -

- A millennial who has grown up using computer and being online….
- Was a victim of social media scam (Cyber Tales by Tenali Vol I, Dec 2020), yet trusts easily on every online content

Chutki -

- Neophyte yet savvy netizen…
- Imprudent on risks, threats and dangers of digital world…

Mogambo -

- Cybercon… into luring gullible users on popular platforms
- Small towner but reach spans the nation

Tenali -

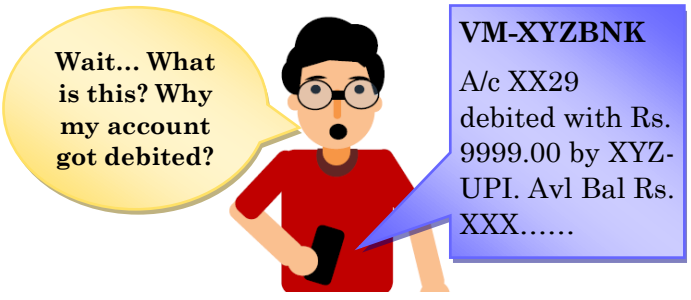
- Cyber Skill Expert & ***narrator of the story***
- Goal is to increase awareness on cyber safety and create safe, digital environment

Fraudulent Callers

Scenario 1

One day, Tinku got a phone call from Online KBC Team….

Tinku immediately entered his UPI PIN to receive the prize money, meanwhile, the phone call got disconnected... and Tinku got a message from his Bank...



Contd... Fraudulent Calls using Mobile Numbers similar to Bank's Toll Free Number

Scenario 2

Few days back, Chutki opened a savings account in ABC Bank. She eventually forgot that she already have submitted all documents in the Bank Branch while account opening.

One day, while Chutki was in a hurry with her college project work, she received a call from ABC Bank's Customer Care Executive.

Hello...

Hello Ma'am.. I am calling from ABC Bank...
You have not completed your KYC updation.

But I can't come to Branch today.
I have some urgent work.

No problem... I can update your details over the call.

Okay...That will be the better option

Just for security reasons... please verify your ATM card number....Expiry date...CVV...

4321 123XX ....11/23...321

Okay ma'am, now you will receive a 6-digit verification code for confirmation....Please tell that one....

Yes yes... it's 654321

Thank You... Your KYC details are updated successfully !

OTP is a 6-digit code, usually sent to user's registered phone number to authenticate a transaction or login in an application.

Purpose of OTP is to prevent fraud by confirming the identity of the user.

After disconnecting the call...

Oh My God !!!
What's happening !

New SMS

VM-ABCBNK

Rs. 9,999.00 spent on Card XX1234 on 19-12-20, 17:02:02 at XYZ Retail. Avl Bal Rs. XXX.....

ALERT

OTP should never be shared with anyone.

Contd... Fraudulent Calls using Mobile Numbers similar to Bank's Toll Free Number

What has actually happened ?

Both Tinku & Chutki have been victims of phone call phishing fraud, popularly known as vishing.

Don't rely on names displayed in caller identifier apps like Truecaller, True ID, CallApp etc. They may not always reflect the real identity of the caller.

In the first scenario, Mogambo, posing as Online Lottery Agency Executive , called Tinku from a number showing 'Online KBC' in Truecaller. Tinku did not verified the authenticity of the caller. Moreover, Tinku also did not noticed the UPI prompt whether it was for 'sending' or 'receiving' money. And while in hurry, he entered the UPI PIN to authenticate 'sending' the amount.

UPI PIN is required only for sending money, not while receiving it.

In the second scenario, Mogambo, impersonating as Bank's customer care executive, has called Chutki from a number which looks similar to that of the actual toll free number of ABC Bank. Chutki got tricked easily since the number showed 'ABC Bank abc' in Truecaller app and she was already pre-occupied with some other works.

What should they do now?

- Immediately report to their Banks by calling the Toll Free Number 1800XXXXXXX or visiting the nearest Bank Branch.
- 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 copy of complaint letter submitted to bank, details of the fraudulent transactions etc.
- Chutki should debit freeze her account and disable the debit card through ABC Bank's mobile banking app.
- Also, change PINs and passwords of all digital banking services availed such as - mBanking - MPIN, TPIN, ATM card PIN, E-Banking - Password, UPI - PIN etc.

Always check Bank's Toll free number from Bank's Official Website or that given in the backside of debit card issued by the Bank.

UCO Bank's Toll Free No.

1800 274 0123

~~8002740123 or +918002740123~~

What other tricks could have been used by Mogambo to lure users like Tinku & Chutki?

- Bank account has expired
- Credit card / Debit card will expire soon
- Increase credit card limit, provide add-on card, provide more benefits in credit card
- Internet banking / Mobile banking account has expired
- Won a lottery / coupon in some random show
- KYC verification for wallets like Paytm, Phonepe, Googlepay etc
- Upgrade SIM to e-sim / 5G sim
- 'Work from home' employments opportunities in Bank
- Call from the Income Tax department regarding income tax return

Contd... Fraudulent Calls using Mobile Numbers similar to Bank's Toll Free Number

- For pensioners - Call from ex-employer regarding pension details etc.

Warning Signs of Vishing

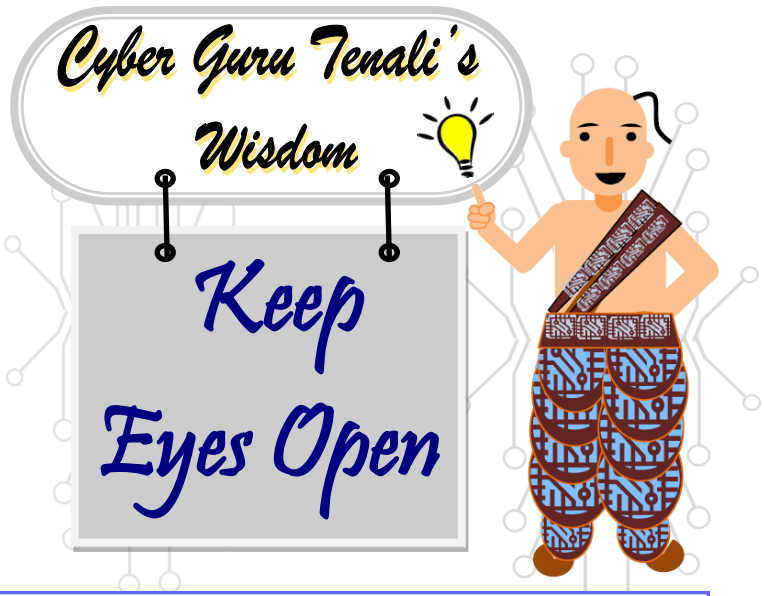
- Call from unknown number claiming to be bank / other representative
- Gain confidence of user by telling some details of the user (usually obtained from social media)
- Offer products and services which seem too good to be true
- Depict urgency to get user's response
- Warn or threaten users about negative consequences
- Ask for sensitive information like OTP, CVV, passwords, PINs etc which are not to be shared with anyone
- May ask for personal information like:
  - Date of Birth, Email id
  - Office / Residential Address
  - Family Member details
  - Aadhaar no. , PAN no. etc
- May ask for financial information like:
  - Account no., online banking user id, PIN / Password
  - Card no., PIN, expiry date, CVV
- May ask user to install remote access app like Anydesk, Teamviewer etc and then ask for code displayed in app upon installation in user device
- May send SMS / Email with malicious link and ask user to click on it

How to stay protected?

- Carefully check the number before responding. If a caller impersonates as Bank Customer Care Executive, immediately disconnect the call without divulging any sensitive information.
- Most of the OTP messages mention the reason for generation of the OTP. Read every message carefully before taking any actions.
- Check and verify the details before approving any transaction through UPI. Always remember that PIN is required while sending money, not for receiving it.
- Do not share sensitive personal / financial information with anyone.
- Do not click on links given in unknown mails or messages. Also, never install unknown apps if someone tells you over phone for 'customer support' purposes.

Online banking services has eased our lives. And following good cyber hygiene shall help us in staying safe online.

Stay Positive on Cyber Hygiene
Be Negative on Fraudulent Callers



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