

# Cyber Tales by Tenali

- a fortnightly series



## ANGLER PHISHING 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 17, August 2021, I Issue

**Published by:**  
UCO Bank, CISO Office

### What's Inside:

1. Introduction & Cover Story of Angler Phishing Scam
2. How innocents are targeted
3. How this Scam works
4. Safety Measures & Advisories



In the present covid scenario, people are staying at home and becoming more dependent on the social media and social networking sites. This widespread use of social media provides plenty of opportunities for criminals to connect with consumers and commit fraud using a range of tactics. Scammers are constantly devising new and innovative ways to trick people or harvest personal data to cause significant harm in terms of financial loss.

In this Edition, I will narrate you about a new form of cyber fraud called Angler phishing which mainly uses social media

platforms to catch its victims.

## HOW RAHUL WAS TARGETED ?

One Sunday Rahul was trying to book an online train ticket from IRCTC website. He was unable to make payment through his Net banking Account, as he was continuously getting the “server down” error.

### Error



The server is temporarily unavailable. Please try again later.

OK

Rahul, having a lot more addiction over social networking sites, immediately posted his grievance on his social media page and tagged his Bank into it.

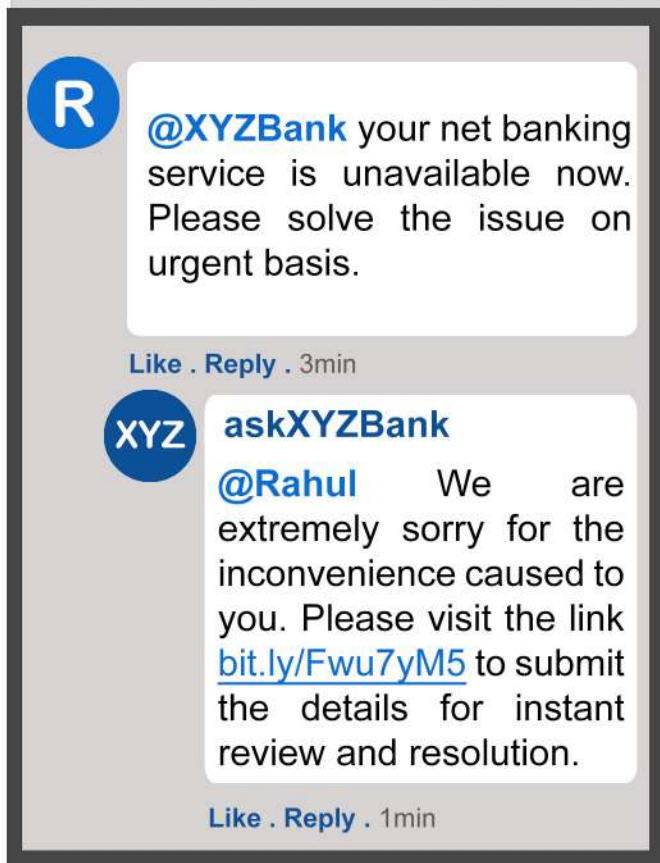


@XYZBank your net banking service is unavailable now. Please solve the issue on urgent basis.

Like . Reply . 1min

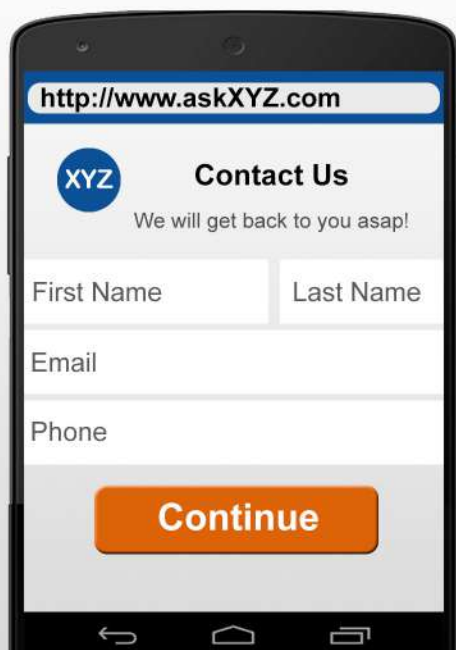
## ANGLER PHISHING SCAM... Contd

After few minutes he received a reply on his post.



The screenshot shows a social media post and its reply. The post is from a user with a blue profile picture and the letter 'R'. The text of the post says: "@XYZBank your net banking service is unavailable now. Please solve the issue on urgent basis." Below the post are the options "Like . Reply . 3min". The reply is from a user with a blue profile picture and the letters "XYZ". The text of the reply says: "askXYZBank @Rahul We are extremely sorry for the inconvenience caused to you. Please visit the link [bit.ly/Fwu7yM5](http://bit.ly/Fwu7yM5) to submit the details for instant review and resolution." Below the reply are the options "Like . Reply . 1min".

Rahul got happy seeing the reply from **askXYZBank** and immediately clicked on the link.



The screenshot shows a mobile app interface for "askXYZ.com". At the top, it says "http://www.askXYZ.com". Below that is a blue circle with "XYZ" and the text "Contact Us" and "We will get back to you asap!". There are four input fields: "First Name", "Last Name", "Email", and "Phone". At the bottom is an orange button labeled "Continue".

On submitting the details, rahul was redirected to another page.



The screenshot shows a mobile app interface for "askXYZ.com". At the top, it says "http://www.askXYZ.com/change". Below that is a blue circle with "XYZ" and the text "Welcome Rahul !". The text says: "It seems that your net-banking account has been locked due to multiple login attempts. Please change your net-banking username & password below:". There are four input fields: "Current username", "New username", "Current login password", and "New login password". Below that are two more input fields: "Current transaction password" and "New transaction password". At the bottom is an orange button labeled "Submit".

Rahul changed his credentials and got a confirmation message.




The screenshot shows a confirmation message from "XYZ". The text says: "Dear Customer, You have successfully changed your username & password for your net-banking account. Your account will be activated shortly after verification."

After few minutes Rahul got a call from an unknown number.



The illustration shows a person wearing a black hoodie and a black balaclava, holding a red phone to their ear. A green speech bubble contains the text: "Hello ! I am calling from Customer Support Division of XYZ Bank."

This call is based on your complaint regarding our net banking service. Please stay with us while we are verifying your net-banking account.



The illustration shows a man with black hair and glasses, wearing a red shirt, holding a black phone to his ear. A light blue speech bubble contains the text: "Thanks a lot for your quick assistance. Please unlock my account as I have to complete my ticket booking."

## ANGLER PHISHING SCAM... Contd

Sure Sir, we will verify your account with a transaction of Rs. 1 which will be deducted from your account and we will be reversing the same within a minute.



Ok.. Please complete the verification process quickly and activate my account.



Ok Sir, now you will receive a six digit verification code for confirmation. Please tell that one.



Its 12XXXX.



Thank you. Now please confirm that you have received the debit confirmation message of Rs.1.



Rahul immediately checked his phone and saw two messages. One is for debit confirmation and another is for credit of Rs.1.

Yes.. Yes.. Rs.1 deducted and also reversed.



Ok.. Now please tell the second verification code you received.



This time Rahul received an OTP for transaction of Rs.9999/-.

But this is for transaction of Rs.9999/- !



Yes we need this for testing purpose. We have to check that your net banking is working properly for multiple amount. Don't worry amount will not be deducted.



Ok.. Its 35XXXX.



Waiting after few seconds...

Sorry some problem has occurred this time. We are trying to solve that. We are again sending you the verification code.



Rahul checked his inbox and found Rs.9999/- deducted from his account.

But I got SMS of money being debited.



Sir, Please be assured, we are checking the complete process. Don't worry.. We have sent one more message. Please confirm the OTP.



Rahul trusted the customer care executive and again told him the OTP.

Thanks for cooperating with us. Your account will be activated within 10-15 minutes. Have a good day!



After disconnecting the call...

Till now I haven't received the amount for the last two transactions !



Rahul called Tenali and briefed the complete scenario.

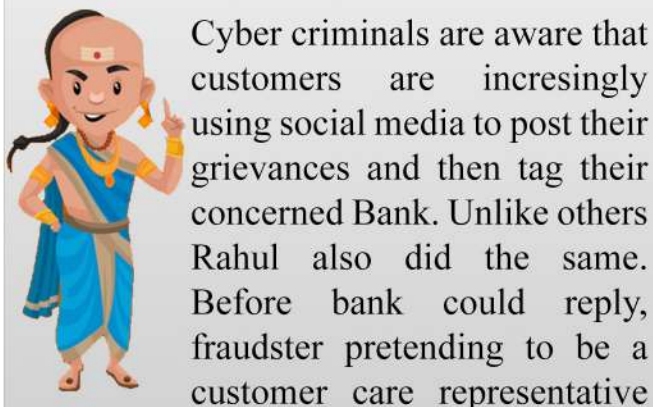
## ANGLER PHISHING SCAM... Contd



You have become a victim of an Angler Phishing Scam. That caller was fake! With a fake account in Social Media he pretending to be a customer care executive of your Bank, sent you a fake link for stealing your net-banking credentials. He then logged onto your net-banking account and did multiple transactions. He also gained your trust by reversing Rs.1 and then convinced you for sharing the OTPs for the next multiple high value transactions.



### WHAT HAPPENED HERE?



Cyber criminals are aware that customers are increasingly using social media to post their grievances and then tag their concerned Bank. Unlike others Rahul also did the same. Before bank could reply, fraudster pretending to be a customer care representative

started communicating with Rahul through an account named similar to Rahul's Bank. Fraudster convinced Rahul that his problem will be resolved by clicking on a link. After clicking the link, Rahul was redirected to a fraudulent website which captured his personal information and net-banking credentials. Fraudster then logged onto his net-banking account and did multiple transactions.

Fraudster gained the trust of Rahul by reversing the first transactional amount and tricked him for sharing OTPs for the next high value transactions. Thus using an Angler phishing technique Rahul was duped and he became the victim of monetary loss.

### SAFETY MEASURES TO FOLLOW

- ✓ Always read the description of the Social Media Account carefully and check the account from which response came is same as the official account of the organisation.
- ✓ Do not click on any external link. If someone entices to click on any link, that person may be a scammer.
- ✓ Never share personal or sensitive information (OTP, PIN etc) with any unknown caller under any circumstances.
- ✓ Never search customer care number on search engine or Social Media Sites. They may come up with wrong information. Customer care no. should always be taken from Official Website of the Organisation.

# ANGLER PHISHING SCAM... Contd



Rahul has lost Rs.19,998/- in Online Fraud.

## DON'T BE ANOTHER RAHUL !!



**KEEP EYES OPEN**

Scan this QR Code to Download & know the whole story



युको बँक UCO BANK



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 dital 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](mailto:ciso.office@ucobank.co.in)