UCO Bank, CISO Office

Cyber Tales by Tenali

- a fortnightly series

NEW TECHNIQUE INTRODUCED BY FRAUDSTERS...

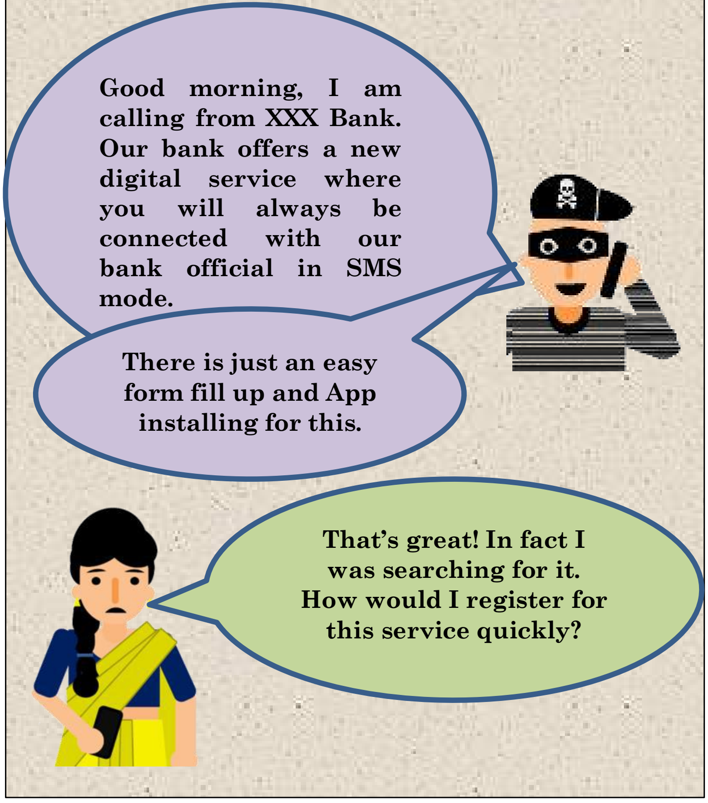
Volume No 13 June 2021/ I Issue

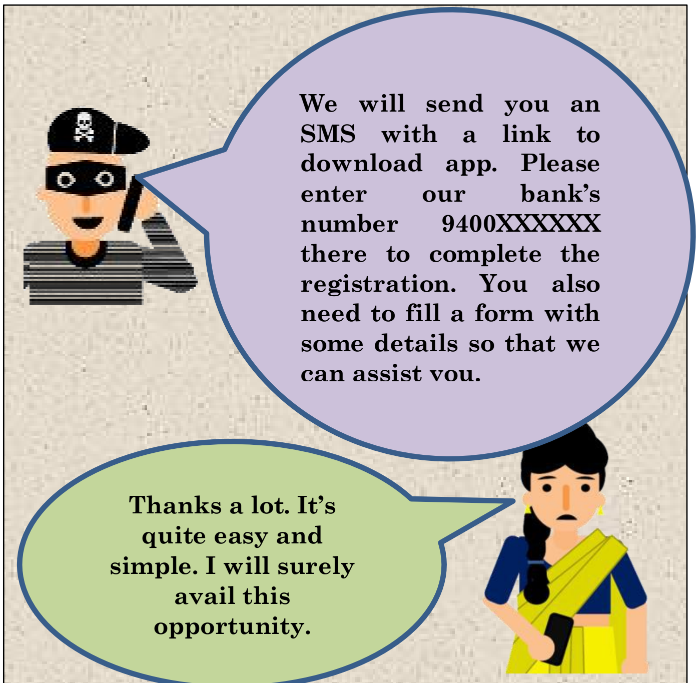
Today's consumers demand more online and mobile services from their financial institutions. In the process, Banks are trying to differentiate themselves by providing easy-to-use and digital-native experiences to customers. Opportunistic hackers are also taking advantage of this digital banking era to commit even more fraudulent activity.

In this edition, I will narrate you an amazing technique adopted by fraudsters for defrauding bank's customers.

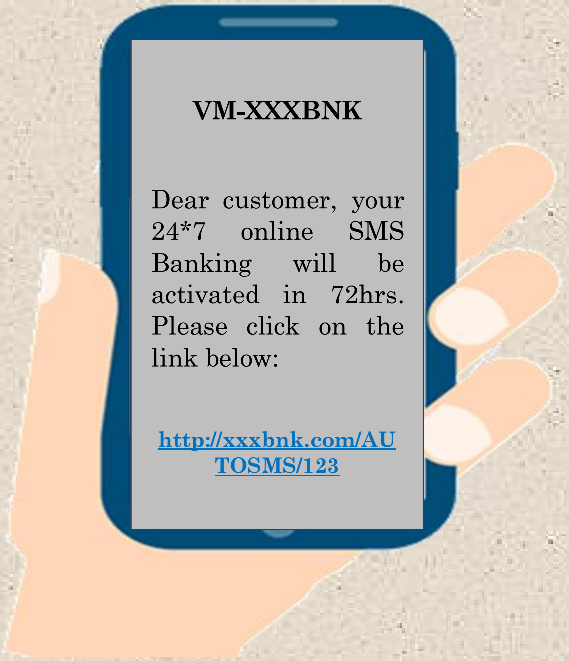
Sonali got scammed

Sonali was searching online for whatsapp banking with the facility of 24*7 banking for her new start-up business. One day she got a call from an unknown number.


Good morning, I am calling from XXX Bank. Our bank offers a new digital service where you will always be connected with our bank official in SMS mode.
There is just an easy form fill up and App installing for this.
That's great! In fact I was searching for it. How would I register for this service quickly?


We will send you an SMS with a link to download app. Please enter our bank's number 9400XXXXXX there to complete the registration. You also need to fill a form with some details so that we can assist you.
Thanks a lot. It's quite easy and simple. I will surely avail this opportunity.

After this, Sonali receives an SMS:



VM-XXXBNK

Dear customer, your 24*7 online SMS Banking will be activated in 72hrs. Please click on the link below:

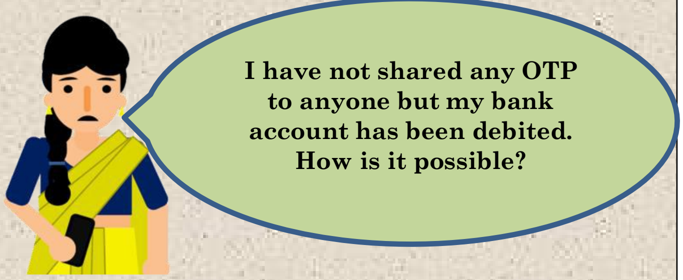
http://xxxbnk.com/AUTOSMS/123

Sonali immediately clicked on the link, which redirected her to a form where she filled her name, mobile no., ATM Card No., Expiry Date of Card, CVV etc.. Thereafter, she was redirected to Download App option. She downloaded

NEW TECHNIQUE INTRODUCED BY FRAUDSTERS...

and successfully installed the app. She also entered the mobile number in the app as prompted by the caller person.

After 2 days, Sonali found her Bank Account has been debited with Rs.10,000/-. She was puzzled and so she called me.


I have not shared any OTP to anyone but my bank account has been debited. How is it possible?

After listening all the story from Sonali, I made her realise that she has been defrauded by Auto-SMS Forwarder App.

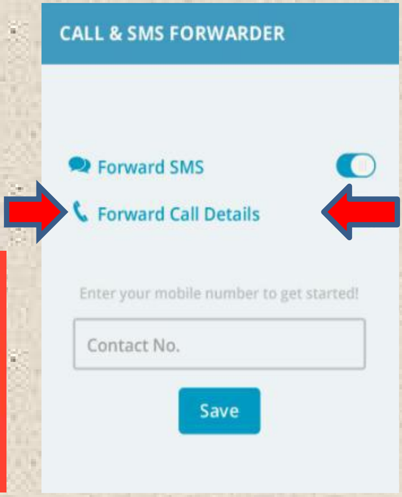
What actually happened here?

Sonali, in ignorance, has provided the card details to the customer and installed an Auto SMS Forwarder App in her mobile. She also entered the fraudster's mobile number in the App due to which all SMS (even containing personal, vital information and OTP) coming into her mobile were being forwarded automatically to fraudster's number.

Fraudster initiated an online transaction with Sonali's ATM card and got OTP by this Auto SMS Forwarder App and Sonali's account got debited. Sonali did not notice the OTP message and became the victim of vital information loss.

SMS forwarder app enables the user to sync texts (SMS) across multiple devices such as mobile to another mobile or laptop.

Auto Forward is a monitoring software designed to track another person's mobile phone. It is an easy-to-use app that includes a set of handy features, such as monitoring GPS location, calls, SMS, and social media chats of a target user.



Think before You Act

- ➢ Do not trust any unknown caller offering easy banking services. Always remember easy things can put us on easy risk.
- ➢ Do not click on any link without verifying its authenticity.
- ➢ If someone entices to install any app, that person may be a Fraud (scammer)

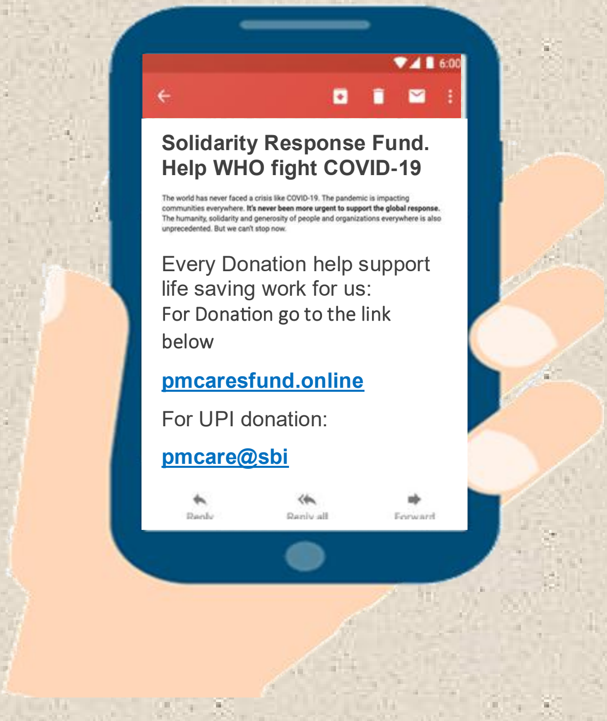
We welcome your valuable suggestions / feedback at ciso.office@ucobank.co.in

COVID-19 related Cyber frauds on rise...

Ruma saved her friend from getting tricked

During the coronavirus crisis, we have seen great examples of humanity helping each other. Around the world, an army of volunteers has stepped up to help the vulnerable and those in need. Unfortunately, we have also witnessed a rise in charity scams, as fraudsters seek to exploit the crisis to carry out cybercrime. Scammers are taking advantage of fears surrounding the coronavirus. They're setting up websites to trick people and using fake emails, texts, and social media posts as a ruse to take our money and get our personal information.

One day Vishal received an email on Solidarity Response Fund:



Solidarity Response Fund. Help WHO fight COVID-19

The world has never faced a crisis like COVID-19. The pandemic is impacting communities everywhere. **It's never been more urgent to support the global response.** The humanity, solidarity and generosity of people and organizations everywhere is also unprecedented. But we can't stop now.

Every Donation help support life saving work for us:
For Donation go to the link below

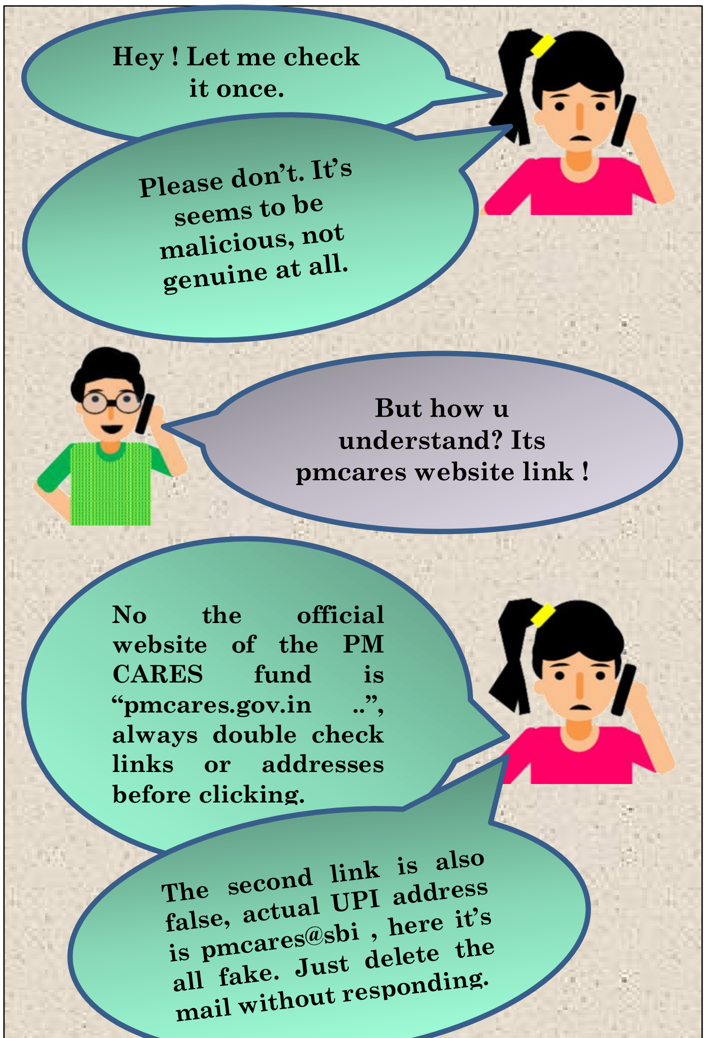
pmcaresfund.online

For UPI donation:

pmcare@sbi

Vishal forwarded the mail to his friend Ruma and asked.

Hello Ruma ! I've forwarded a mail to you. I want to donate via this...



Hey ! Let me check it once.
Please don't. It's seems to be malicious, not genuine at all.
But how u understand? Its pmcares website link !
No the official website of the PM CARES fund is "pmcares.gov.in ..", always double check links or addresses before clicking.
The second link is also false, actual UPI address is pmcares@sbi , here it's all fake. Just delete the mail without responding.

What actually happened here?

Here the scammer uses phishing method for tricking. Phishing is a method of trying to gather personal information using deceptive e-mails and websites.

The goal is to trick the email recipient into believing that the message is something they want or need. Emails are sent to millions of potential victims to try to trick them into logging in to fake versions of very popular websites. The fake website looks almost similar with the actual one and saves all personal information of the victim and sometimes asks for banking information for siphoning off Money.

COVID-19 related Cyber frauds on rise...

जागरूक रहें और अपनी आँखें खुली रखें

- ❖ *लिंक और अटैचमेंट से सावधान रहें: किसी अनजान व्यक्ति से प्राप्त किसी भी लिंक या अटैचमेंट पर क्लिक करने से बचें। क्लिक करने से पहले हमेशा लिंक और ईमेल पतों की दोबारा जांच करें।*

- ❖ *ऑनलाइन दान में भेंट या भुगतान करने से पहले, यह सत्यापित करना सुनिश्चित करें कि संस्था और लिंक वैध हैं।*

- ❖ *COVID-19 के बारे में जानकारी प्राप्त करने का सबसे सुरक्षित स्थान विशेष रूप से सरकारी वेबसाइटों के माध्यम से है; .gov पर समाप्त होने वाले URL खोजें।*

- ❖ *किसी ऐसे व्यक्ति को कभी भी पैसे न भेजें या व्यक्तिगत जानकारी, कार्ड विवरण, या ऑनलाइन खाता विवरण प्रदान न करें जिसे आप नहीं जानते या भरोसा नहीं करते हैं।*

चेतावनी

क्लिक करने से पहले लिंक और ईमेल पतों को दोबारा जांच लें। नकली लिंक अक्सर अतिरिक्त शब्द या अक्षर और .online जैसे दुर्भावनापूर्ण एक्सटेंशन जोड़कर स्थापित वेबसाइटों की नकल करते हैं। URL या ईमेल पते में गलत वर्तनी वाले शब्द या अनियमित अक्षर और संख्याएं भी एक धोखे का संकेत दे सकते हैं।

यदि आप ऐसी किसी धोखाधड़ी में फंस गए हैं-

निकटतम साइबर अपराध पुलिस स्टेशन और राष्ट्रीय पोर्टल को तुरंत रिपोर्ट करें

https://cybercrime.gov.in