Cyber Tales by Tenali

- a fortnightly series

REMOTE SCREEN SHARING APP FRAUD

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 16, July 2021, II Issue

Published by:
UCO Bank, CISO Office

What's Inside:

Online fraud has been prevalent and going strong these days. Fraudsters have been adapting to the remote working situation and coming up with creative ways to defraud innocent people. With COVID-19 still largely affecting how and where we work today, it's important to stay up to date on any new malicious activity from online sources.

In this edition we will look how scammers use the most recent tactics - Remote Screen Mirroring process to steal personal information of user, UPI Pin and many more.

HOW ANITA GOT TRICKED ???

One day Anita got a call from Amazon Customer Care Executive.

Hello ! I am calling from Amazon Customer Care Division.

Your Amazon account has been credited with Free 10,000 reward points having 2 days validity to redeem. You are eligible for free online purchase worth Rs.5000 through Amazon App only.

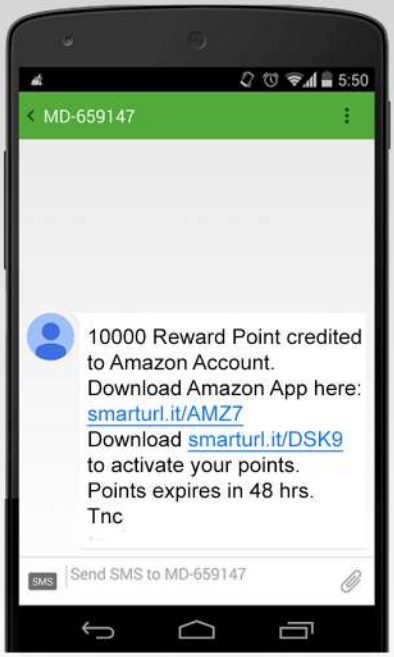
Wow that's great ! I am a frequent buyer of Amazon products through website, but I haven't used Amazon App till now.

No problem Mam ! I will help you to install this App on your phone.

I am sharing two downloadable links - one for the App and another for activation of your free reward points in your Amazon account. Please be on the line Madam!

REMOTE SCREEN SHARING APP FRAUD... Contd

After that Anita received an SMS like this:



Anita clicked on both the links and installed both the Apps.

Anita opened the second App and the screen was something like below:

Anita was very excited to avail this offer. As per the instructions of the customer care executive, she made two purchase orders. She made payment for her first purchase through netbanking and for another purchase she used UPI App. She was eagerly waiting for the notification from Amazon for receipt of the purchase amount.

But next morning Anita was surprised to see a series of messages in her mobile regarding OTPs for different transactional amount, and SMS for debit confirmation. Her account balance was showing only Rs.989 in the last SMS. She called Tenali and briefed the total scenario.

REMOTE SCREEN SHARING APP FRAUD... Contd

Oh No ! How can you trust an anonymous caller and clicked unknown links for App installation?

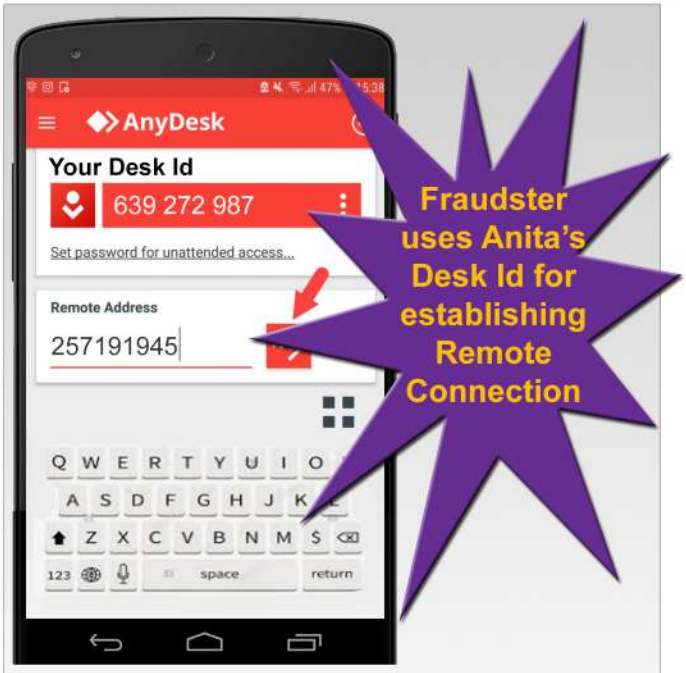
You have become a victim of fraud via remote screen sharing app. This type of App allowed the fraudulent caller to gain access on your mobile screen and he recorded all sensitive information which you have used for making online payment.

Oh No ! What should I do now?

Immediately uninstall the App, call the cybercrime police helpline, block all of your ATM Cards and accounts, change all your digital channel passwords including UPI PIN, net banking.

WHAT HAPPENED HERE?

This is a new tactic involving instances of fraud stemming from Screen sharing application that gives scammers access to targeted devices where it has been installed. Fraudster here posing as a customer care executive from Amazon, tricked Anita with a fake offer and took this opportunity to direct her for downloading a Remote Screen-sharing App in her mobile. Sharing 9 digit Desk ID from the app allowed him to connect with the Remote Address of Anita's mobile from his own device.



After gaining the full access on the victim's device, he was able to view and record the screen live. The moment Anita typed the ID/password of his net- banking or pin for UPI app for purchasing from Amazon App, the fraudster simply noted it down. These type of apps continued to work in the background even when the phone is locked.

SAFETY PRECAUTIONS

- ***Do not Trust on Any Unknown Caller.***
- ***If someone entices to install any app, that person may be a scammer because authentic customer care executives will never ask anyone to download apps or send codes.***
- ***Download only those apps which are authentic, verified and known to you.***

contd..

REMOTE SCREEN SHARING APP FRAUD... Contd

SAFETY PRECAUTIONS

contd..

- ☑ *Do not click on any link came from unknown or untrusted sources.*
- ☑ *Do not fall prey to free offer or rewards.*
- ☑ *Never share confidential details like UPI PIN, OTP, etc. with anyone.*

IMPORTANT ADVISORY

In case of a UPI fraud, report it to the bank or e-wallet firm and get the wallet blocked 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 App. It is also advisable to file an FIR or report the incident to the cyber-crime cell. Avoid searching for the customer care number on search engine. Random Google searches might take you to fake call centre. In case of any issue, file complaint on the platform itself or get the number from the official website.

Scan this QR Code to Download the complete edition:

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

Cyber Guru Tenali's Mantra

KEEP EYES OPEN

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