UCO Bank, CISO Office

Cyber Tales by Tenali

– a fortnightly series

Volume No 12 May 2021/ II Issue

COVID-19 related Cyber Frauds on rise...

The second wave of Covid-19 has come as a blessing for cyber fraudsters, who are taking advantage of the shortage of emergency drugs and other emergency equipment, to dupe unsuspecting users. Fraudsters are leveraging several techniques like posting fake posts on social media platforms or offering to provide the needed drug or equipment by clicking malicious links, for duping innocent people.

In this edition, let us be aware about some techniques adopted by scamsters for defrauding users.

Srinivas was tricked

Since few days, Srinivas had been searching for oxygen cylinders for his Covid-19 positive wife who has been admitted to a local hospital. In order to find leads on oxygen resources, Srinivas joined numerous WhatsApp groups where people had been sharing leads to help others in crisis.

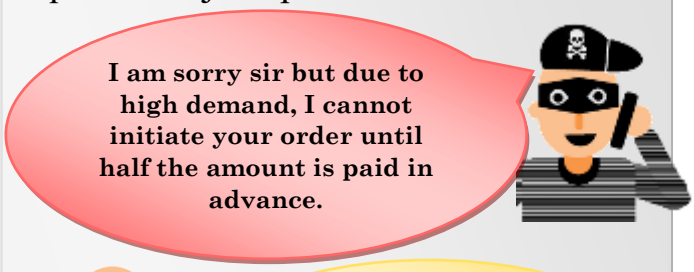
In that group, suddenly he came across a post quoting Rs 27,500 for a 50 kg oxygen cylinder from one of the oxygen suppliers named Raju Kumar. The contact details of the supplier was also provided in that post.

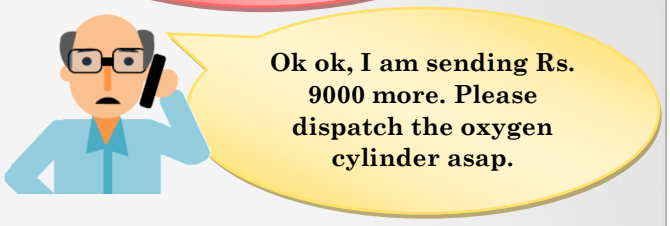
Srinivas immediately contacted Raju.

As Raju kept on refusing to entertain Srinivas's request if not paid in advance, Srinivas sensed something fishy and disconnected the call.

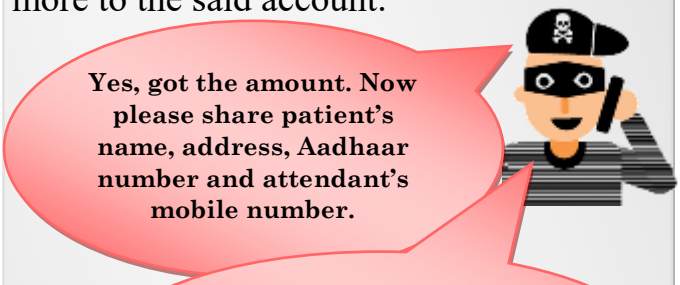
However, the next day, things changed when Srinivas was told that his wife's Oxygen Saturation (SpO2) had dropped down to 80, and the temporary oxygen arranged by the local hospital was about to finish. Srinivas was left with no other option but to take the risk. He made an advanced payment of Rs 5,000 and

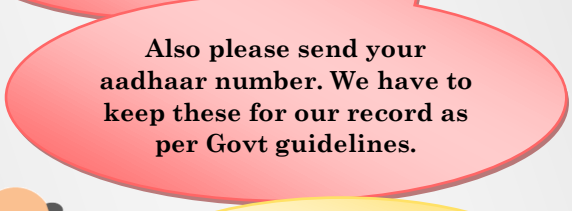
requested Raju to process his order.



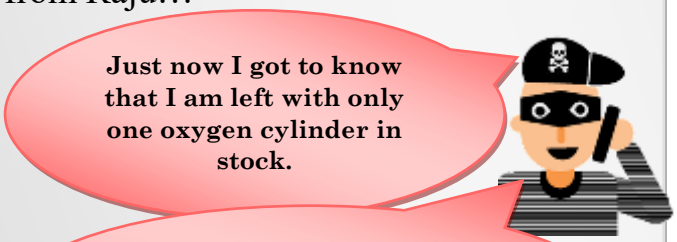


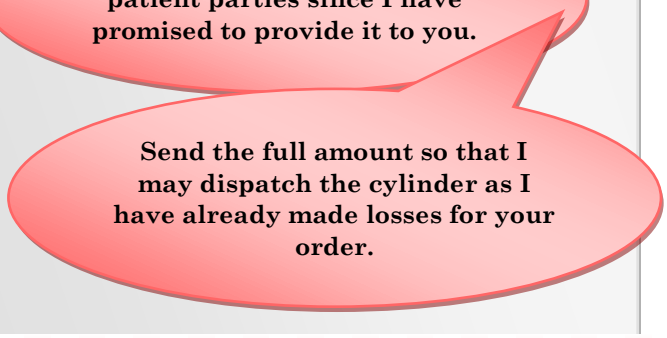
Srinivas immediately transfers Rs 9000 more to the said account.



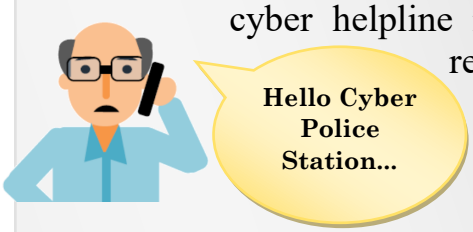


A few minutes later, Srinivas got a call from Raju…





Srinivas was now assured of his previous hunch of fraud and decided to cancel the deal and told Raju to refund the money paid as advance. But Raju dropped the call and switched off his phone. Being sure that it was a scam, Srinivas immediately contacted the local Police cyber helpline number and reported the issue.



What actually happened here?

Srinivas is one of the many victims who have recently been duped by the "Covid SOS Scammers" targeting thousands of people who are using social media posts to seek help in these desperate times. Caught in a troublesome situation, Srinivas also fell into the trap and shared his Aadhaar number with the unknown caller. Apart from losing money, Srinivas has also become the victim of identity theft.

Protect Your Identity

- Do not share sensitive personal / information like Aadhaar number, PAN number, PIN, OTP etc with anyone.
- Do not blindly follow social media posts purporting 'verified' leads of necessary items.
- Beware of suspicious social media profiles pretending to be doctors and posting leads on essential items. These accounts, apparently representing doctors, are created very recently and have zero to no followers / posts in their profile.

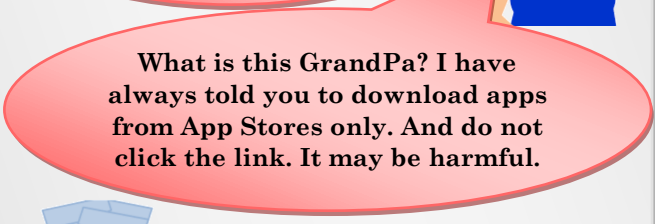
Chutki saved her GrandPa from getting tricked

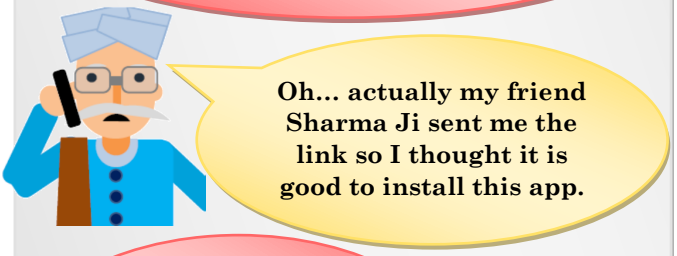
The Covid-19 pandemic has accelerated use of mobile health apps and virtual care. But it also brings along multifarious threats especially making the senior citizens more vulnerable.

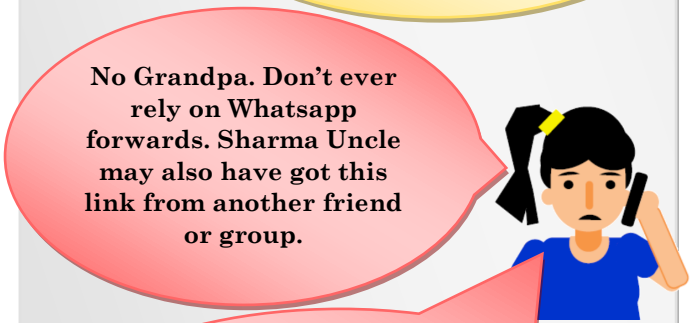
Aged people are being forced to be tech-savvy due to circumstances and so they had to go digital overnight. The elderly group does always seem to advocate Whatsapp forwards. But the crucial issue remains verification of these messages.

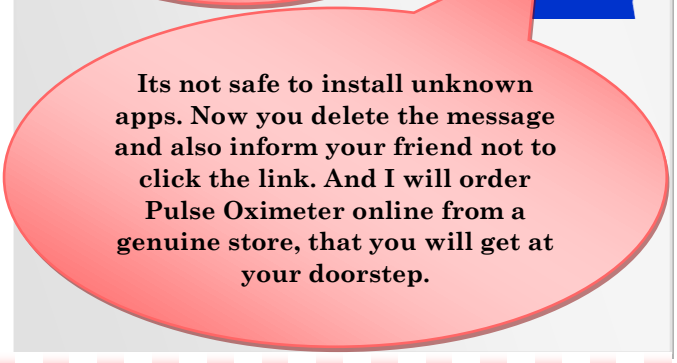
One day, Chutki's Grandfather got a message from one of his friend in Whatsapp.

Since long, GrandPa was searching for a pulse oximeter device in his locality but could not get due to lack of supply in local stores. He got relieved on seeing this message and thought to download the app mentioned in it. He clicked the link and it redirected to his phone's browser. Since the browser was not updated, the app's apk file could not get downloaded into his mobile. GrandPa tried again but it showed some error. Then he called Chutki for her help in installing the app.









COVID-19 related Cyber Frauds on rise...

What is actually happening?

- In the virtual world, most of us rely on random forwarded messages in family as well as friends' groups.
- But this may increase the possibility of an elder ending up clicking malicious link or installing a malware app that could cost him / her even banking passwords.
- Messages are widely circulating on Whatsapp advising users to install apps which claim to detect oxygen level by 'just keeping fingers over the camera.'
- On installing, multiple permissions like access to camera, gallery, SMS etc are asked by the app. Once allowed, these access can potentially be used by cyber criminals to access confidential / biometric information of the user.
- Apart from this, many elders do not use the two-factor authentication to protect accounts and some of them have been found to use simple & old passwords across multiple accounts.

Let us keep our Elders Cyber Safe & Sensitise them on Cyber Safety Practices

- Beware of fake messages. Refrain from forwarding them.
- Do not download apps from unknown links. Instead, download them from application stores only.
- Before downloading any app, verify the developer's name, ratings and reviews.

User's must understand that fingerprint scanner / camera in mobile can never calculate oxygen level.

For checking oxygen level, a proper sensor is required.

In case user is not able to recognise a fake app and ends up installing it, then, while in the process of checking the oxygen level, the user should not allow permission to share location, camera, fingerprint, SMS and call logs.

In case you have fallen prey to any such fraud, immediately-

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