

Cyber Tales by Tenali

- a fortnightly series

Volume No 7

Mar 2021/ I Issue



Cyber Smart Woman



International Women's Day is celebrated on 8th of March every year. This year, International Women's Day 2021 is being celebrated with the theme,

“Women in leadership: Achieving an equal future in a COVID-19 world”

In this special edition, I will focus on a few cyber safety issues specific to women.



Women has always been target of cybercriminals for years and the lockdown has made the stalkers much bolder. In the post pandemic world, whether we use Zoom, Webex or Microsoft Teams, the camera on our laptop, tablet or phone has probably never been as active as it is now-a-days.

Most of us are using our devices for work, study or virtual socialising. Unfortunately, this privilege has left us vulnerable to a cyber attack called camfecting, a blend of the words camera and infecting. This is when hackers take control of our device's camera remotely.

Today, I will narrate how Rashmi became a victim of camera hacking.

Rashmi got scammed

Rashmi is a Internet freak user. She plays random games & contests in social media apps and is also quick in accepting friend

requests from unknown persons.

Obsessed with likes and comments by followers in her social media posts, she used to carry her phone everywhere along with her for checking updates every now and then.

One day, Priya, a friend of Rashmi, informs about Rashmi's private video in some random website.

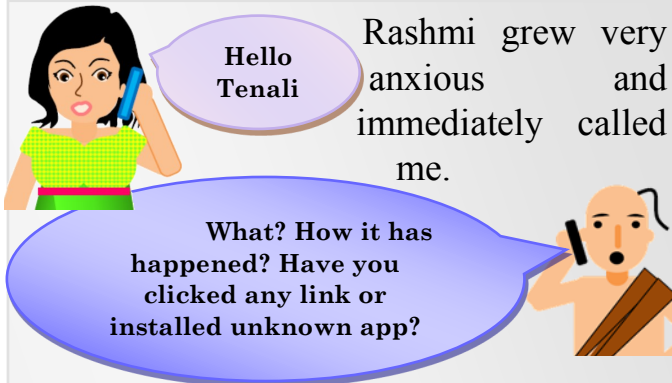


Rashmi, just check the screenshot I have sent you. My friend saw this in a website.

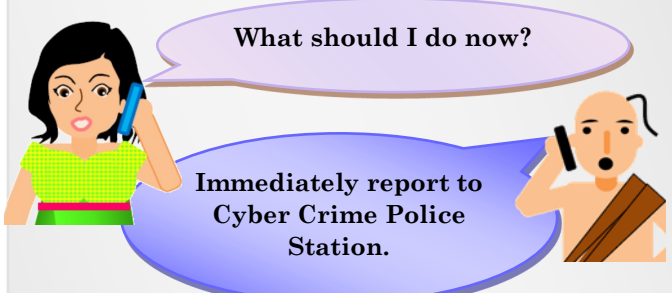
Oh! No. How is it possible? What should I do now?




I don't know exactly how to take it down. You can contact Tenali. I heard that he has helped Tinku in many cyber scams.



Rashmi grew very anxious and immediately called me. Rashmi started crying and told me that she frequently used to download new apps & games. Off late, she has been experiencing several issues in her phone. Her phone was getting slow day by day. I understood that she has been victim of camera hijacking via malware installed in her mobile phone.



What should Rashmi do now?

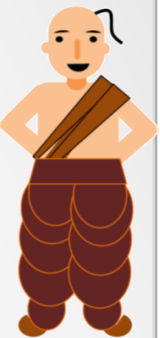
- 
- ◆ Immediately report the incident to the nearest Cyber Crime Police Station for getting the video clip down
 - ◆ Report to National Cyber Crime Reporting Portal
 - ◆ Uninstall unknown apps and do a full factory reset after backing up important data
 - ◆ Update mobile device OS, apps & antivirus

What actually happened here?

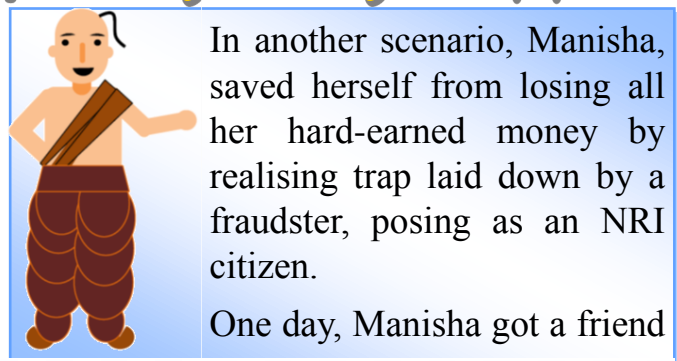
Since long, Rashmi has not updated her device's OS & antivirus. She had no idea that a recently installed game contained malware. While installing the game, she allowed all permissions, unnoticeably. The

malware switched on the front and back cameras of her phone without her consent, discreetly capturing videos. Unaware of the malware, one day, Rashmi kept her phone aside in the trial room at a shopping mall while giving trials for dresses. This might have led to recording of her private video by the malware and thereafter uploading to offensive sites.

How to Stay Safe?

- 
- ◆ Do not click on suspicious links / random games / ads in social media.
 - ◆ Disable media-auto-download feature in instant messaging apps.
 - ◆ Exercise caution while allowing permissions to apps.
 - ◆ As a precautionary measure, keep webcam / mobile phone camera covered when not in use.
 - ◆ Power-off laptop / desktop, when not in use. Don't let a device's hibernation or sleep mode lure you into a false sense of safety.
 - ◆ Routinely clear unnecessary apps from mobile devices.

Manisha saved herself from getting trapped



Contd... Cyber Smart Woman



Friend Request Accepted

request from 'Aryan' in Facebook. The guy looked handsome and decent. She accepted the request. Within minutes, she got a message from Aryan who introduced himself as a software engineer, settled in

USA. Soon they shared mobile number and started chatting frequently.

Hi

Hello

After chatting for a few days, Aryan told Manisha that he is sending some gifts & cash for her worth \$60,000 through US-based ABC Courier. Manisha got surprised and happy hearing that. Aryan also gave Manisha tracking id of the courier.

Next day, Manisha received an email from ABC Courier, stating that her parcel is ready for shipping and that she would receive it the following day. The courier company also gave her the name of the delivery agent - Aparna along with Aparna's Bank account details, stating that Manisha would have to pay ₹20,000 before the delivery. Manisha immediately calls Aryan.

New Email



Courier Company is asking for payment of Rs 20,000/-

I know. But, this is the only process for sending any item via international courier.



Don't worry, the amount will be refunded after the item is delivered.



Rs 20000 Paid

Manisha got convinced and immediately transferred the amount to the courier agent's account through mobile banking app. However, the same day

Manisha receives another email appearing from 'Customs', stating that the parcel contained US dollars, which was illegal to be couriered to India. It further stated that Manisha would have to get permission from the government or pay ₹40,000 as fine. Manisha immediately called Aryan to ensure genuineness of the procedure.

New Email



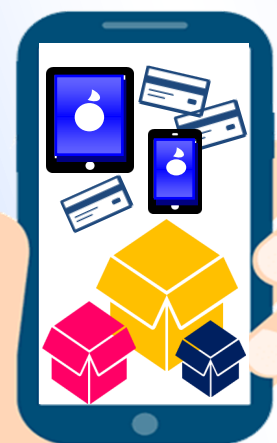
Hello Aryan...



Manisha, this is part of the process. And the fine amount is negligible compared to the gifts. Check I have sent you a photo in WhatsApp.

Manisha gets startled seeing the gifts Aryan is sending. Gradually, she also got emotionally attached to Aryan and developed blind faith on his words.

Manisha



Contd... Cyber Smart Woman

again pays the amount and receives an email confirming that her parcel has reached India. She was very excited about the parcel. But, the next day, Manisha receives another email stating that she would have to pay ₹1.5 lakh to get the parcel as it again got stuck in 'Customs'.

New Email



This time, as the amount

was

Hello Aryan...

considerably high, Manisha grew suspicious and

confronted Aryan. Aryan told

her this is the part of the process and I will give you the money when I come back to India. While Manisha kept on querying things from different perspective, Aryan tried to persuade her but when he realised that Manisha is reluctant in paying the amount then he stopped answering Manisha's calls or replying to her messages.

Hello Tenali...

Manisha then realised that she was cheated and approached me.

What have you done?
Why you transferred the money?

Now immediately report to
Cyber Crime Police Station.

What should Manisha do now?

- ◆ Immediately report the fake profile to Facebook.
- ◆ Block the contact in phone, email & other messaging apps.
- ◆ Keep screenshots of all communications, phone call logs and call recordings, if any.

- ◆ Report to Cyber Crime Police Station & also at National Cyber Crime Reporting Portal.

What actually happened here?

Manisha has been a victim of dating fraud. In these type of scams, fraudsters, after gaining confidence of women met via online sites, plot a story, promise expensive gifts and ask for money to clear exchange procedures between countries.

Sometimes they also ask to transfer money into their bank accounts citing medical emergency. Then, they disappear without a trace as soon the money is transferred.



OTHER VICTIMS

Nov 2019 | A 79-year-old man from Mulund lost ₹1.5cr in a customs parcel clearance scam after befriending woman on European social media app

June 2017 | An executive with Vile Parle firm lost ₹4.5L after befriending 'UK-based med director'



STAY SAFE ONLINE

- Never accept friendship requests from unknown persons on social media
- Do not exchange phone numbers with strangers online nor engage in conversations with them
- Do not indulge in monetary transactions with unverified sources

Safeguard Yourself

- ◆ Perform thorough profile check before responding to any request in social media.
- ◆ Skip dedicated video chats.
- ◆ Periodically review internet contacts and unfriend / block people you don't want to interact with.
- ◆ Do not post too much online. Refrain from geo-tagging yourself while uploading photos. These may be targeted by stalkers / fraudsters to better understand and target you.

International Women's Day

8th MARCH



Image Source: [istockphoto.com](https://www.istockphoto.com)

Empowering Women... Empowering Nation

How to identify fraudsters

- ◆ Reluctant to meet in person
- ◆ Sound inconsistent or confusing when asked for personal details
- ◆ Often enquires about properties and income etc.

Manage Device Permissions

- ◆ **On Android:** Go to Settings > Apps > Advanced > App permissions > Camera > Tap the toggle next to an app to revoke permission. Then go back and do the same under the 'Microphone' menu.
- ◆ **On iPhone:** Go to Settings > Privacy > Camera > Tap the toggle next to an app to revoke permission. Then go back and do the same under the 'Microphone' menu.
- ◆ **On Mac:** Go to the computer's Settings > Security & Privacy >

Privacy > Camera > Uncheck the box next to an app to revoke permission. Then go back and do the same under the 'Microphone' menu.

- ◆ **On Windows:** Go to the computer's Settings > Privacy > Camera > Turn off Camera access altogether, or use the toggles next to individual apps to adjust permissions. Then go back and do the same under the 'Microphone' menu.

Cyber Guru Tenali's Mantra

*Stay Aware
Stay Safe*



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