36. FRAUDS USING MALICIOUS APPLICATION

One day, Raju received a message seeking his willingness to do freelance work. As Raju was unemployed, he immediately dialled the number mentioned in the SMS.

"Hi, I received an SMS regarding freelance work. What is the work profile?"

(This is very easy, even my kid can do it.)
"Okay, I am interested."

After downloading the application, Raju started working. The work seemed genuine; however, he did not know that the fraudster was observing all his activities on his laptop.

Over time, the fraudster was able to get all the secure credentials from Raju's device through his application. Unaware of the malafide intention, Raju continues to use the application. The fraudster was also able to get the OTP sent on Raju's email since the fraudster got access to his email.

Do's:

- ✓ Verify the authenticity of the offer on the official website of the concerned entity offering jobs.
- ✓ Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in."

After a few days, Raju received SMS alerts stating Rs 50,000 was debited from his account Raju had no clue how his account was compromised or money was debited.

After investigation, it was found that his device contained a malicious application, observing all his activities and the passwords were being skimmed.

Don'ts:

✕ Do not download any application through links sent via SMS, email or instant messaging applications, especially from strangers, without verifying its authenticity.