I S LITERACY, LEARNING AND LESSON

February 2020

Screen Sharing application software have been used both by personal and professional users to troubleshoot and fix issues remotely. These applications allow complete access and control to a user's phone.

This has led to a number of fraudulent activities by scammers who use these applications to take full control of the victim's device using a remote location and view the device's activities resulting in financial fraud. The scammer entices the user to install third party screen sharing applications so that they can assist them online or update some documents enabling full access to the user device.

How it works

A. The scammer poses as representatives of companies and pretends to solve issues being faced by the victim.
B. The fraudsters ask the user to download screen sharing apps which can be accessed by the fraudster remotely.
C. Once the target user downloads the screen sharing app, the fraudster gets complete control and access to the user's information from a remote location.
D. The fraudster will then entice the user to type personal details such as card type, bank details, UPI PIN or OTP.
E. The scammer takes this opportunity to record this personal information.
F. They either send an OTP for transferring funds into their own account through an SMS or check the OTP details using the screen sharing app on the user's device.
G. This results in transferring of funds from the user's account to their own account.

Best practices

A. Never respond to calls coming from unverified sources claiming to be from genuine companies.
B. Never call customer support numbers available on search engines. Use phone numbers available on the company website.
C. Never download any unknown/unauthorized application on your device.
D. Never give permission to any third-party application to be installed on your device.
E. Never give your personal, credit card or online account details over the phone unless you have made the call and the phone number came from a trusted source.
F. Report any such call/suspicious activity on the helpline number mentioned at the back of your credit card.

Source - Cert-in