RAJ CYBER LAW

V. Rajendran M.A., M.Com., B.L., CAIIB
Advocate, Cyber Law Consultant

Mobile: **+91 94440 73849** : Email: **rajcyberlaw@gmail.com**
Guha Nivas, 7 First Main Road, Bharat Nagar, Madipakkam, Chennai 600091

SIM SWAP

Mobile data including voice travels through the SIM Card which connects to a network. SIM Swap actually means swapping the SIM ie just creating a cloned sim card or a duplicate sim. This can be done either by deactivating the original sim card (like when you give a complaint to the service provider that your mobile phone is lost). While giving a duplicate sim, the provider has to observe strict security procedures like taking the Aadhaar and other id verification, and any violation is viewed very seriously by the regulatory body as well as by the investigators like police etc. Such violation may result in criminal prosecution too.

Operators' connivance or negligence: Sometimes, the provider, often the branch head or the service desk official may not insist on the Aadhaar verification and give a duplicate. This results in a sim swap. Suddenly, your sim may become inactive (since the duplicate is activated). The provider with criminal intention may temporarily deactivate your sim and issue a duplicate temporarily for a few hours and then deactivate the duplicate after a few hours and by that time your original may become active again. If this is for a few hours say at night, the original user may not even realise that his sim is inactive. During such period of duplicate sim becoming active, the sim swap becomes a useful weapon for criminals. Later, police may question the user, who may be caught innocently.

According to some tech experts, in some cases, the original sim is not deactivated and both the sims will keep receiving signals. Whoever picks up first will have the active call. This technology, I understand is highly 'sophisticated' and very rarely used. To make this happen, since tower communication cannot go to both the sims and hence there must be some software re-direction at the tower communication level too.

Any mobile small-time dealers too has the list of available sim with mobile numbers which are not active for some reasonable time (especially the prepaid ones, which are not promptly re-charged and sometimes re-charged after a gap of a month or two). Such cases would be easy for the criminally intent dealers to activate such numbers temporarily for a few hours or a few days. The branch head or the desk head at the branch even accesses to see what id was

provided by such user when the mobile – sim was procured. Having access to the aadhaar (and date of birth, address etc) is by itself a great tool for him to issue a duplicate sim.

Without connivance of the operator: Even when you give your mobile for a few seconds to a criminal, that few seconds would suffice for him to download a malware into your mobile, which may have one or more of these features, viz accessing your contacts details, accessing your financial transactions and reading the password if saved there, redirecting all your text messages from there to his own mobile (ie including the OTPs), and accessing your WhatsApp messages etc.

In some cases, when there is a message or a WhatsApp which innocuously asks you to click a link, to get more details or asks you to scan an image etc such a simple action may also be dangerous, enabling downloading of a malware to your mobile. Messages like ‘if you are not vaccinated, please click the link or enter 1’ and then click the link etc or ‘do you want to encash your reward points in SBI or ICICI Bank credit cards, please enter 1 and click the link’ etc work in this manner. Just by clicking something like this, may easily enable the malware to enter your mobile.

Safeguards: Never give your mobile to any stranger, even for a few seconds. If you give it, be cautious about what he is doing. If you do not receive any message for a reasonably long time, in an unusual manner, note the developments and report it to the provider immediately. If suddenly, the mobile handset does not connect to the tower or does not identify, immediately bring it to the knowledge of the provider and report abuse. Checkout for any new and unwanted apps in your mobile. Check for all the settings like where the camera is on, speaker is on, location is on etc. There are many free tools available for these.

To know the number of mobile connections ie SIM cards, you have taken with your mobile number, OR to block the SIM or mobile number which you have lost, you can go to the Govt of India website as below and enter the details. It is a very simple step. This Govt of India website gives you details on how many mobiles have been taken in your number or your Aadhaar.

https://tafcop.sancharsaathi.gov.in