# Subscriber Identification Module (SIM) Card Swapping: How to Protect Your-self From Being a Victim?

Mr. Somnath Hadalgekar[#1]

[#]*Dr D Y Patil Institute of Management Studies, Akurdi, Pune*

[1]somnath.hadalgekar@gmail.com

***Abstract*— SIM swap fraud is a relatively new form of cyber fraud that permits hackers to gain access to bank accounts, credit card numbers and other personal data. Now a day's most of the banking services are available on smartphones. Now maximum number of banking customers have mobile phone numbers linked with their accounts, for online transactions it needs One Time Passwords (OTP), unique registration number etc. which is all proved through registered phone numbers of users. SIM fraud attacks are usually targeted at profitable victims that have been specifically aimed through successful social engineering. According to RSA research 65% of all fraud in 2018 is mobile based. This is a popular method among hackers and SIM SWAP fraudsters alone have made citizens lose more than Rs 200 crores. This paper explains what SIM swap fraud is, how does it work and how an individual can be protecting themselves from SIM swap fraud?**

***Keywords*— Subscriber Identification Module, SIM Fraud, SIM Scam, SIM Swapping, phishing, GSM**

## INTRODUCTION:

From India to California, to the UK and Europe, and near to a neighbourhood, the most recent new scam trend involves is called as "SIM-Swap" scam. This type of fraud is not new. It has been started few years back, but the numbers of cases have been less. With the growth and complexity of mobile banking, new security vulnerability has become the smartphone. Fraudsters have moving their attention from desktop-based fraud to mobile attacks, because now most people are used mobile for financial transaction like to check balance, to transfer money, for online purchasing etc. Millions of people universal use online banking to rapidly and suitably do their regular bank-related transactions. By doing their banking online, they are susceptible to falling victim to fraud scams such as SIM swap fraud. The easy meaning of the word swap is exchanging one thing for another.

Suppose you have 2G/3G SIM card and you want to upgrade to 4G. What you do in such case is that you exchange your old SIM to 4G SIM from your mobile service operator. This is what an authenticate SIM swap is.

Subscriber Identification Module (SIM) commonly knew as SIM cards, which store user data in Global System for Mobile (GSM) cell phones. In simple words, your phone's SIM card stores identifying information that authenticates your cell phone service and allows you to connect to mobile networks.

Here we are putting the request to our service provider who deactivates old SIM and gives us a new SIM, which activates within a few hours. Our mobile phones are loaded with information, right from contact lists, photos, emails, and Short Message Services (SMSS) to financial details such as Automated Teller Machine (ATM) withdrawals alerts and one-time passwords (OTPs) sent by banks for net banking transactions.

SIM card's number is an entrance for criminals. With something as simple as a string of digits, hackers can quickly empty your bank account. Do you want to know the scariest part? Cybercriminals don't even need to steal your phone to gain access to your number and personal information. This recent trend in hacking is known as SIM card swapping. Sim swap or Port out service is offered by telecom providers in India. Sim swap offers a simple way to get your stolen sim card number again by blocking the old sim and activating the new sim with the same phone number.

## WHAT SIM CARD SWAPPING SCAM IS?

A Cell phone SIM card stores user data in GSM (Global System for Mobile) phones. A mobile is a suitable tool for personal banking. One can get account related alert, OTP, Unique Registration Number (URN), 3D secure code etc. which required for financial transactions or to make financial inquiries through mobile phones. Swapping is nothing but exchanging two things or objects. Here in SIM swapping a fraudster exchange a SIM of target person with new SIM held by fraudster without knowing by the target. As a result, all calls and text messages to the victim's number are directed to the impostor's phone, including one-time passwords for banking transactions. After getting a one-time pin (OTP) or password from a bank, the impostor can then access the victim's bank account and transfer funds. A SIM swap scam is a type of scam that involves a criminal register existing mobile number of a victim to new SIM card and makes the fraud.

### EXAMPLES OF SIM SWAP FRAUD:

Example 1: Mahim businessman loses Rs 1.86 crore in six late-night missed calls:

The victim received the six missed calls on the mid night of 27-28 December 2018 from two mobile numbers, after which his SIM was deactivated. He was informed by mobile service provider that the SIM was deactivated by himself for new SIM card. But he did not request for deactivation of SIM and become a victim of fraud. He rushed to his bank to find Rs 1.86 crore. He was told that his money was transmitted to 14 accounts across the country through 28 transactions. The bank was able to retrieve only 20 lacs.

*Source: Mumbai Mirror on 02 Jan 2019*

Example 2: Caller posing as Airtel employee clones Pune man's SIM, steals Rs. 93.5 lakh:

The fraudster called to Pune based man saying he is employee of Airtel and asked the share information otherwise his SIM card will stop working. The victim shared details of his SIM card which was linked to bank account. The victim came to know later that Rs 93.5 lacs were transferred from his bank.

*Source: Hindustan Times on 14th November 2018*

Example 3: Telecom Company told to pay Rs 8 lakh to victim of SIM-swap fraud:

The civil court for cybercrimes in Maharashtra on Thursday directed Telecom Company to compensate Rs 8.2 lakhs to bank account holder for issuing a duplicate SIM. The SIM card was used by fraudster to get Rs. 7.8 lakh using internet banking.

*Source: The Times of India on 01 Mar 2019*

Example 4: 27-year-old woman loses Rs 1 lakh to SIM swap fraud:

A 27-YEAR-OLD Powai-based woman lost Rs 1 lakh after she allegedly received a call ostensibly from her mobile service provider asking her to forward a text message to a mobile number. The woman said that she was in a hurry and forwarded the message to fraudster's number. The next day at the bank, the woman was informed that there had been three transactions on her bank account in the past 24 hours. While one transaction worth Rs 20,000 was carried out through a bank in UP, two other transactions totally worth Rs 80,000 were carried out through a bank in West Bengal.

*Source: The Indian Express on June 27, 2018*

HOW DOES SIM SWAP WORKS?

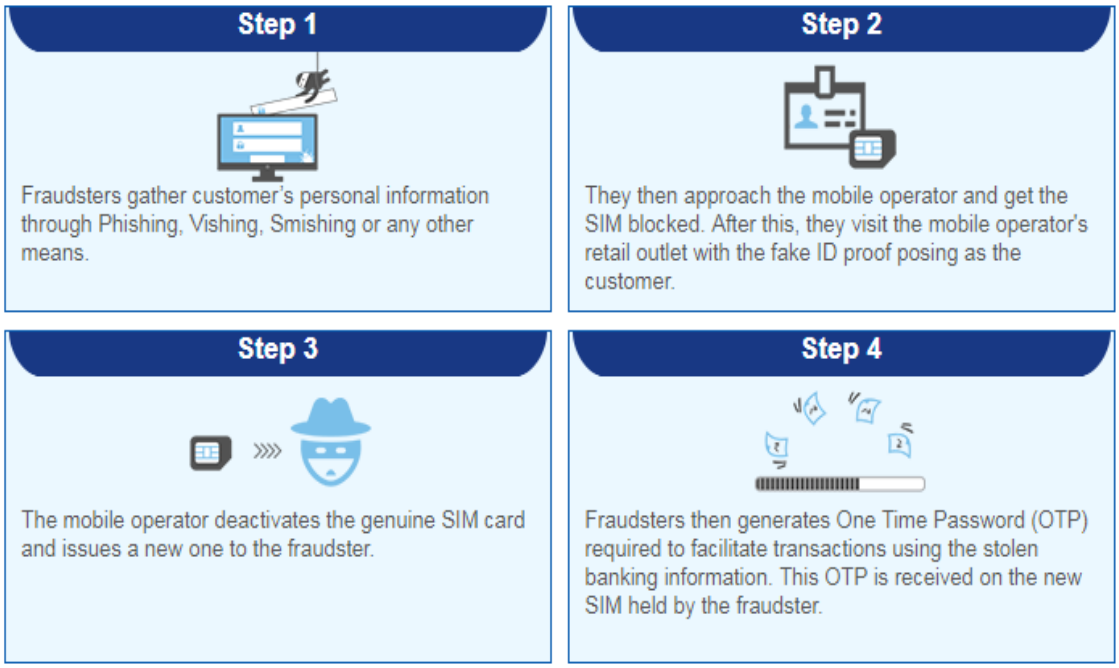


*Figure 1: SIM Swapping Process*

Step 1: There are two stages to this fraud, SIM swap fraud and net banking fraud. SIM swap fraud involves collecting so much information about the victim. Fraudster might send phishing mail or through Trojans/Malware to collect sensitive information from victim. Information of interest to the hacker includes ID numbers, contact details, residential and postal addresses, banking details such as account numbers, credit card numbers, debit card number, CVV number, Expiry date of card, and online banking credentials (username and password) etc. Sometimes they call to target acting as a mobile service provider, customer care unit or bank and asks for private information like CVV/ATM card number or secret PIN etc. And victim provides all sensitive information in hands of fraudster. Alternatively, they might search public websites, social media etc. from criminals who specialize in collecting personal data.

***Few Known illustration of fraud:***

- *Hello, I am calling from XXXXX branch. Your account will be deactivated today due to non-linking with Aadhar card. Please share your Aadhar number and bank details for linkage.*

- *Hi, Sir/Ma'am, you have ab exclusive offer reserved for our top customers only. Please share you debit/credit card details so we can transfer the gift money to your bank account.*

- *Hi, I am calling from XXXX. We are happy to let you know that you have won additional Rs. 10000/- cashback on you latest purchase. Please share your debit/credit card number so that we can credit the money directly on your bank account.*

- *Hello Sir/ma'am, you have owned an exclusive offer reserved for our top customers only, please share your credit/debit card details so we can transfer the gift money to your bank account.*

Step 2: Once criminals have gathered enough information; they create false identity of victim. First, they call to mobile operator and request them to block original SIM with fake reason like loss theft or damage.

Step 3: After this they visit the mobile operator's retail outlet with fake ID proof posing as a genuine owner and gets new SIM with owner's name. Once new SIM is issued, then genuine customer's mobile phone will not receive any phone calls or messages because mobile phone will be without mobile network. This happens within some hours before real owner lodging the complaints against mobile has stopped working.

Step 4: The fraudster initiates financial transactions by generating One Time Password. Since this OTP received on new SIM which held by the fraudster, the money can be transferred into an account of someone else person who is known to fraudster. So, fraudster will not be caught by police and that person will get reward who had kept money in his bank account from fraudster.

## HOW DO THE FRAUDSTERS GET BANK DETAILS?

There are two phases to this scam, SIM swap scam and net banking fraud. In second fraud victim provides bank details to fraudster mistakenly. Initially, hackers send a phishing email to get all your banking details like account number, user id or password etc. Remember, phishing is a type of e-mail fraud method in which the fraudster sends out genuine-looking emails or website links in try to gather your private and financial information. These details can be stolen by using Malware/Trojans also. Simultaneously they generate fake ID of victim. To use all this collected information, they need to use victim's mobile messages. Hence the SIM swap. This attack may be launched in following ways:

***Phishing Email*** – Attacker sends a fake email to the victim containing a form or a link to a spoofed website to capture personal information.

***Vishing (voice phishing)*** – Attacker calls the victim, posing as a bank executive or an official of a reputed company and collects personal information.

***SMiShing (SMS phishing)*** – Attacker sends fake SMSs to the victim containing links to a fake website or a malware that can steal user information.

## HOW TO AVOID BECOMING A TARGET OF A SIM SWAP FRAUD?

- Don't reply to doubtful emails. Your bank would never ask you to enter any private information into an email.
- Don't ever click on web links that may lead you to phishing websites.
- Use private email address that nobody but you and your bank know for net banking purpose.
- Always visit official website of your bank by typing URL in address bar. Don't bookmark website name because malware could tamper with bookmarks and redirect you to phishing website.
- Change net banking password regularly and make sure it should be strong password too.
- Do not share personal sensitive information like Customer ID, Credit/Debit card number, expiry date of card, CVV number to anybody including bank person (on Phone), customer care executive of mobile service provider over call, email or SMS.
- If your phone is out of network continuously for a few hours, it is an alert and you should complain the same to your mobile operator immediately.

- Never switch off your phone in the case of receiving multiple unknown calls continuously. It could be a strategy to get you switches off your phone. Instead you just cut the phone call or keep your phone in silent mode.
- SIM swap happens generally on weekends or on continuous holidays. So that it's very difficult to communicate with mobile service provider or with bank to lodge a complaint. So, in these days if you doubt about sim swap action very fast.
- Check your bank account statement regularly and register email and SMS alter for banking transaction.
- Never share 20-digit SIM number mentioned on back of SIM card to anyone.
- Do not put your mobile number on public display on social media and other websites.
- Suppose someone gives you some amount for transferring money on your account, don't allow him to do so, it could be SIM swap scam.
- Don't ever give your important document copies to anyone without knowing the reason. If you must do so then mention the reason on document and document should not be used to any other purpose.

## SIM SWAP IS LEGAL BUT THEN WHY IS IT A PROBLEM NOW?

Suppose you have 2G/3G SIM card and you want to upgrade to 4G. What you do in such case is that you exchange your old SIM to 4G SIM from your mobile service operator. This is what an authenticate or legal SIM swap is. You had used the same SIM Swap technology to register your new SIM card with the present phone number suddenly from the ease of your house. Also, the time when you transferred from old-style SIM cards to the new Nano SIM cards you had also used the SIM swap technology.

SIM swap is totally illegal when instead of you someone, who creates false identity of yours, exchanges old SIM with new one very smoothly with old mobile number. The swapping process simply registers your phone number with the new SIM card that is in the hands of the fraudster. The fraudster will use new SIM card (swapped) to transfer the money to his account.

## WHAT SHOULD YOU DO IN CASE OF SIM SWAP SCAM?

- ✓ First, call your bank and block your debit and credit card transactions in case you have identified a fraud transaction.
- ✓ Second, call your operator, and file a proper complaint. You are required to visit them with original ID proof and address proof to complain about your case.
- ✓ If you see no service on your SIM, contact the mobile service operator at the earliest. If your SIM has been deactivating at midnight, you can't do much about it really.
- ✓ If your phone is out of coverage network constantly for a few hours, then you must take it seriously and be alert and complain the same to a mobile operator.
- ✓ Never switch off your mobile for long period of time to avoid unsolicited calls. Instead, try not to pick them. Otherwise, activate DND (Do Not Disturb) service for your SIM.
- ✓ It is a good idea to safeguard your account, mobile number through various ways. What is more important is awareness of where and how you share your personal information.

## CONCLUSION:

SIM swap is comparatively new, sophisticated method of scam that permits hackers to gain access to bank accounts, credit card numbers, and/or other personal data. It's tough to find, and even harder to undo the resulting damage. So, protect your accounts. Do not load critical access data on your smartphones, but, if you do, maintain a constant care on account balances and transactions. SIM Swapping is actual and will not be going away quickly. Sadly, senior citizens or who are less digitally literate are the main targets of these types of frauds. It is important to guide them regularly and inform them to strictly not entertain unknown callers. It is always advisable to stay alert, and don't let your SIM card or mobile phone fall under wrong hands.

## REFERENCES:

[1] Frauds in Indian Banking: Aspects, Reasons, Trend-Analysis and Suggestive Measures by Dr. Sukhamaya Swain published in International Journal of Business and Management Invention in July 2016 Vol 5 Issue 7
[2] Literature review on Cyber Crimes and it's Prevention Mechanisms by Annamalai Lakshmanan
[3] A Biometrics-based Solution to Combat SIM Swap Fraud by Louis Jordaan
[4] Advisory report of Odisha Police published in June 2018.
[5] https://mumbaimirror.indiatimes.com/mumbai/cover-story/mahim-bizman-loses-rs-1-86-crore-in-six-late-night-missed-calls/articleshow/67342458.cms
[6] https://timesofindia.indiatimes.com/city/mumbai/telecom-company-told-to-pay-rs-8-lakh-to-victim-of-sim-swap-fraud/articleshow/68210489.cms
[7] https://indianexpress.com/article/cities/mumbai/mumbai-27-year-old-woman-loses-rs-1-lakh-to-sim-swap-fraud-5234866/
[8] https://www.forexfraud.com
[9] https://securelist.com
[10] https://www.expresscomputer.in/news/how-to-protect-yourself-from-sim-swap-fraud/31326/
[11] https://www.hdfcbank.com/security/beware_of_frauds/sim_swap_fraud