‘Sim Swap Scam’
How Can You Protect Yourself

Why In News

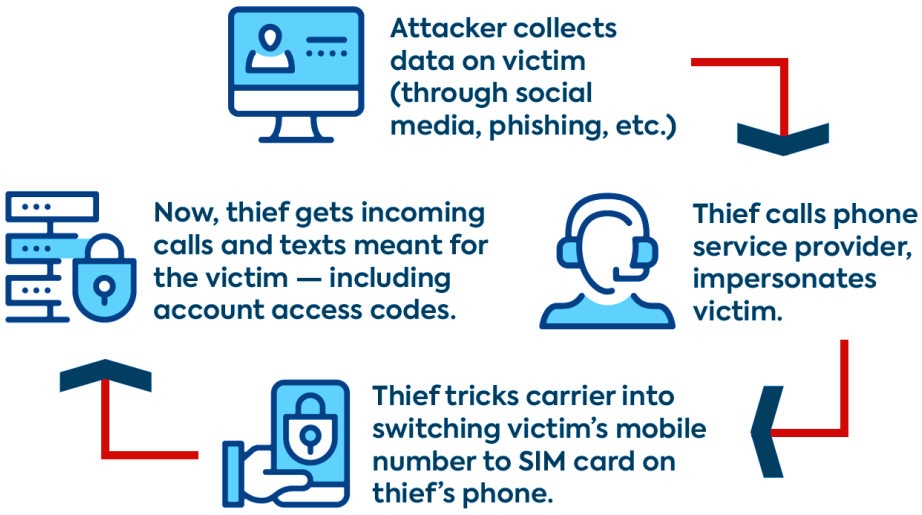
- Earlier this month, a **North Delhi-based advocate** became the latest victim of the ‘SIM swap scam’ in the national capital after she received three missed calls from unknown numbers and lost money from her bank account.

What is the SIM swap scam?

- With the **advancement in banking services**, easy payment applications and seamless transactions on smartphones, cybercriminals are misusing the link between physical SIM cards and banking applications.
- All banking applications are linked to phone numbers which help in generating OTPs (to authenticate transactions) or receiving important bank-related messages.

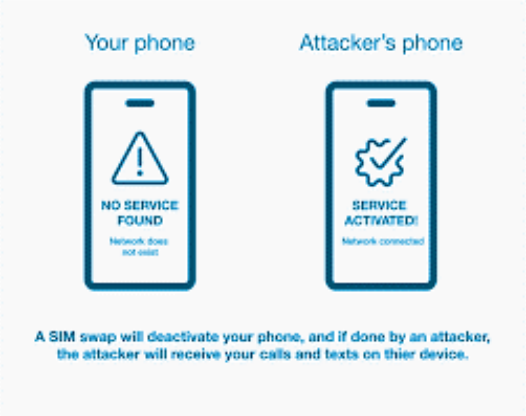
- **In the SIM swap scam**, fraudsters first take personal details such as phone numbers, bank account details, and addresses with the help of phishing or vishing.
- **Phishing is a technique** in which scamsters send malware links to victims through mail or messages. Once the link is opened, the malware steals all of the victim's personal information.

- After receiving the personal information, **fraudsters visit the mobile operator's retail outlet**, posing as the victim with a forged ID proof and report a fake theft of the victim's SIM card and/or mobile phone.
- By doing this, they attain a duplicate SIM. Notably, scamsters can get a duplicate SIM even when the original is working as they reported a theft of the original SIM card. All the activation messages and details go to the scamster and not the victim.



Why Do Victims Receive Multiple Missed Calls?

- SIM swap scam doesn't require direct communication with the victims.
- However, fraudsters do give missed calls to their victims so that the **latter leave their phones** and ignore the lost network connectivity.
- "Since SIM activation takes time, the accused give calls to the (victim's) mobile number to check where the call goes. Hence, the missed calls are received.



How Can You Protect Yourself From SIM Swap Fraud

- **Be vigilant** of vishing or phishing attacks.
- **Not neglect messages** or switch off their phones after receiving multiple missed calls. They should enquire with the mobile operator immediately if such an activity takes place on the phone.
- One should **change bank account passwords** regularly.
- They should register for regular SMS as well as e-mail alerts for their banking transactions.
- In case of fraud, one must **immediately get in touch with bank authorities** to have their account blocked and avoid further fraud.