Topic: SIM Swap Fraud – Your Mobile, Their Control

Why It Matters:

Cybercriminals can take control of your phone number by tricking your mobile provider into issuing a new SIM card. Once they have your number, they can intercept OTPs and gain access to your bank, email, and social media.

Real-Life Example:

A victim lost access to all their accounts after receiving "No Service" on their phone. A fraudster had convinced the telecom provider to port the number and used it to reset bank passwords and steal money.

Tips to Stay Safe:

Set a strong PIN or password with your mobile service provider for SIM changes.

Be alert if your phone suddenly loses signal or shows “No Service” for a long time.

Don’t share personal details like date of birth, address, or ID over unknown calls or SMS.

Report Fraud Immediately:

Visit: https://cybercrime.gov.in

Helpline: 1930

BY DETECTIVE GURU

Stay Smart. Stay Safe.