Retiring the phone-based OTPs

Why in news?

There is need to replace ageing OTP model with alternative options.

What is the problem with the current OTP model?

- Customers with good cell receptions are requesting for OTP resend & it doesn't function in dead zones.
- SMS-based OTPs are not secure & can be decrypted i.e. they are susceptible to call forwarding attacks or SIM jacking.
- SIM jacking means gaining access to phone accounts by sending malware to followers.
- If 0.1 % of OTP request fail, it will lead to lakhs of incomplete banking transactions.

What are the alternative options to OTP?

- OTP's can be sent to the customer's registered email address, as a password-protected PDF file as State Bank of India does.
- ATM machines can be repurposed to become OTP generators. Customer can request an ATM screen to print a backup set of five OTPs (expire in 30 days) which could be used when OTPs don't arrive promptly.
- WhatsApp messages can be another viable option as it does not require SIM card, can work with WiFi & message delivery is more reliable.
- Moreover WhatsApp messages cannot be snooped as they are secured with 128-bit encryption, 100% add free unlike like Google, Facebook, Twitter, or YouTube & every Indian mobile phone has WhatsApp installed.
- Another option can be employing an authenticator app- from Google or Microsoft- which generates a new 6-8 digit code each minute in customer's phone. Once activated, it does not require a network connection to generate the OTP.
- Indian banks have tried their own authenticators but have rejected them because of technical glitches.
- Hence, banks should add backups to the ageing OTP/SMS platform, and over time, transit to a more secure, internet-based, or app-based mechanism to deliver the second-factor authentication code.

Source: The Hindu

