Safety Guide: Banking Scams

Phone & SMS Safety

1. Never share OTPs, PINs, or passwords over the phone or SMS.
2. Avoid clicking links in SMS messages.
3. Do not trust unknown callers pretending to be from your bank.
4. Even if you think you recognize the voice, it's best to call them back.
5. Banks will NEVER ask for your password, PIN or OTP over the phone.

Email Safety

6. Ignore emails that ask for bank details.
7. Ignore emails that say "we detected an unauthorized login" or "you need to change your password".
8. Never assume that an "official-looking" email is actually from your bank.
9. Always type the official website directly instead of clicking links in emails.

Password and PIN Hygiene

10. Keep important login details in a safe off-line notebook.
11. NEVER carry this notebook with you – keep it in a safe location at home.
12. Do not use birthdays or repeated digits as your PIN
13. Ideally, change your banking passwords once a year (optional)

ATM & Debit Card Usage

14. Cover the keypad while entering your PIN.
15. Do not accept help from (or offer help to) strangers at ATMs.
16. Block lost/stolen cards immediately.
17. Keep a limited amount of cash in your savings bank accounts
18. Try to use ATMs that are inside bank branches – not roadside or standalone
19. When paying at a restaurant, ideally don't let your card out of your sight.

UPI & Cashless Payments (Google Pay)

1. Scan QR codes only from trusted shops/people.
2. Always check the vendor name after scanning the QR code.
3. Do not approve unknown requests on UPI apps.
4. Never enter your PIN to receive money.

The Golden Rule

- When in doubt, do not act. Call your bank or family first.

Safety Guide: Other Scams and Dangers

Family-Member-in-Distress Scams

- Scammers pretend a relative is in trouble (accident, jail, hospital).
- Stay calm, verify by calling the actual family member directly.
- Set up a code word with your family in advance.

Fake Police or Officials

- Fraudsters threaten with arrest or fines.
- Real officials never demand money on the spot.
- Ask for ID and written notice; call the local police station.

Charity & Donation Frauds

- Donate only to registered charities.
- Avoid giving cash at the door without receipts.

Home Visit & Service Scams

- Do not let unknown service workers inside without ID.
- Verify with the company's helpline before allowing entry.
- Don't pay in full in advance for services.
- For medium or large projects, always work through referrals / introductions.

Lottery & Delivery Frauds

- Ignore claims of lottery wins requiring upfront fees.
- No legitimate prize requires advance payment.
- Ignore messages saying that your delivery needs an extra payment

WhatsApp/Phone Impersonation

- Scammers may use fake accounts with family photos.
- These days, even voices can be faked.
- Always call back / use the family code phrase if applicable.

Golden Rules

- Pause, verify, and consult before acting.
- Never act in fear or hurry.
- Don't make decisions while stressed or under time pressure.
- If it's important, they will call back.
- Don't be afraid of a little embarrassment
- You can always stop and say no to anything.