Dos and Don'ts for Safe Digital Banking

DOs

1. **Use strong, unique passwords** — Use a combination of uppercase, lowercase, numerals, and special characters for your Internet/Mobile Banking login. Change passwords regularly.
2. **Enable Multi-Factor Authentication (MFA)** — Always activate two-factor/OTP-based authentication for all transactions.
3. **Access only official bank websites** — Verify the URL begins with `https://` and ends with `bank.in` (RBI-mandated domain from October 2025).
4. **Register for transaction alerts** — Subscribe to SMS and email alerts for all debits, credits, and account changes.
5. **Log out after every session** — Always click "Log Out" after completing banking transactions; never just close the browser window.
6. **Keep your devices updated** — Regularly update mobile banking apps, operating systems, and antivirus software.
7. **Use secure, private networks** — Conduct banking only over trusted, private Wi-Fi connections.
8. **Report unauthorised transactions immediately** — Report to the bank within 3 working days to limit liability under RBI's framework on Unauthorised Electronic Banking Transactions (UEBT).
9. **Set transaction limits** — Activate daily transaction limits and enable/disable international transactions on your cards as required.
10. **Report fraud at 1930** — In case of financial fraud, immediately call the national cybercrime helpline **1930** or visit **cybercrime.gov.in**.

DON'Ts

1. **Never share credentials** — Do not share your Account Number, Login ID, Password, PIN, UPI-PIN, OTP, or card details with anyone — including persons claiming to be bank officials.
2. **Do not click unverified links** — Never click links in SMSes or emails claiming to be from your bank. Check for spelling errors in URLs.
3. **Do not use public/shared computers** — Avoid logging into your bank account from cybercafés, shared computers, or public Wi-Fi hotspots like airports or railway stations.

4. **Do not respond to KYC update requests via SMS/email —** Any message threatening account blocking for KYC non-updation and directing you to click a link is a fraud.
5. **Do not download unknown apps —** Never download unofficial or unverified applications on your device; use only the bank's official app from Google Play or the App Store.
6. **Do not allow remote access —** Never grant remote access to your device to any person, even if they claim to be bank/tech support.
7. **Do not save passwords on the device —** Never store your banking password in your phone's notes, browser autofill, or messaging apps.
8. **Do not fall for RBI-impersonation scams —** RBI never deposits money on behalf of customers or collects fees for foreign remittances or lottery winnings.
9. **Do not ignore unauthorised OTPs —** If you receive an OTP for a transaction you did not initiate, immediately inform your bank and block all debit channels.
10. **Do not become a Money Mule —** Do not allow your account to be used by others for routing transactions in exchange for money or commissions.