🏦 Banking Safety Guide

Complete Guide to Secure Banking & Fraud Prevention

🔐 Your Bank Will Never Ask for OTP, PIN, or Passwords Over Phone/Email

Legitimate banks only verify identity through secure channels and never demand immediate money transfers

🔒 Safe Banking Practices

✅ Online Banking Security

✓ Always type bank URL directly in browser

✓ Look for 'https://' and padlock icon

✓ Use strong, unique passwords

✓ Enable two-factor authentication

✓ Log out completely after use

✓ Never save passwords on public computers

✅ ATM & Card Safety

- ✓ Cover keypad while entering PIN
- ✓ Check for suspicious devices on ATM
- ✓ Collect transaction receipts
- ✓ Report lost/stolen cards immediately
- ✓ Use ATMs in well-lit, secure locations
- ✓ Monitor your account regularly

✅ Mobile Banking Tips

- ✓ Download apps only from official stores
- ✓ Keep banking apps updated
- ✓ Use app lock and biometric authentication
- ✓ Avoid banking on public WiFi
- ✓ Set transaction limits
- ✓ Enable SMS/email alerts

✅ UPI & Digital Payments

- ✓ Verify recipient details before paying
- ✓ Use UPI PIN, never share it
- ✓ Check transaction limits

- ✓ Review payments before confirming
- ✓ Keep UPI apps updated
- ✓ Report unauthorized transactions immediately

🚩 Red Flags - Signs of Banking Fraud

⚠️ Phone Call Red Flags

- 🚩 Caller asks for OTP, PIN, or passwords
- 🚩 Claims your account will be blocked
- 🚩 Demands immediate money transfer
- 🚩 Creates urgency about "suspicious activity"
- 🚩 Asks you to download remote access apps
- 🚩 Threatens legal action or arrest

⚠️ Email/SMS Red Flags

- 🚩 Generic greetings like "Dear Customer"
- 🚩 Spelling and grammar mistakes
- 🚩 Urgent requests to "verify account"
- 🚩 Links that don't match bank's official website

- 🚩 Requests for personal information
- 🚩 Offers that seem too good to be true

⚠️ Website/App Red Flags

- 🚩 URL doesn't match official bank website
- 🚩 No security certificate (no https://)
- 🚩 Poor design or broken links
- 🚩 Asks for excessive personal information
- 🚩 Pop-ups asking for sensitive data
- 🚩 Unsolicited software download prompts

🛡️ Steps to Secure Your Bank Accounts

🛡️ Account Security Checklist

1 **Enable SMS/Email Alerts:** Get notified for all transactions, logins, and account changes instantly.

2 **Set Transaction Limits:** Configure daily/monthly limits for online transfers, ATM withdrawals, and card payments.

3. **Use Strong Authentication:** Enable two-factor authentication, biometric login, and secure PINs.
4. **Regular Account Monitoring:** Check statements monthly and report discrepancies immediately.
5. **Update Contact Information:** Keep phone number and email address current with your bank.
6. **Secure Your Devices:** Use antivirus software, keep devices updated, and avoid public computers for banking.

🚨 If Your Account is Compromised

⚡ **ACT IMMEDIATELY - Time is Critical in Fraud Cases**

🚨 Emergency Response Steps

1. **Call Your Bank Immediately:** Use the customer care number on your card/statement. Block your cards and accounts.
2. **Report to Cybercrime:** Call 1930 or file complaint on cybercrime.gov.in with transaction details.
3. **File Police Complaint:** Visit nearest police station with all transaction records

and communications.

4. **Contact Bank's Fraud Team:** Escalate to specialized fraud investigation team through branch manager.

5. **Document Everything:** Save all messages, emails, call logs, and transaction screenshots as evidence.

6. **Change All Passwords:** Update passwords for all banking apps, email, and related accounts immediately.

7. **Monitor Credit Reports:** Check for unauthorized accounts or credit applications in your name.

💡 **Important:** Banks typically have a zero-liability policy for fraudulent transactions if reported within 3 days. Report immediately!

✅ Banking Do's and Don'ts

✅ DO's

- ✓ Verify caller identity independently
- ✓ Use official bank phone numbers
- ✓ Keep transaction records safe
- ✓ Update security settings regularly
- ✓ Report suspicious activities immediately

✓ Use secure networks for banking

✓ Read all transaction confirmations

✓ Keep software and apps updated

✓ Use different passwords for different accounts

✓ Check account statements monthly

❌ DON'Ts

✗ Never share OTP, PIN, or passwords

✗ Don't click links in suspicious emails

✗ Don't download apps from unknown sources

✗ Don't use public WiFi for banking

✗ Don't ignore security alerts

✗ Don't write down PINs or passwords

✗ Don't trust caller ID completely

✗ Don't rush financial decisions

✗ Don't ignore transaction notifications

✗ Don't assume emails from banks are genuine

☎ Emergency Banking Fraud Numbers: 155260 | Cybercrime: 1930 | Police: 100