Security Awareness Tips

DO's	Don'ts
Online Banking Transactions @ Public Terminals	
1. Always reboot when starting to use the public PCs 2. Use Private/Incognito Mode to access email or any sensitive information. 3. Clean up cache files after use	1. Don't leave without closing all browsers and logging out from the public PCs 2. Avoid checking 'Keep me logged in' or 'Remember me' options on websites, especially on public computers. 3. Don't let others watch over your shoulder while logging in or doing online transactions
Unified Payment Interface(UPI) System	
1. Beware of Mobile phishing: always download legitimate UPI applications from bank's official website, and be cautious before you download it from App store. 2. Keep strong passwords for your phone as well as for your UPI application. 3. Use biometric authentication if possible. 4. Update your mobile OS and applications as often as possible to be secure from vulnerabilities. 5. It is advisable for users to enable encryption, remote wipe abilities and antivirus software on the phone. 6. Keep your SIM card locked with a Pin to avoid misuse, in case of loss or theft of the mobile device; you can contact your subscriber to block the subscription of the SIM card.	1. Do not share MPIN with anybody (not even with bank), and be suspicious of unknown callers claiming to be from your bank. 2. Avoid connecting phones to unsecured wireless networks that do not need passwords to access.

Security Awareness Tips

Mobile Banking	
1. Use Trusted Mobile Apps 2. Always download Mobile Apps from trusted source only such IPhone - AppStore, Android – Play store etc. 3. Check the Bank's website for the details of the ways to receive App download URL. 4. Enable strong Passwords on Devices 5. Bank account number/Customer ID or MPIN should not be stored on the user's mobile phone 6. Report loss of mobile phone to the bank to disable the user's MPIN & access to the bank's account through Mobile Banking app. 7. Download and use antimalware protection for the mobile phone or tablet device. 8. Use security software: Applications for detecting and removing threats	1. Don't use untrusted software with suspicious review and poor rating 2. Don't use outdated Mobile Banking Apps 3. Don't use Jail Broken or Rooted Device

Security Awareness Tips

USB	
1. Use USB, only after proper antivirus scanning. As it may contain viruses. 2. Use Write protection, Keep USB in read only mode, if write permission not required. 3. In case you need to charge your Smartphone via USB port on a computer, make sure it is in charge only mode. 4. Protecting individual files: Enable write protection on certain files and folders that are not supposed to be modified or overwritten.	1. Avoid sharing data through USB 2. Don't Store data in un-encrypted format as if lost, it can be misused 3. Don't keep USB without password protection.
USSD (Unstructured Supplementary Service Data) Banking	
1. Keep strong passwords for your phone as well as for your mobile banking app. 2. Update/change your MPIN or passwords on a regular basis. 3. Generate OTP for every transaction as it gives another factor of authentication. 4. Use biometric authentication if possible. 5. Users to enable encryption, remote wipe abilities and antivirus software on the phone. 6. In case if your phone is stolen or lost, Please inform your bank at the earliest to deactivate Mobile banking services. 7. Keep your SIM card locked with a PIN to avoid misuse. In case of loss or theft of the mobile device, contact your subscriber to block the subscription of the SIM card.	1. Don't share MPIN with anybody (not even with bank), and be suspicious of unknown callers claiming to be from your bank. 2. Don't use outdated mobile OS and applications as it may contain vulnerabilities.