SECURITY TIPS FOR INTERNET BANKING CUSTOMERS

HFC
Dreams Made Possible

1. Access & Login Safety

- Always access the bank's site by typing the URL directly into your browser or accessing the link availed directly from the bank's official website — avoid clicking links in emails or SMS.
- Check for HTTPS and the bank's official domain before logging in.
- Confirm the date of last login once you have logged in. The date is available on the landing page. If date and time for the last login is different from your ACTUAL last login, report this immediately to the bank.
- Never share your username, password, PIN, or OTP with anyone, not even bank staff.
- Enable multi-factor authentication (MFA) wherever available.
- Avoid logging in on public Wi-Fi or shared computers.

2. Password & Credential Hygiene

- Use a strong, unique password (long + mix of letters, numbers, symbols).
- Do not reuse your banking password on other sites.
- Change your password periodically.
- Use a reputable password manager if needed.

3. Device Security

- Keep your PC, tablet, or phone updated with the latest security patches.
- Install and update a reputable antivirus/anti-malware program.
- Avoid jailbreaking/rooting your device — it weakens built-in security.
- Enable screen lock and set your device to auto-lock when idle.

4. Transaction Safety

- Review your account and transaction history frequently.
- Set up transaction alerts (SMS/email/app notifications).
- Be cautious when making payments — double-check recipient account details.
- If something looks suspicious, pause the transaction and verify.

5. Phishing & Social Engineering Awareness

- Be alert to emails, calls, or texts claiming to be from the bank asking for login details.
- Watch out for urgent messages like "Your account will be blocked unless you…".
- Do not download attachments or click links from unknown sources.
- If in doubt, contact the bank directly using official channels.

6. App Security (Mobile Banking)

- Download the official banking app only from Google Play Store or Apple App Store.
- Keep the app updated.
- Disable app installations from unknown sources.
- Log out after completing your session (if the app does not auto-log out).

7. Emergency Response

- Immediately report to the bank if:
  - o You suspect your credentials are compromised.
  - o You lose your phone/tablet used for banking.
  - o You notice unauthorized transactions.
- The bank can block your account/cards and reissue credentials.