

General Security Tips

- Do not jailbreak your device as this can leave it open to infection from a virus or Trojan. We recommend you also install security software, if available.
- DO NOT disclose your personal or any other information relating to your accounts through unknown telephone calls or any other communication channels. Even if the caller claims that she/he is calling—say from Dhofar Islamic, contact us at **24775777** if you receive such calls.
- Do not open or follow links in SMS/MMS or email from misleading URL, suspicious or untrusted sources.
- Do not install illegal or unauthorized software on the mobile device.
- Do not allow wireless connections from unknown or untrusted sources on your device.
- Don't reveal too much personal information that can be used to cause harm. For e.g. sharing date of birth should be avoided. If you still want to share, just mention the date/month and not the year.
- Do not download or accept programs and content from unknown or untrusted sources.
- PINs should not be shared with anyone and always kept confidential.
- Lock your phone when not in use. This protects your device so that nobody else can use it or view information. Also be sure to store your device in a safe location.
- Clear your mobile frequently by deleting text messages from financial institutions, especially before sharing, discarding, or selling your device.
- Watch what you send - never disclose via text message any personal information (account numbers, passwords, or personal info that could be used in ID theft).
- Stick with a secure network by ensuring wherever possible that all internet connections are password protected.
- Use trusted apps - always download mobile apps from reputable sources. Publisher or seller. If you have suspicions about the authenticity of a mobile banking app, please contact call center on **24775777**.
- Stay alert on security vulnerability on mobile devices and apply the latest patches and fixes when available.
- Be cautious when connecting to publicly available Wi-Fi hotspots and avoid accessing sensitive data unless with adequate security protection.