



## mobile banking security tips

**At Reliant, we take safeguarding your personal and financial information seriously. The following mobile security tips and precautions will help protect your account and keep sensitive information private.**

- When not in use, keep your mobile device locked with a password.
- Turn off your mobile browser's "remember password" function.
- Do not store login information on your mobile device.
- Do not store private information on your phone.
- Always pay attention to your mobile Security Image and Passphrase (where applicable).
- Never send sensitive account information via text message or unsecure email.
- Take advantage of all security options available on your device.
- Install anti-virus software and a locate/kill/wipe application on your mobile device.
- Frequently delete browser history and text messages.
- Do not open messages from an unknown sender.
- Never click directly on links in emails unless you are sure of the destination.
- Take extra precautions when downloading applications to your mobile device.

### SMS Text Banking

SMS Text Banking messages are NOT encrypted and there is no application time out. If you lose your mobile device, log into your account from another computer to deactivate the service so others cannot view message content or prevent unauthorized access to your mobile banking application. Please contact us with any questions or concerns.

**If you ever feel that your personal information has been compromised, please contact Reliant immediately at 800-724-9282.**