Protect your Online Banking experience on your mobile phone and tablet

There are a variety of best-practices you can do to keep your Online Banking access and information safe when using your mobile phone and tablet, including:

- When downloading mobile apps, only download the KS Mobile Banking app directly from Google Play for Android™, and the App Store for iPhone® and iPad®, and not from any 3rd parties who may try to post download links
- Protect your Online Banking password and do not reveal it to anyone
- Memorize your password - never store it on your mobile device or write it on paper that you keep near your mobile phone or tablet
- Do not choose passwords that incorporate your name, telephone number, address or birthday or those of any close friend or relative
- Never leave your mobile phone or tablet unattended
- Use your mobile phone and tablet's built-in lock function - set up password protection for startup or time-out
- Disable features like WiFi, Bluetooth, and Near Field Communications (NFC) when not in use
- Routinely clear your text message history if you use Text Banking and delete Online Banking email alerts from your mobile phone's email inbox after you have read them

If your mobile phone or tablet is lost or stolen, it is unlikely that someone could access your account information unless they also know your Online Banking Login ID and Password. No personal information from your Online Banking account is ever stored on the mobile phone or tablet. Your password is never stored. However, to be safe you should contact KS Bank as soon as possible by calling 1.800.592.6994. You should also contact your mobile carrier to suspend or deactivate your mobile phone's network connectivity. Your carrier may also be able to perform a remote reset, which will reset your mobile phone to factory settings and remove more information from your mobile phone.

Most mobile phones and tablets include easy access to email, app stores, and other Internet services such as Netflix, eReader stores, etc. These usually rely on passwords being stored on the device. Since this would allow an unauthorized user of your mobile phone and tablet ready access to these services, as soon as possible, logon to those services from another device and change your password to prevent charges to your credit or bank cards.