

# Protect Your Mobile Device

## Protecting Your Phone

### Android

- On an Android, create a password that is easy for you to remember, but difficult for others to guess.
- Set the “Lock Phone After” feature (Note: feature names may differ depending on your device) to require a password after a set period of time. We recommend no longer than 5 minutes.
- Turn off the “Visible Passwords” feature to keep your password from displaying on the screen so others can’t easily learn your password.
- Turn off “Use Secure Credentials” which automatically allows applications to access secure certificates and credentials.
- Turn off “Wi-Fi” when you are not connecting to a wireless network to ensure you don’t inadvertently connect to a wireless network.
- Only download applications from trusted app stores such as the Android Market or the Amazon App Store. There are other app stores selling Android apps; take the time to research them prior to downloading.
- Delete any messages with sensitive information.
- Set a separate password for every application you access that contains sensitive data or information.
- Google provides updates to the Android operating system which may contain security patches. Check with your service provider or the manual that came with your device for information on how to get the most recent updates. For many devices, the updates are automatically provided.
- For more information about how to protect your Android, visit the [Android security page](#).



**PROTECT PRIVACY**