



Mobile Banking Security

Protecting your interests is our job. With our security measures, you can rest assured that our mobile banking services employ industry best practices to protect your information and privacy. Oak Bank's mobile banking services have been assessed by a number of independent system security experts and meet industry security criteria. At a high level, our mobile banking services offer the following security safeguards:

Authentication – Mobile browser and application solution customers are authenticated by username and password for every interaction with any mobile banking component. For single sign-on authentication, we utilize existing login credentials.

Encryption – 128-bit encryption is used for all transactions within mobile banking and between mobile banking and other Oak Bank systems (e.g., core banking and payment systems).

Fraud Prevention – Our mobile banking services incorporate mechanisms such as transaction validation and transaction reconciliation processes to detect fraud.

We know how easy it is to lose or misplace a phone. In the unfortunate case that it happens, your account and information is still protected. No one can access your account without knowing your password and, in some cases, your unique username. By storing your bank information on our secure servers, we ensure that no information resides on your phone hardware or software.

If your phone is lost or stolen, you can take extra precautions to protect your information. Simply log into iBank and click on "Manage Profile," then locate the "Mobile Banking Profile" section and click on "Manage Devices." On the "My Phones" tab, locate the appropriate phone number, select "Stop using this phone for Mobile Banking" and then "Go." Click "Yes" to confirm.