
Foothills Bank & Trust: Mobile Banking Security Tips

- Notify your bank immediately if you receive an alert about activity that you did not initiate. It is possible that access to your account has been compromised and an immediate response may be necessary.
- If you are unable to access our site, please notify us immediately because this may be an indication that either your account or the Bank's site are subject to criminal activity.
- Lock your phone with a PIN to prevent unsophisticated takeover of your bank account.
- Do not download software or apps from unofficial or unfamiliar sources which can result in downloading viruses or malware. The best place to download an app is from the official Web site of the institution or company that you are doing business with or from a legitimate app store.
- Do not allow a vendor or anyone to "jail break" your phone. (It can eliminate or diminish inherent phone security features)
- Update applications and device software as soon as the security updates are available to reduce your phone's security vulnerabilities.
- Eliminate or uninstall applications that you do not use.
- Be careful who you allow to use your phone.
- Be careful in disposal of your phone to insure that information about you, your contacts or your banking access is not on the phone.
- Be careful about where and how you conduct transactions. Don't use an unsecured Wi-Fi network, such as those found at coffee shops, because fraud artists might be able to access the information you are transmitting or viewing. Also, don't send account numbers or other sensitive information through regular e-mails or text messages because those are not necessarily secure.
- Be aware of what your phone can access and what would be at risk if your phone was lost or stolen.