Quarterly Newsletter

INVESTAR Brilliant Banking

Securing Your Mobile Devices

The information provided in this message is simply intended to help increase security awareness.

Securing Your Devices
The number one thing you should do to protect your device is enable automatic screen locking when the device is idle. This means when you are ready to use your device, you have to unlock the screen with a strong passcode, your face or fingerprint. This helps ensure that it is more difficult for anyone else to access your information if your device is lost or stolen.

More tips on how to help protect your devices:

1. **Updating**: Enable automatic updating on your devices, so they are always running the latest version of the operating system and apps. Attackers are always looking for new weaknesses in software, and vendors are constantly releasing updates and patches to fix them. Keeping your devices up-to-date makes them much harder to hack. When choosing a new Android device, look at the vendor's commitment to keeping the device updated. Apple iOS devices are updated by the company itself, while Android mobile devices are updated by the vendor that sold you the device, and not all vendors actively update their devices. If you are using an old device that is no longer supported or cannot be updated, consider purchasing a new device that is fully supported.
2. **Tracking**: Install or enable trusted software to remotely track your mobile device over the Internet. This way, you can connect to it over the Internet and find its location. If your device is lost or stolen, you can remotely wipe all of your information in a worst-case situation.
3. **Trusted Mobile Apps**: Only install apps you need and stick to trusted sources. For Apple devices, use Apple's App Store and for Android devices, use Google Play. While apps can be downloaded from other sites they are more likely to be infected and could compromise your privacy. Also, check to make sure the app has lots of positive reviews and is actively updated by the vendor before downloading it. It is best to stay away from brand new apps, apps with few reviews, or apps which are rarely updated.
4. **Privacy Options**: Mobile devices collect extensive information about you, especially since you take them everywhere you go. Thoroughly review your device's privacy settings, including location tracking, and make sure sensitive notifications (such as verification codes) don't appear on-screen when the device is locked.
5. **Work**: Be sure any mobile device you use for work is authorized for work use. When at work, be extra careful and never take any pictures or video that may accidentally include sensitive information.

For any questions, please contact our Online Banking team toll-free at 855.306.8574. Thanks for banking brilliant with Investar!