Mobile Device Security

Mobile devices such as tablets and cell phones are frequently used for financial transactions and other important tasks.

Tips

A few key tips can significantly enhance your data security.

1. Review permissions BEFORE installing new mobile apps. Be cautious of apps that request access to your GPS location, contact list, cloud file storage, or other potentially sensitive actions. While some apps like digital maps may require GPS access, there's little reason why a simple game would need such access.

2. Only install apps from reputable sources, such as the Apple App Store store and Google Play Store. While the occasional malicious app may appear in these stores, both Apple and Google review each app before publication to reduce the risk of downloading malicious apps to your phone.

3. AVOID "jailbreaking" or "rooting" your phone, as these actions significantly increase the risk of malicious activity on your device in the long run.

4. Set a PIN and enable security features on your device. Typing in a PIN each time you access your phone might be a minor inconvenience but consider the wealth of information tied to your phone, including online banking, email, contact lists, and more. A simple PIN can safeguard your finances and personal information from potential threats.

STAR is committed to your financial security and privacy. For more tips and information, please visit STAR's security page. STAR also has a dedicated Fraud team ready to assist with any fraud-related matters.