THORLEY
WEALTH MANAGEMENT
Trust. Experience. Performance.
www.thorleywm.com

Mobile Device Security Best Practices

Despite their convenience, mobile devices pose unique security risks. These eight best practices can help you lock down the information on your mobile devices.

1) Update your firmware and applications regularly. Although it might be tempting to postpone an update for just one more day, it's crucial that you keep your devices—all their firmware, operating systems, and applications—up to date with the latest security patches. So when prompted, install!

2) Use a strong lock-screen passcode. A passcode is the first line of defense in protecting any mobile device.

- Don't pick consecutive (e.g., 123456) or repeating (e.g., 111222) digits.
- Opt for a longer passcode, preferably at least six digits.
- Pick a short auto-lock time so that your device never stays unlocked for too long.
- Set a maximum number of failed attempts before your device locks or wipes its information.

3) Ensure that your device is encrypted. Encryption helps prevent unauthorized users from accessing your information without a passcode.

- All iPhones starting with iPhone 3GS (2009 and later) are encrypted by default.
- On Android, check that your phone is encrypted at **Settings > Security > Encrypt phone**.

4) Back up your information. It's always a best practice to regularly back up your mobile devices to reduce the impact of lost, deleted, or corrupted information, whether from physical damage or from mobile malware.

5) Enable remote tracking and wiping. Today's devices come equipped with tracking software (Find My iPhone for iOS or Android Device Manager for Android) so that you can locate them if they are lost or stolen—and remotely wipe them if necessary.

6) Look out for "clone" apps. Before downloading an app, always check that:

- The app title is correct
- The company is legitimate
- The number of reviews or ratings is consistent with the app's popularity

If you're ever in doubt, a quick Internet search can help verify the authenticity of an app.

1478 Marsh Road
Pittsford, NY 14534
P: (585) 512-8453
F: (585) 625-0477
www.thorleywm.com

7) Avoid jailbreaking or rooting. A jailbroken (iOS) or rooted (Android) device is one that has been intentionally "hacked" by the user so that it can do more than the manufacturer had intended. Although this practice is legal, it overrides the device's built-in security features and bypasses regular controls. Because of this, **jailbroken or rooted devices pose a major security risk**.

8) Manage what connects to your device.

- Avoid connecting to potentially unsecure Wi-Fi network access points.
- If you go on a public Wi-Fi network, avoid situations where you need to enter sensitive information (e.g., passwords, credit card numbers).
- Consider using a virtual private network (VPN) connection when working with sensitive information.
- Most cell providers now offer ample data plans, so consider using your device's data (e.g., 3G, 4G, LTE) rather than risking an unknown network.
- Disable the Wi-Fi auto-connect option. This reduces the chances of your mobile device automatically connecting to a malicious Wi-Fi access point.
- Disable Bluetooth when you're not using it, as it could also be a potential attack vector.