Mobile Device Security: A Moving Target

As the use of smartphones increases in the workplace, so does the need for robust security measures. Smartphones, acting as mini computers, hold a wealth of sensitive corporate information that could be catastrophic if fallen into the wrong hands. Cyber threats such as data leakage, unauthorized access, and malware attacks pose a real and growing risk. Having a clear workplace smartphone use policy is crucial as it helps to maintain productivity, ensures security of sensitive company information, and fosters professionalism. After a policy itself is written up, it's time to put the gritty in the nitty of employee's understanding of basic good practice for smartphone security.

Intrada's Safety Recommendations

1. **Devices should be passphrase, passcode, or passkey protected. These could include biometrics such as face, fingerprint, or iris recognition or PINs that use a string of numbers, letters, or a geometric pattern.**

2. **Connected to the recommendation above, devices should be set to lock themselves after a reasonable period of time. A device lock of two to five minutes strikes a near-ideal balance.**

3. **Update your applications and OS. Most devices are very (if not overly) faithful to remind users to update their operating systems. Just make sure you don't put off the restart for too long.**

4. **Disable Bluetooth when you're not using it. If hackers don't have access to it, it can't be compromised.**

5. **Lastly, encrypt your device. When you are signed in with your Apple ID, the information is encrypted every time your phone is locked. Most Android devices are now also encrypted by default, if you have set up a lock screen with the passcode feature.**

31 Ashler Manor Drive
Muncy, PA 17756

intradatech.com
800-858-5745

Exceeding Expectations.