

Protect the Data on your iPhone

The iPhone can be an excellent tool to incorporate in your company's IT business plan. Not only does it provide mobile voice, text and email communication solutions, it can also give you access to most of your onsite business data. However, security steps should be taken to ensure your data is protected at all times, whether the phone is in your pocket during a board meeting or on the counter beside you at your favorite watering hole. As such, All Covered has identified ten important security steps to ensure that your business, data, and IT network are protected at all times:

1. **Enable auto-lock-** when your iPhone has been inactive for more than a minute, the phone will automatically lock up and turn off the monitor. A previously set 4-digit password will unlock it. This feature will protect your phone and data from being accessed by unauthorized users.
2. **Adopt safe Wi-Fi habits-** make sure that you are connecting to a trusted network to avoid system attacks from another computer.
3. **Use corporate web mail-** whenever possible, email should be securely stored on your corporation's physical email server and accessed through a webmail interface.
4. **Use Exchange ActiveSync-** if you need to travel out of cellular reception range, download pertinent emails to your phone through Exchange ActiveSync.
5. **Surf the web with Safari-** this user-friendly, built-in web browsing application can be set to automatically update itself every time you sync.



6. **Set device usage restrictions-** enable device usage restrictions to ensure that your iPhone complies with your business information security policies.
7. **Use “Find My Phone” and “Remote Wipe”-** if you lose your phone, you can log into Apple’s secure website and locate it through its GPS homing beacon. If your phone is unrecoverable, you can “remote wipe” it and ensure that all data has been permanently deleted.
8. **Activate encryption-** prevent accidental exposure of data stored on your iPhone with the included encryption app.
9. **Update regularly-** keep your iPhone patched and updated to ensure that it is always protected against the newest malware threats.
10. **Don’t hack your phone-** the technical term for self-initiated hacking is “jailbreaking” and is typically done when you want to install an app that isn’t approved by Apple. Altering the iPhone’s security software can create security breaches that may expose your company’s data.

The iPhone is an excellent IT tool for small business users. Not only does it provide immediate communication capabilities through voice, email and text, it also gives you web browsing capabilities and access to data on your corporate servers. Of course, with mobile IT solutions, security is always a concern, but by following the ten steps above and working with technology experts, you can reduce the risks of security threats to your iPhone, corporate IT network, and data. To learn more about how to securely use an iPhone as part of your comprehensive corporate IT plan, please contact All Covered.