7 Things You Can Do to Secure Your Mobile Device

Everyone is mobilizing. Our lives, both business and personal, have become dependent on our smartphones and other mobile devices such as iPads, tablets, etc. This makes our mobile devices and the data they contain just as important as our laptops and desktops. Add a direct Internet connection, and the likelihood of physical loss or theft and you've got a recipe for disaster. Viruses, spyware, phishing scams, data loss and theft are all serious threats to your smartphones security. Here is a list of security measures that will help you to protect your mobile devices:

1. Set up a password / pin code.

It's the simplest step you can take to help protect your smartphone and also one of the most effective.

iOS - Open the **Settings app -> General -> Passcode Lock**. Turn it on and enter your new password or passcode.

Android - Security comes in the form of a swipe pattern (unless you're running Android 2.2 Froyo, in which case you can also set a PIN or password). To set one, **go to Settings -> Security -> Change Unlock Pattern**. Check Require Pattern and you'll be able to enter a swipe pattern.

2. Use mobile antivirus software.

The number of virus attacks on smartphones has dramatically increased over the past year. Antivirus will detect and remove viruses and other forms of malware. There are a number of new mobile antivirus programs available and you can find them by searching in your App Store.

3. Back-up your data.

As you should back-up data on your computer, you should back-up data on your smartphone. Enough said.

4. Install updates.

Smartphone developers often discover security vulnerabilities in their operating system after a smartphone has been released. They address and fix these problems by issuing updates, which you should always install once one becomes available. You should also update any apps that you have on your smartphone as they also might have security updates.

5. Turn off both Bluetooth and Wi-Fi when you are not using them.

Hackers use open Wi-Fi and Bluetooth networks to steal information from your smartphone. Be careful when you are in a coffee shop or an airport lounge as this is where they have been known to target. You should never connect to untrusted Wi-Fi points. It may be tempting, but it's an easy way for people to gain access to your smartphone.

6. Don't unlock your phone (referred to as "jailbreak" –ing).

It might be tempting to unlock your smartphone, but you should remember that it can make your phone vulnerable to security threats.

7. Enable Remote Wipe.

If you've added a passcode/password/pattern to your smartphone and you're still paranoid, it may be time to explore remote wipe. Remote wipe does what the name implies - it remotely wipes the data on your phone and restores it to the factory settings. This is not something you want to do every day, but should be prepared to initiate should your phone fall into the wrong hands.

***iOS* -** Setting up remote wipe on an iOS device is easy, but only if you have all the right ingredients. You need a paid MobileMe account that's currently active on your iOS device if you're running a version of iOS prior to 4.2. You also need to Enable Push and Find My iPhone. Here's how:

Open the Settings app -> "Mail, Contacts, Calendars" -> "Fetch New Data" -> Enable Push. When you're done, go back to the "Mail, Contacts, Calendars" screen and choose your MobileMe account. On the next screen you'll see an option to enable Find My iPhone. Do that and you'll be all set. Once Find My iPhone is enabled, you'll be able to log into MobileMe and wipe your iPhone.

***Android* -** Remote wipe is a built-in possibility on an Android device, but it requires Android 2.2. Additionally, you need to have Exchange set up. In the event Exchange is set up, a remote wipe can only be performed by an administrator. You can also add remote wipe via the Mobile Defense app. It's free in the Android Marketplace and you can wipe your Android phone from the Mobile Defense website.

"Tech Talk" is authored by Chamber member John Kalli, proprietor of Trinity Worldwide Technologies, and will cover important technical topics that we believe can help our members/readers. Typical topics can range from be alerted to possible threats, to learning how to get the most out of your system/network and learning about new technologies, software and online offerings. Basically, our goal is to provide you with the knowledge that can save you time, money and potential disaster. Trinity is a Microsoft Certified Partner, Microsoft Small Business Specialist and has vast experience in all realms of computer networking, repairs, installation and more. If you have a suggestion for a topic or would like to submit a question for possible inclusion in a future column, please contact John at JKalli@trinityww.com. To inquire about their services and see if you qualify for a no cost, no obligation assessment of your business' technology, you can reach them at services them at 732-780-8615 or via www.trinityww.com.