Our Top 16 Security Tips for Smartphones

by Sharon D. Nelson, Esq. and John W. Simek

The age of the pocket computer is upon us. Smartphones are no more than small computers that happen to make phone calls. According to a Neilsen report, more than 50% of United States mobile subscribers now own a smartphone. Lawyers, for the first time in memory, are at the technology forefront, with 89% of them owning smartphones. Smartphones are extremely powerful devices, capable of storing contacts, calendar entries, e-mail communications, electronic files, voice messages and a host of additional confidential client information. As an attorney, you have an ethical obligation to protect the client data that is stored on the smartphone. We're here to give you some security tips for protecting the data and some easy measures designed to avoid having the data compromised.

1. Encryption

Such a simple word, but most attorneys are petrified at the thought of having to encrypt anything and avoid it like the plague. Encryption is simple and very easy to accomplish on a lot of smartphones. A BlackBerry device is built with encryption as part of the base design. Enabling 'Content Protection' on the BlackBerry will encrypt the device. If you use BES (BlackBerry Enterprise Server), you enforce encryption as part of the security policy. Just setting a PIN on an iPhone enables encryption and many Android devices have encryption capabilities as part of the operating system installation. Bottom line…enable encryption and you'll go a long way towards protecting the data on the phone.

2. Encrypt Expansion Memory

Besides the main memory, be sure to encrypt any memory expansion cards that may be used. iPhone users don't have to worry about this since you can't expand an iPhone, but others need to protect any data that may be saved to the card.

3. Lock Code

Be sure to set a lock code for your smartphone. This will help prevent unauthorized access to the information. Set a code that is longer than the typical 4-digit PIN to make it more difficult to crack the number. For iPhone users, turn off 'Simple Passcode' in order to enter more than 4-digits. Why? Because there is software available that can brute force an iOS 4-digit PIN in several minutes.

4. Inactivity Timer

Set a fairly short inactivity timer for your smartphone. This will automatically lock the phone if it hasn't been used for a period of time. Don't be tempted to set your timer at five or more minutes. You should configure the value to be no more than two minutes. Many attorneys complain that the phone will lock too quickly with such a short value, but larger numbers leave you exposed should you leave your phone in the cab (one of us has done that).

5. Location Services

Turn on the location services of your smartphone to facilitate finding the phone if it is ever lost. iPhone users would enable the 'Find My iPhone' feature through iCloud. The ability to locate your smartphone must be turned on before you lose your phone, something many lawyers seem unaware of. Android users can install the free Lookout application, which has device location capabilities. Another advantage of the location services is that you can send a message to the device or have the smartphone play an alert sound, even if the sound is turned off or the phone is in vibrate mode.

6. Remote Wipe

Make sure you have the ability to remotely wipe the phone should you lose it. This is different than being able to locate the phone. Remote wipe means you can remotely send a command to wipe the information from the phone. This is a built-in feature for the BlackBerry devices. Remote wipe is part of the 'Find My iPhone' feature for iPhones and it is also included with Lookout for the Android phones.

7. Security Software

Security software for mobile devices is no longer an option. Malware writers are now targeting smartphones in a major way. All of the major security software vendors have products for the popular manufactures and models of smartphones. As we've already mentioned, Lookout is a great free product for Android devices. iPhone users pretty much have to trust Apple since they don't allow any third party access to the core of the operating system. There are security products for the iPhone, but they are not real-time scanners such as those available for the other smartphone operating systems.

8. URLs and QR Codes

This security tip doesn't require any specialized software or hardware device. Our advice here is not to click on any URL that you receive in a message (e-mail or text) that you are not familiar with. Also, we're not big fans of any shortened URL (e.g. tiny URL or bitly) since you really don't know where it will take you. The same goes for QR codes. The QR code is a picture type barcode and you really don't have any clue where the code will take you. Think of it as the Wild, Wild West of the Internet.

9. Wireless Networks

Many smartphone users will connect to wireless networks in order to avoid the data charges associated with accessing the 3G/4G data network of the cellular provider. Using wireless networks is not a problem, but make sure you are connecting to a secure wireless network. Many of the free wireless networks available at businesses (McDonald's, Starbucks, etc.) are open networks with no encryption. This means that someone else could be monitoring the network traffic and capturing your data transmissions. This means you should only use secured wireless networks. WPA2 encrypted wireless networks are the only ones we prefer. WPA encryption was cracked long ago and WEP encryption can be broken in a matter of minutes.

10. Update Your Device

Always run the latest version of the operating system for your smartphone. Just like your computer, vendors provide updates for the operating system to patch security vulnerabilities and add additional features. iPhone users can get the latest updates through iTunes. Other users typically get the updates directly from the cellular provider. You may not have a choice when it comes to updates as the carrier may force it to your phone. There doesn't seem to be any consistency with the operating system updates. We've had Windows Mobile phones for which we had to manually download updates from the carrier's website. Our BlackBerry smartphone was updated by checking for updates from the phone, which would download them directly from RIM. Finally, our current Android phone has updates pushed to it automatically from our cellular provider.

11. Don't Jailbreak or Root

Do not attempt to bypass the security or normal operation of the smartphone by jailbreaking or rooting the phone. Bypassing the security certainly makes you vulnerable to potential compromise.

12. Application Installations

Be wary of any applications from unknown sources. The applications available through iTunes are pretty safe, but there have been several instances where malware slipped past Apple's review process. Google has been criticized for letting malware laden applications "camp out" in their store, but it has improved policing application safety through Bouncer. Bouncer still isn't bullet proof and some malware is still slipping into Google Play. RIM seems to be pretty clear of malware apps, but that may be because there is so little interest in third party apps for the BlackBerry. Just make sure you review what others say about an application before you load it, which should help you stay out of trouble.

13. Terms of Service

It still amazes us that lawyers tend not to read the terms of service. They will read contracts for their clients, but not for their own use. The Terms of Service will tell you what you are agreeing to, which in turn, tells you what the application wants to do. The app may want to record your phone number and location. It may have the ability to actually make a phone call without your involvement. Some apps even say they will access your contacts. Reading the TOS could keep you out of trouble by protecting access to your data when you realize all the information that the developer wants to access to. On a regular basis, we are mystified by some of the functions that apps demand.

14. Turn Off Unneeded Interfaces

This will also help conserve battery life. Turn off anything you don't need or use at the moment. As an example, shut off the Bluetooth if you are not using it. You should also shut off the WiFi radio if you are not connected to the Internet.

15. Mobile Device Manager

You may or may not need a Mobile Device Manager to enforce policies on the smartphone. The free BES Express for BlackBerry devices is very popular among law firms. There are other MDMs, but they tend to be implemented in larger environments. Whether you purchase a MDM or not, something should be in place to enforce and control certain aspects of the smartphone. Items such as enforcement of a

password, password complexity and length, encryption, inactivity timeout, etc. should all be required items and the user should have no option to bypass them. The ActiveSync policies available with a Microsoft Exchange server should be sufficient for most small firms.

16. Backup

Backup your data and applications. iTunes (not iCloud) should be used for the backup of iPhones. This is because ITunes provides a local backup and because the iCloud's Terms of Service are not security-friendly. BlackBerries can be backed up using the BlackBerry Desktop Manager. Typically, the manufacturer of the smartphone will provide software to be used for backup. If possible, you should also encrypt the backup. There are also third party applications that can be used for backup. Why backup? Because this is another layer of protection should you misplace your smartphone and have to remotely wipe it.

Conclusion

We sometimes hear lawyers say that they don't store client data on their smartphones. In many cases, data is written to your phone without your knowledge. Just opening and reviewing a document may result in the document being written to the phone. This is particularly true of iPhones.

No matter what phone you use, be conscious of the changes to the ABA Model Rules of Professionalism. You are now required, under those rules, to use technology competently and to assess the risk of using any particular technology and the sensitivity of the data you are handling against the expense and trouble of measures to secure the data. If you follow our sixteen tips, you'll be far more secure than the average lawyer and you will have adopted reasonable precautions for protecting client data – without breaking the bank.