10 Simple Steps for Securing Your Mobile Device

By Steven L. Butler, Esquire

In today's world, it has become normal to find most attorneys attached to mobile devices like smartphones, tablets, and laptops whenever they are outside of their office. These devices have basically become necessities for most lawyers, regardless of the type of practice in which they are engaged. Since mobile devices are relied upon so heavily, it is important that simple security precautions are taken to secure the data stored on the devices.

> *Even though a mobile device is normally in closer proximity to an individual than a desktop computer, this does not make it more secure.*

1. Password protect.

Yes, entering a password takes time, but without a password there is no protection between data on the mobile device and a potential intruder. Even a weak password is better than no password at all. In addition to the simple numeric PINs found on most smartphones, all major vendors also offer much more secure alphanumeric passwords. With technologies like Apple's TouchID, even fingerprints can be used to authenticate identity.

2. Auto-lock device after period of inactivity.

Whether it is a laptop, tablet, or smartphone, there is a likely an option to automatically lock the mobile device and require a password after a period of inactivity. By enabling this option, an unattended device will be locked with no action required by the user. It is best to select a relatively brief period before auto-lock is invoked. With the emergence of smartwatches, some devices can even auto-lock when a smartwatch is a certain distance from the device.

3. Be careful entering passwords in public.

A password is only good if it is not easily discovered by others. In addition to staying away from easily guessed passwords (like a birthday), be aware when entering passwords in front of others. If anyone standing around can watch the password being entered into the device, the password is not serving an effective purpose.

4. Do not share devices with others.

It is becoming less common for individuals to have a separate work device and personal device. Although it is nice to no longer have to carry two separate smartphones, this means that mobile devices with confidential client data are being used around family members, roommates, and friends on a much more frequent basis. If client data cannot be sequestered under a separate password or user profile, mobile devices should only be used by the lawyer.

5. Do not save app passwords.

Many apps installed on mobile devices require a separate login and password before information can be accessed. These apps often provide an option of saving the login and password information to allow quicker access in the future. Instead of retaining the login credentials, enter the login and password on every use. Use a different password for the apps than what is used to login into the device. This way, even if the device's primary password is obtained, data in third-party apps cannot necessarily be accessed.

6. Encrypt data stored on mobile devices.

In addition to password protection, most mobile devices allow encryption of data. Although passwords will prevent someone from easily accessing the contents of the mobile device, without encryption, some information can still be pulled off of a password protected device. With Apple phones and tablets, data is encrypted whenever a password is used. With Android and Windows devices, encryption normally needs to be enabled in settings.

7. Only store necessary client data on mobile devices.

Data should only be stored on mobile devices while it is actively being used. If a client file was closed two years ago, there is no reason to still have it on the mobile device. Remove documents with confidential information immediately after the matter is completed. Know what information is being stored on the device, and use a schedule to purge data from the mobile device.

8. Update mobile devices with newest security patches.

Even if steps are taken to secure a mobile device, new vulnerabilities are discovered frequently. Apply software and firmware updates on mobile devices as soon as possible to protect from the

vulnerabilities. Do not install software from untrusted sources, and only install apps and services that are needed.

9. Refrain from using public WiFi networks.

Public WiFi networks can be used to intercept data that is being transmitted using mobile devices. Since these networks are often available to use without any login or password credentials, it is hard to determine if they have been established by a malicious user. Any unencrypted data that is being transmitted over a public WiFi network can potentially be intercepted by a malicious third-party. If public WiFi access cannot be avoided, it is best to use a VPN connection on the mobile device.

10. Use remote wipe and remote location tracking service.

Android, Microsoft, and Apple mobile devices all have free remote wipe and remote location tracking services available. With these services, a free account is established with the software publisher, and then the mobile devices can be located on a map by using a website or app. If the device is still communicating with the internet, a message can be displayed, a tone can be played, or a command can be sent to remote wipe the device. Remote wipe will remove all data from the mobile device.

Bonus: 11. Use common sense.

If an activity does not feel safe and secure, it probably is not. Even though a mobile device is normally in closer proximity to an individual than a desktop computer, this does not make it more secure. Putting on a seat belt or making children sit in the backseat of a car did not always feel natural to many people, but as habits are formed, initial inconveniences quickly feel normal.

Steven L. Butler is a partner with Linarducci & Butler, PA. His practice is limited to Social Security Disability. Mr. Butler is a member of the Delaware Supreme Court Commission of Law and Technology and is a blogger at http://iPlugDelaware.com, http://Mobile4Law.com, and http://DelawareDisability.com/Blog.