MOBILE DEVICE SECURITY – which system?

Most people know that mobile devices today operate on either an Android or an iOS (Apple) system, but to a novice to the world of Smartphones, tablets and E-book readers these terms can be meaningless. Yes, there are obvious differences between these two platforms (regardless of the lawsuits won and lost in the interim): multi-tasking abilities, lock screen facility, calendar layouts, quick settings controls, messaging features, and visual cosmetics all vary. One system can even be more user-friendly than the other – depending on the user!

In light of every new security threat that arises – the latest being "Heartbleed"– personal data is always at risk. The question is which of the two systems is **MORE** secure? As users fill their devices with more information, it is unsettling to consider that all this data can be hacked and used by others. In 2013 the U.S. Department of Justice reported that 0.7% of mobile malware targeted iOS devices, vs. 79% that aimed at Androids. But that is just a statistic. Yes, iOS security is built in but their features must be enabled, while Samsung has introduced its best security, named KNOX.

The key is in how the hardware integrates with its operating system and right now, the iOS has the advantage because its system has been optimized. Android manufacturers still do not have the same level of control over this integration, or the available Apps in the App Stores. In layman's terms, the ***API*** or interface in Android systems is generally still not at the same level as the iOS systems although both systems have made great advances in beefing up their native security capabilities. Android's 4.4 system (nicknamed KITKAT), provides among other things, increased support for digital certificate warnings, a more secure booting process, creating trusted zones for certain applications. Although this may seem promising, every manufacturer still produces and manages their APIs differently, hence the difficulty in unifying the end result to the same level. KNOX may have great controls but with over 400 controls and 1000 APIs supporting them, the entire process is confusing and unwieldy.

Where does that leave us? First, understand that operating systems are inherently different and must be managed differently. Second, installing any kind of internet security software still requires the user to limit access to their device, i.e. you are still at risk if you permit downloads, apps or links that are infected. Plus most anti-virus software is still not up to snuff with regard to mobile devices as systems and apps are constantly changing and they cannot keep up; furthermore some devices outright reject the software.

If you understand that the base concept of design, manufacture and interface are different, you will either accept or reject one system over the other – high prices notwithstanding. Just remember that **ALL** wireless devices run risks by simply being wireless. Malware and hackers prefer mobile devices to PCs because of their vulnerabilities and the ease with which people use them to store personal data and transactions. Remember: no banking or credit card purchasing on any mobile device.