In his article “Mobile Security: Finally a Serious Problem?” Neal Leavitt analyzes the future potential threat to users from mass smartphone usage, because “the more widely a technology is used, the more likely it is to become the target of hackers” (Leavitt, 2011). Especially when you consider what people use smartphones for such as bank transactions, mobile pay options, and sending private business data over the network, mobile phone hacking could mean devastating losses for individuals and organizations. Leavitt then goes on to describe the various forms of how mobile phones can be compromised, including botnets, malicious applications, social networking, spyware, Bluetooth, wi-fi, and phishing.

Botnets generally come in the form of email attachments or compromised applications or websites that infect the mobile device with malware, turning it into a “zombie” device so that it can help infect other devices. Malicious applications are generally free applications installed by the user that can steal information and download and execute other malicious software to cause other problems. Through links on social media, hackers can install Trojans, spyware, and backdoors on mobile devices and through those methods steal personal information such as passwords or identity information. Spyware installed could allow a hacker to listen in on calls, view text messages, keep track of a person’s location through GPS, or turn on the device’s microphone so they can listen to what otherwise would have been a private conversation. Over Bluetooth, hackers have the ability to transmit executables onto other devices. Through wi-fi (specifically hot spots which have no encryption architecture), hackers can intercept communications and other data as the “man in the middle.” Lastly, phishing – especially social media phishing – is rapidly becoming popular among hackers since they can phish to mobile devices via the internet or SMS and MMS. Security-wise, antivirus and firewall products are extremely useful as they are on PCs, analyzing the new product being installed/accessed by the user for malicious software. In addition, stores like MobileIron can directly install safe applications onto devices so there is significantly less possibility of a hacker ever gaining control via the new application. AT&T and Verizon Wireless have noted the importance of mobile device security and are creating departments to research and design effective mobile phone security for customers on their networks.

Although this article was written in 2011, the importance is still absolutely true today. In the article, it was mentioned there are 370 million mobile phones in use worldwide, but there are now upwards of 3.8 *billion* mobile devices in use worldwide. If mobile devices were not in enough use to be a worthwhile target in 2011, they certainly are now.