Understanding the vulnerabilities of a smartphone

“ They have an app for that” is the mantra of most smartphone users, but an improperly configured smartphone can be an open invitation to hackers looking for easy information. Today’s modern smartphone can do anything from controlling your home computer to handling your online banking to watching TV to making video calls. With all the features included in them, they are very easy to stockpile important (and sometimes sensitive) information about the user. Since smartphones are essentially tiny computers, they suffer the same vulnerabilities of PC’s, including viruses, malicious applications, and hacking.

If there is the tiniest flaw in the smartphone’s armor, hackers can gain access and take an enormous amount of data from it. With the rise in popularity of Wi-Fi and Bluetooth technology embedded into smartphones, it has gained the attention of hackers out to gather information as another way to get into a system. Bluetooth technology is a very small area networking device, meaning that it can communicate wirelessly to other Bluetooth devices in the vicinity of 25-30 feet. But that also means that any hacker with that same technology can gain entry into a smartphone and wreak havoc that way.

Any information stored on that phone is now available to them to take and do with as they please. The only disadvantage to a hacker using Bluetooth is that they have to be within range, so they typically target large crowds of people if they are going to use that transmission medium to gather information. Embedding Wi-Fi into smartphones is another way for hackers to gain access to information easily. If a smartphone has Wi-Fi enabled, it

means that it can connect to a number of access points or “ hotspots” to access the internet, just like a PC would.

Alternatively, this also means that it opens it up so that a hacker looking for information can access that smartphone though a computer with more ease than going through Bluetooth. Once a hacker has linked up to a smartphone through their computer, any sensitive information available on that device is now open to anyone’s eyes. Sometimes a hacker doesn’t need to link up to a smartphone through Wi-Fi or Bluetooth to get information. Due to the enormous amount of “ apps”, or applications that are designed to run on a smartphone, available through the various cell phone markets, it has made collecting information and violating sers privacy that much easier.

Apps can be made to do almost anything, with the only limits being the amount of processing power of a particular smartphone. Sometimes apps can be made to look like they are doing one thing, while performing a malicious task in the background. These types of malicious apps are becoming more and more prevalent due to the rise in use of smartphones. One of the more popular ways to get information (particularly credit card or banking information) is to design an app that requires you to purchase something through it.

The most common option is a game that you can either upgrade or buy in-game items using your credit card. That card information goes through an unsecured server (usually owned by the developer of the app), leaving it vulnerable to being stolen and used illegally. There are very easy solutions to protecting a user’s smartphone from these types of attacks, however. The

easiest of these solutions is to have your device properly setup so that little to no vulnerabilities exist. Having a professional go through all the options and settings to tune it to a particular user is one of the most effective ways.

This reduces the natural vulnerabilities built in to a smartphone’s operating system. Turning certain features off when not in use is another very commonplace practice of eliminating those vulnerabilities. It is quite hard for someone to link up to a smartphone if both Bluetooth and Wi-Fi are turned off, therefore not accepting connections from outside devices. Another way of cutting down on the possibility of losing information is to monitor what apps are installed on a particular device. Understanding what a certain app does and what it’s doing in the background is one of the most important ways to find out if it’s malicious or not.

Using simple tools built into the phone it is very easy to find out if a certain app is running in the background when it shouldn’t be, or if it’s using more resources to do something that it’s not supposed to be doing. Any of those suspicious behaviors are indications that it might be involved in malicious activities. Keeping tabs on what’s installed and uninstalling unneeded or unknown applications helps with this. Smartphones are considered cutting edge technology. They’re constantly being upgraded and improved with new breakthroughs in technology.

Used properly, they can be one of the most useful tools that any person can own. But they are susceptible to the same types of attacks that computers are. And since smartphones can now do almost everything that a normal PC can do, more information is being handled through them. Utilizing simple

techniques such as learning more about smartphones and their features, or speaking with a professional on the subject are the easiest ways to safeguard sensitive information against hackers. The less information is openly available to those hackers, the less damage they can do in the long run.