The Weaknesses of Smartphones

Introduction

Let's face it, the times are changing. We are at a point now in society where everything seems converge all together in one place, namely our Smartphone. It has literally become an extension of both our personal and professional lives. For example, much of our office work can be done on the Smartphone if we work remotely. We can exchange files and emails with our coworkers and colleagues, and even type up a document and create a spreadsheet.

With our family and friends, we can exchange pictures, videos, and even share content from our own personal Social Media Sites. In the end, who really even makes a direct call anymore? Most of our communications is now done via texting and instant messaging on Facebook or WhatsApp.

But just imagine for a second, what if something were to happen to our Smartphone? What if it was lost, or stolen, or even hit by a Cyber-attack? As individuals, we would be totally and completely paralyzed. We would not know what to do, and fear desperation would take complete hold of us.

Therefore, it is important to know what some of the security vulnerabilities are out there, whether it is associated with our iPhone, Android, Samsung, or even Windows device.

The Major Security Vulnerabilities Posed to Smartphones

1) Data Leakage:

   We all love to download mobile apps onto our Smartphone. It's fun, and a very quick, convenient way in which to access information and data in just two seconds or less. But believe it or not, these very same mobile apps which you use on a daily basis can also be the biggest source of what is known as "Data Leakage". This occurs when the app secretly sends your private or work related information to the provider whom made that specific available. Also, mobile malware can use specific distribution code to in which to inflict damage to iOS and Android based Smartphones, through the mobile app.

2) Unsecured Wi-Fi Access:

   Gone are the days of using a hard-wired Ethernet computer in order to gain access to the Internet, or other critical files and resources which you need to perform your everyday job functions. With the advent of wireless access, we can now access these same items literally anywhere or at any time in the world, either from our Smartphone or tablet. But, this new founded freedom comes at a cost: The Wi-Fi connection is very insecure. This is best exemplified by using your device at Starbuck's. The username and password is publicly known, and because of that, the connection is extremely vulnerable to any covert Cyber security attacks. The best way to know if you are on a secured Wi-Fi connection is if you see in the URL address an "https" versus the usual "http". The former stands for "Hyper Text Transport Protocol Secure", which means that the connection is encrypted to a certain degree. It is highly recommended that if you have to use an unsecure Wi-Fi, so sparingly without submitting any type of confidential information (such as your credit card or Social Security number).

3) Network Spoofing:

Suppose once again that you are at Starbuck's. In order to login, once again, you have to access their wireless connection from list of available of Wi-Fi connections, and enter in the provided username and password. But, did you know that a Cyber attacker can also set up a fake dialog box to enter these credentials? Although you may think you are connected to a legitimate Starbuck's wireless access point, there is a probability that you could actually be connected to a fake wireless access point which looks like the real thing. Once this happens, the Cyber attacker can then monitor all of your activity covertly, and even launch Identity Theft attacks (using the information they have captured) at a much later point in time. How can you tell if you are at a fake Wi-Fi connection? Normally, if you are at Starbuck's it will say something to the effect of "Starbuck's Wireless Connection"; whereas a spoofed connection will be more general, such as "Free Airport Wi-Fi" or "Free Coffeehouse Wi-Fi". In these situations, you will also be asked to create a separate account, whereas with the Starbuck's Wi-Fi connection, you will not be asked to do this.

4) Phishing Attacks:

With our Smartphone, we are also able to very easily access both our personal and work E-Mail. Cyber attackers are well aware of this, and thus they love to send messages which have a link to send you to a spoofed website, which once again, looks like the real thing (such as a banking or a brokerage website). At this fake website, you will be asked to enter your username and password. So, how can you tell if you received a Phishing E-Mail onto your Smartphone? Here are some of the telltale signs:

- The E-Mail message has improper spelling or grammar in the content and/or the subject heading;
- The hyperlinked message is different from the one that is shown in the text of the message;
- The E-Mail content urges you to take immediate action, or that you must reply immediately;
- The first thing that the E-Mail asks you for is your personal information;
- It asks you to make a donation to a legitimate non-for profit charity;
- The E-Mail message has a statement that you have won a contest (which you never entered in the first place) or a lottery, and that you have to click a link in which to claim your winnings;
- The E-Mail contains attachments you don't know about, and has file extensions which look suspicious.

5) Spyware:

This is a much more covert threat that Cyber attackers are using now to infiltrate Smartphones. This is a type of malware which ". . .is installed on a computer without the knowledge of the owner in order to collect the owner's private information. Spyware is often hidden from the user in order to gather information about internet interaction, keystrokes (also known as keylogging), passwords, and other valuable data." (SOURCE: http://www.pctools.com/security-news/what-is-spyware/). But, be warned it is not just a Cyber attacker that can install Spyware

onto your Smartphone. If you have an employer issued Smartphone, your boss may have already installed Spyware on it before handing it you, so that he or she can keep tabs as to how you are spending your workday.

6) Improper Session Handling:

   A bulk of the Smartphone apps now make use of what are known as “Tokens”. Simply put, this allows the end user to access different parts of the app without having to enter their login credentials (such as the username and password) each and every time. These tokens have been designed to act like a password, but the advantage of this is that the mobile app should create a new token (or a “new session”) each time something is accessed from within it. The purpose of these secure tokens is to constantly identify the device which is accessing that particular app. Improper session handling occurs when the mobile app unintentionally shares these tokens with a Cyber attacker, thus impersonating a legitimate user.

Conclusions

Yes, Smartphone technology is evolving at a very rapid pace, and as a result, so will the level of the sophistication of the Cyber-attacks against it. What is the best way to stay protected? First and foremost, make sure that your Smartphone is always updated with the latest security patches and upgrades. Your device should automatically tell you when to do this.

Second, always be vigilant. As the old adage says: “If it doesn’t feel right, don’t do it!!”.