Are you Smarter than your Smartphone?

2011 was the year of the Social Networking boom. 2012 is set to be the year mobile phone hackers expand their reach worldwide. Since the first iPhone was launched in 2007, there has been a steady growth in the quality and popularity of "smartphone" technology. Today, almost 30% of mobile phone users have either Apple or Android phones…and they're growing. As more attributes and applications become available, more people are discovering that phones can be wallets, email centers, photo albums, contact files, and music libraries….meaning they are loaded with unprotected personal information. People don´t realize that the same security concerns they have for their PCs they should extend to their smartphones which are more vulnerable since they're strictly wireless.

All smartphones have security vulnerabilities but for the moment most mobile malware is aimed at Android devices mainly because it is an open platform, thus making is easier for the bad guys to disperse their malicious software. One reason is that Apple does not license its software to other phone manufacturers but Google freely gives Android to phone makers, so these are growing faster and price points are lower. Regardless of the operating platform, hackers are capable of installing Trojans that intercept financial transactions and use your personal information for their gain; some malware can send text messages to premium SMS services unbeknownst to you until you get your monthly bill; spyware can harvest information about your personal activities and record phone conversations; "Quick Response" codes (those new black and white squares appearing in ads) can link to malicious text messages or websites.

Even though this is an early warning stage for smartphone users, there are some basic things you can do now to protect yourself:

1. Have a very personal password that would be tough for strangers to decipher.
2. Change your password frequently.
3. Make sure you are running the latest version of your phone´s operating system and apps you may have.
4. Use encryption whenever possible.
5. Think before you download apps by checking reviews. If you stay with major apps and app stores like **Amazon** or **iTunes**, your chances of getting malware are low but of course still possible. Bad apps can look like legitimate ones.
6. Obviously follow the same safe practices on your smartphone that you have for your PC or tablet.

It took almost 15 years for serious hacking problems to surface in the PC world but it has only taken 2 years on the mobile platform. The bad guys are at their experimental stages of development so don´t panic yet – unless you´re a celebrity you aren´t likely to be a target. Just bear in mind that as mobile devices like the tablet and smartphone

become more prolific (in 2011 combined tablet and smartphone purchases eclipsed those of desktops and laptops), remember that it only takes a couple of seconds to steal personal information. It´s OK to be smartly mobile – with a bit of protection.