Fraud and Identity Theft Go Mobile

November 9, 2011 - I just got a new Android phone and I love it. I've been downloading new applications like crazy, browsing the internet, pulling mail, and doing just about everything else you typically do on a computer. But the first thing I did was install anti-virus and anti-malware applications. Why? Well because cybercrime is going mobile. And the most vulnerable devices are actually built on the Android platform.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

Criminals are nothing if not resourceful. With the advent of personal computers and the internet, numerous scams cropped up designed to drain bank accounts, rob merchants and steal identities. Flash forward about 15 years and you get to where we are today.

More and more people are now leaving behind their computers and moving to mobile devices. Things like the iPad, tablet computing and smart phones. And where the public goes, criminals are sure to follow.

Over the course of the past year, there has been an explosion in mobile based crime. Most of the increase has targeted users of Android based devices. There are two reasons for this. First, the adoption of jAndroid by the public has been itself been explosive. And second, Android is an open-source community. Virtually anyone with a little computer knowledge can write Android based applications. And unlike with Apple, you don't need to go through a centralized marketplace to distribute any applications you write.

The upside of the Android approach is that users of the platform have numerous applications that they can choose to use on their phones, and many of them are free. The downside is that there is nothing to prevent the bad-guys from

developing applications of their own. And that is just what they are doing.

Just as with regular computers, there are now viruses and Trojans that target Android phones. These can infect your phone, delete data, make the device unusable, steal your user names and passwords, drain your bank accounts and even steal your identity if you don't do something to protect yourself.

The good news is that there is also a booming antivirus software market for Android. If you use one of these devices, make sure that you install this type of program. But only from a reputable source. There are also scam artists out there that are making fake antivirus software that will do nothing but damage to you and your phone.

And as a failsafe, make sure that you install software that will allow you to track, disable and wipe your phone clean .You can get this type of software for free. If you lose your phone, all you have to do is send it a text message that will render it useless to anyone who finds or steals it. And, because some of the programs available actually activate the GPS service in your phone, you may actually be able to give the police enough information that they can arrest the person who stole your phone and get it returned to you.

The bottom line is that if you use a smart mobile phone built on Android, you need to do the same things you would do on a computer to make sure that your data is safe. If you don't, you could easily wind up a victim of fraud or identity theft.

byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter: