How Secure is Your Cell Phone?

By: Robert M. Kresson
CEO Empire Investigations & Security LLC

The threat to your security from everyday cell phone use is much greater than most consumers realize. Eavesdropping can occur either remotely or with the installation of software that does not modify the phone's hardware. Remotely, such illegal spying is achieved by "roaming the airwaves" using unrestricted scanning devices that can unscramble even digitally encrypted signals. Spyware installation without the owner's knowledge is the growing trend for such clandestine operations. This illegal spyware is widely available on the internet and being used with greater frequency to access call histories, contact directories, phone locations and emails and transmit them to a remote website. In addition, "spy phones" specifically designed for eavesdropping are becoming available in smaller sizes and being built into other devices (e.g. outlets) to make them more physically undetectable.

Eavesdropping is one of the most costly security threats with espionage costing US corporations over $500 billion dollars a year and rising. Although there are more powerful encryption technologies and anti-spyware software being developed, these are not yet widely available. There are several precautions an educated consumer can take to enhance cell phone security.

1) Beware of discussing any sensitive or confidential information on your cell phone and turn it off and take out the battery for optimal protection. With the advent of Global Positioning System (GPS) technology, simply turning off your phone is not enough.

2) Password-protect access to your phone in case it is lost or stolen. This simple and obvious solution is rarely utilized by most cell phone consumers.

3) When your cell phone is working as a bug, regular calls cannot occur in most cases. While there are cell phones being developed that can run very high speed data in which additional voice channels can be simultaneously transmitted, these prototypes are not yet widely available.

4) If you notice that your cell battery is performing poorly or if your phone is unexpectedly warm even when not placing calls, it may be bugged.

5) Given that your phone must be physically accessed to load spyware, change your phones frequently.

6) If you have a GMS phone and notice a "buzzing" interference noise when you are not making a call, it is possible your phone is bugged. If delayed bugging is occurring (i.e., data recorded from phone stored in compressed format in phones memory to be uploaded later), this type is more difficult to detect since shorter transmission time is involved and often a poor battery performance is the biggest hint.

7) Be aware that systems such as Voice over IP, Caller ID, and voicemail options can also pose security risks. To avoid becoming a victim, be aware that the caller may not be who appears on your caller ID and use a PIN with all voicemail accounts so that someone without this PIN code cannot access your voicemails.

There may be instances when regardless of putting in place protection measures against eavesdropping, criminals may still intercept valuable information about you or your company. The best counter-measure is to work with a reputable, knowledgeable professional, such as Empire Investigation LLC, with over twenty five years of experience and the latest in high technological equipment to offer you counter-espionage measures both regarding your cell phone and other aspects of your company's security.

Visit our website at *www.empireinv.com* for biographical background of Robert Kresson.

This article can be found in the FALL 2008 Edition of C&K Magazine. Visit www.CK-Magazine.com