Mobile Spy & Cellular Bugging:
How Can I Tell If My Mobile Phone is Tapped?

by ComSec / Saturday, 22 March 2014 / Published in Uncategorized

Most cell phone owners aren't fully aware of the fact that their own mobile phones can turn them into misfortunate victims of modern espionage.

Nowadays, advanced technology has led to the creation of highly sophisticated spyware programs that can transform your cell phone into an accurate source of information, an open microphone exploited by eavesdroppers eager to uncover and sell your most carefully guarded secrets. Moreover, such programs can be easily installed by skilled specialists and can be virtually impossible to detect.

In case you own an old model of mobile phone with no Internet, email or text options, then you can rest at ease. Your private information is not in danger, because the phone that you are using doesn't have an operating system compatible with a spyware programs designed to disrupt your privacy. On the other hand, the owners of smartphones and any other kind of phones allowing them to download apps, send emails or use the Internet have all the right reasons to worry about victim of cell phone spying.

Currently, there are various spyware programs such as Flexispy, Mobile Spy, & SpyBubble, etc. that can be used by skilled spies, eager to get their hands on your valuable information. Such programs can be downloaded to your mobile in a matter of seconds. As a result, the eavesdropper would receive a copy of your personal data, stored on your mobile phone. All in all, all your files, videos, pictures sent and received emails, text, phone calls would stop being private. Do you think that you could become the next victim of cell phone spying? Below you will find a list of some of the most "active" spies, interested in uncovering your personal information:

#1: Law Enforcement & Wireless Service Providers

The NY Times reveals the fact that, only last year, law enforcement representatives made over 1.3 million requests for subscriber cell phone data from wireless service providers. Most of these claims were not based on the authority given by a warrant, even though 4th Amendment of the American Constitution clearly indicates that one would need a warrant to attain this goal.

It seems that cell phone providers earn a significant amount of money every year, as a result of their cooperation with law enforcement officers who need fast access to private information to solve some of their most difficult cases. Moreover, this unlawful practice has flourished over a relatively short period of time, since important cell phone companies have decided to hire people and to put them in charge of spying on your mobile phone to trace all your emails, phone calls and texts.

In this case, the best thing to do is to be cautious at all times, when it comes to using your mobile phone. Make sure you don't store information that you consider extremely important, encrypted in texts, videos or emails, because spying activities conducted by your wireless service provider, in collaboration with law enforcement officers can't be identified and annihilated by your reliable TSCM provider.

#2: Your own employer, turned into a perseverant, meticulous spy

A rule issued by the Supreme Court two years ago stipulates the fact that your employer doesn't have the right to monitor your mobile phone, unless his/her actions are driven by a powerful "legitimate work-related purpose." The truth is that, if the employer owns the cell phone that you're currently using or if he/she is paying a monthly fee for the service, you shouldn't expect your phone calls, text, emails, photos and any other kind of files to remain private. In case you cherish your privacy at work, but you still have to make a few personal phone calls regularly, think about purchasing your own mobile phone to serve this purpose. Also, if you are compelled to use the mobile phone owned by your employer even during non-working hours, always leave it in the car of in a place in which your private conversations could never be recorded or monitored. This type of situation is very difficult to solve, because a TSCM provider doesn't have the right to interfere, since the cell phone you might blame for obvious information leakage is owned by your employer.

#3: An "Ex" or Future "Ex" is one of the most dedicated spies that you'll ever meet

Jealous partners or former partners are likely to invest all their resources in effective spyware programs, in order to catch you on the wrong foot, while various important stakes are on the table: a great divorce settlement, custody, blackmail or personal satisfaction. The best way to attain this goal involves the presence of free or fee-based tracking applications installed on your mobile phone, indicating your exact location, your itinerary and following your every single move 24/7. The best part is that your spy can be notified via SMS, allowing him/her to discover your current location without having to depend on Internet access. In this particular case, the specialists from ComSec LLC can solve your problem, by filtering the transmissions from your cell phone while looking for downloaded spyware programs installed on your mobile.

#4: Competitors trying to get their hands on your well-kept secrets

Quite often, powerful, perseverant competitors would do everything in their power to discover the key to prosperity and notoriety, even at times when such a goal can be attained only by relying on unlawful methods, such as corporate espionage. Usually, most business owners spy on their competition to destroy their reputation or to steal their ideas, strategies, clients or staff members. A

spyware program enables them to get fast, unlimited access to everything that you could consider private, including business meetings, recent deals and sensitive company secrets. Every single time you lose sight of your mobile phone, it could end up in the wrong hands. Nowadays, spyware programs can be easily installed on your phone by various people, employees or professional spies using clever disguises, eager to uncover and distribute your valuable confidential information for more than a few dollars.

This article only touches on the edges of cellular or mobile phone attacks. The newest & most difficult to detect of these forms of attack are those conducted remotely via GSM, 3G or 4G. These type of attacks enable eavesdroppers to gain unauthorized access from anywhere in the world with a mobile phone signal. Please stay tuned for the next ComSec article on “Cyber Advanced Cellular Eavesdropping” or “Cyber ACE” Attacks.

Need to know if your smart phone – mobile phone is compromised ? ComSec’s cellular forensic department uses the Cellebrite suite of mobile forensic solutions. The most advanced analysis, spyware-malware detection, decoding and reporting application in the mobile forensic industry. Contact ComSec to inquire about our super fast mobile & smart phone TSCM forensic service. Most mobile – smart phones and iPad’s (iPhones, Android, Blackberry & iPads, etc) can be processed the same day they are received, and returned via Fed Ex overnight service the next day. Full pdf report of findings included and forwarded to your email.

Stop wondering if your cell phone, smart phone, iPad or tablet is bugged! Click Here to complete the Cellular Forensics Service Request Form, or call: 1-800-615-0392 to speak with the cellular forensic services dept.