CELLULAR PHONES

Can someone listen in on my calls? Can someone listen to my voicemail? Can they send texts from my phone? Can it be done, yes. Is it likely, no. It is extremely hard, expensive and time-consuming to tap/bug your cell phone. Are you and your information that important, that special?

Who are the targets? Corporate Executives, Government Officials, Defense Contractors, Diplomats, Lawyers, Doctors, and Celebrities are all subject to being targeted by Information Intercept Operators, who for a robust payday will take the time and use their technology to gain access to your information.

Leverage espionage has become a multi billion dollar a year business, yet businesses and celebrities do little to protect their operational security. Business executives see the results in sales not losses. It's often hard to quantify those deals that got away, those cases that were lost, those pictures leaked to the press, those proprietary methodologies and protocols that someone else came up with as well.

While the main players in this Interception Operation are rarely the highly paid Intercept Operators, they are most likely law-enforcement and government agencies, using court-ordered warrants to gain access. In the corporate world Information Intercept Operators are a real threat and are highly paid for their nefarious and illegal activities. So in reality unless you're doing something wrong, you are more than likely not a target for cellular information intercept.

THE PHONE:

This is how the phone works. When cell phones are turned on there is a continual exchange of information between the unit and the company's main computers. This data exchange occurs every few minutes and is the means by which the telephone company knows which towers are closest to your phone and the next tower it's coming into contact with, thus constantly tracking your cell phone. Even while not in use the phone must exchange data with the host company to ensure it is letting them know it is available for use.

Each cell phone has three identifiers; **ESN**; Electronic Serial Number, **MIN**; Mobile Identification Number and the **SID**; System Identification Designator.

ESN; Electronic Serial Number consist of a series of bits of information representing the unique *identifying serial number of each individual cellular telephone*. Think of this number as a unit serial number. This number is properly programmed into the cellular telephone at the factory and is as unique as a person's fingerprint.

MIN; Mobile Identification Number is the *standard 10 digit telephone number* of your cell phone. When there is an incoming call the telephone company uses this number to identify the location of cellular coverage in the area the phone is located in, it also

determines the originating cell number and its location. This number can always be changed.

SID; System Identification Designator is a 32 bit code that *identifies the specific cellular company* and its location to which the user subscribes for their telephone service and to where their bill goes to. Each individual company throughout the world has its own unique identification code. This is how companies know where to send the bill.

Older technology phones do not have the computing capacity to use Spyware, that's why an old pre-paid TracFone cell phone is a very secure option. Also if you purchase a non-smart phone/cell phone, Spyware cannot be downloaded on it. This would be like a cell phones we used 10 years ago.

SPYWARE:

Spyware is the same as a computer virus. It has to be installed on your phone. 60% of the time the Spyware is loaded on your phone by nefarious operator manually. 40% of the time you do it yourself by downloading an infected application, program or game.

If you believe there is Spyware in your phone the best way to rid yourself of this is to have your service provider reset your software back to its default. Spyware is extremely stealthy. The full forensic examination cannot guarantee that the Spyware can be found and that you will be able to discover who installed it. If by some chance the evidence leads back to an individual, it is highly unlikely they will be prosecuted because this is seen as a victimless crime. When and if prosecuted, the sentence is rarely stiff.

INTERCEPT OPERATORS:

The same technology that is led to the current popularity of cell phones has also made cell phone systems all the more susceptible to unauthorized interception. Tapping or Bugging your phone is far from being easy, the formidable and highly trained Information Intercept Operator who is well-funded can gain access to use your cell phone as a bug. They can either get hold of it manually or use their expensive signals intercept equipment to eavesdrop.

The Information Intercept Operator. Mercenary. This would be the professional operator with a technical background and a well-funded employer. Leverage intelligence is the bullseye and a large budget is required.

The Corporate Operator. Climbing the ladder. This individual sees the value in the information in their office and around them. Either makes himself vulnerable to exploitation or seeks out a competitor to sell the information to.

The Emotional Operator. Divorce and relationships. This individual becomes an operator out of their emotional disposition. The budget is limited as is their time. They use Internet acquired devices and time is not on their side.

The Stalker. Focused and targeted. This individual becomes an operator out of desperation and desire. The budget is limited, but their advantage is that they have time on their side. They are aggressive, relentless and reckless.

With today's Internet marketplace programs and devices are easily attained from around the world and the cost of this technology is becoming cheaper and cheaper.

SIGNS THAT YOUR PHONE IS INFECTED.

The most notable indication that your cell phone may have Spyware on it is that it has an unusually short battery life, as well as it feeling warmer than ususal. It's working on overload and the Spyware is always transmitting data, thus using more of the battery, thus getting warmer.

- The phone's battery life noticeably decreases.
- The phone is warmer to the touch than normal.
- You notice your screen lights up when not in use.
- The phone beeps or makes noises when not in use.
- The phones text messages display odd errors.
- Your phone takes longer to turn off then originally.
- Don't want to be heard, put it in a Faraday Cage or take out the battery.

PROTECTION METHODS.

The best way to defeat suspected Spyware is to get a new phone. Next, would be to reload your firmware/operating system software on your phone back to the default setting, thus removing all added applications. Lastly, you have the option of returning the phone to your service provider and having them reset the firmware/operating system.
In the military we have for years kept cell phones out of classified conversation areas. We leave them in metal boxes outside the room. A metal box that fully encloses the cell phones acts like a Faraday cage. This would be like losing your cell phone signal in an elevator. The metallic cage blocks the signal. If you put a cell phone inside a metallic can and cover it with a book, the cell phone which still transmit and receive.

Now if you put that same cell phone in the metallic can and placed it on top of the sheet of aluminum, thus completing the cage effect, the cell phone will not transmit and receive. The signals cannot go out or come in due to the metal surrounding them. As the signal contacts the metal, it flows around it, taking the line of less resistance and not getting to the phone. You can also purchase *pouches* that you can insert your cell phone into that also shield your phone.

PROTECTING YOUR PHONE.

Have a backup plan and purchase a secondary phone of older technology, not a smart phone. A good example would be a prepaid TracFone.

- Reset your firmware/operating system software.
- Set up a new password and always keep your phone in your possession.
- Don't unlock/jailbreak your phone's operating system.
- Don't put your current Sim card into a new phone.
- Don't synchronize your new phone with your former backup software.
- Don't download e-mail attachments or unfamiliar/unsafe applications.
- So, the easiest method to prevent your phone from being used as a listening device is to use a cell phone *Faraday cage pouch* when you absolutely don't want to be overheard.

It's simpler to just place it in a case (Faraday cage pouch) and then in a drawer, than to shut it down, take the cover off and remove the battery. These pouches can be purchased on Ebay and over the Internet. An inexpensive example is the silver metallic bag a computer hard drives come in. These are called anti-static bags and relatively inexpensive.

Information security represents the biggest potential loss for a company, and can usually be easily avoided with some simple attention from the proactive corporate security professional.