Initial Steps to Protect Yourself

The following special precautions should be practiced if you believe you or your company may be the subject of electronic eavesdropping:

1. DO NOT discuss your suspicions with anyone within your circle of influence. Period! The spy or eavesdropper may be the one you least suspect or trust the most. Your case may be easily compromised because the client discussed their concerns with those within their circle of influence. This is paramount! The number one rule is to maintain silence about your concerns. Act natural, and do not change your routine. Otherwise, you will alert the eavesdropper or corporate spy that you are aware of their presence. If you feel you must discuss your concerns, do yourself and/or your company a favor and contact a professional Counter Surveillance Specialist that will guide you through the correct steps to resolve your concerns.

2. Use a safe phone away from your office or home, i.e. use a friend's phone, pay phone, etc. Never use a 2.4 GHz cordless phone! If your suspicions are on the upper corporate level, you may even want to consider purchasing a "track phone" or "throw away" pre-paid phone from a grocery store or chain store (Best Buy, Radio Shack, etc.) and, keep it in your physical possession at all times. Be very discreet…watch what you say at home and at the office, and never discuss your concerns inside, outside, or near any suspect facility. Remember, any place that you feel comfortable to converse on a landline or cellular phone, will be a prime target for electronic eavesdropping. This includes your vehicle, yacht, plane, bedroom, etc.

3. Your computer may be subject to electronic eavesdropping as well. There are a number of methods utilized in "cyber spying" such as keyboard sniffing, keystroke logging, remote monitoring, wireless hacking, etc. Never open an attachment to an e-mail from a person that you do not know. Spyware is placed on your computer when you open an attachment. If you receive e-mail and click on an attachment and nothing apparently happens, you may have allowed spyware to be placed on your computer. If you are contacting us via e-mail, use caution. Use a computer other than your own if possible. You may also want to consider creating a "sterile e-mail address" (i.e. Yahoo, Gmail, etc.) When you contact us, use our encrypted secure contact form.

4. How do I know if I'm Bugged? Warning signs of eavesdropping or bugging: Corporate spies find new soft targets. How would you like the new emerging technology you have been working on for a defense contract or plans for future corporate takeovers you are planning to become public knowledge? Would copies of your product designs be of any use to your competitors? Would it be beneficial for your competitors to know how much you are quoting for the same project? You are a potential target. Could eavesdropping on anything you say, write, or do increase someone else's wealth or influence? If the answer is yes, you are a potential target. The higher the value of your information, the more likely it is that you are a target.

5. Here are some questions to ask yourself:

   Do others seem to know your confidential business or professional trade secrets?

   Does information about closed meetings and bids seem to be widely known?

   Have you noticed strange sounds or volume changes on your phone line?

   Have you noticed static, popping, or scratching on your phone lines?

   Are sounds coming from your phones handset when it's hung up?

6. What NOT to Do If You Think You Are Bugged:

   DO NOT use your office telephone to talk about your suspicions.

   DO NOT use your cellular or cordless phone to talk about your suspicions.

   DO NOT discuss your suspicions at the office, in your car, or at home.

   DO NOT purchase a spy shop bug detector.

   DO NOT send e-mails about your suspicions.

   DO NOT try to find the bug or wiretap yourself.

   DO NOT contact the telephone company.

   DO NOT contact the FBI/Secret Service.

   DO NOT try to get the local police to help.

Contact Legaltek via our Secure Contact Form or call: 714.313.1300 using a safe phone away from your area of concern.