Don't Be Frightened by BUGS

Bugs hide in the shadows and darkness waiting to strike fear and horror in their victims this Halloween…. but there's no need to be frightened! While the bugs we eradicate are not of the creepy crawly nature, they are equally if not more disturbing for those needing this specialized type of "pest" control. Bugs are listening devices that can be easily hidden inside rooms, cars, and people's clothing. Bugs, video cameras, and tracking devices are usually very small and almost undetectable. They use simple microphones that can listen, record, and transmit conversations. Some bugs transfer their signal to external sources by sending transmissions from your house or place of business via specialized equipment.

While the knowledge that someone may be covertly recording you or your loved ones professional or personal conversations and activities can send a shiver of disgust and concern down your spine; don't be frightened by bugs because Bearden Investigative Agency can help. A Technical Surveillance Counter Measure (TSCM) survey will provide a professional evaluation of your home or facility's technical security posture. It consists of a thorough visual, electronic, and physical examination in and about the surveyed facility utilizing the most advanced equipment and skilled agents.

What to look for if you think you have been bugged:

- *Your confidential business negotiations, trade secrets or business activities are known by people outside of your inner circle.*

This is the most prevalent red flag that your company is being targeted by covert eavesdropping techniques. Are your trade secrets or ideas coming out from competitors before your release? Is the media finding out about internal memos or scheduled releases prior to their intended dates? Are labor and settlement negotiations anticipated and not productive? These rhetorical questions are designed to look for the results of eavesdropping.

The purpose of eavesdropping is to extract some usable information or intelligence that the eavesdropper can leverage for some financial, legal or political gain. Although in violation of the law, illegal eavesdropping is a quick and exact way to accomplish the above. However, just because the effect exists, it may not be the byproduct of illegal eavesdropping. It could just be good old espionage.

- *Your confidential meetings, bids or internal memos are disclosed in pain staking detail.*

When looking for feedback, details are the upmost importance. Disclosure of prices, specific bid provisions, contract dates, settlement or negotiation figures or the exact phrase used in a meeting are high red flags. Information is a bit like a chocolate cake. At some point, we all need to have our piece. Critical information becomes too good not to use and flaunt. So, be careful who utters such information.
Also, realize that gossip, in any form, is easily spilled from another's lip. Many times, the disclosure of information is not from the eavesdropper but, rather a secondary person. The timing and substance of gossip can many times lead to the eavesdropping source.

- *Your phone and communications equipment are not working properly.*

Are sounds coming from your headset when it is hung up? This is generally indicative that someone is listening to everything you're saying or doing within distance of the phone receiver. Most device speakers are also in fact microphones as well. The turning of the telephone receiver into a microphone is common wiretap method named the Hook Switch Bypass.

Do you hear faint tone, high pitched sequels/ beeps or do you hear a tone when your phone is on the hook or the phone rings and no one is there. Such noises are an indicator that a "slave" device, harmonic bug, or infinity transmitter device is being utilized.

All of these could simply be a flaw in the line, but you should still have it checked out. Understanding the exact malfunction in any system helps assist us with getting an idea of the potential method used.
Depending on the type of malfunction and noise, it may be indicative that you have been comprised by a certain method. Have you heard volume changes or odd noise coming from your telephone? Are their popping noises, scratchy sounds, feedback, or mis-rings? These anomalies can be caused by capacitive discharge and may be the indication of line interference or the presence of a listening device. Such issues are more common with amateur eavesdropper and on older systems. However, many corporations still use older phone systems in long time occupied buildings. Not to mention the many times more successful venture of wiretapping an executive's home as opposed to the corporate headquarters.

- *You have noticed odd observations, moved furniture, and unauthorized physical access not necessarily tied to your communications equipment.*

Almost all illegal wiretapping involves access to the target area. Methods can include professional repeated break-ins to a home or office to conduct covert searches, scout and plant eavesdropping devices. Sometimes access can be done under a pretext. That can include unknown maintenance men, new cleaning crews or unwanted gifts which are meant to be placed in or near your office or meeting rooms. Have you noticed caulk or paint disturbed from the wall plates or wall plate screw? Is the wall plate moved or slightly ajar? Have you noticed dry-wall dust or debris on the floor next to walls, on your desk, tv stands or other furniture? Many times, this can be indication of a hastily installed listening device or pin hole camera.

Even in modern cell phones, access must be had to the underlying software to download monitoring software. Understand that access is almost essential to eavesdropping. Any indication that unauthorized individuals have accessed your computer, phone, telecommunications closet, office or conference room can be a tip that something is amiss.

- *You have been the subject of surveillance, dumpster diving, odd hang-up calls and other espionage.*

The decision to wiretap is either made hastily out of desperation or by someone who has spent time targeting for a purpose. That being said, most illegal wiretap operations are limited in time. Sometimes, they can be preceded by other means of espionage. Those include surveillance, pretext interviews, attempts to place informants into the organization and dumpster diving through company trash. Surveilling a person or company can reveal one's daily routine. What a person does, who that person meets up with, when a company opens, closes, when trash day is and method of disposing documents and papers from the location. Who is coming and going from the location like vendors, customers, sales persons and clients.

Carefully planned phone calls can obtain information, such as schedules, employment, personal information, company information and internal operations. Trash pick-up and dumpster diving is a very effective a resourceful manner of obtain confidential information legally. The information that is discarded unconsciously can be a wealth of knowledge. Look for these other methods to precede a potential wiretapping attempt.

Equipment BIA uses for TSCM sweeps

- Bearden Investigative Agency uses the most advanced Multi tear Portable RF Detectors designed for the detection of eavesdropping signals originating in rooms, phones, and body bugs. The Portable detectors analyze communication systems and conduct radio frequency analysis of the premise, carrier current, acoustic leakage, and infrared transmitters.

- We offer same day data extraction of phone and computers. This service provides digital analysis and complete extraction of suspected bugged or compromised device or networks.

How long does the process take?

- An average bug sweep can take anywhere from 4 to 7 hours depending on the size of the location to be inspected, the volume of items inside the location, and the quantity of electronic devices to be analyzed.

Example of a Recent Successful TSCM Sweep

A concerned client contacted this agency about suspicions that their coming and goings were being monitored. Furthermore, an adversarial party seemed to know who their acquaintances where. Upon inspection of the client's residence and electronic devices, a covert camera was found in their neighborhood. This camera had no discernable reason to be in such a location and was found to be covering the front yard of our client's residence. A forensic analysis of our client's phone found a malicious tracking application had been covertly installed and was tracking GPS locations. The application had an innocuous name and was suspected to have been installed manually when the client had left their phone unattended. These illicit tracking tools were found to have originated from a contentious divorce proceeding the client had been a party to. Once uncovered, our agents were able to provide detailed documentation that our client was then able to use during their court proceedings.

I'm concerned that I may have been bugged. What do I do?

If you see any of the above and suspect a wiretap, contact Bearden Investigative Agency and request a TSCM ("sweep") examination. We are well versed at privacy security evaluations and detailed TSCM sweeps. Using the latest equipment, we can identify electrical, wireless, infrared and hard-wired devices. Talk to a representative about the possibility of combining your corporate office, satellite offices and personal residences for regular sweeps and evaluations.

Don't be frightened by bugs…no matter how big or small your concern, enlist the team at Bearden Investigative Agency today. Call us at 1.800.943.2670 or email info@beardenonline.com.

CORPORATE OFFICE:
1341 West Mockingbird Lane, Suite 820
Dallas, TEXAS 75247

T 1.800.943.2670
F 1.800.946.2670
BeardenInvestigations.com

State Licensing
TX: #C-7124
LA: #9374-072618
NY: #11000215749