

Being Bugged

Here are some tips if you think you are being bugged.

1. Others know your confidential business or professional trade secrets.

This is the most obvious indicator of covert eavesdropping activities. Theft of confidential information is a billion dollar underground industry in Canada. Often the loss of your secrets will show up in very subtle ways so you should always trust your instincts in this matter. When your competitors know things that are obviously private, or the media finds out about things they should not know, then it is reasonable to suspect technical eavesdropping or bugging.

2. Secret meetings and bids seem to be less than secret.

Confidential meetings and bids are very popular targets for corporate spies. How would you like the plans for the corporate takeovers you're 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're quoting for the same project?

3. People seem to know your activities when they shouldn't.

4. You have noticed strange sounds or volume changes on your phone lines.

This is commonly caused by an amateur eavesdropper when they attach a wiretap, or activate a similar listening device. Surveillance devices often cause slight anomalies on the telephone line such a volume shift or drop-out. Professional eavesdroppers and their equipment usually do not make such noises; so if this is going on it could indicate that an amateur eavesdropper is listening in. On the other hand you could simply be experiencing a flaw in the line, but you should check it out.

5. You have noticed static, popping, or scratching on your phone lines.

This is caused by the capacitive discharge which occurs when two conductors are connected together (such as a bug or wiretap on a phone line). This is also a sign that an amateur eavesdropper or poorly trained spy is playing with your phone lines. It could be nothing more than a problem with your phone line or instrument, but a TSCM person should evaluate the situation to make sure.

6. Sounds are coming from your phones handset when it's hung up.

This is often caused by a hook switch bypass, which turns the telephone receiver into an eavesdropping microphone (and also a speaker). There is probably somebody listening to everything you say or do within twenty feet of the telephone (if this is happening).

D.E. RODWELL

INVESTIGATIVE SERVICES LTD

7. Your phone often rings and nobody is there, or a very faint tone or high pitched squeal/beep is heard for a fraction of a second.

This is an indicator of a slave device, or line extender being used on your phone line. This is also a key indicator of a harmonica bug, or infinity transmitter being used. Of course it may also be nothing more than a fax machine or modem calling the wrong number.

8. You can hear a tone on your line when your phone is on the hook (by using an external amplifier).

To check for something like this you would have to obtain a "recorder starter" interface (with a VOX option), or some kind of a high gain audio amplifier such as a uAmp or Kaiser 1059. Then with the phone hung-up listen to your telephone wiring. If you hear a faint solid dual tone it is a dead giveaway of someone using a "slave" eavesdropping device on your (or one of your neighbors) telephone lines. Such devices create a "command tone" when the subject hangs up the phone (so you must ensure that all of your phones are hung-up).

9. Your AM/FM radio has suddenly developed strange interference.

Many amateur and spy shop eavesdropping devices use frequencies within or just outside the FM radio band, these signals tend to drift and will "quiet" an FM radio in the vicinity of the bug.

Look for the transmissions at far ends of the FM radio band, a sound at any quiet area within the FM band. If the radio begins to squeal then slowly move it around the room until the sound become very high pitched. This is referred to as feedback detection or loop detection and will often locate the bug.

The "stereo" function should be turned off so the radio is operating in "mono" as this will provide a serious increase in sensitivity. If you find a "squealer" in this manner then immediately contact a security technician and get them to your location FAST.

10. Your car radio suddenly starts "getting weird"

Keep in mind that the antenna your car radio uses may be (and often is) exploited by an eavesdropper, and that such usage may interfere with radio reception (so be concerned if you automobile radio suddenly starts getting weird).

11. Your television has suddenly developed strange interference.

Television broadcast frequencies are often used to cloak a eavesdropping signal, but such a devices also tends to interfere with television reception (usually a UHF channel). Televisions also "suck in" a lot of RF energy and because of this are very sensitive to any nearby transmitters (this is technically called "Bandwidth, and TV signals use a lot of it). A small handheld television with a collapsible antenna may be used to sweep a room. Carefully watch for interference around channel numbers 2, 7, 13, 14, 50-60, and 66-68 as these frequencies are very popular with eavesdroppers.

12. You have been the victim of a burglary, but nothing was taken.

Professional eavesdroppers often break into a targets home or office, and very rarely leave direct evidence of the break-in; however, occupants of the premises will often "pickup on something not being right" such as the furniture being moved slightly.

D.E. RODWELL

INVESTIGATIVE SERVICES LTD

13. Electrical wall plates appear to have been moved slightly or "jarred".

One of the most popular locations to hide eavesdropping devices is inside, or behind electrical outlets, switches, smoke alarms, and lighting fixtures. This requires that the wall plates be removed. Look for small amounts of debris located on the floor directly below the electrical outlet. Also, watch for slight variations in the color or appearance of the power outlets and/or light switches as these are often swapped out by an eavesdropper. Also note if any of the screws which hold the wall plate against the wall have been moved from their previous position.

14. A dime-sized discoloration has suddenly appeared on the wall or ceiling.

This is a tell tale sign that a pinhole microphone or small covert video camera has been recently installed.

15. One of your vendors just gave you any type of electronic device such as a desk radio, alarm clock, lamp, small TV, boom box, CD player, and so on.

Many of these "gifts" are actually Trojan horses which contain eavesdropping devices. Be very suspicious of any kind of pen, marker, briefcase, calculator, "post-it" dispenser, power adapter, pager, cell phone, cordless phone, clock, radio, lamp, and so on that is given as a gift. That little gift the salesman left for you may be a serious hazard.

16. A small bump or deformation has appeared on the vinyl baseboard near the floor.

Strong indicator that someone may have concealed covert wiring or a microphone imbedded into the adhesive which holds the molding to the wall. Such deformation will often appear as a color shift, or lightening of the color.

17. The smoke detector, clock, lamp, or exit sign in your office or home looks slightly crooked, has a small hole in the surface, or has a quasi reflective surface.

These items are very popular concealment for covert eavesdropping devices. Often when these devices are installed at a target location they are rarely installed straight. Also watch out for things like this that "just appear", or when there is a slight change in their appearance.

18. Certain types of items have "just appeared" in your office or home, but nobody seems to know how they got there.

Typical items to watch for and beware of are: clocks, exit signs, sprinkler heads, radios, picture frames, and lamps.

19. White dry-wall dust or debris is noticed on the floor next to the wall.

A sign that a pinhole microphone or video camera may have been installed nearby. It will appear as if someone has dropped a small amount of powdered sugar either on the floor, or on the wall.

D.E. RODWELL

INVESTIGATIVE SERVICES LTD

20. You notice small pieces of ceiling tiles, or "grit" on the floor, or on the surface area of your desk. Also, you may observe a cracked, chipped, or gouged ceiling tiles, or ones that are sagging, or not properly set into the track.

Prime indicator that a ceiling tile has been moved around, and that someone may have installed a hidden video camera or other eavesdropping device in your office or near your desk. Also watch

for cracks or chips in the ceiling tiles. Amateur and poorly trained spies tend to crack or damage acoustical tiles. The ceiling tiles in any executive areas should never contain any cracks, nicks, gouges, or stains. Any ceiling tile that becomes damaged (for what ever reason) should immediately replaced and the cause of the damage documented. In such cases it is also wise to have a TSCM specialist inspect the area around the chipped, broken, or damaged tile to determine if a hostile eavesdropping device may have been introduced.

21. You notice that "Phone Company" trucks and utilities workers are spending a lot of time near your home or office doing repair work.

22. Telephone, cable, plumbing, or air conditioning repair people show up to do work when no one called them.

A very common ruse which eavesdroppers use to get into a facility is to fake a utility outage, and then show up to fix the problem. While they are fixing "the problem" they are also installing eavesdropping devices. Some of the more popular outage involve power, air conditioning, telephone, and even the occasional false fire alarm.

23. Service or delivery trucks are often parked nearby with nobody (you can see) in them.

These vehicles are commonly used as listening posts, be very cautious of any vehicle which has a ladder or pipe rack on the roof. Also, be wary of any vehicle which has tinted windows, or an area which you cannot see though (like a service van). The listening post vehicle could be any vehicle from a small Geo Tracker, Suburban, Blazer, Trooper, or Cargo Van. Look for any vehicle which could conceal a person in the back or has tinted windows. Also, keep in mind that the eavesdropper may relocate the vehicle several times, so look around. Typically, eavesdroppers like to get within 500-750 feet from the place or person they are eavesdropping on.

24. Your door locks suddenly don't "feel right", they suddenly start to get "sticky", or they completely fail.

Prime evidence that the lock has been picked, manipulated, or bypassed. Try to always use biaxial locks with sidebars (such as ASSA or Medeco). Also, only use double sided deadbolts in all doors, and good quality window bars on all windows, and a good quality door bar on all doors not used as a primary entry doors.

D.E. RODWELL

INVESTIGATIVE SERVICES LTD

25. Furniture has been moved slightly, and no one knows why.

A very popular location for the installation of eavesdropping device is either behind, or inside furniture (couch, chair, lamp, etc.) People who live or work in a targeted area tend to notice when furnishings have been moved even a fraction of an inch. Pay close attention to the imprint which furniture makes on rugs, and the position of lamps shades. Also watch the distance between furniture and the wall as eavesdroppers are usually in a hurry and rarely put the furniture back in the right place.

26. Things "seem" to have been rummaged through, but nothing is missing (at least that you noticed).

A "less than professional spy" will often rummage through a targets home for hours, but very rarely will they do it in a neat and orderly fashion. The most common "rummaging" targets are the backs of desk drawers, the bottom of file cabinets, closets, and dresser drawers.

27. An eavesdropper sends you a copy of your private conversations.

As simple as it seems this is the strongest indicator, and solid proof of eavesdropping. An eavesdropper will sometimes send a victim a copy of a private conversation they intercepted in an attempt at blackmail, or in an attempt to terrorize, or to just stalk the victim. This is commonly seen in civil lawsuits, criminal court cases, marital problems, shareholder disputes, custody battles, and other situations where one side has a position of weakness and is trying to physiologically undermine their opponent.