

Signs of Covert Eavesdropping or Bugging

Are You a Potential Target?

If someone could benefit financially or gain influence from your private conversations or actions, then you are likely a potential target for eavesdropping.

Warning Signs:

If you notice any of these indicators, contact TS Counter Measures at +61 0408443507 for a “Bug Sweep” or TSCM Inspection. Avoid calling from a suspect phone, whether it is a landline, cellular, or cordless phone. It is crucial to arrange the inspection discreetly and swiftly.

- 1. Leak of Confidential Information:** When others are aware of your confidential business or trade secrets, it may suggest eavesdropping. If competitors or media know private information, trust your instincts.
- 2. Compromised Secret Meetings:** If private meetings or bids seem to be exposed, corporate espionage might be involved.
- 3. Unusual Knowledge of Activities:** If people seem unusually aware of your private or business activities.
- 4. Strange Phone Line Sounds:** Volume changes or odd sounds on your phone lines can indicate a wiretap or listening device.
- 5. Static or Scratching on Phone Lines:** This may be caused by the capacitive discharge from a bug or wiretap.
- 6. Sounds from Handset When Hung Up:** This can be caused by a hook switch bypass, turning the receiver into an eavesdropping device.
- 7. Phone Rings with No Caller:** If your phone rings but no one is there, or you hear a faint tone or beep, it could be a sign of a listening device.
- 8. Tone on Phone Line When Hung Up:** Using an external amplifier, listen for a faint tone on the line when the phone is hung up, indicating a “slave” eavesdropping device.
- 9. Interference on Radio:** Strange interference on your AM/FM radio can indicate nearby eavesdropping devices.
- 10. Interference on Car Radio:** Sudden issues with your car radio reception could suggest an eavesdropping device using the antenna.
- 11. Interference on Television:** Eavesdropping devices can interfere with TV reception, especially on certain UHF channels.
- 12. Unusual Burglary with Nothing Missing:** Repeated break-ins with no apparent theft can be a sign of bugging activity.

13. **Moved Electrical Wall Plates:** Slightly moved or jarred electrical wall plates can indicate hidden eavesdropping devices.
14. **Discoloration on Wall or Ceiling:** This can indicate the installation of pinhole microphones or covert cameras.
15. **Gifts of Electronic Devices:** Be wary of electronic gifts like radios or alarm clocks, as they may contain eavesdropping devices.
16. **Bump on Vinyl Baseboard:** A small bump or deformation can indicate concealed wiring or a microphone.
17. **Crooked Smoke Detector or Lamp:** Such items can conceal eavesdropping devices and may appear crooked or have small holes.
18. **Unfamiliar Items:** If unknown items like clocks or radios appear in your space, they could contain eavesdropping devices.
19. **Drywall Dust on Floor:** This can indicate the installation of covert microphones or cameras.
20. **Debris from Ceiling Tiles:** Cracked or displaced ceiling tiles can indicate hidden eavesdropping devices.
21. **Frequent Utility Worker Presence:** Repeated presence of utility workers or trucks can be a sign of surveillance.
22. **Unrequested Repair Work:** Repair workers showing up unrequested can be a ruse for installing eavesdropping devices.
23. **Suspicious Service Trucks:** Unoccupied service trucks parked nearby can be used as listening posts.
24. **Changed Door Locks:** Locks that suddenly don't work right may have been tampered with.
25. **Moved Furniture:** Slightly moved furniture can indicate the installation of eavesdropping devices.
26. **Rummaged Through Items:** Signs of rummaging without anything missing can indicate a search for information.
27. **Proof of Eavesdropping:** Receiving a copy of your private conversations is strong evidence of surveillance.

Who Gets Bugged?

High-risk situations include public trading, labor issues, litigation, layoffs, and industries like fashion, automotive, advertising, or marketing.

High-Risk Individuals:

Anyone with money, power, influence, or access to sensitive information can be targeted.

This includes:

- Politicians
- Spouses, parents, and children
- Businesspeople and scientists
- Students and professors
- Lawyers and clients
- Insurance companies and claimants
- Construction companies
- Salespeople and clients
- Police and suspects
- Recruiters and directors
- Rock fans and musicians
- Department stores and customers (change rooms etc.)
- Public accessing change rooms in gymnasiums, swimming pools or other public or private facilities.

High-Risk Occupations:

Professions at higher risk include politicians, lawyers, doctors, chiropractors, dentists, architects, police officers, judges, elected officials, school principals, professors, engineers, software developers, executives, scientists, defence contractors, religious leaders, corporate buyers, sales and marketing, labour or union officials, and those in business who wish to maintain their competitive advantage and trade secrets.

Extreme Risk Businesses:

- **Materials:** Synthesis, processing, photonic materials, ceramics, composites, high-performance metals
- **Manufacturing:** Flexible computer-integrated manufacturing, intelligence processing equipment, micro- and nanofabrication
- **Information and Communications:** Software, micro and optoelectronics, high-performance computing, imaging and displays, sensors, data storage, computer simulation
- **Biotechnology and Life Sciences:** Applied molecular biology, computational chemistry, medical technology

- **Transportation: Aeronautics, surface transportation technologies**
- **Energy and Environment: Energy technologies, pollution minimization, remediation, waste management**