Kiamalu Consulting & Investigations LLC

Specializing in the UCMJ and Criminal Defense Investigations.

Serving All The Islands Of Hawaii And Worldwide

"Providing Peace of Mind In An Uncertain World"

THE KIAMALU REPORT ISSUE: FEBRUARY 2018

Are You Being BUGGED?

Detecting Bugging Devices & Espionage Threats = **TSCM** [technical surveillance counter-measures]

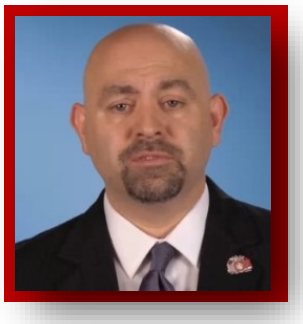
The object to the right is a **bug** - a tiny microphone that can be hidden almost anywhere. It is but one in a startling arsenal of devices used today to spy on personal enemies, competing companies, and other world powers.

KCI IS A U.S VETERAN OWNED & RUN COMPANY

SPECIALIZING IN THE UNIFORM CODE OF MILITARY JUSTICE (UCMJ)

SEMPER FI !

INSIDE THIS ISSUE:



Nathan Moores
Director of Operations
CEO

"Your case will be fully and expertly investigated."

Nobody is immune from spying. Companies, law firms, non-profit entities and charities, governments, private individuals—it happens everywhere.

If a party discusses valuable information that's of benefit to anyone, e.g., business competitors, opponents in a lawsuit, or some other adversary, they are a potential target.

It is illegal to install eavesdropping devices in every jurisdiction in the United States. To report it to the authorities you have to actually locate the device. People have the mistaken idea that the FBI or police will send someone out to do a bug sweep. ***They will not***.

Fight Back!

Are You Being BUGGED?

A little about eavesdropping devices

Just to dispel a few myths and misinformation about **"bugs" or covert transmitters** for a moment before we go into more detail about countering these threats.

Most people's understanding of bugging or eavesdropping devices comes from watching television, films or popular fiction books such as of course the legendary James Bond or The good shepherd, starring Matt Damon. This is not the 1980's and the Cold War, times and technology have moved on in leaps and bounds; that is not to say that some espionage technique developed then is still not applicable today.

The Cold War saw the real birth in eavesdropping devices, not only a change in the size of the devices, but the ingenuity of planting and of disguising the devices. Almost 40 years on and times have indeed changed, "99% of the capabilities of bugging devices that are depicted in popular film and television are not technically possible."

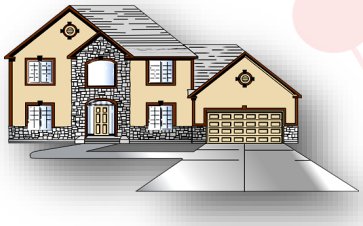
"99% of the capabilities of bugging devices that are depicted in popular film and television are not technically possible."

Why would anyone carry out an electronic eavesdropping attack on you?

1st. Nobody is immune from spying. Companies, law firms, non-profit entities and charities, governments, private individuals—it happens everywhere.

2nd. If a party discusses valuable information that's of benefit to anyone, e.g., business competitors, opponents in a lawsuit, or some other adversary, they are a potential target.

Reasons You Might Be a Target for Spying in your home



- You own a company.
- You are a suspected activist
- Your neighbor hates you.

IN THE NEWS

Are You Living With A Live Mic In Your House?

The New Smart Speakers devices that are connected to the voice-controlled intelligent personal assistant service which responds to the name is now becoming common in many homes.

The Amazon echo is not the only such device; others include personal assistants like Google Home, Google Now, Apple's Siri, Windows Cortana, as well as other devices including televisions, game consoles, cars and toys.

We can safely assume that the number of live microphones scattered throughout American homes will only increase to cover a wide range of "Internet of Things"

It is a significant thing to allow a live microphone in your private space (just as it is to allow them in our public spaces). Once the hardware is in place, and receiving electricity, and connected to the Internet, then you're reduced to placing your trust in the hands of two things that unfortunately are less than reliable these days: **1) software, and 2) policy.**

How It Works

You activate most commercial IVCSs with a "wake word". For a Amazon Echo or Echo Dot, you can choose one of 3 words, Alexa, Amazon or Echo. Unless you turn off the microphones {Echo has 7}and use a mechanical button or remote control to activate its capabilities it is always on. Could a hacker tap into one or all of them and eavesdrop on me? The official answer is no, and specific technical reasons are cited. However, "Anything that can be hacked will be hacked."

What do you think?

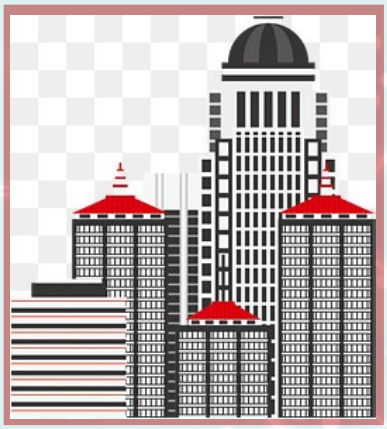
Are You Being BUGGED?

Reasons Your home my be a Target for Spying cont.....

- You are a scientist/politician/journalist/attorney/judge/police officer local government official.
- You were arrested for, but never convicted of, terrorist-related crime.
- You have an important, responsible, or secretive job.
- Your partner or spouse believes you are having an affair.
- You are getting divorced.
- You have to attend confidential interviews or meetings.
- You are interested in conspiracies and frequent certain websites.
- Your friend, neighbor, or relative is under suspicion.
- You have recently made a substantial insurance claim.
- You are very wealthy.
- You are a celebrity.
- You are the victim of a stalker

Keep in mind that anybody with money, power, influence, or access to sensitive, classified, or personal information is at serious personal risk.

Reasons You Might Be a Target for Spying in your Business



Anyone can be the target of covert eavesdropping, however; some people are under greater risk than others because of financial position, occupation, or legal.

High Threat Business Situations:

- Your company has stock which is publicly traded (or will be soon)
- Your company is having labor problems, union activities, or negotiations
- Your company is involved in any type of litigation or lawsuit
- Your company has layoffs pending (or they have just happened)

Are You Being BUGGED?

Some warning signs that your home, car, or office is Bugged

- If you believe you may be a target for a covert operation, the first thing to do is to be on the lookout for evidence that someone is watching or listening to your private conversations.

- Someone you know (your partner, a colleague, or neighbor) may inadvertently let slip something that they could only have overheard. If you question them, they will glibly deflect you by saying they guessed, that someone else told them or they made an assumption.

Don't argue or pursue the point.

- If information appears in the press that no one except you and your trusted friends/personnel have access to, **that's a major sign that you are under surveillance.**

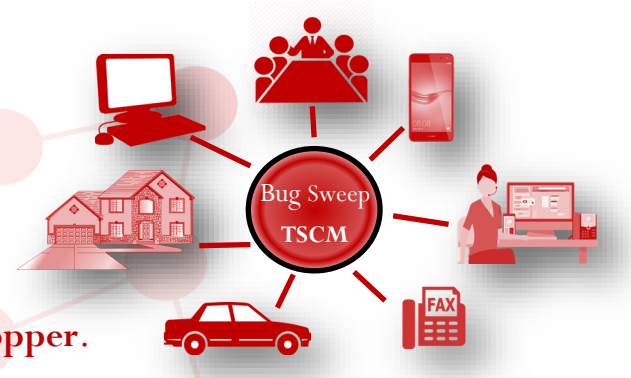
- A stalker likes his victim to be aware that he has access to private conversations – it adds to the fear-factor— and he will **often find ways to let you know you are being watched, followed, or listened to.**

- **If your home was burgled but nothing significant was taken.** You may not even notice if a door was left open or a window forced and you won't ever know that someone has been inside your home. Check if there is an unlocked door that isn't usually left unlocked, or an open window downstairs.

What areas are usually targeted

- the Company boardroom
- telephone system
- mobile phones
- fax machines
- computers

are examples of confidential information sources that may be targets for the eavesdropper.



Also, eavesdropping is **not always confined to the office.**

Executives and other key personnel can be targets at home and in cars.

Kiamalu Consulting & Investigations LLC

Are You Being BUGGED?

What should you do if you suspect an electronic bug is in your home or office?

You should call a professional. Do not try to remove it yourself. In the last fifteen years eavesdropping devices have got smaller and smaller as surface mount technology has got cheaper; batteries too have become more stable and of course smaller. It is pointless to try and save on the cost of a professional TSCM inspection by doing it yourself. The Specialized electronic equipment used in a professional TSCM inspection is useless in untrained hands and it requires a counter-surveillance specialist with years of knowledge and experience to be proficient in the TSCM field.

Beware of companies offering TSCM services with ineffective equipment and a lack of experience and training. These companies usually charge much less than the cost of a professional sweep and they will leave you with nothing more than a false sense of security.

Look for a TSCM specialist who has formal TSCM training, a broad spectrum of technical experience and professional TSCM equipment. **Kiamalu** Security has this extensive TSCM training, professional countermeasures equipment and through years of experience, we have acquired substantial knowledge of the TSCM profession.

Contact us to discuss which service is best for you and how we can reduce the potential for future problems and increase the level of security for your business.

Our goal is protecting and safeguarding your privacy.

We provide services which include;
Counterespionage, Technical Surveillance Countermeasures, Security Consulting, and Technical Bug Sweeps.

Call Us…. We will take the time to answer your questions and provide the Security you need and deserve!

In today's economic climate Kiamalu Consulting & Investigations realizes how important it is to get the most from your budget, without sacrificing on the quality of the services you need. With Kiamalu you can rest assured that we take pride in our work and because of our high skill level and extensive experience, we are able to offer services that are customized to your budget and your needs, resulting in a successful relationship.

Contact Kiamalu Consulting & Investigations to discuss the facts and circumstances of your particular case with an experienced investigator.
Kiamalu Consulting & Investigations LLC offers free initial 30-minute consultations. However, no advice beyond that initial consultation can be provided without a signed engagement letter and payment of KCI fees. Please call our offices or visit us online at: Kiamalu-ci.us

Toll Free Call for a FREE initial consultation!
(855) 542-6258

Kiamalu-ci.us (855) 542-6258

Insured and Bonded - Licensed by the State of Hawaii Department of Commerce and Consumer Affairs # PDA-1053