



From dumpster divers to hackers to mobile phone leeches, they're out to steal secrets from you and your clients.



Business snoops: The top 10 spy-busting tips they don't want you to know

BY KEVIN D. MURRAY

Who are these snoops?

Snoops can be competitors, vendors, investigators, business intelligence consultants, colleagues vying for positions, overbearing bosses, suspicious partners, the press, labor negotiators, government agencies. The list is long.

Why would I be a target?

Money and power are the top two reasons behind illegal surveillance. If anything you say or write could increase someone else's wealth or influence, you are a target.

Is snooping common?

Yes. The news is full of stories about stolen information. In fact, many news stories themselves begin with leaks.

Can I protect myself?

Yes. Espionage is preventable. If you know the vulnerabilities, you can take the proper security precautions. Some spy tricks are obvious, if you stop to think about it. Some are clever abuses of the new technology we live with every day. All are devastating. Time has shown that many of the same tricks are used successfully over and over again. We present the top ten. Prepare to fight back.

Trash trawling

Dumpster diving, waste archeology or trashing are all terms that refer to rifling garbage in an effort to cull valuable information. This is believed to be the number one method of business and personal espionage. In and of itself, stealing garbage is legal, and in 1988, the U. S. Supreme Court confirmed that there is no expectation of privacy or ownership once an item is left for garbage pickup. Scraps of seemingly useless information are synergistically related. To protect your privacy, engage in the counterespionage process, which is where you reduce the availability of these puzzle parts. Shred-



ding all waste paper is a major step in the protection process.

Recommendations and tips to protect yourself from trash trawlers:

- Encourage the destruction of all waste paper.
- Purchase the appropriate shredders for your needs.
- Use crosscut shredders for high levels of security.
- If you have a lot of computer paper-work and large volume waste, you need to use a central bulk shredder.

Snoops love it when you save confidential papers in a cardboard box under the desk. Shred them all now! Do *not* entrust wastepaper destruction to paper recycling vendors. Destroy it before recycling. Don't forget: you also need shredders next to copiers and in the home offices of partners and associates.

The big shredder purchasing mistake: Buying just one large shredder for everyone to use. Reason: Not everyone will use it. Why? Some people are too busy to be bothered with shredding documents.

The better decision is to purchase several convenient desk-side shredders. This is one perk or status symbol that has a very positive payback.

Bonus: Some firms actually promote their extensive use of shredders to protect their clients' privacy interests, which is generally not done by most law firms.

Bugs and wiretaps

Although most snooping involves other methods described in this article, electronic surveillance is the most devastating spy trick there is. Very private – and irrefutable – secrets are the target of this attack. A common mistake people make is to say, “Oh, I'm just being paranoid,” when they suspect electronic surveillance.

But think: You would not be suspicious if everything were fine. Something is probably wrong. Here is what your course of action should be:

- Do not discuss your suspicions with others unless they have a real need to know.

- Do not discuss suspicions in the areas you suspect are being tapped.
- Do not attempt a do-it-yourself solution.
- Do not waste money buying spybuster toys.
- Seek professional guidance without delay. Contrary to what you see on television, in the movies or in catalogs, auditing for bugs and wiretaps is intensive work requiring expensive equipment and specialized knowledge. You should expect a professional sweep team to have about \$250,000+ dollars invested in their instrumentation. Their personnel will have extensive experience in security, investigations, electronics and telecommunications.

Hint: Don't bother to check the Yellow Pages for someone to assist you. Contact a corporate security director or professional security organization for a knowledgeable recommendation.

Although this might be more costly initially, it will be worth the effort and save you time and money in the long run.

The drop-by spies

Check and photocopy the credentials and work orders of anyone performing technical work in or around your offices. Double-check the information. Verify that the work was actually requested and was necessary. This includes:

- Telecommunications technicians;
- Computer technicians;
- Office equipment repair persons;
- Paper recyclers;
- Cleaning crews;
- Electricians.

Have someone representing your interests accompany these visitors while on your property. If possible, have them complete their work during normal business hours. Outside contractors and unauthorized company employees should never be allowed to roam unescorted within areas containing sensitive information.

One professional snoop brags openly that any building can be entered at any time, simply by posing as the air

conditioning/heating repairperson. His props include a clipboard with forms and an industrial thermometer. Sometimes he uses a two-way radio and wears a hard hat. If he is challenged, he threatens not to come back for three weeks. Busy schedule, you know. No one wants responsibility for denying this guy entry so they let him in.

Other tips: Check your locks and alarm system regularly. Make sure each component really works. It is surprising how many effective-looking broken locks and alarm sensors are relied upon for protection. If key control has long since gone out of control, tackle the problem now. Change locks and set up a system that will work, and consider using card key access.

If you seek assistance with security matters, be sure to hire consultants who don't also sell products and who will not accept remuneration from the companies that they recommend.

Hacking, cracking and whacking

Espionage aimed specifically at personal computers, laptop computers, networks and remote access ports is rampant. Explain to everyone at your firm that keeps sensitive data in their computers why these security precautions are necessary.

For example: *Enforce the “Protect your laptop at all times” rule.* The replacement cost of a stolen laptop is not just the loss of the machine; it is also the loss of:

- The valuable competitive and confidential data and the time it took for someone to compile the data;
- The time it will take to reconstruct the data;
- The firm's modem telephone numbers; and
- The mainframe passwords probably stored on the drive.

When this information is lost, the law firm is vulnerable to wholesale theft/corruption of mainframe data and sabotage via viruses, Trojan horses, etc.



Bottom-line cost of a stolen laptop: lower profitability and reduced job security for everyone.

Here are some more computer security tips:

- Develop a communal sense of security responsibility.
- Limit physical access to computers by outsiders.
- Limit software access.
- Use quality passwords.
- Secure PC-related materials, such as disks, backups, etc.
- Never leave an active terminal. Always log-off.
- Report suspected intrusions and altered data.
- Remove sensitive data from the PC when not in use.
- Protect memory media, such as floppies and optical disks.
- Copy commands can move sensitive data inadvertently.
- Do not rely on deletion commands. Format disks instead.
- Erase disks before disposal or transfer to another use.
- Disconnect PCs from networks when not in use.
- Computers using phone lines need access protection.
- Do not use unsolicited or borrowed software.
- Backup all data on a regular basis. [Editor's note: Please see Michael Mortimer's articles on painless backups in the January 2009 issue of Plaintiff.]
- Do not use unencrypted 802.11b wireless for sensitive data transmissions.
- Reformat hard drives before retiring old computers.
- Do not discuss system security with anyone you don't know, no matter what they tell you.

Mobile phone leeches

Analog cordless telephones and analog wireless headsets are among the easiest of eavesdropping targets. Contrary to common perception, reception of these conversations is generally crystal clear,

without static or interference. Each and every word can be understood. Switch to models that use Spread Spectrum technology for added security. The new DECT cordless phones also make eavesdropping more difficult.

Monitoring cellular and cordless telephone transmissions is illegal. Do not rely on the laws to protect your privacy, though. They are generally considered unenforceable.

Cell phones switched from analog to digital transmission several years ago. While this improved security greatly, smarter instruments created new privacy problems – spyware.

Here are the usual spyware questions I hear: Can someone:

- Listen in on my calls?
- Listen to my voice mail messages?
- Remotely steal my contacts list?
- Send fake texts from my phone?
- Activate my microphone 24/7?
- Make my phone dial someone else?
- Get a text stating the length of my call?
- Get a text when I use my phone?
- Send me texts using a fake number?
- Get my new phone number when I switch SIM cards?
- Get a text message with the numbers I call and receive?
- Track where I am on a computer map using the phone's GPS?
- Track where I am on a computer map even if my phone lacks GPS?
- Can they do all this from anywhere in the world?
- Record my calls using my phone's own internal memory?
- Trick me into installing spyware by making it look like a game?

The answer to all of these questions: Yes. Although interception of digital cell phone transmissions is difficult, spyware is the great compensator.

Here are some smart cell-phone tips: Don't give anyone the opportunity to plant spyware on your phone. If you suspect spyware is on your phone, changing the SIM card is not a sure-fire cure. Purchase a new phone and SIM card, or

send your current phone to the shop for a complete reloading of its software. Engage the services of a forensic cell-phone examiner if you want to try to track down the culprit.

Here are some general phone tips: Be careful where you speak. The eavesdropper might be standing near you. Be careful who you call. That person might be using an old analog cordless phone or headset, or their wires might be tapped. Consider using encryption if you call the same location often and the stakes are high. Call in on a number that is not answered with a company name or other identifying information. Use first names and code words to identify special projects. Speak in general and uninteresting terms.

Technology traitors

Technological advancements give us many communications conveniences, such as portable telephones, for example. Unfortunately, they also bring new opportunities for the snoops. Here are a few vulnerabilities you need to know about:

- **Answering machines.** Messages left on many home units can be remotely accessed using a simple two or three digit code. Answering machines are easy to hack, especially since most people never change the code that comes preset in new machines. Some units also have a remote listen-in feature. Read your manual carefully!
- **Voicemail.** The business version of an answering machine can also be monitored. Use the longest password possible and change it often.
- **Baby monitors.** In reality, baby monitors are very sensitive room bugs that transmit 24-hours a day. They can be monitored by passing burglars to see if the house is empty and by nosy neighbors. Use baby monitors sparingly. Plug the transmitter into a light timer and keep baby's bedroom door closed.
- **Fax machines I.** Some fax machines use disposable rolls of black film in their



JUNE 2009

printing process. Used rolls contain an exact copy of all faxes received.

- **Fax machines II.** Receiving an after-hours fax transmission is similar to receiving mail without an envelope.

Sensitive messages are routinely read by bored guards or employees who roam around the building generating overtime hours. Solution: use a fax vault or encrypted e-mail instead.

- **Cordless microphones.** Presenters at meetings love using them. Unfortunately, FM analogue wireless microphones transmit crystal-clear audio about a quarter mile. Their transmissions are easily intercepted. Ban them from any meeting to which the general public would not be invited or use systems that transmit digitally/encrypted or via infrared light.

- **Dictation machines.** (Yes, some lawyers still use them.) You may shred the rough drafts, lock up the file copies and send the originals in security sealed envelopes . . . but the dictation tape sits on the secretary's desk waiting to be swapped or reused.

Meeting chameleons

Off-site meetings, conventions, trade shows, seminars, etc., present the snoop with excellent opportunities for infiltration and information collection. Alert your people to the problems. A simple briefing should include the following advisories:

- Off-site meetings are prime targets for snoops.
- Spy methods used may be unethical or illegal.
- Security will control meeting room access (24 hours).
- Electronic eavesdropping audits will be employed.
- Attendees must wear ID badges at all times.
- Never leave your laptop or briefcase unattended.
- Leave written proprietary information with security.
- Proprietary data should remain in the secured area.

- Do not discuss business in public areas.
- Be suspicious of strangers who befriend you.
- Report suspicious activity to security immediately.

Define "Proprietary Information" for your employees. It is information that is not general knowledge and is related to the company's products, methods, customers, plans, etc. It is any information that would cause the loss of profit, or a competitive advantage, if it fell into the wrong hands.

The silver platter

Sometimes we just give information away. How many of the following items apply to someone you know?

- Leaving offices, desks and file cabinets unlocked.
- Leaving confidential paperwork out overnight.
- Posting, sharing, or using simpleton passwords.
- Being listed in directories that seem to provide everything but salary.
- Posting credit card, social security and unlisted phone numbers in Rolodex files left on desktops.
- Answering probing questions over the phone from people you don't really know.
- Discussing sensitive topics with known gossips.

The list gets longer the more you think about it. Solution: Think about how to shorten your list.

Business phone attacks

Feature-rich business phones provide snoops with a variety of powerful eavesdropping options. The phones themselves provide electrical power, built-in microphones and speakers that can serve dual purposes and provide ample hiding space for bugs and taps. Here is a security checklist for classic business phone systems:

- Provide high-level security for telephone rooms.

- Restrict direct dialing into the main telephone switch.

Some dangers of unauthorized phone system access include:

- Complete deprogramming of the switch.
- Secret reprogramming to allow access to free calls and voicemail,
- Executive override features (which allow forced access to busy extensions),
- Bridge tap creation, allowing silent monitoring from other extensions,
- Hands-free intercom, allowing room monitoring from other phones,
- Monitoring of the station message detail recording which maintains a record of all phone calls.

Recommendation: Replace the regular dial-up modem (which connects the switch to the outside line) with a call-back type modem. With this configuration, PBX connections are limited to authorized phone numbers. Here are some additional tips:

- Secure the on-site programming terminals.
- Be sure the system administrator is trustworthy.
- Conduct periodic inspections for wire-taps.
- Conduct surprise audits of the software settings.
- Remove all unused wiring from sensitive areas.
- Make sure that voicemail and switch access passwords are of high quality.

Ask phone system users to report all suspicious calls and voice mail aberrations to the security department immediately. In addition to snooping, these may also be indications of hackers trying to enter to steal services.

Voice over Internet Protocol (VoIP) telephones present a new set of security problems, including:

- Eavesdropping.
- Denial of Service (DoS) attacks.
- Spam over Internet Telephony (SPIT).
- Service theft.
- SIP registration hijacking.
- VoIP directory harvesting.
- Voice Phishing, or Vishing



JUNE 2009

Some tips for securing VoIP business phone systems:

- Install all security measures suggested by the manufacturer. Keep patches current.
- Enterprise systems should augment their systems with security hardware from companies like Sipera or Radware.
- Route calls through a Virtual Private Network (VPN). This is a good solution for inter-company conference calls.

Here are some do it yourself tips for VoIP phone security:

- Set up encrypted conference calls via VoIP using ZFone.
- For conference calling, combine this with an online conference call service that uses Asterisk software.

The participant will need access to the Internet and ZFone software on their computer (lap or desktop) which is free.

- For added privacy use a plug-in headset with microphone.

Treason

Another type of spy – the trusted employee – is one of the most dangerous and hardest to spot. The most likely candidates are employees who may:

- Be disgruntled, possibly related to insufficient raises, promotions, etc.
- Have incurred large debts due to gambling habits, unavoidable personal circumstances or drug use.
- Be involved with labor/management issues.
- Have entrepreneurial personalities.

Here are some tips to protect yourself from the treasonous employee:

- Inspect for eavesdropping devices. These people have the time and opportunity to place and monitor bugs.
- Selectively drop false bits of information and watch to see where they surface.
- Conduct background checks on all new employees and periodic checks on anyone with access to sensitive information.
- Check previous employment carefully.
- Uncover any periods of employment that are not mentioned.
- Verify periods of unemployment.
- If the employee is living beyond his or her means, that may indicate extra income paid by the recipient of your business secrets.

The good news...

Espionage is preventable, and knowing a snoop's tactics is the first step toward obtaining protection. You now have enough knowledge to begin that process confidently.

Kevin D. Murray has been solving electronic eavesdropping, security and counterespionage matters for business and government since 1973. He has authored several articles and books and taught a course, Electronic Eavesdropping Detection & Industrial Espionage, especially prepared for the John Jay College of Criminal Justice in New York. He is a



Murray

Board-Certified Forensic Examiner; a Board Member of the International Association of Professional Security Consultants; a member of the American Society for Industrial Security and is a Board-Certified Protection Professional (CPP). Visit his Web site at <http://www.spybusters.com>.

