



## The Corporate Security Director's Briefing On Portable Telephone & Voice Mail Security Strategies

by Kevin D. Murray - CPP, CFE, CCO, BCFE

Information may be inadvertently leaked when employees discuss company information on their home cordless or cellular phones. Detailed messages left on the voice mail system can also become public knowledge this way.

Basic information security awareness training should be given to any employee who handles confidential information. Some training information you can use follows...

### **Point #1: Portable phones are radio transmitters**

These are very easy eavesdropping targets, and must be used with discretion.

Cellular phone communications can be received by the general public over hundreds of square miles; cordless phones can be received up to a one mile radius of their base units. Monitoring of phone calls has become an underground national pastime. Opportunistic hobbyists are selling their interesting intercepts. Professional spies are targeting specific business calls, and trawling for interesting catches to peddle on a free-lance basis.

Contrary to common perception, reception of these conversations is generally crystal clear, without static or interference. Each and every word can be understood. New techniques in cellular eavesdropping include computer-assisted, *totally automated* monitoring. This allows monitoring of *specific cellular telephones*: every call, 24-hours a day, from cell to cell, without human assistance.

Monitoring portable telephone transmissions is a federal offense. Unfortunately, you cannot rely on this law for privacy, as enforcement is nearly impossible.

### **Point #2: Follow basic portable telephone security and etiquette rules.**

Sometimes regular use of a portable phone is unavoidable, so think ahead...

- Avoid the use of portable phones when your topic of conversation is business information.
- Set aside an incoming number for portable phone calls. That way the person who answers will automatically know that the conversation will not be secure or private.
- Answer this number with a simple hello. Don't give listeners a reason to keep listening.
- Remind the called party that they are *on-the-air*.
- Your reminder should trigger the following security etiquette rules:
  - Be discreet.
  - Use first names only.
  - Use code names for projects, companies and places.
  - Avoid discussing information in specific terms.

**Point #3: The combination of portable phones and voice mail is hazardous.**

When you retrieve voice mail via portable phones, eavesdroppers hear your private messages. They also hear your password tones. Knowing these tones, they can access your new messages all by themselves. If you must listen to your voice mail over a portable phone, remember...

- Your password becomes public every time you call in. Change it often.
- Stop listening to a message *as soon* as you realize its content is sensitive.
- When leaving a voice mail message, alert the listener if *your* message is sensitive.

**Point #4: Other communications are routinely monitored by hobbyists and spies too.**

- Commercial airline telephone calls - including your credit card data.
- Ocean liner telephone calls - including your credit card data.
- Train telephone calls - including your credit card data.
- Long distance calls via satellite.
- Long distance calls sent via microwave radio links.
- Home baby monitors. Eavesdroppers hear everything in the area, 24-hours a day.

**Point #5: Do what snoops hate.**

- When buying a home cordless telephone, purchase a model which operates in the **900 MHz** frequency range and transmits using **digital spread spectrum** technology. These telephones are – *for all practical purposes* – eavesdropper proof.
- When buying a mobile phone, purchase one of the new PCS phones which operate in the **1.9 GHz** frequency range. They use digital modulation exclusively. Some systems also provide automatic encryption. They may look and act like, the common **800 MHz** cellular phones, but these are very secure.
- Keep your calls short, low-profile and uninteresting.
- Do not let your portable phone calling become predictable.  
(Like retrieving voice mail on the way to work each day.)
- Consider adding voice scrambling capabilities to your current cellular phones. Today's technology makes this low cost, effective and easy to use. Many voice scramblers are easy to attach, and are small enough to serve multiple functions: office, cell, home, and hotel phones. Contact us for a full list of manufacturers.

**Point #6: Know the warning signs of voice mail hacking, eavesdropping and espionage.**

- Repeated access attempts with wrong passwords.
- User reports of lost or undelivered messages.
- Unusually high voice mail activity after normal business hours.
- User reports of being *locked out* of their voice mailboxes.
- Unusual out-dialing patterns.
- User reports of possible wiretapping due to leaks from phone calls.
- Graffiti greetings and bogus broadcasts.
- A massive increase in the telephone bill.
- A large loss of voice mail storage capacity.
- Authorization codes coming in from two different places simultaneously.
- Reports of frequent hang-ups, increased requests for outside lines, etc.
- Callers /visitors posing as telephone techs asking for passwords and codes.

**Point #7: Know how to create effective - and easy to remember - passwords.**

- Use two to three words, mixed case, separated by numbers or punctuation.
  - Computer: **My/DoG+roVer** - is superior to **MY/DOG** - is superior to **ROVER**.
  - Voice Mail: **ME2YOU, 4EVER, 182MUCH, 24TEA...**
- Do not reveal, loan, or write passwords down.
- Do not use the same password for computer and voice mail.
- Employ software which forces a change of password on a regular basis.

**Point #8: Test for Information Leaks and Electronic Eavesdropping.**

Suspected information leaks can be verified and tracked to their source. Conduct each one of these tests using a different piece of information each time. The type of espionage / eavesdropping being used will be revealed by which tidbit of leaked information surfaces.

1. Selectively salt one-on-one conversations with false bits of information. One tidbit per person being tested. This reveals loose-lips and false friends.
2. Prearrange a telephone conversation with a trusted party. Discuss one interesting (but false) item. If word gets out, suspect a wiretap.
3. Simulate one side of a phone call. (Do not really use the phone.) Discuss something which is likely to get back to you. This test detects room bugs.
4. Create *interesting* memos to leave on the desk overnight. When word gets back you will know you had an intruder, and on which night.
5. Create *interesting* memos each night to leave crumpled or torn in half in the trash can. This detects surveillance via *garbage archeology*. A very common spy trick.

**ABOUT THE AUTHOR...**

Kevin D. Murray - BCFE, CPP, CFE, CCO has been solving electronic eavesdropping, security and counterespionage matters for business and government since 1973.

His many written works include: the *Electronic Eavesdropping Detection* chapter of **The Protection of Assets Manual**; articles for Security Management magazine; and *Electronic Eavesdropping Detection and Industrial Espionage - The Missing Business School Courses*.

His course - *Electronic Eavesdropping Detection & Industrial Espionage* was taught at John Jay College of Criminal Justice in New York.

Mr. Murray is: a Board Member the International Association of Professional Security Consultants, is on the Advisory Board of the Business Espionage Controls & Countermeasures Association; is a Board Certified Forensic Examiner; and is a member of the American Society for Industrial Security.

He may be reached at 908-832-7900, P.O. Box 668, Oldwick, NJ 08858 (USA), or via the Murray Associates web site at: [www.spybusters.com](http://www.spybusters.com)

Murray Associates services are available throughout North America and selected foreign countries.