Anyone can use even an ordinary mobile phone as a microphone (or cameras) by covertly dialing out; for example, one can call a recording device at a listening station and then simply place the phone in a pocket or briefcase before entering a conference room. However, my friend and colleague Chey Cobb, CISSP recently she pointed out a device from Nokia that is unabashedly being advertised as a “Spy Phone” because of additional features that threaten corporate security.

On <http://wirelessimports.com/ProductDetail.asp?ProductID=347> we read about the $1800 device that works like a normal mobile phone but also allows the owner to program a special phone number that turns the device into a transmission device under remote control. In addition, the phone can be programmed for silent operation: “By a simple press of a button, a seemingly standard cell phone device switches into a mode in which it seems to be turned off. However, in this deceitful mode the phone will automatically answer incoming calls, without any visual or audio indications whatsoever. . . . A well placed bug phone can be activated on demand from any remote location (even out of another country). Such phones can also prove valuable in business negotiations. The spy phone owner leaves the meeting room, (claiming a restroom break, for instance), calls the spy phone and listens to the ongoing conversation. On return the owners negotiating positions may change dramatically.”

It makes more sense than ever to ban mobile phones from any meeting that requires high security.

David Bennahum wrote an interesting article in December 2003 about these questions and pointed out that businesses outside the USA are turning to cell-phone jamming devices (illegal in the USA) to block mobile phone communications in a secured area. Bennahum writes, “According to the FCC, cell-phone jammers should remain illegal. Since commercial enterprises have purchased the rights to the spectrum, the argument goes, jamming their signals is a kind of property theft.” Seems to me there would be obvious benefits in allowing movie houses, theaters, concert halls, museums, places of worship and secured meeting locations to suppress such traffic as long as the interference were clearly posted. No one would be forced to enter the location if they did not agree with the ban, and I’m sure there would be some institutions catering to those who actually _like_ sitting next to someone talking on a cell phone in the middle of a quiet passage at a concert.

Bennahum mentioned another option – this one quite legal even in the USA: cell-phone detectors such as the Cellular Activity Analyzer from NetLine <http://www.netline.co.il/Netline/CAAdetector.htm>. This hand-held computer lets you spot unauthorized mobile phones in your meeting place so that you act accordingly.

Finally, one can create a Faraday cage <http://en.wikipedia.org/wiki/Faraday_cage> that blocks radio waves by lining the secured facility with appropriate materials such as copper
mesh or, more recently, metal-impregnated wood. A high-security version of such a room is called a SCIF (Sensitive Compartmented Information Facility) in US military security jargon.

In my next column, I’ll briefly look at some new research about a different kind of security: the possible health effects of using cell phones.

* * *

For further reading


Faraday Cage

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2005 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.