

Phony Pictures and Songs

Time and time again stories come up about "Cell Phone Viruses" or "Mobile Threats." These are generally not fabricated, but they *are* currently blown way out of proportion. The fact is that these threats will increase in numbers and severity.



Randy Abrams

Currently the features of most mobile devices, combined with a little bit of knowledge, will protect you from all of the cell phone viruses and other mobile threats. If you refuse to learn enough to protect yourself from what is out there now, then you will become a victim at some point, regardless of what security software you use. No seat belt in the world can allow you to drive safely without steering, and no security software can allow you to safely operate a multi-function computer without a little knowledge. Cell phones, by and large, have become multi-function computers.

There are two primary methods used to infect cell phones and PDAs. One avenue of attack is to exploit wireless technologies, such as "Bluetooth." The second avenue of attack is social engineering... tricking you. Ignorance is to a social engineering attack what gasoline is to a fire.

Bluetooth is a technology that allows you to use a wireless headset, synch your PDA to a laptop and perform other activities without the need to physically connect one device to another. Most cell phones today are Bluetooth enabled. To connect a device, such as a headset, to a cell phone you need to put the cell phone in "discovery mode." Discovery mode is a feature of Bluetooth that allows the phone to be seen by the headset so you can "pair" the two devices. A cell phone in discovery mode can also accept connections from other devices, such as other infected cell phones. Once you have paired your cell phone with your headset, the Bluetooth feature — called discovery mode — needs to be turned off. Your phone and headset will still work together, but you will eliminate an entire attack vector.

A new cell phone virus was recently discovered. This virus sends attachments that claim to be pictures or songs. When a user opens the attachment on their cell phone they are prompted to install the virus. This is where an ounce of education becomes a pound of prevention. If you know that pictures and sounds are viewed and listened to, but not installed, you should know not to install the virus. If you lack this basic understanding then you will likely install the virus.

One day security software on phones will be a requirement. Today, proper configuration and basic education are sufficient defenses.

If you wish to submit questions or comments to "Ask the Expert" please feel free to send them to askeset@eset.com.



Randy Abrams is Director of Technical Education for ESET

AskESET@eset.com

www.eset.com

610 West Ash Street, Suite 1900

San Diego, CA 92101 • 866.496-ESET

ESET paid for this space and is solely responsible for its content.