

# Beware of cellphone snoops



**New malware version can activate microphones on mobile devices, posing a threat that experts say will increase significantly in coming months.**

By Jeff Cox  
May 23 2007

NEW YORK (CNNMoney.com) -- The nightmare begins early in the morning with an innocuous-looking e-mail on your mobile phone instructing you to check a specific Web site for information about repairing your credit score.

You go to the Web site, decide it's just another piece of spam, and move on through your normal daily routine. There's the check-by-phone payment of your credit card bill, a high-level confidential business teleconference discussing sensitive company information, and finally arranging a dinner with that cute co-worker you don't want your boyfriend to know about.

Little do you know that all the while, someone else has been watching - and listening. Welcome to the brave new world of smartphone spying, where dark-souled hackers with bad intentions use readily available technology to track every move you make with your cell phone, Bluetooth or personal digital assistant.

"You're going to see a dramatic proliferation of threats," said John Vigna, CEO at SMobile, a Columbus, Ohio-based mobile security provider. "More and more devices are synchronizing, more and more people are loading data and corporate information, and malware attacks are going to go through the roof."

From identity thieves to corporate raiders to jealous boyfriends, the world of smartphone spying is open to anyone with a rudimentary knowledge of digital technology and the hundred bucks or so it takes to buy eavesdropping software on the Internet.

## **A threat with many facets**

While adware, spyware and other such programs have been around for years, programs known as snoopware are emerging as a new threat in targeting the proliferation of smartphones thrust into the digital marketplace.

While the threat so far has been largely confined to Europe and Asia, where use of mobile devices is generally more advanced than other countries, experts agree it will be the next big thing in computer menaces to hit the United States.

About 400 or so malicious strains of snoopware are available now through the dark portals of cyberspace, but that number is expected to swell to about 1,000 by the end of 2007. This as Americans will buy about 81 million mobile communication devices this year, allowing them to send information to desktop and laptop computers - as well as to hungry eyes with a thirst for highly personal information.

SMobile executives say the past five months have seen a decided proliferation of new threats to smartphones that go beyond common dialer trojan viruses and are more sophisticated and geared toward stealing more valuable personal information.

Prior to this year, the main criminal use for malicious snoopware in cell phones was to swipe wireless provider account data, and thus steal telephone minutes from the user. But as technology has grown, so have the multitude of odious purposes for which snoopware can be used.

Almost always installed without the user's knowledge, snoopware can be introduced in a variety of ways - most commonly through short message service (SMS) or multimedia messaging service (MMS) sent between mobile phones. Information taken is transmitted to the user at the other end who triggered the snoopware infiltration for download and perusal.

While there are multiple legitimate, or at least legal, uses for the various snoopware programs available - dotting parents and suspicious company managers, most notably - bad intentions abound when it comes to the newfangled nefarious systems.  
Internet crime gets personal

"New malware is capable of monitoring activities on mobile devices, including phone calls, messages, and e-mails, and we view it as an invasion of users' privacy," said Neil Book, president of SMOBILE.

New snoopware can activate a microphone or cameraphone even if the device isn't being used at the time. That means that the user at the other end can listen in on conversations and extract all types of personal and corporate information, or even activate a camera that can survey the activities of the owner. The mobile-targeting snoopware also offers a view of contact lists, text messages, e-mails, passwords - you name it.

Even government and the military could be targeted, though an attack there would be more difficult due to the complex anti-virus systems employed by government communication devices. Still, it wouldn't be impossible, and it's something about which experts have raised caution.

"That's where it becomes very interesting and very dangerous, especially when it comes to government workers at secure locations," Book said.

### **Solutions on the horizon**

Companies like SMOBILE and Symantec (Charts) provide security products that include firewalls and anti-virus and anti-spam filters to protect devices under attack. Such products also often are equipped with provisions that allow security monitors to remotely shut down an entire Internet network under attack until the problem is fixed.

Paul Henry, a consultant with Secure Computing, said the threat of attacks on mobile devices in the U.S. will grow as people here use the devices more and more in their daily lives and catch up with what other countries are doing.

"In Malaysia, people use on a regular basis what's referred to as a mobile wallet that allows them to pay their bills through their cell phones. In Kuala Lumpur, someone I was with bought a Coke from a Coke machine using his cell phone," Henry said.

"When you have the ability to pay bills via cellphone, that makes it even a more valuable target for bad guys."

Symantec, maker of Norton Antivirus software, is rolling out its own mobile security solution May 29.

Khoi Nguyen, a mobile security expert at Symantec, said the company's product will automatically put unsolicited SMS messages in a spam folder and delete them. The product also will protect all confidential files on the mobile devices through password-protected encryption.

Symantec considers the attacks against smart phones as a major threat to domestic computer security.

"We definitely view the smartphone as the next new destination for hackers, especially as the smartphones have become minicomputers in a sense," he said. "It's a natural next destination for hackers."