

## **Do Hackers Pose a Threat To Smart Phones?**

By JOSEPH DE AVILA  
*May 27, 2008; Page D1*

<http://online.wsj.com/article/SB121184343416921215.html>

In addition to placing calls, smart phones pack many of the functions found on computers: Internet, email, multimedia programs and even word-processing and spreadsheet capabilities. But, like computers, smart phones are vulnerable to viruses and other types of malicious software.

By all accounts, the risk of a smart-phone attack is low. But as people start using the devices for more sensitive tasks -- handling customer data and transferring corporate files -- security experts say smart phones may become more vulnerable to attack. So companies are working to protect both the devices and the networks behind them.

At the corporate level, IT departments are cracking down, mainly by limiting access these devices have to internal networks. And on the consumer front, computer-security companies are selling antivirus software that scans for rogue applications.

"They are real but rare" threats, says Jan Volzke, head of world-wide mobile marketing for Santa Clara, Calif., based McAfee Inc., which sells computer-security software.

Smart phones are used mainly by professionals who want to access corporate email and send documents on-the-go. But the market for these high-end devices is growing. Last year, Apple Inc. introduced the iPhone, a consumer-friendly device that appeals to students and others who like the touch screen and multimedia features. Market-research company NPD Group estimates that smart phones comprised 17% of all mobile-phone sales in the first quarter, an increase of 10 percentage points since the same period a year ago.

We've gotten to the point where smart phones are almost as sophisticated as desktop computers, says Ken Silva, chief technology officer for VeriSign Inc. So users should be just as protective of their smart phone as their home computer, he says.

So far, there are about 300 to 500 known versions of malicious software, or malware, written for phones -- a small number compared to those that attack personal computers. Malware infects phones through email attachments and text messages that ask users to

download an application. They also can be delivered over wireless connections using Bluetooth technology.

Still, one reason why malware hasn't gained traction is a lack of a dominant operating system for attacker to focus on, says Nick Magliato, chief executive for Trust Digital, a security vendor. "It's very inefficient to write a virus for phones."

The majority of mobile malware has been written for phones using the Symbian operating system, which is found in about 65% of the global smart-phone market, according to ABI Research. Phones that run Symbian include some models made by Nokia, Samsung and Sony Ericsson.

Security experts at Symbian Ltd. monitor networks for potential malware outbreaks but haven't identified any serious threats so far, says David Wood, executive vice president of research. But, he adds, "we can never say never."

Another 11% of smart phones use the Windows Mobile operating system, which is used by some models made by Samsung and Palm. Phones on other platforms, such as Research In Motion Ltd.'s BlackBerry and Apple's iPhone, haven't had any serious malware outbreaks, says David Frazer, director of technology and services for security vendor F-Secure Corp.

Regardless of the operating system, the greatest risk of infection comes from third-party applications, such as games and ringtones, which give users an easy way to customize their phones. But people should exercise caution and only download software from trusted sources, says John Traynor, senior director of product marketing for Microsoft Corp.

Some types of malware can disable all the applications on a phone, including the ability to make calls, says Mark Komisky, chief executive for Bluefire Security Technologies, which makes antivirus software for smart phones. Another type of malware is so-called "snoopware," which was originally sold in Asia as a spouse-monitoring tool, says Paul Miller, managing director for mobile security at Symantec Corp. Now attackers see this application as a way to eavesdrop on conversations, intercept text messages or peek at call logs.

Several years ago, Symbian started requiring third-party software vendors to provide a "digital signature" when writing applications, Mr. Wood says. If the software is signed, Symbian can track which developer wrote the malware. The Windows Mobile operating system also uses digital signatures for software written by third-party developers.

Beyond downloading software only from trusted companies, individuals who own personal smart phones can protect themselves with antivirus software. Symantec and McAfee both offer programs that typically cost \$30 for a one-year consumer subscription. Bluefire Security offers antivirus software for businesses and plans to release a consumer product next month.

Still, the majority of smart phones are connected to corporate networks, putting the onus on IT departments to protect the work force.

Rob Israel, chief information officer for John C. Lincoln Health Network in Phoenix, is in charge of guarding the data flowing through the company's network of hospitals and physician practices that employs about 4,400 people. A year ago Mr. Israel installed a system that prevented employees from uploading or downloading files to the company's computer network.

"Before that, it was the Wild West," and anyone could bring in any device and upload files to their computers, Mr. Israel says. "This was a real security hole."

Chief among his concerns was that an infected phone would transfer malware to the company's network. Mr. Israel acknowledges that chances are slim that a phone could get infected with malware, but says he doesn't want to take any chances.

For now, though, the greatest threat to corporate security is the loss of a smart phone -- especially one that's crammed with sensitive personal or corporate data.

Miriam Neal, vice president of information systems for South Western Federal Credit Union based in La Habra, Calif., says she worries mostly about lost smart phones. "We are a financial institution, and we need to protect the privacy of our members," Ms. Neal says.

Many companies are investing in technologies that will wipe clean all the information stored on a lost or stolen phone so that the data can't be used for criminal purposes, says Paul Roberts, a senior analyst with the 451 Group, a technology-research firm.

**Write to** Joseph De Avila at [joseph.deavila@wsj.com](mailto:joseph.deavila@wsj.com)