

**MATTRESSFIRM**

Can't wait to sleep great?
Get Free & Fast Delivery* to your door.

[Home](#) > [Smart Home](#)

'Bluejacking,' 'bluesnarfing' and other mobile woes

Study tells us exactly what we don't want to hear: we aren't nearly as proactive as we should be when it comes to protecting ourselves.

**Don Reisinger**

Aug. 23, 2007 10:10 a.m. PT

3 min read





Keep your mobile devices safe!

Palm

In a world where security cognizance has quickly become one of the most important aspects of any person's day, a study has come out that tells us exactly what we don't want to hear: we aren't nearly as proactive as we should be when it comes to protecting ourselves.

According to a study performed by research firm InsightExpress, 73 percent of mobile device users are either unaware or not cognizant of the security issues that could plague their cell phones, Bluetooth-equipped notebooks and even their digital audio players. Believe it or not, you're almost as likely to run malicious code on one of your mobile devices as you are on your PC.

So what does all of this mean? It means it's time you brush up on your mobile security lingo and get to know your friends over at McAfee and Norton because security software will soon begin to take over (and slow down) your favorite mobile gadget.

Much like the early '90s when the public was largely ignorant about the possibility of security issues on home computers, we are currently ignorant about security threats that could plague our mobile devices. And while a few software solutions have been released that promise a modicum of safety, we're not even close to where we should be.

Have you ever heard of the terms "bluejacking" or "bluesnarfing"? If not, you're not alone. Bluejacking is a technique in which nearby users try to push through malicious data via Bluetooth. Bluesnarfing follows suit and aims at copying the contents of your device. And while it may seem like these terms have nothing to do with the daily commute or trip to the coffee shop, think again. Every day, thousands of computers, smart phones, and any other Bluetooth-equipped device that the hacker believes may be holding valuable information, is put at risk. And as Bluetooth becomes more ubiquitous, so will mobile security threats.

Sad as it is, we're just not prepared to face mobile dangers. If we've learned anything over the past decade, we now know that the people who create malware and other harmful code are always one step ahead of us. When it comes to security, the bad guys are years ahead.

Companies like McAfee and Norton have come out with programs that claim to protect your device, but they often leave the house. And while I can't argue with the implementation. Today, the vast majority of security solutions are only available to government and enterprise users, leaving you and me out to dry. Sure, there are some solutions that are available to consumers, but each program's ability to detect and secure your device against an attack is abysmal.

Malicious hackers have gone out of their way to make a business model out of annoying and upsetting people. And what first began as a "hey, look what I can do" practice, has now become a profitable business. Mobile platforms are just the next logical place for malicious hackers to establish themselves; home

computing is becoming more difficult to exploit and with a short list of security solutions on the mobile platform, there is very little anyone can do to stop them.

But perhaps this study did us all some good. As a person who carries a Treo and iPhone around town without any security software installed, it's good for me to hear that I'm not nearly as safe as I would like to think. And while it would be nice to have added security, I won't be downloading junk software that only takes up room and slows my device down. But with any luck at all, these security companies will stop wasting time on products that do nothing and get to work on real--effective--solutions.

Smart Home Guides

Smart Home



Advertisement



Why You Can Trust CNET

Our advice is [expert-vetted](#) and based on independent research, analysis and hands-on testing from our team of Certified Sleep Coaches. If you buy through our links, we may get a commission. [How we test mattresses](#)