PERSONAL FINANCE

Cell ... Savings Plans Get Efficient

GADGETS

Bluetooth May Put You at Risk of Getting 'Snarfed'

By Jeremy Wagstaff

If you spot someone tailgating you on the road or standing next to you wearing a backpack, then watch out: You may have been "snarfed." All the data on your cellphone, including addresses, calendars, whom you called and who called you, may now be in that person's computer.

Many cellphones use Bluetooth technology, which allows them to communicate wirelessly with other Bluetooth-equipped devices—computers, personal-digital assistants and other cellphones. This means you don't need a cable, for example, to synchronize the address books on your laptop and your cellphone. It is convenient, but that makes it possible for someone to steal your data, or even hijack your cellphone for their own purposes.

Last year, London security consultant AL Digital spotted flaws in the way some Bluetooth cellphones swapped data with one another—flaws that could be used to gain unauthorized access to everything stored on that phone without the user ever knowing. AL Digital's Adam Laurie, who discovered the problem, shared his findings with cellphone makers and with the public (leaving out the detail that might allow ne'er-do-wells to copy his experiments at street level). He termed the trick Bluesnarfing.

Not a lot has happened since then. **Nokia** Corp., the market leader in the cellphone industry, acknowledges the flaw but says in an e-mail response to questions that it is "not aware of any attacks against Bluetooth-enabled phones." Sony Ericsson, a joint venture of **Telefon AB L.M. Ericsson** and **Sony** Corp., didn't reply to an e-mail. Even those highlighting the danger say they haven't heard of specific attacks.

Still, these attacks—also known as Bluejacking—nevertheless are possible. Mr. Laurie cites a scenario in which paparazzi could steal celebrity data. He says he was able, with permission, to snarf from a friend's phone details of her company's shops, door codes and safe combinations. "There's any number of angles you can look at, and they are all bad as far as I can see," he says.

Martin Herfurt, a 27-year-old German student at Salzburg's Research Forschungsgesellschaft, last month set up a laptop at a technology trade fair in Hanover, Germany, and ran a snarf attack. He found nearly 100 cellphones from which he could have stolen data, sent text messages or even made calls. He has published his findings to prove that this kind of thing can be done easily.

How does it work? The attacker can use a Bluetooth-enabled laptop to discover other Bluetooth gadgets within range. Anything with Bluetooth activated and set to "discoverable" will show up, usually identified by its default device name. Being "discoverable" means your gadget is visible to anyone searching, but even if it isn't, an attacker still can find it, using software freely available on the Internet. The attacker then can use more software to take, delete, change or add data.

So what is a consumer to do? Turn off Bluetooth on your phone unless you really need it to communicate with your other gadgets. In most cases, phones that have Bluetooth will have prominently displayed the fact on the box the phone came in, or you can expect to find "Bluetooth" in the index of your phone's manual. Otherwise, the Bluetooth settings can usually be found in the "Communications" or "Connections" menu on your phone. More importantly, there shouldn't be anything on your phone that you don't want someone else to have.