PRINT CLOSE

jungle

| **FEATURES** | David Wallace |

## Chicken Soup for the Cell

**Phones and PDAs are the latest victims of the hacker's flu. Learn what preventive measures you should take to keep your gadgets healthy.**

You probably didn't realize it, but Paris Hilton did you a huge favor when she unwittingly spilled the contents of her T-Mobile Sidekick several months ago. Although not known for her public service, the hotel heiress highlighted one of the biggest security mistakes people make with their mobile phones, PDAs, and other devices. She used a lame security question—"What is your dog's name?"—to which any enterprising hacker can find the answer (it was Tinkerbell).

Although Boston-area data security consultant and Sidekick owner Chris Wysopal doesn't have a dog whose name is known to global celeb-watchers—or a nasty sex video, for that matter—he isn't safe from hackers either. That's because T-Mobile stores customers' personal data (along with security questions and answers) on Web-accessible servers that can be hacked from anywhere in the world.

"It's not as if someone has to have physical access to your device to get hold of your information," says Wysopal. "There are so many devices and types of networks that there won't be a traditional worm that goes around killing everyone's phone the way it can happen on a PC." Over the last few years, hacking has changed from an annoyance to a criminal operation, and any smartphone or PDA is a likely target. Crooks go where the juicy data is.

Hackers, for instance, are increasingly spamming phones and PDAs with unwanted Bluetooth data or instant messages—or taking control of account information and sticking you with the bill. Others are stealing or intercepting sensitive company as well as credit card information.

As a rule, new electronic gadgets are often the most likely targets for abuse, because consumers buy them for the "coolness factor" but rarely spend time learning their security settings. Also,

providers and corporate users may not have policies about what data may or may not be stored on the device.

Even the ubiquitous BlackBerry—designed by Research in Motion to securely transfer data using the same protection companies choose for email sent from computers—is vulnerable to attack, since the messages need to be handed off from network to network until they reach their destination.

"We've been in such a rush to send email to handheld devices or connect the Internet to a phone that the security wasn't properly architected," says Karl Feilder, a wireless industry veteran and CEO of Identum, a London-based software company. "And we are pushing ever-more-personal data off the desktop and into mobile devices—whether it's credit card data or conversations with your husband or lover."

So who are you going to call and what are you going to do to prevent your cell phone or PDA from coming down with the flu? One solution is personal control of data, argues Feilder. Because encryption programs built into devices can be switched off remotely by hackers unbeknownst to the owner, users need additional protection that works as easily as a one-time-install anti-virus program with no further passwords or delays. Identum's flagship product, Private Post, installs itself in a single email to authenticate data and the user, creating another layer of security.

PDASecure—and other programs like it—will add a similar layer of encryption to PDAs running on Windows CE, BlackBerry, or Symbian operating systems. If someone tries to get their digital hands on your information, the program will automatically trash it.

Criminals, though, seem to stay one step ahead of even the most vigilant gadget addict. They have turned to wireless Bluetooth hacking, known as Bluesnarfing—sending messages to unsuspecting users or capturing data such as phonebooks or the device's account details. You can still take steps to protect yourself. For instance, be sure that the Bluetooth device is not left in open or "discoverable" mode: Use the feature only when linking with a known Bluetooth device.

A little digital reconnaissance may also help prevent future break-ins of your personal data. Log on to www.bluejackq.com, where hackers regularly brag about their exploits and proudly report a security flaw. Or go to www.bluestum bler.org, which posts known attacks and vulnerable phones and devices.

The future of the fight against phone and PDA hackers looks brighter. A new Nokia phone is outfitted with a sensor that lights up to tell users when encryption is on, says Identum's Feilder. That way you will know whether you're yakking to the world or

texting securely. Maybe then, you can finally discuss with impunity those hair implants, drunken misadventures, and insufferable bosses. •

**Flight to Safety: The 5-Step Plan**

1. Ask your service provider where data is stored. Find out if it's backed up on a server.

2. Avoid the basic security questions supplied by providers. Create your own security "challenge" question with data that only you know.

3. Use password protection to lock the machine in case it's lost or stolen. Open systems can use programs like PDA Secure, which wipes out your data if someone tries to crack the device without the right passwords.

4. Clean your device thoroughly before selling or exchanging it. Like a PC's hard drive, your phone or PDA can be restored even after you delete entries.

5. Don't put any data on your phone or in a remotely typed email that you wouldn't want someone else to read. Like the perennial advice of treating email as a postcard, the same is true for remote email, instant messages, or even text messages.

**Hints Your BlackBerry Has Sprung a Leak**

- Joan Rivers's butt suddenly, and inexplicably, appears on your cell phone welcome screen.
- Your Coldplay ring tone has morphed into Menudo.
- You begin receiving constant text entreaties with subject lines like, "Intercontinental drugstore with nonpricey medications from Shondra Fox."
- You get home and find a stranger wooing your sweetie with her favorite flowers and wine.