



## Risky Business

Corporations invest in elaborate systems to protect their computer networks from savvy invaders, yet security sleuths at RocketReady know that low-tech cons are the most dangerous. What can be done? / By Paul Abercrombie / Photography by Mark Wagoner

**C**OMPANIES SPEND BILLIONS OF DOLLARS every year on computer security systems to protect their corporate secrets. Yet it is people, not computers, that are the weakest link in corporate security programs.

And that's where Todd Snapp comes in. Snapp isn't a real con artist, but he does lie, wheedle, and cajole for a living. A legitimate living, at that.

On one recent morning, a benign-sounding Snapp was working the phone, his voice friendly and apologetic. He's trying his best to trick an employee of a small computer-consulting firm into spilling important company secrets.

Snapp's inviting chit-chat works like a charm. A few minutes later, he's scored a fresh user name and password, which gives him access to the company's private network. That's not all: Snapp gets access to all of the consulting company's client networks, as well.

And Snapp gets one final thing: an apology from the unsuspecting computer consultant for any inconvenience.

Formerly the head engineer in charge of network security for a telecom behemoth, Snapp now heads Tampa-based RocketReady, a business security firm that specializes in finding human, as opposed to technical, security weaknesses. The information that Snapp and his firm are able to get from client companies big

and small—often in just a few hours—would make any CEO shudder.

"It's truly scary how easy it is to get even the most sensitive company information, and all without computer hacking," says Snapp. "It can feel like shooting fish in a barrel."

Notorious ex-hacker Kevin Mitnick and other security experts warn that, as companies focus on whiz-bang computer protection, they often neglect educating employees about the perils of low-tech con artistry. Rich Mogull, research director for information security and risk at global research firm Gartner Inc., predicts that such old-fashioned swindles will be "the single greatest security risk in the decade ahead." Well-meaning employees often inadvertently help hackers pilfer company secrets, including information about

**Well-meaning employees often inadvertently help hackers pilfer secrets, including information about products, customers, and pricing.**

### Hackers, Away!

*Online safeguards*  
**snopes.com** / debunks e-mail and online scams  
**networksolutions.com/whois** / tells who owns a particular domain name  
**consumer.gov/idtheft** has facts on identity theft; run by the Federal Trade Commission  
**phishregistry.org** / has information on fraudulent Web sites and e-mail "phishing" scams  
**google.com/support/webmasters/bin/topic.py?topic=8459** / allows you to remove cached online information in an effort to keep it out of the hands of hackers  
**cissponline.com/name-news-article-sid-2.html** social-engineering article

customers, products in development, pricing, and other data.

Security experts point to the much-publicized hacking of hotel heiress Paris Hilton's high-tech wireless ►

phone last year as a cautionary example of the more serious security challenges that companies face. In this case, the culprits used only a low-tech phone call—to a T-Mobile carrier help-desk technician—to gain access to a trove of personal data.

Prominent people and companies seem to be likely targets for such crimes, but smaller companies are frequently victims. “Small companies are often more vulnerable to cons because they think, ‘We’re small so nobody would want to bother us,’” says corporate espionage expert Ira Winkler, the author of *Spies Among Us*.

Human security flaws most often are exploited by so-called social engineering—tricking people into giving away sensitive information—typically over the telephone. RocketReady’s team members start by researching a client online, familiarizing themselves with company products and services, even company lingo. Online chat rooms and bulletin boards yield more personal information about, say, which employees enjoy sport fishing or have a son or daughter who’s a star soccer player.

With a detailed dossier on a company and its employees, the RocketReady team is prepared to call or send e-mail to employees, posing as clients or colleagues who need a forgotten password, a user name “updated,” or a lost document e-mailed or faxed. Doctored caller ID and phony Web sites contribute to RocketReady’s credibility.

RocketReady employees even have posed as headhunters and representatives of rival companies looking for new talent. “A prospective employee wants to impress you, so they’ll tell you anything and everything,” Snapp says.

Snapp has hoodwinked folks in human resources into adding him to a company’s employee roster, treating him like a real employee, and assigning him company voice-mail and computer-network accounts. And with passwords comes access to secure networks—and to just about all a company’s secrets.

Maybe scarier still is that even when employees smell a scam, they rarely tattle. “No one wants to admit they’ve

People can be susceptible on the road. Hectic itineraries may cause travelers to let their guard down. That gabby passenger could be a fellow road warrior just making conversation—or a competitor angling for company information.

been duped,” Snapp says. “I would say it goes double for CEOs. They often feel like they are not targeted. I am here to tell you that they are, and they are vulnerable.”

Employees may be most susceptible to social engineering on the road. Hectic itineraries and the hardships of travel can cause people to let down their guard. Remember, the gabby passenger sitting next to you on a flight could be a fellow road warrior just making conversation, or he could be a competitor angling for information.

Even seemingly mundane activities aboard an airplane or train, such as chatting on a cell phone, typing on a laptop, or checking your schedule on your PDA, can be risky. The guy squeezed into the seat next to you could be peeking, or “shoulder surfing,” at the e-mail you’re composing to colleagues. A fellow passenger might be tapping into your PDA, thanks to your handy wireless modem.

Flash memory drives no bigger than a stick of chewing gum and other super-portable data-storage gizmos make life easier for businesspeople on the go—and for those who want to prey on them. Indeed, consider that stolen U.S. military flash drives containing information about intelligence-gathering methods and about al-Qaida and the Taliban recently showed up for sale at bazaars in Afghanistan.

Plugging human security holes in a company is not easy. Entrenched habits and a corporate culture that emphasizes service with a smile can work ►

against attempts to teach employees to be skeptical.

Companies such as RocketReady train client employees to watch for evidence that they're in a spy's sights, incorporating these lessons in employee-training programs and reinforcing them through follow-up exercises, some of which RocketReady offers online. The company often operates along with sister company RavenEye, which tests for vulnerability in computer networks. In tandem, the two outfits

provide clients with full-scale low- and high-tech screenings.

Still, security experts such as Winkler caution that effective defense against malicious social engineering can't be accomplished merely by rewriting the employee handbook or offering occasional refresher courses in security awareness. "The only way to protect your company is to change your corporate culture," Winkler says. "That takes long-term commitment. No single security assessment and awareness program or

Web-based training program can do that."

That said, Winkler offers a few pointers from *Spies Among Us* for making sure your company avoids becoming a victim of social engineering:

**Protect Yourself During Travel**

- ▶ Realize that fellow passengers can listen to your conversations and look over your shoulder. Remember that people behind you might be able to see your materials.
- ▶ Turn off your wireless functions when not in use to reduce opportunities for spying.
- ▶ Don't read confidential information onboard or open confidential information on your computer.
- ▶ If you must use your computer for sensitive work on a flight, turn your monitor away from the person next to you.

**Protect Yourself From Social Engineering**

- ▶ Don't be afraid to say "no" or to ask why a person needs information. Never give out sensitive information to an unknown party.
- ▶ If someone unknown to you contacts you and needs sensitive information, call him or her back at a number in a company telephone directory.
- ▶ Nobody will ever legitimately ask for your password; never give it out. If someone asks, report the incident to security.
- ▶ Don't rely on common corporate identifiers, including employee numbers on identification badges, as a way to verify identity.
- ▶ Be aware that social engineering is generally accomplished through several inconsequential attacks, so be aware of unusual calls.
- ▶ Always look for your own company's badges on people when they "tailgate" you through a door.
- ▶ Shred all sensitive documents.
- ▶ If a credit card company calls you, call back at the number on your card before discussing any details about your account. ■

**rocketready**  
THE HUMAN SIDE OF SECURITY™

**www.rocketready.com**  
**888.395.1996**

**Paul Abercrombie** lives in Tampa. He shamelessly eavesdrops on fellow airplane passengers, but just for amusement.