

RocketReady Incognito (from left to right): the senior manager team of Brent Bennett, Wesley Mallory and Todd Snapp.



Member profile

Name: RocketReady

President: Todd Snapp

Employees: 12 to 20

Address: 10730 N. 56th St., Suite 200, Tampa, Florida 33617

Phone: 1-888-395-1996

Web site:

www.rocketready.com

Comments about Costco:

"Costco is our first option when we shop for any supplies or office purchases. Not only do we enjoy shopping there, but they make us feel important, even though we're a small company."

Who ya gonna call?

When companies get hacked, they summon RocketReady

By Leah Ingram

TODD SNAPP is proud to admit he's not a techie—this despite his past jobs managing technical people at software companies and his current gig as president of a company that's designed to foil hackers of all kinds. All Costco member Snapp ever wanted to do is "find nontechnical solutions in a technical environment," says the Tampa-based entrepreneur.

At his old job, he says, "we were doing software development, and our clients asked us to test if their systems were hacker-proof." So Snapp and his colleagues started using "social engineering" (read: scam) tactics to see if employees would spill the beans on trade secrets or customer passwords. Through e-mail phishing and convincing phone calls, Snapp discovered something disturbing: "We thought we could breach their security maybe 2 to 5 percent of the time," he recalls. "But 80 percent of the time we were able to convince employees to let us have access to sensitive information."

Thus, in 2004, RocketReady was born. Its

mission is simple: to help companies figure out where they have holes in their security systems via loose-lipped or well-meaning employees, and then to retrain those employees to plug those holes.

Snapp says the problem lies in organizations training their employees to be service oriented to a fault. One of the most popular ways for a con artist to access a customer's private information is to convince customer support that he needs a password reset. Employees in customer services are happy to help.

When on the job, Snapp's team of 10 employees dons virtual disguises, then makes phone calls and sends e-mails to see how well an employee holds up in a hacking test.

Whenever there's a big news story on the subject, "such as when someone hacked into socialite Paris Hilton's cell phone," RocketReady's switchboard lights up. Who's on the line? Not the company that was hacked, but rather its competitors, who want to prevent that from happening to them.

Social engineering, which Snapp calls the modern-day phrase for con artistry, occurs

both online and off. Snapp warns that it's easier to find a person in a weak security moment than most people think. "I was in the airport the other day, and from my chair in the waiting area I could see 21 people using laptops—10 of which I could see the screen," he says. "If I can see that many laptops, I can see sensitive information." In addition, sometimes hackers literally walk into a workplace. They gather with smokers outside a company's entrance, then slip inside in the employees' footsteps. "To a degree," Snapp says, "that's breaking and entering, without the breaking part."

"I believe that, at any given time, about 90 percent of American companies are under attack," he says. "E-mail phishing goes on thousands of times a day." He hopes that employees and others have learned that "you cannot click on a link in an e-mail, log in and give away personal information."

At the same time he wants companies to know that they need to create an environment where employees feel comfortable reporting any potential breach. "I can't tell you how many times we were on the job and got caught red-handed," he says. "Then we found out that the employee never reported us."

That troubles Snapp. Because if employees don't report attempted breaches, companies will never know when they're being targeted—and will never be able to prevent future attacks. ☹

Gone phishing

EVERY BUSINESS is vulnerable to "social engineering" attempts. Todd Snapp says these two tips can help keep your (and your customers') data safe.

- Always design your validation process to be multitiered. Have employees ask a number of questions about the customer before providing access to information. Questions about mother's maiden

name and birthdates simply aren't enough.

- When another employee calls, don't use caller ID as the only way to recognize the person. "We can doctor caller-ID numbers to match company locations," says Snapp. Instead, ask questions like "Who's your manager?" or "What building do you work in?" Hackers aren't likely to know those answers.—LI

Leah Ingram, based in New Hope, Pennsylvania, writes profiles for many national magazines.