CNNMoney
A Service of CNN, Fortune & Money

How a lying 'social engineer' hacked Wal-Mart

By Stacy Cowley @CNNMoneyTech August 8, 2012: 12:54 PM ET

PHOTO: STACY COWLEY/CNNMONEY

Organizer Chris Hadnagy (right) oversees a Defcon contest that challenges competitors like Shane MacDougall (at left) to trick companies into disclosing sensitive data.

LAS VEGAS (CNNMoney) -- A Wal-Mart store manager in a small military town in Canada got an urgent phone call last month from "Gary Darnell" in the home office in Bentonville, Ark.

Darnell told the manager Wal-Mart had a multi-million-dollar opportunity to win a major government contract, and that he was assigned to visit the handful of Wal-Mart stores picked as likely pilot spots. First, he needed to get a complete picture of the store's operations.

For about 10 minutes, Darnell described who he was (a newly hired manager of government logistics), the outlines of the contract ("all I know is Wal-Mart can make a ton of cash off it") and the plans for his visit.

Darnell asked the manager about all of his store's physical logistics: its janitorial contractor, cafeteria food-services provider, employee pay cycle and staff shift schedules. He learned what time the managers take their breaks and where they usually go for lunch.

Keeping up a steady patter about the new project and life in Bentonville, Darnell got the manager to give up some key details about the type of PC he used. Darnell quickly found out the make and version numbers of the computer's operating system, Web browser and antivirus software.

Finally, Darnell directed the manager to an external website to fill out a survey to prep for the upcoming visit. The manager dutifully plugged the address into his browser. His computer blocked the connection, but Darnell wasn't fazed. He said he'd call the IT department and have it unlocked.

The manager didn't think that was a concern. "Sounds good," he answered. "I'll try again in a few hours."

After thanking the manager for his help, Darnell made plans to follow up the next day. The manager promised to send Darnell over a list of good hotels in the area.

Then "Gary Darnell" hung up and stepped out of the soundproof booth he had been in for the last 20 minutes.

"All flags! All flags!" he announced, throwing his arms up in a V-for-Victory symbol.

His audience of some 100 spectators at the Defcon conference in Las Vegas burst into applause. They had been listening to both sides of the call through a loudspeaker broadcast.

"That was *insane*," the person next to me murmured, shaking her head in appreciation.

Darnell is actually Shane MacDougall, the champion of this year's **social engineering "capture the flag" contest**. He had

pinched the identity of a real Wal-Mart executive, who had no idea his name was being used in MacDougall's con.

MacDougall managed to capture every single data point, or "flag," on the competition checklist -- a first for the three-year-old event.

The hackers' playground: Held every July, Defcon is where hackers come to swap tips and show off cutting-edge technical exploits.

The social engineering hackathon is an old-fashioned display of con artistry. With nothing more than a phone line and a really good story, a hacker can pry secrets loose from America's biggest and most guarded corporations.

"Social engineering is the biggest threat to the enterprise, without a doubt," MacDougall said after his call. "I see all these [chief security officers] that spend all this money on firewalls and stuff, and they spend zero dollars on awareness."

MacDougall would know: The security firm he runs, **Tactical Intelligence** in Nova Scotia, specializes in a broad range of corporate espionage defense services. He regularly conducts social-engineering audits for clients, calling their employees to see what sensitive data he can extract.

In his view, it's a battle everyone is losing. MacDougall picks his victims carefully. Sales employees are a favorite target: "As soon as they think there's money, common sense goes out the window."

When asked about the "hack," Wal-Mart (**WMT**, **Fortune 500**) said it views MacDougall's exploit as a cautionary tale.

"We take the safeguarding of our business information very seriously and we're disappointed some basic information was shared," Wal-Mart spokesman Dan Fogleman told CNNMoney.

"When you're in the customer service business, sometimes our people can be a bit too helpful, as was the case here," he said. "We emphasize techniques to avoid social engineering attacks in our training programs. We will be looking carefully at what took place and learn all we can from it in order to better protect our business."

But Wal-Mart is not alone. Defcon's game takes aim at a different set of major corporations each year. This year's target list had nine other companies: UPS (NYSE), Verizon (**VZ**, **Fortune 500**), FedEx (**FDX**, **Fortune 500**), Shell, Exxon Mobil (**XOM**, **Fortune 500**), Target (**TGT**, **Fortune 500**), Cisco (**CSCO**, **Fortune 500**), Hewlett-Packard (**HPQ**, **Fortune 500**) and AT&T (**T**, **Fortune 500**).

Every single one gave up at least a few of the data points competitors sought.

"A lot of the attacks we saw this weekend could have been thwarted just by critical thinking," **contest organizer Chris Hadnagy** said toward the end of the showdown. "We need to train people that it's ok to say 'no.'"

Defcon's contestants are given two weeks to "passively" research their targets and gather any information they can get online. The best competitors come prepared with thick dossiers of background gathered from corporate sites and **social networks like LinkedIn**.

Then they have 20 minutes at the show to make phone calls. Live ... while an audience watches.

The information they're seeking from their targets includes sensitive corporate details like what e-mail software they use and the name of the outside contractor that cleans their office. Contestants don't ask for dangerously personal information like passwords, Social Security numbers or customer data.

Another critical safeguard: The calls aren't recorded. Nevada requires all parties to consent to phone taping, but there's no law against broadcasting them live to an audience. That's why the Defcon audience was legally allowed to listen in as MacDougall shook down Wal-Mart.

'I just couldn't do it': Some contestants got nowhere with their calls, especially when they posed as outside marketers or researchers. Others froze up when they got a live human being on the line.

One first-time contestant landed a receptive HR representative, only to visibly collapse with guilt. She signaled the tech crew to cut the line.

"I just couldn't do it," she said afterward. "I'm an honest person. I didn't realize it would feel so wrong to sit there lying."

Then there were the competitors like John Carruthers, who dove in with glee. Carruthers, posing as a systems administrator

for a Target data center in Minnesota, got a Target store manager on the line with his first phone call and proceeded to rattle off details about the company's supplier software.

Trying to figure out why a software patch hadn't been deployed, Carruthers deftly blended small talk -- "I've got my son's birthday that I'm trying to make it to" -- with a ruthlessly efficient, technical interrogation.

In less than 10 minutes, he extracted all of the high-value flags he wanted. Then, with time left on the clock, he called a second store and repeated the entire stunt.

He had Target's lingo nailed and had a surprising level of technical knowledge about the company. Carruthers reassured one mildly suspicious manager by citing her store number.

I asked Carruthers how he prepared for his calls. Are store numbers something Target releases publicly? "I used the store locator on Target's website," he answered. Pull up the details about a store and you'll find the number included in the URL.

Target spokesman Antoine LaFromboise told CNNMoney that the company doesn't consider store numbers confidential information. He added that Target "takes information protection very seriously."

The contest has ruffled some feathers, but Hadnagy said that some companies actually appreciate having security flaws exposed.

"I've had a few call afterward and ask, 'Hey, can you tell us more about how you did it?'" he said.

America's top spymaster, National Security Agency director Gen. Keith Alexander, is one of the game's fans.

Attending Defcon this year for the first time, Alexander dropped by to praise the competition for raising awareness about social engineering attackers and their methods. He even pulled Hadnagy aside for a private chat.

"He shook my hand and thanked me for teaching people to socially engineer," Hadnagy said, sounding mildly stunned. "That's first time I've ever had *that* happen."

First Published: August 7, 2012: 11:02 PM ET