

From: www.csoonline.com

Social engineering stories: The sequel

Two more social engineering scenarios demonstrate how hackers still use basic techniques to gain unauthorized access, and what you can do to stop them

by Joan Goodchild, Senior Editor,

May 27, 2010

John Sileo, an identity theft expert who trains on repelling social engineering, knows from first-hand experience what it's like to be a victim. Sileo has had his identity stolen—twice. And both instances resulted in catastrophic consequences.

The first crime took place when Sileo's information was obtained from someone who had gained access to it out of the trash (yes, [dumpster diving still works](#)). She bought a house using his financial information and eventually declared bankruptcy.

"That was mild," said Sileo, who then got hit again when his business partner used his information to embezzle money from clients. Sileo spent several years, and was bankrupt, fighting criminal charges.

Also see part one of the Social Engineering Stories series

Now that he has come out of it all innocent, he spends his time assisting organizations train employees on what social engineering and identity theft techniques look like.

"I'm trying to inspire employees to care about privacy," he said. "If they don't care about it at a human level, they are not going to care about the company's privacy policy or IT security. You've got to get it at a primal personal level."

Sileo ran through some memorable social engineering scenarios he's heard during his years as a security lecturer. The first is taken from his upcoming book "[Think like a spy](#)."

Social Engineering Scenario 1:

Doctor Who?

Not long after Dr. Yamitori shared her username on a handout at a medical conference, she received an invitation to become friends with Dr. Xavier on a social networking site built for the medical community. Dr.

BUSINESS TECHNOLOGY FORESIGHT

In Collaboration With **MIT Sloan** Management Review

SPONSOR ADVERTISING

REPLAY

It's time to ask smarter questions.

Learn more about IBM Information & Analytics >

Let's build a smarter planet

FOR ENTERPRISE | **FOR MIDSIZE BUSINESS**

The 4 Ways IT is Driving Innovation
MIT Sloan's Erik Brynjolfsson discusses how IT is driving corporate innovation

Decisions 2.0: The Power of Collective Intelligence
Wikis and other applications that tap into the collective intelligence of groups have recently generated tremendous interest. But what's the reality behind the hype?

Doq Eat Doq

sponsored by **IBM** | Let's build a smarter planet.

Yamitori had shared her impressions of the conference on the site, and Dr. Xavier had been taking note. Over the course of the next month, the two never communicated directly via the network; rather, they received regular updates and comments posted by the other doctors in the network.

On Friday afternoon at 2:00 P.M., Dr. Xavier (Dr. X) posted a comment directly to Dr. Yamitori (Dr. Y). Dr. X explained that he was in the process of researching software packages for his office and, knowing from the conference that Dr. Y ran an efficient operation, wanted to find out what software she used to manage her patient files.

Dr. Y happened to be at her computer and responded immediately to the query. Because both were part of a doctor's network, and concluding that the questions were innocuous, Dr. Y shared that she used Patient Relation 10.0 and was very happy with it. Dr. X thanked her, asked no further questions, and concluded the thread somewhat abruptly.

At 2:06 P.M., Dr. Y's assistant sent an internal instant message (the silent and preferred form of communication in the office) to her saying that Dr. Xavier was on hold and had a quick follow-up question to their online chat. When Dr. Y picked up, Dr. X apologized for any trouble he was causing, but said he had one last question and thought it was a good excuse to meet in person. Dr. X then asked Dr. Y if she would mind sharing the name of the software technician from Patient Relation Software who had installed the package for her so that he could ask some technical questions. Dr. Y gladly told him that her contact at the software company was Kenneth, and gave him Kenneth's phone number.

On Monday morning, before most doctors are in their offices, Dr. X's accomplice called Dr. Y's office and reached the receptionist, Priscilla. He told her that his name was Terry, that he was from Patient Relation Software, and that he was filling in for Kenneth, who was out sick. After flattering her (Dr. Y says you're the real brains of the operation), Terry explained that he needed to make a critical security update (version 10.1) to Dr. Y's software system. If it didn't happen right away, he added, her system could be the one that allowed hackers access into patient files. Immediately, Priscilla felt personally responsible. (Read [Mind Games: How Social Engineers Gain Your Confidence](#) for more on this tactic.)

Because Kenneth was out sick, Terry explained, he didn't have the username and password to dial in to Dr. Y's server and make the changes. He told Priscilla that as soon as the changes were made, he would call her back and let her know so that she could change her password. It was critical, he said, to change it as soon as he called in order to maintain security. In fact, he added, he would just send her a message on the social networking site, if she told him her username. She shared that as well, thereby giving him access to all of her friends who filled a similar role at other medical offices.

Knowing that Patient Relation was in fact the software package her office used to track patient records, that they were currently using version 10.0, that Kenneth was the name of their regular technician, and that she didn't want to be responsible for a data breach, Priscilla never suspected she was being socially engineered into revealing highly sensitive information. She gave Terry her password and, thus, full access to more than 17,500 private patient records, including their Social Security numbers, insurance data, medical histories, and even blood types.

Takeaway: "It used to be about who we trust. Now it's about how we trust," said Sileo, who gives his clients a three-step process to instill in employees in order to repel a social engineering attack.

1. The hogwash reflex: Training includes having employees develop a catch word or phrase that will go off in their head when someone requests information.
"You immediately have a trigger event," he said "A word that pops into your head that reminds you that you may be at risk."
2. Ask the right questions: Teach employees to ask "Can I call you back at XYZ Software to verify you are who you say you are?"
"If they get an excuse, they should know immediately it's a red flag to do more research without giving up information."
3. Stop. And think through the options: Instead of being hurried through an event and acting on a panic reflex, take it slow and consider what you need to do in order to maintain privacy.

Social Engineering Scenario 2

The Hurt Locker

"There is a lot of theft from women's lockers at work out facilities. What happens is a woman goes to work out, puts her cell phone and wallet into a locker and puts on a combination lock. Somebody who has recorded it with a mini-camera standing behind her knows the combination. They get into, they open up the cell phone, they click

a few keys, close it up and put the cell phone back in the locker. Grab the wallet or purse, close the locker, lock it and leave.

The woman comes back from working out, gets into her clothes, grabs the cell phone, goes for the wallet: It's missing. They usually think first they've left it in the car or out front. As they are walking out, the person who stole the wallet is there. They ring their phone. They say "This is Whatever Bank and we have reason to believe someone is trying to cash-out your account. Has your purse been stolen recently?"

Also see 9 Dirty Tricks: Social Engineers' Favorite Pickup Lines

The person is immediately in a panic and willing to do whatever it takes to make themselves safe. The bank person on the other end, who is not actually a bank person, says "Hey, we are here to protect you. That's what we do. But In order to shut down access to the account, I need to verify your social security number."

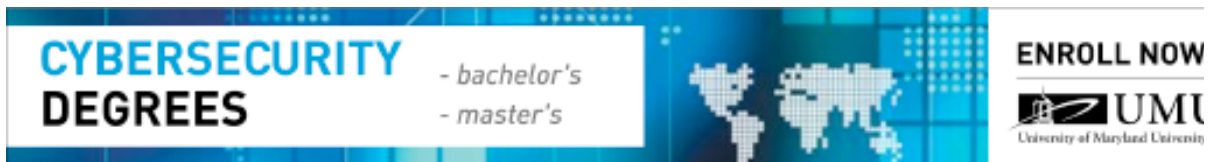
It may sound stupid on the outside looking in for someone to give up their social security number, but when you are in a panic, 90 percent or so of people will give that information away. And then the person will also say "OK, we can shut down the card, too. What is your PIN?"

Because they are rushing through it, because they are in fear, they don't give it a second thought.

Takeaway: It goes back to point three of Sileo's three steps. Take control of that interaction, he says.

"Stop and ask yourself 'Should I call the bank myself? Should I contact them to let them know what is happening?' If you just slow down and take control, that gets rid of the majority of social engineering."

© CXO Media Inc.



The banner features a blue background with a world map and a grid pattern. On the left, the text reads "CYBERSECURITY DEGREES" in large, bold, white letters, with "- bachelor's" and "- master's" in smaller white text below it. On the right, the text "ENROLL NOW" is displayed in bold white letters above the UMU logo, which includes the text "UMU" and "University of Maryland University" below it.