

What is Social Engineering?

The following is an excerpt from the U.S. DOE's Computer Incident Advisory Capability (CIAC)

Number 94-03:July 5, 1994

<https://infosec.navy.mil/ps/?t=main/main.tag&bc=main/tip8.html>

In today's world of computer crime, all perpetrators don't have to come in over the Internet; they may just as easily get information simply by asking. Beware of the friendly insider or the official sounding outsider; they may be playing on your good will or naiveté to get what they need. A few examples should help...

A technician answers the telephone. "Bill Jones, Telecom Operations."

"Hello. This is Martin White with AT&T Operations. We think someone may have broken into your PBX switch. Can I talk to the technical person in charge?"

"That's me," Bill says.

"How're you doing, Bill?"

"Good. And you?"

A deep breath. "Not too bad, except that it's Friday afternoon and I think we're going to have to wade through a mountain of paper. Anyway, as I was saying, we think your switch has been compromised."

"What makes you think so?"

"Your toll free dial in is 800-555-1212 isn't it?"

"Yeah."

"We alarmed on someone sequence dialing all the 555 numbers. The sequence stopped on yours, then randomly searched for dial out access codes. If they found it, you know how bad that can be."

"Well, can't you tell for certain?" Bill asks.

"Sure, I'm searching now, but it's so much paper." The sound of a page being flipped. "What scares me is that while I'm doing this, the bad guys could be selling your long distance on the streets right now. Maybe you better take your 800 service off line or change the access code."

"Jeez, I can't do that. The people in the field...our business depends on it."

Martin sighs. "That's too bad. The intruders may not have even cracked the code." The sound of another page being flipped and then fingers snapping. "Bill, I just thought of something. I have all this on line. It would just take a minute to search for your access code."

A heavy sigh. "Why didn't I think of this before? It's been a long week-too many hours looking at numbers." A pause. "Okay, what's your access code?"

"I...er," Bill hesitates.

"Oh, yeah, you shouldn't give it out. I understand. "The sound of another page being flipped. "It was such a good idea, too." Pause.

"These guys sure tried a lot of permutations. These eight digit codes..." Another page.

"Hey," Bill says, "we could be here all night. Forget I told you this: the code is 98765432."

"Thanks. Great. Hold on." The sound of keys being typed. "Okay. Let me double check." More typing. "That's it. Good news, they never got to it." Pause. "Thanks a lot, Bill. We would have been here half the night for a non-event. By the way, once they pass you by, it's very rare that they'd come back. You're in good shape. Though you probably want to change that access code."

"Nah, that would be a real pain. Everyone in the field would have to be informed. Maybe I'll kick it up to the boss on Monday. Have a good weekend."

"You too."

"Martin White" will have a good weekend. He and his confederates will sell discount long distance service on the streets of New York City at public phone booths, a zero overhead pure profit enterprise. The costs to Bill's organization will be over \$150,000. This is one (fictionalized but only too realistic) example of what's called "Social Engineering," an ironic characterization of the non-technical aspect of Information Technology (IT) crime. In other human interactions it's called a "Con (or Confidence) Game" where Martin is the "Con Artist." The underlying idea is simple: deceive the victim into revealing secret information or taking inappropriate action for the attacker's benefit.

Most of us are helpful and trusting - it's human nature. We want to be good neighbors and have good neighbors. Americans are especially trusting and as foreign industrial espionage increases, we must check on requesters before we hand over either access or information. Social Engineers exploit this cooperative inclination. They also employ intimidation and impersonation as well as plain old fashioned snooping and eavesdropping.

A confused and befuddled person will telephone a clerk and ask for his password to be changed. An important sounding man identifying himself as an executive will telephone a new system administrator and demand access to his account NOW! A person at an airport will look over your shoulder ("shoulder surfing") as you key in your telephone credit card or ATM PIN (they even use binoculars and camcorders). A visitor will watch you type your username and password at your keyboard. A confident person will call up a computer operator and ask him or her to type in a few lines of instruction at the console. An attacker will sift through your paper trash ("dumpster diving"), looking for clues to unlock your IT treasures.

Unlike the technology it targets, social engineering is an old profession with a new name. It succeeds frequently because our culture has not caught up with its own technology. A social engineer would have a much more difficult time getting the combination to a safe than a password, or even the combination to a locker at the health club. The best defense is simple: it's education, training, and awareness.