

# Social Engineering Examples from “The Art of Deception” by Kevin Mitnick

## 1) Flying out

---

### Peter Abel's Phone Call

“Hi,” the voice at the other end of the line says. “This is Tom at Parkhurst Travel. Your tickets to San Francisco are ready. Do you want us to deliver them, or do you want to pick them up?”

“San Francisco?” Peter says. “I'm not going to San Francisco.”

“Is this Peter Abels?”

“Yes, but I don't have any trips coming up.”

“Well,” the caller says with a friendly laugh, “you sure you don't want to go to San Francisco?”

“If you think you can talk my boss into it...” Peter says, playing along with the friendly conversation.

“Sounds like a mix-up,” the caller says. “On our system, we book travel arrangements under the employee number. Maybe somebody used the wrong number. What's your employee number?”

Peter obligingly recites his number. And why not? It goes on just about every personnel form he fills out; lots of people in the company have access to it – human resources, payroll, and, obviously, the outside travel agency. No one treats an employee number like some sort of secret. What difference could it make?

## 2) Video store

---

### The First Call: Andrea Lopez

Andrea Lopez answered the phone at the video rental store where she worked, and in a moment was smiling: It's always a pleasure when a customer takes the trouble to say he's happy about the service. This caller said he had had a very good experience dealing with the store, and he wanted to send the manager a letter about it.

He asked for the manager's name and the mailing address, and she told him it was Tommy Allison, and gave him the address. As he was about to hang up, he had another idea and said, “I might want to write to your company headquarters, too. What's your store number?” She gave him that information, as well. He said thanks, added something pleasant about how helpful she had been, and said goodbye.

"A call like that," she thought, "always seems to make the shift go by faster. How nice it would be if people did that more often."

### **The Second Call: Ginny**

"Thanks for calling Studio Video. This is Ginny, how can I help you?"

"Hi, Ginny," the caller said enthusiastically, sounding as if he talked to Ginny every week or so. "It's Tommy Allison, manager at Forest Park, Store 863. We have a customer in here who wants to rent *Rocky 5* and we're all out of copies. Can you check on what you've got?"

She came back on the line after a few moments and said, "Yeah, we've got three copies."

"Okay, I'll see if he wants to drive over there. Listen, thanks. If you ever need any help from our store, just call and ask for Tommy. I'll be glad to do whatever I can for you."

Three or four times over the next couple of weeks, Ginny got calls from Tommy for help with one thing or another. They were seemingly legitimate requests, and he was always very friendly without sounding like he was trying to come on to her. He was a little chatty along the way, as well – "Did you hear about the big fire in Oak Park? Bunch of streets closed over there," and the like. The calls were a little break from the routine of the day, and Ginny was always glad to hear from him.

One day Tommy called sounding stressed. He asked, "Have you guys been having trouble with your computers?"

"No," Ginny answered. "Why?"

"Some guy crashed his car into a telephone pole, and the phone company repairman says a whole part of the city will lose their phones and Internet connection till they get this fixed."

"Oh, no. Was the man hurt?"

"They took him away in an ambulance. Anyway, I could use a little help. I've got a customer of yours here who wants to rent *Godfather II* and doesn't have his card with him. Could you verify his information for me?"

"Yeah, sure."

Tommy gave the customer's name and address, and Ginny found him in the computer. She gave Tommy the account number.

"Any late returns or balance owed?" Tommy asked.

"Nothing showing."

"Okay, great. I'll sign him up by hand for an account here and put it in our database later on when the computers come back up again. And he wants to put this charge on the Visa card he uses at your store, and he doesn't have it with him. What's the card number and expiration date?"

She gave it to him, along with the expiration date. Tommy said, "Hey, thanks for the help. Talk to you soon," and hung up.

### **Doyle Lonnegan's Story**

Lonnegan is not a young man you would want to find waiting when you open your front door. A one-time collection man for bad gambling debts, he still does an occasional favor, if it doesn't put him out very much. In this case, he was offered a sizable bundle of cash for little more than making some phone calls to a video store. Sounds easy enough. It's just that none of his "customers" knew how to run this con; they needed somebody with Lonnegan's talent and know-how.

People don't write checks to cover their bets when they're unlucky or stupid at the poker table. Everybody knows that. Why did these friends of mine keep on playing with a cheat that didn't have green out on the table? Don't ask. Maybe they're a little light in the IQ department. But they're friends of mine—what can you do?

This guy didn't have the money, so they took a check. I ask you! Should of drove him to an ATM machine, is what they should of done. But no, a check. For \$3,230. Naturally, it bounced. What would you expect? So then they call me; can I help? I don't close doors on people's knuckles any more. Besides, there are better ways nowadays. I told them, 30 percent commission, I'd see what I could do. So they give me his name and address, and I go up on the computer to see what's the closest video store to him. I wasn't in a big hurry. Four phone calls to cozy up to the store manager, and then, bingo, I've got the cheat's Visa card number. Another friend of mine owns a topless bar. For fifty bucks, he put the guy's poker money through as a Visa charge from the bar. Let the cheat explain that to his wife. You think he might try to tell Visa it's not his charge? Think again. He knows we know who he is. And if we could get his Visa number, he'll figure we could get a lot more besides. No worries on that score.

## **3) Credit check**

---

### **CREDITCHEX**

For a long time, the British put up with a very stuffy banking system. As an ordinary, upstanding citizen, you couldn't walk in off the street and open a bank account. No, the bank wouldn't consider accepting you as a customer unless some person already well established as a customer provided you with a letter of recommendation.

Quite a difference, of course, in the seemingly egalitarian banking world of today. And our modern ease of doing business is nowhere more in evidence than in friendly, democratic America, where almost anyone can walk into a bank and easily open a checking account, right? Well, not exactly. The truth is that banks understandably have a natural reluctance to open an account for somebody who just might have a history of writing bad checks—that would be about as welcome as a rap sheet of bank robbery or embezzlement charges. So it's standard practice at

many banks to get a quick thumbs-up or thumbs-down on a prospective new customer.

One of the major companies that banks contract with for this information is an outfit we'll call CreditChex. They provide a valuable service to their clients, but like many companies, can also unknowingly provide a handy service to knowing social engineers.

### **The First Call: Kim Andrews**

"National Bank, this is Kim. Did you want to open an account today?"

"Hi, Kim. I have a question for you. Do you guys use CreditChex?"

"Yes."

"When you phone in to CreditChex, what do you call the number you give them—is it a 'Merchant ID'?"

A pause; she was weighing the question, wondering what this was about and whether she should answer.

The caller quickly continued without missing a beat:

"Because, Kim, I'm working on a book. It deals with private investigations."

"Yes," she said, answering the question with new confidence, pleased to be helping a writer.

"So it's called a Merchant ID, right?"

"Uh huh."

"Okay, great. Because I wanted to make sure I had the lingo right. For the book. Thanks for your help. Good-bye, Kim."

### **The Second Call: Chris Talbert**

"National Bank, New Accounts, this is Chris."

"Hi, Chris. This is Alex," the caller said. "I'm a customer service rep with CreditChex. We're doing a survey to improve our services. Can you spare me a couple of minutes?"

She was glad to, and the caller went on:

"Okay - what are the hours your branch is open for business?"

She answered, and continued answering his string of questions.

"How many employees at your branch use our service?"

"How often do you call us with an inquiry?"

"Which of our 800-numbers have we assigned you for calling us?"

"Have our representatives always been courteous?"

"How's our response time?"

"How long have you been with the bank?"

“What Merchant ID are you currently using?”

“Have you ever found any inaccuracies with the information we've provided you?”

“If you had any suggestions for improving our service, what would they be?”

And:

“Would you be willing to fill out periodic questionnaires if we send them to your branch?”

She agreed, they chatted a bit, the caller rang off, and Chris went back to work.

### **The Third Call: Henry McKinsey**

“CreditChex, this is Henry McKinsey, how can I help you?”

The caller said he was from National Bank. He gave the proper Merchant ID and then gave the name and social security number of the person he was looking for information on. Henry asked for the birth date, and the caller gave that, too.

After a few moments, Henry read the listing from his computer screen.

“Wells Fargo reported NSF in 1998, one time, amount of \$2,066.” NSF – non sufficient funds – is the familiar banking lingo for checks that have been written when there isn't enough money in the account to cover them.

“Any activities since then?”

“No activities.”

“Have there been any other inquiries?”

“Let's see. Okay, two of them, both last month. Third United Credit Union of Chicago.” He stumbled over the next name, Schenectady Mutual Investments, and had to spell it. “That's in New York State,” he added.

### **Private Investigator at Work**

All three of those calls were made by the same person: a private investigator we'll call Oscar Grace. Grace had a new client in the midst of divorce. Her husband had already pulled the cash out of their savings account and an even larger sum from their brokerage account. She wanted to know where their assets had been squirreled away.

## 4) Network outage

---

### **The First Call: Tom Delay**

"Tom DeLay, Bookkeeping."

"Hey, Tom, this is Eddie Martin from the Help Desk. We're trying to troubleshoot a computer networking problem. Do you know if anyone in your group has been having trouble staying on line?"

"Uh, not that I know of."

"And you're not having any problems yourself?"

"No, seems fine."

"Okay, that's good. Listen, we're calling people who might be affected 'cause it's important you let us know right away if you lose your network connection."

"That doesn't sound good. You think it might happen?"

"We hope not, but you'll call if it does, right?"

"You better believe it."

"Listen, sounds like having your network connection go down would be a problem for you..."

"You *bet* it would."

"... so while *we're* working on this, let me give you my cell phone number. Then you can reach me directly if you need to."

"That'd be great. Go ahead."

"It's 555 867 5309."

"555 867 5309. Got it. Hey, thanks. What was your name again?"

"It's Eddie. Listen, one other thing—I need to check which port your computer is connected to. Take a look on your computer and see if there's a sticker somewhere that says something like 'Port Number'."

"Hang on No, don't see anything like that."

"Okay, then in the back of the computer, can you recognize the network cable."

"Yeah."

"Trace it back to where it's plugged in. See if there's a label on the jack it's plugged into."

"Hold on a second. Yeah, wait a minute – I have to squat down here so I can get close enough to read it. Okay – it says Port 6 dash 47."

"Good – that's what we had you down as, just making sure."

### **The Second Call: The IT Guy**

Two days later, a call came through to the same company's Network Operations Center.

"Hi, this is Bob; I'm in Tom DeLay's office in Bookkeeping. We're trying to troubleshoot a cabling problem. I need you to disable Port 6-47."

The IT guy said it would be done in just a few minutes, and to let them know when he was ready to have it enabled.

### **The Third Call: Getting Help from the Enemy**

About an hour later, the guy who called himself Eddie Martin was shopping at Circuit City when his cell phone rang. He checked the caller ID, saw the call was from the shipbuilding company, and hurried to a quiet spot before answering.

“Help Desk, Eddie.”

“Oh, hey, Eddie. You've got an echo, where are you?”

“I'm, uh, in a cabling closet. Who's this?”

“It's Tom DeLay. Boy, am I glad I got a hold of you. Maybe you remember you called me the other day? My network connection just went down like you said it might, and I'm a little panicky here.”

“Yeah, we've got a bunch of people down right now. We should have it taken care of by the end of the day. That okay?”

“NO! Damn, I'll get way behind if I'm down that long. What's the best you can do for me?”

“How pressed are you?”

“I could do some other things for right now. Any chance you could take care of it in half an hour?”

“HALF AN HOUR! You don't want much. Well, look, I'll drop what I'm doing and see if I can tackle it for you.”

“Hey, I really appreciate that, Eddie.”

### **The Fourth Call: Gotcha!**

Forty-five minutes later...

“Tom? It's Eddie. Go ahead and try your network connection.”

After a couple of moments:

“Oh, good, it's working. That's just great.”

“Good, glad I could take care of it for you.”

“Yeah, thanks a lot.”

“Listen, if you want to make sure your connection doesn't go down again, there's some software you oughta be running. Just take a couple of minutes.”

“Now's not the best time.”

“I understand... It could save us both big headaches the next time this network problem happens.”

"Well... if it's only a few minutes."

"Here's what you do..."

Eddie then took Tom through the steps of downloading a small application from a Web site. After the program had downloaded, Eddie told Tom to double-click on it. He tried, but reported:

"It's not working. It's not doing anything."

"Oh, what a pain. Something must be wrong with the program. Let's just get rid of it, we can try again another time." And he talked Tom through the steps of deleting the program so it couldn't be recovered.

## **5) Just testing**

---

"Hi, this is Peter Sheppard. I'm with Arbuclde Support, the company that does tech support for your firm. I'd like to run a couple of tests with you, he said. "I'm able to see on my screen the keystrokes you type, and I want to make sure they're going across the network correctly. So every time you type a stroke, I want you to tell me what it is, and I'll see if the same letter or number is appearing here. Okay?"

After a few moments, she told him, "I have the login screen, and I'm going to type in my ID. I'm typing it now--M...A...R...Y...D."

"Great so far," he said. "I'm seeing that here. Now, go ahead and type your password but don't tell me what it is. You should never tell anybody your password, not even tech support. I'll just see asterisks here--your password is protected so I can't see it. Listen, he went on, "we just installed an update that allow people to change their passwords. Would you be willing to take a couple of minutes with me so I can see if we got it working right?"

She was grateful for the help he had given her and readily agreed. Peter talked her through the steps of launching the application that allows a user to change passwords, a standard element of the Windows 2000 operating system. "Go ahead and enter your password," he told her. "But remember not to say it out loud."

When she had done that, Peter said, "Just for this quick test, when it asks for your new password, enter 'test123.' Then type it again in the Verification box, and click Enter."

He walked her through the process of disconnecting from the server. He had her wait a couple of minutes, then connect again, this time trying to log on with her new password. It worked like a charm, Peter seemed very pleased, and talked her through changing back to her original password or choosing a new one--once more cautioning her about not saying the password out loud.