chapter 2

When Innocuous Information Isn't

What do most people think is the real threat from social engineers? What should you do to be on your guard?

If the goal is to capture some highly valuable prize—say, a vital component of the company's intellectual capital—then perhaps what's needed is, figuratively, just a stronger vault and more heavily armed guards. Right?

But in reality penetrating a company's security often starts with the bad guy obtaining some piece of information or some document that seems so innocent, so everyday and unimportant, that most people in the organization wouldn't see any reason why the item should be protected and restricted.

THE HIDDEN VALUE OF INFORMATION

Much of the seemingly innocuous information in a company's possession is prized by a social engineering attacker because it can play a vital role in his effort to dress himself in a cloak of believability.

Throughout these pages, I'm going to show you how social engineers do what they do by letting you "witness" the attacks for yourself—sometimes presenting the action from the viewpoint of the people being victimized, allowing you to put yourself in their shoes and gauge how you yourself (or maybe one of your employees or coworkers) might have responded. In many cases you'll also experience the same events from the perspective of the social engineer.

The first story looks at a vulnerability in the financial industry.

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—nonsufficient 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, one of his first. A cop until a few months before, he found that some of this new work came naturally, but some offered a challenge to his resources and inventiveness. This one came down firmly in the challenge category.

The hardboiled private eyes of fiction—the Sam Spades and the Philip Marlowes—spend long nighttime hours sitting in cars waiting to catch a cheating spouse. Real-life PIs do the same. They also do a less written about, but no less important kind of snooping for warring spouses, a method that leans more heavily on social engineering skills than on fighting off the boredom of nighttime vigils.

Grace's new client was a lady who looked as if she had a pretty comfortable budget for clothes and jewelry. She walked into his office one day and took a seat in the leather chair, the only one that didn't have papers piled on it. She settled her large Gucci handbag on his desk with the logo turned to face him and announced she was planning to tell her husband that she wanted a divorce, but admitted to "just a very little problem."

It seemed her hubby was one step ahead. He 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, and her divorce lawyer wasn't any help at all. Grace surmised the lawyer was one of those uptown, high-rise counselors who wouldn't get his hands dirty on something messy like where-did-the-money-go.

Could Grace help?

He assured her it would be a breeze, quoted a fee, expenses billed at cost, and collected a check for the first payment.

Then he faced his problem. What do you do if you've never handled a piece of work like this before and don't quite know how to go about tracking down a money trail? You move forward by baby steps. Here, according to our source, is Grace's story.

I knew about CreditChex and how banks used the outfit—my ex-wife used to work at a bank. But I didn't know the lingo and procedures, and trying to ask my ex- would be a waste of time.

Step one: Get the terminology straight and figure out how to make the request so it sounds like I know what I'm talking about. At the bank I called, the first young lady, Kim, was suspicious when I asked about how they identify themselves when they phone CreditChex. She hesitated; she didn't know whether to tell me. Was I put off by that? Not a bit. In fact, the hesitation gave me an important clue, a sign that I had to supply a reason she'd find believable. When I worked the con on her about doing research for a book, it relieved her suspicions. You say you're an author or a movie writer, and everybody opens up.

She had other knowledge that would have helped—things like what information CreditChex requires to identify the person you're calling about, what information you can ask for, and the big one, what was Kim's bank Merchant ID number. I was ready to ask those questions, but her hesitation sent up the red flag. She bought the book research story, but she already had a few niggling suspicions. If she'd been more willing right way, I would have asked her to reveal more details about their procedures.

You have to go on gut instinct, listen closely to what the mark is saying and how she's saying it. This lady sounded smart enough for alarm bells to start going off if I asked too many unusual questions. And even though she didn't know who I was or what number I was calling from, still in this

lingo

MARK The victim of a con.

BURN THE SOURCE An attacker is said to have burned the source when he allows a victim to recognize that an attack has taken place. Once the victim becomes aware and notifies other employees or management of the attempt, it becomes extremely difficult to exploit the same source in future attacks.

business you never want anybody putting out the word to be on the lookout for someone calling to get information about the business. That's because you don't want to burn the source—you may want to call the same office back another time.

I'm always on the watch for little signs that give me a read on how cooperative a person is, on a scale that runs from "You sound like a nice person and I believe everything you're saying" to "Call the cops, alert the National Guard, this guy's up to no good."

I read Kim as a little bit on edge, so I just called somebody at a different branch. On my second call with Chris, the survey trick played like a charm. The tactic here is to slip the important questions in among inconsequential ones that are used to create a sense of believability. Before I dropped the question about the Merchant ID number with CreditChex, I ran a little last-minute test by asking her a personal question about how long she'd been with the bank.

A personal question is like a land mine—some people step right over it and never notice; for other people, it blows up and sends them scurrying for safety. So if I ask a personal question and she answers the question and the tone of her voice doesn't change, that means she probably isn't skeptical about the nature of the request. I can safely ask the sought-after question without arousing her suspicions, and she'll probably give me the answer I'm looking for.

One more thing a good PI knows: Never end the conversation after getting the key information. Another two or three questions, a little chat, and then it's okay to say good-bye. Later, if the victim remembers anything about what you asked, it will probably be the last couple of questions. The rest will usually be forgotten.

So Chris gave me their Merchant ID number, and the phone number they call to make requests. I would have been happier if I had gotten to ask some questions about how much information you can get from CreditChex. But it was better not to push my luck.

It was like having a blank check on CreditChex. I could now call and get information whenever I wanted. I didn't even have to pay for the service. As it turned out, the CreditChex rep was happy to share exactly the information I wanted: two places my client's husband had recently applied to open an account. So where were the assets his soon-to-be ex-wife was looking for? Where else but at the banking institutions the guy at CreditChex listed?

Analyzing the Con

This entire ruse was based on one of the fundamental tactics of social engineering: gaining access to information that a company employee treats as innocuous, when it isn't.

The first bank clerk confirmed the terminology to describe the identifying number used when calling CreditChex: the Merchant ID. The second provided the phone number for calling CreditChex, and the most vital piece of information, the bank's Merchant ID number. All this information appeared to the clerk to be innocuous. After all, the bank clerk thought she was talking to someone from CreditChex—so what could be the harm in disclosing the number?

All of this laid the groundwork for the third call. Grace had everything he needed to phone CreditChex, pass himself off as a rep from one of their customer banks, National, and simply ask for the information he was after.

With as much skill at stealing information as a good swindler has at stealing your money, Grace had well-honed talents for reading people. He knew the common tactic of burying the key questions among innocent ones. He knew a personal question would test the second clerk's willingness to cooperate, before innocently asking for the Merchant ID number.

The first clerk's error in confirming the terminology for the CreditChex ID number would be almost impossible to protect against. The information is so widely known within the banking industry that it appears to be unimportant—the very model of the innocuous. But the second clerk, Chris, should not have been so willing to answer questions without positively verifying that the caller was really who he claimed to be. She should, at the very least, have taken his name and number and called back; that way, if any questions arose later, she may have kept a record of what phone number the person had used. In this case, making a call like that would have made it much more difficult for the attacker to masquerade as a representative from CreditChex.

mitnick message

A Merchant ID in this situation is analogous to a password. If bank personnel treated it like an ATM PIN, they might appreciate the sensitive nature of the information. Is there an internal code or number in your organization that people aren't treating with enough care?

Better still would have been a call to CreditChex using a number the bank already had on record—not a number provided by the caller—to verify that the person really worked there, and that the company was really doing a customer survey. Given the practicalities of the real world and the time pressures that most people work under today, though, this kind of verification phone call is a lot to expect, except when an employee is suspicious that some kind of attack is being made.

THE ENGINEER TRAP

It is widely known that head-hunter firms use social engineering tactics to recruit corporate talent. Here's an example of how it can happen.

In the late 1990s, a not very ethical employment agency signed a new client, a company looking for electrical engineers with experience in the telephone industry. The honcho on the project was a lady endowed with a throaty voice and sexy manner that she had learned to use to develop initial trust and rapport over the phone.

The lady decided to stage a raid on a cellular phone service provider, to see if she could locate some engineers who might be tempted to take a walk across the street to a competitor. She couldn't exactly call the switchboard and say, "Let me talk to anybody with five years of engineering experience." Instead, for reasons that will become clear in a moment, she began the talent assault by seeking a piece of information that appeared to have no sensitivity at all, information that company people give out to almost anybody who asks.

The First Call: The Receptionist

The attacker, using the name Didi Sands, placed a call to the corporate offices of the cellular phone service. In part, the conversation went like this:

Receptionist: Good afternoon. This is Marie, how may I help you?

Didi: Can you connect me to the Transportation Department?

R: I'm not sure if we have one, I'll look in my directory. Who's calling?

D: It's Didi.

R: Are you in the building, or . . . ?

D: No, I'm outside the building.

R: Didi who?

D: Didi Sands. I had the extension for Transportation, but I forgot what it was.

R: One moment.

To allay suspicions, at this point Didi asked a casual, just-making-conversation question designed to establish that she was on the "inside," familiar with company locations.

D: What building are you in—Lakeview or Main Place?

R: Main Place. *(pause)* It's 805 555 6469.

To provide herself with a backup in case the call to Transportation didn't provide what she was looking for, Didi said she also wanted to talk to Real Estate. The receptionist gave her that number, as well. When Didi asked to be connected to the Transportation number, the receptionist tried, but the line was busy.

At that point Didi asked for a *third* phone number, for Accounts Receivable, located at a corporate facility in Austin, Texas. The receptionist asked her to wait a moment, and went off the line. Reporting to Security that she had a suspicious phone call and thought there was something fishy going on? Not at all, and Didi didn't have the least bit of concern. She was being a bit of a nuisance, but to the receptionist it was all part of a typical workday. After about a minute, the receptionist came back on the line, looked up the Accounts Receivable number, tried it, and put Didi through.

The Second Call: Peggy

The next conversation went like this:

Peggy: Accounts Receivable, Peggy.

Didi: Hi, Peggy. This is Didi, in Thousand Oaks.

P: Hi, Didi.

D: How ya doing?

P: Fine.

Didi then used a familiar term in the corporate world that describes the charge code for assigning expenses against the budget of a specific organization or workgroup:

D: Excellent. I have a question for you. How do I find out the cost center for a particular department?

P: You'd have to get ahold of the budget analyst for the department.

D: Do you know who'd be the budget analyst for Thousand Oaks— headquarters? I'm trying to fill out a form and I don't know the proper cost center.

P: I just know when y'all need a cost center number, you call your budget analyst.

D: Do you have a cost center for your department there in Texas?

P: We have our own cost center but they don't give us a complete list of them.

D: How many digits is the cost center? For example, what's your cost center?

P: Well, like, are you with 9WC or with SAT?

Didi had no idea what departments or groups these referred to, but it didn't matter. She answered:

D: 9WC.

P: Then it's usually four digits. Who did you say you were with?

D: Headquarters—Thousand Oaks.

P: Well, here's one for Thousand Oaks. It's 1A5N, that's N like in Nancy.

By just hanging out long enough with somebody willing to be helpful, Didi had the cost center number she needed—one of those pieces of information that no one thinks to protect because it seems like something that couldn't be of any value to an outsider.

The Third Call: A Helpful Wrong Number

Didi's next step would be to parlay the cost center number into something of real value by using it as a poker chip.

She began by calling the Real Estate department, pretending she had reached a wrong number. Starting with a "Sorry to bother you, but . . . ," she claimed she was an employee who had lost her company directory, and asked who you were supposed to call to get a new copy. The man said the print copy was out of date because it was available on the company intranet site.

Didi said she preferred using a hard copy, and the man told her to call Publications, and then, without being asked—maybe just to keep the sexy-sounding lady on the phone a little longer—helpfully looked up the number and gave it to her.

The Fourth Call: Bart in Publications

In Publications, she spoke with a man named Bart. Didi said she was from Thousand Oaks, and they had a new consultant who needed a copy of the company directory. She told him a print copy would work better for the consultant, even if it was somewhat out of date. Bart told her she'd have to fill out a requisition form and send the form over to him.

Didi said she was out of forms and it was a rush, and could Bart be a sweetheart and fill out the form for her? He agreed with a little too much enthusiasm, and Didi gave him the details. For the address of the fictional contractor, she drawled the number of what social engineers call a *mail drop*, in this case a Mail Boxes Etc.-type of commercial business where her company rented boxes for situations just like this.

The earlier spadework now came in handy: There would be a charge for the cost and shipping of the directory. Fine—Didi gave the cost center for Thousand Oaks:

"1A5N, that's N like in Nancy."

A few days later, when the corporate directory arrived, Didi found it was an even bigger payoff than she had expected: It not only listed the names and phone numbers, but also showed who worked for whom—the corporate structure of the whole organization.

The lady of the husky voice was ready to start making her head-hunter, people-raiding phone calls. She had conned the information she needed to launch her raid using the gift of gab honed to a high polish by every skilled social engineer. Now she was ready for the payoff.

Analyzing the Con

In this social engineering attack, Didi started by getting phone numbers for three departments in the target company. This was easy, because the numbers she was asking for were no secret, especially to employees. A social engineer learns to sound like an insider, and Didi was skilled at this

lingo

MAIL DROP The social engineer's term for a rental mailbox, typically rented under an assumed name, which is used to deliver documents or packages the victim has been duped into sending.

Just like pieces of a jigsaw puzzle, each piece of information may be irrelevant by itself. However, when the pieces are put together, a clear picture emerges. In this case, the picture the social engineer saw was the entire internal structure of the company

game. One of the phone numbers led her to a cost center number, which she then used to obtain a copy of the firm's employee directory.

The main tools she needed: sounding friendly, using some corporate lingo, and, with the last victim, throwing in a little verbal eyelash-batting.

And one more tool, an essential element not easily acquired—the manipulative skills of the social engineer, refined through extensive practice and the unwritten lessons of bygone generations of confidence men.

MORE "WORTHLESS" INFO

Besides a cost center number and internal phone extensions, what other seemingly useless information can be extremely valuable to your enemy?

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?

The answer isn't hard to figure out. Two or three pieces of information might be all it takes to mount an effective impersonation—the social engineer cloaking himself in someone else's identity. Get hold of an employee's name, his phone number, his employee number—and maybe, for good measure, his manager's name and phone number—and a halfway-competent social engineer is equipped with most of what he's likely to need to sound authentic to the next target he calls.

If someone who said he was from another department in your company had called yesterday, given a plausible reason, and asked for your employee number, would you have had any reluctance in giving it to him?

And by the way, what is your social security number?

mitnick message

The moral of the story is, don't give out any personal or internal company information or identifiers to anyone, unless his or her voice is recognizable and the requestor has a need to know.

PREVENTING THE CON

Your company has a responsibility to make employees aware of how a serious mistake can occur from mishandling nonpublic information. A well-thought-out information security policy, combined with proper education and training, will dramatically increase employee awareness about the proper handling of corporate business information. A data classification policy will help you to implement proper controls with respect to disclosing information. Without a data classification policy, all internal information must be considered confidential, unless otherwise specified.

Take these steps to protect your company from the release of seemingly innocuous information:

- The Information Security Department needs to conduct awareness training detailing the methods used by social engineers. One method, as described above, is to obtain seemingly nonsensitive information and use it as a poker chip to gain short-term trust. Each and every employee needs to be aware that when a caller has knowledge about company procedures, lingo, and internal identifiers it does not in any way, shape, or form authenticate the requestor or authorize him or her as having a need to know. A caller could be a former employee or

contractor with the requisite insider information. Accordingly, each corporation has a responsibility to determine the appropriate authentication method to be used when employees interact with people they don't recognize in person or over the telephone.

- The person or persons with the role and responsibility of drafting a data classification policy should examine the types of details that may be used to gain access for legitimate employees that seem innocuous, but could lead to information that is sensitive. Though you'd never give out the access codes for your ATM card, would you tell somebody what server you use to develop company software products? Could that information be used by a person pretending to be somebody who has legitimate access to the corporate network?
- Sometimes just knowing inside terminology can make the social engineer appear authoritative and knowledgeable. The attacker often relies on this common misconception to dupe his or her victims into compliance. For example, a Merchant ID is an identifier that people in the New Accounts department of a bank casually use every day. But such an identifier is exactly the same as a password. If each and every employee understands the nature of this identifier—that it is used to positively authenticate a requestor—they might treat it with more respect.
- No companies—well, very few, at least—give out the direct-dial phone numbers of their CEO or board chairman. Most companies, though, have no concern about giving out phone numbers to most departments and workgroups in the organization—especially to someone who is, or appears to be, an employee. A possible countermeasure: Implement a policy

mitnick message

As the old adage goes—even real paranoids probably have enemies. We must assume that every business has its enemies, too—attackers that target the network infrastructure to compromise business secrets. Don't end up being a statistic on computer crime—it's high time to shore up the necessary defenses by implementing proper controls through well-thought-out security policies and procedures.

that prohibits giving internal phone numbers of employees, contractors, consultants, and temps to outsiders. More importantly, develop a step-by-step procedure to positively identify whether a caller asking for phone numbers is really an employee.

- Accounting codes for workgroups and departments, as well as copies of the corporate directory (whether hard copy, data file, or electronic phone book on the intranet) are frequent targets of social engineers. Every company needs a written, well-publicized policy on disclosure of this type of information. The safeguards should include maintaining an audit log that records instances when sensitive information is disclosed to people outside of the company.
- Information such as an employee number, by itself, should not be used as any sort of authentication. Every employee must be trained to verify not just the identity of a requestor, but also the requestor's need to know.
- In your security training, consider teaching employees this approach: Whenever asked a question or asked for a favor by a stranger, learn first to politely decline until the request can be verified. Then—before giving in to the natural desire to be Mr. or Ms. Helpful—follow company policies and procedures with respect to verification and disclosure of nonpublic information. This style may go against our natural tendency to help others, but a little healthy paranoia may be necessary to avoid being the social engineer's next dupe.

As the stories in this chapter have shown, seemingly innocuous information can be the key to your company's most prized secrets.