A 21st Century BANK HEIST

A Crash Course in Social Engineering

ABOUT THE AUTHOR

Barry Thompson, *Thompson Consulting Group, is a retired banker, consultant and writer with 30 years of service in the financial industry.*

"Social engineering" is a technique employed by penetration companies, consultants, and criminals to compromise financial institutions. You might recall Frank Abagnale, whose story was made into the movie Catch Me If You Can: He was nothing more than a social engineer of the 1960's. Abagnale eventually got caught, but the best social engineers today don't.

Social engineering enables criminals to compromise victims without their knowledge, yet with their help. We used to call this "confidence games." But confidence games are conducted a bit differently in the twenty-first century. For example, there are two ways to break into a computer system: 1) by breaking through firewalls, virus protection, or physically compromising the computer system; or 2) by just asking people to give you their passwords, which is much easier. The amazing thing is, people are all too willing to do the latter if you give them a reason to trust you.

One type of attack using this technique has been particularly successful recently. In this scenario, a caller tells the person at the other end of the line that they're a Microsoft technician, and that the computer owner's system has sent a notice to Microsoft indicating that their PC has been compromised. If the computer owner believes the caller, he/she will hand over access to his/her PC, right down to the required passwords.

Here's another example, but one targeting entire financial institutions. This attack depends on the social engineer knowing two things: 1) When an institution has more than five branches or locations, it's rare for all staff members to know each other personally; and 2) every bank has its own slang when it comes to discussing the general ledger, loan department, or operational procedures. (Imagine, for the purposes of this example, that a social engineer has discovered the crucial piece of information that a bank refers to its general ledger as the "yellow book" — because before the ledger was converted to an automated system, reports were actually kept in a yellow book.)

The social engineer uses this information to make telephone calls to departments within the bank and is able to talk to staff using its own vernacular. The goal? To discover the procedure the bank employs to make wire transfers. But whom to call first? Typically, a branch or the call center. Here's how the call would go:

XYZ Bank: *"How may I direct your call?"*

Social engineer: *"I need to talk to someone about making a wire transfer."*

Then, while the social engineer is waiting to be connected, he listens carefully to the on-hold advertising announcement that describes the services the bank offers — the first and easiest step to discovering more information about a bank.

"This is Karen. How may I help you?"

"Karen, I may have to wire money to my son at college. How do I do this?"

Karen responds quickly:

"The money will need to be in collected funds in your savings account so we can wire it to his bank. You'll need to have the bank's routing number and your son's account number. Before we can wire the funds, you need to sign our wire transfer agreement in person at one of our locations."

"Can I do that online?"

"I'm sorry, but because of our security procedures, you'll need to come into the branch to sign the agreement."

"OK. Will I need to do anything else?"

"The bank will call you at the time of the transfer to verify your intent to send the wire."

Now, our social engineer knows that he needs to find a way around the agreement obstacle. Of course he wants to avoid entering the bank for any reason; in fact, he may even be on another continent. So he needs some more information before deciding how he'll conduct the attack and he'll get it by talking to someone who knows how the wire transfer department works from the inside. After downloading the Annual Report from the bank's website, he discovers that someone named Maria is the officer in charge of wire transfers.

He picks up his smart phone to make the call. The goal now is to make the call look like it's coming from a bank employee. Using an application like "spoof call," an app for smart phones that can disguise his voice and even create background sounds to disguise his location, he selects the telephone number he wants Maria's caller ID to display.

Maria, who is trying to hit deadlines and really doesn't need any distractions, sees that her caller ID is displaying the telephone number of the branch that is located the farthest from the Main Office. She knows this could be a problem that needs to be resolved, so she decides to answer the telephone.

"Hi, Maria! I'm a new employee at the branch on Route 6. Our manager has gone to lunch, and a customer is asking me about how to make a wire transfer. Can you help me?"

If Maria actually believes she's talking to a new teller, she might explain how to perform the transfer. And if the social engineer senses reluctance on her part, he might mention the yellow book, as in: "I'm not sure what entry I need to make to the yellow book."

"Debit account 31556 and credit your branch account. Then fill in the paperwork and send it to me. Oh, and have the customer sign our customer service agreement and fax that information to our department at XXX-XXXX."

Success! Now, the social engineer has the inside number to fax requests for wire transfers, but he still lacks that pesky customer service agreement. In order to get it, he's going to use the owner of the local car dealership, "Mr. Big Bucks," as his target because he has already purchased his basic identity—so he knows his social security number, account number, and home address. (Keep in mind that some "confidential" information is as easy to obtain as purchasing a monthly subscription to a website like Spokeo.com.)

Next, our social engineer checks the owner's home address on Google Maps, looking for the location of the branch nearest his home. He decides to call the branch to see if they'll tell him whether the wire service agreement is on file.

XYZ branch: *"How may I help you?"*

"Hi! My name is Dave, and I'm Mr. Big Bucks' bookkeeper. He's going to need to make a wire transfer later, and I wanted to confirm that he's signed a wire service agreement."

"I'm sorry, but because of privacy rules we can't disclose that information to anyone but Mr. Big Bucks."

"Are you sure you can't you help me? He's out of the office now and told me to find out before he got back."

"Sorry, that information is confidential." The branch hangs up.

Since that tactic didn't work, our social engineer thinks about his next move and decides to pose as a bank employee once again. He looks for the branch nearest the car dealership, discovers it's on Yates Avenue, and finds the telephone number. After waiting ten minutes, he uses his smart phone to call the same office he just called, this time making sure that the Yates Avenue phone number is displayed on caller ID.

"Hi, this is Jim, and I'm a new employee over at Yates. Mr. Big Bucks is here and wants to wire money from his personal account. I can't find anything on the computer to show that he's signed a wire service agreement, and I need the off-setting account number for the yellow book."

"Let me check . . . OK, the account number is 31556."

The voice responding is a different one than our social engineer talked to last time -- which is the benefit of waiting ten minutes. And merely mentioning the yellow book is enough to convince this bank employee that he's legit.

"Yes, Mr. Big Bucks signed the agreement."

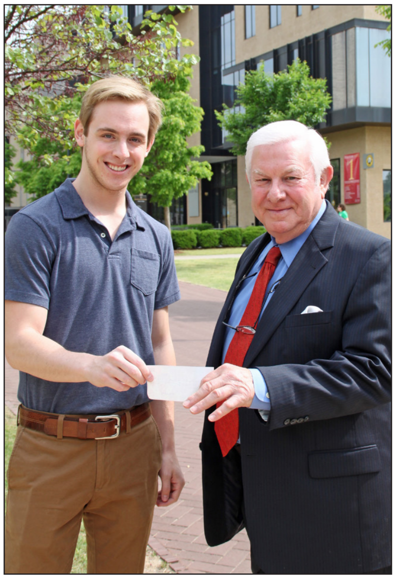
Social engineer, thinking quickly, *"OK, so do I have to have you send a copy of the agreement to Maria?"*

"No, just note on the wire form that the agreement is on file. It's in the system; it just isn't on the home screen. You have to go to the savings screen to find it."

"Thanks! I gotta take care of this right away. He's in a hurry."

Finally, our social engineer has all the information he needs to complete a wire transfer. First, he calls Mr. Big Bucks' home number, claiming to be the telephone company. He tells Mr. Big Bucks' wife, who answers the phone, that he's handling a service problem, and that he needs her to enter some numbers so he can check the system. The nice lady on the telephone willingly helps him by entering the numbers, which results in all of Mr. Big Bucks' calls being forwarded to his phone. The bank soon receives the wire transfer faxed from Mr. Big Bucks' telephone number. (Our social engineer has already obtained the form by visiting a branch a

Continued on page 18



Group 3 Scholarship Winner

John Maus of Morrilton, pictured with Dr. John Dominick of the University of Arkansas - Fayetteville, is the recipient of the ABA Group 3 scholarship.

Maus took Dr. Dominick's Financial Markets & Institutions course last fall and was in his Commercial Banking class this spring; Dr. Dominick states that he is one of the best students he's had in recent years.

Bank Heist

Continued from page 17

month earlier and posing as a photocopier repairman.) The confirmation call is made to Mr. Big Bucks' "home," where our helpful social engineer verifies the transfer.

Attack completed! The bank won't even find out it has been hit until Mr. Big Bucks calls to complain.

And there you have it: a basic social engineering scam that allows the social engineer to maintain anonymity. The ironic thing is that it could have been prevented by using a technique known as the "word of the day." Each morning, a word of the day can be sent to all employees, and every staff member must be able to provide it on demand. This ensures that confidential information isn't leaked to people who aren't staff members.

Indeed, sometimes the simplest and most cost-effective measures are among the most successful solutions to the growing problem of social engineering.