Social Engineering – A Real Story in a Multi-national Company

By Greggory Peck

"Hi! You must be Jan, pleasure to meet you! I just got off the phone with Jim in accounting who assured me you could direct me to the executive VP wing", "Pleasure to finally meet you! "I'm Rob Eldridge, the new Y2K Analyst." "I've been doing some Y2K Audits over in San Francisco in our branch office there. Looks like they finally broke down and sent me to Vegas!".

Confident that my communication skills were steady and ready to be tested I got out of the shower and picked out a nice pair of black slacks, a black silk button up shirt and a Rush Limbaugh Tie that just shouted "LOOK AT ME!" (Hmmm, this should really make me stand out amongst all the black slacks, white cotton shirts, and conservative ties, I thought. It's a funny thing - dress a bit outrageously and they all think about the tie, and miss the obvious…) I completed the outfit with a nice set of Florshiem dress shoes, a close shave and some mild cologne. On the drive to my target I continued to rehearse my cover story.

Pulling into the parking lot I got out of my car and stepped into the calm and collected persona I had generated for myself, Rob Eldridge, Y2K Analyst. I did a brisk walk to catch up with some employees wearing identification badges clipped to their shirts. I quickly begin to make some small talk.

Me: "Oh wow, traffic was terrible. Is it usually this bad?"

Employee: "Yep, every day! Are you new around here?"

Me: "Well kind of, I do most of my work out of the San Francisco office I'm just here to do a quick Y2K Audit."

Employee: "That sounds pretty exciting. The company flies you across the US for this?"

Me: "They sure do, I've never been to Las Vegas, so I was especially looking forward to this trip."

We walked across the parking lot and were now standing in front of a large double glass door with two visible security cameras and a proximity key card system. My new friend, who I later learned was the Director of Marketing, held his badge to the proximity reader and was rewarded by a quick "pop" as the

magnetic locks on the double doors were released. I walked in confidently, giving no sign that I didn't belong. As I approached the front desk, an attractive young lady who proudly wore a nametag identifying her as "Jan" greeted me with a smile.

Me: "Hi Jan, I'm Rob from the San Francisco office. I'm here to do a Y2K audit. Could you direct me to the break room? I haven't had my coffee this morning and, well, I'm just not human until I get some of that devil juice in my system."

Jan: "Oh, nice to meet you, Rob. Sure, the break room is through those double doors and down the hall to your right. Since you're visiting from the San Francisco office, I'll buzz you right through. Oh, I'm out of temporary badges. Just take this yellow sticky note and write your name, office location and the word visitor underneath it, then clip it to your shirt pocket. That way, people will know your name."

Me: "Thanks, Jan. You know, I'm going to have to take you out for lunch so you can show me around Las Vegas, right!" <Innocent friendly flirt>

Jan: "Tee-hee, Sure, babe, if you're buying, I'm game. Oh, by the way, if you need access to the server room, just talk to Mark McMillan. He can get you a temporary access code. The Deloitte & Touche auditors had a lot of problems, though. So if you run into trouble just call x1566."

Social Engineering

Me: "Mark Mcmillan, Mark Mcmillan, now I know I've heard that name a few times."

Jan: "Oh, he's the executive Director of Facilities. His office is in the executive wing which is through the double doors down the hallway to your left."

Me: "Thanks again, Jan."

With this Jan buzzed me through the second set of double doors where I quickly made my way over to the break room. Pouring a large cup of coffee, I took a seat for a moment to quietly rehash the latest set of events and keep my cover story in order. I began getting a little nervous but brushed it off and enjoyed the nice cup of Java. After what seemed to be almost a half an hour (in fact only 5 minutes), I finished my cup of coffee and made my way down a long lavish hall until I reached a sign that read "James Mullen EVP Western Operations". I glanced to my right and noticed another attractive young lady who I presumed was James Mullen's administrative assistant.

Figure 2: Gregg walking down the hall.

Me: "Is James in by chance? I'm here from the San Francisco office to do his Y2K audit"

AA: "Yes, he sure is. Just a moment"

Social Engineering

The lady picked up the phone and informed James that the "Y2K Guy is here to look at your computer". A moment later the large oak door opened up and a tall thin gentleman in his late 40's stepped out. "Come on in," he invited.

After initial introductions, he invited me to take a seat at his computer while he went to the gym. I quickly stopped him and explained that I would need his logon name and password to complete the audit. He pointed to a yellow sticky pad taped to his desk and said "There they are, right there". He then turned to head out again and I quickly stopped him once again. "There is a small chance that the program used to update your computer might damage certain spreadsheets and word documents, could you point me to where you store those files so I can back them up onto this Zip Disk?" I produced a blank Zip Disk from my shirt pocket and he eagerly complied, taking me right to his work files. (That saved me a little bit of time. I thought to myself, this is going to be a breeze!) I thanked James and he assured me it was no bother and headed off just asking that I shut his door when I leave.

Within seconds of him leaving his office, I quickly got to work producing another blank Zip Disk and copying all his word and excel documents to both Zip Disks. I wrote down his login and password information and filed it away for future use. In my last step I perused through James's desk drawers looking for anything that might be helpful. My eyes gleamed with excitement as I located a corporate MasterCard belonging to a one James Mullen. I quickly scooped up the credit card and filed it away in a coat pocket for later.

I left James's office and headed further down the hall. I stopped in every office along the way down the hall, introducing myself to the Admin Assistants and the Executive Vice Presidents. Each and EVERY EVP willingly gave me their login IDs and passwords and allowed me to copy their confidential files. After all, I was the Y2K guy. I was here to help them!

After reaching the end of the hall, 10 offices, 10 login ID and sets of passwords, two hours and a Zip disk filled to capacity with confidential files later I stopped in to visit with Mark Mcmillan. I found mark sitting behind his desk at the end of the hall in an office the size of my living room! Blueprints and CAD drawings littered his office and he looked more like a building

engineer than an executive VP. I walked up to his desk and briefly introduced myself.

Me: "Nice to meet you Mark. I'm Rob Eldridge from the San Francisco office. Jan assured me you were the man to talk to if I needed access to the computer room."

Mark: "Yep, that would be me, the computer room is down the hall and the second room on the right. It has an electronic keypad the combination is 2,4,9,1,5. Here, take this key just in case the combination doesn't work. I've heard its been acting up recently."

I thanked Mark and headed straight for the company's primary server room. (I would really score here, I was sure.) I reached the tall steel reinforced door protected by the electronic combo lock and typed in the magic numbers 2,4,9,1,5. I heard a quick clicking noise, tried the doorknob and, voila, I was now in the heart of the company's technology room. I gasped for a moment as the cold dry air hit me, the thermometer on the wall read 62 degrees. The room was about 4000 sq. ft with rack after rack after rack of Compaq Proliant Servers, HP3000's, and even a very sharp looking Sun Enterprise

Figure 3: Hacker Mecca: the server room.

Social Engineering

Thoroughly taken aback that it was so relatively simple for me, a complete stranger, to talk my way into the heart of the company's operations, I could hardly contain my excitement. Not wanting to stick around in the server room for too long, I headed straight for the wall of DLT tapes. I located the more recent DLT tapes labeled "Registry Backups" and placed them into an oversized FedEx envelope I produced from my pocket. While preparing to leave the server room I noticed a stack of floppy disks labeled ERD. A large smile crossed my lips as I realized that these are likely Emergency Recovery Disks and stood a good chance of containing "Rdisk /s" information, which are the SAM password databases for NT Servers) I quickly added the set of diskettes to my FedEx envelope. It was difficult to seal, as it was so full.

Leaving the server room, I passed the Mail Room on my to the end of the hall. I stopped in to introduce myself to the friendly mail lady who was hard at work.

Me: "Pleasure to meet you, I'm Rob Eldridge from the San Francisco office you must be the person I need to see if I need to get this package mailed out."

MailLady: "Yep that would be me. Where do you need the package to go, and how do you want it sent?"

Me: "Oh send it to…" (I gave her the address of a Days Inn the next county, over figuring I would check in there tonight, receive the package the following day and reap my rewards!).

MailLady: "Sure thing. It was a pleasure meeting you!"

I left for the day and checked into a hotel the next county over. I checked into the same exact hotel as I had addressed the package to. I could have gone home, but I certainly didn't want this package being sent to my house, did I??? I used James Mullen's corporate credit card that I had swiped to pay for the hotel room. They never even asked for my identification just asked me to fill out a piece of paper which of course asked for my name and other information.

I retrieved the laptop computer and portable ZIP Drive from my car and made it into my room. I quickly booted up and inserted one of the ZIP disks. I started going through the files one at a time. I had all kinds of wonderful information that would for

all intensive purposes allow me to "own" this company. I had strategic business plans for the upcoming year, financial numbers, confidential interoffice memos, private acquisition information, and even a couple of documents detailing power struggles at the highest levels of the company. After digesting as much of the information as I could, I quickly fell asleep.

I awoke at about 10am expecting to have the FBI at my hotel door! I had a quick panic attack and cracked the door sticking my head out to look around. Nope, so far so good. I realized I would need to make one more trip inside the company and go for the mother of all prizes: the data and login and password of the company's Chief Executive Officer. I showered, collected my laptop and headed downstairs to check out knowing full well that my FedEx package would be awaiting me. Sure enough, as I was signing out, they handed me a large FedEx envelope. I signed my name, James Mullen, on the bill and headed off back to the office.

I greeted Jan again who pointed me in the right direction to Paul Chamber's office. Paul Chambers, I had learned, was the CEO of my target company. As luck would have it, I bumped into the gentleman I had met the day prior while walking the parking lot. It was now that I learned that he was the Director of Marketing for the company. We made some more small talk as we walked down the hall. He mentioned he was heading in to get a signature from Mr. Chambers. I thought, how perfect, this is my opportunity. My new-found friend lightly knocked on Mr. Chambers' door and was met with a handshake from a gentlemen who was obviously the one in charge. My friend then introduced Mr. Chambers to me. After dispensing with formal introductions, my unknowing partner in crime got the signature he needed and left.

I stayed to explain to Mr. Chambers the very same thing I had told to all the other people whom I had duped into giving me their login ID's and Passwords. Mr. Chambers invited me to have a seat in his chair behind his desk He willingly provided me with his login and password information. This being my ultimate score, I didn't have the tenacity to ask for the location of his word and excel files. Nope, instead I just did a quick file search in the background while he wasn't looking.

The CEO was obviously a bit more interested in what exactly I was doing on his computer because he asked three times the number of questions as the previous victims had. At this point my nerves were on end and I'm certain the hairs on the back of

my neck were sticking up on end but I managed to control my breathing and reassure Mr. Chambers that we were nearly ready for Y2K and everything was progressing smoothly.

Mr. Chambers was far too interested in my activities on his computer for me to dare copying his files to a ZIP disk. Instead, I did a quick sequence of Copy/Paste's to his file share which I knew was located on the File Server and figured I'd go to the server room to make the copies there. When Mr. Chambers went to go flag down a colleague in the hall, I logged him out, smiled with gratification and excused myself from his office explaining that he was already Y2K Compliant and wouldn't be needing any software fixes. He smiled and thanked me for my assistance.

It was at this point that I went to my car and retrieved all the stolen data and business intelligence, the diskettes and registry backups, the zip disks, the passwords written down on paper, the credit card, etc. I placed them all into a small duffel bag and followed another employee back through the magnetically controlled doors. I made my way directly to Mr. Chamber's office. I didn't bother knocking and just walked in taking up a seat in front of his desk. He looked a bit surprised, but asked what he could do for me.
It was at this moment that I opened up the duffel bag, laid all the business intelligence out in front of him and explained:

Me: "Mr. Chambers I have a confession to make, my name is not Rob Eldridge, I do not work out of your San Francisco office, and I know nothing about the company's Y2K status."

CEO: "HuH??? I'm afraid I don't understand, Rob."

Me: "That is what I'm saying Mr. Chambers my name is not Rob, I made the name up. My real name is Greggory Peck."

I then explained the value of the information that was now spread out across his desk.

Me: "It's a good thing you approved that personnel request, I'm your new Security Analyst, and by the looks of things, I have a lot of work to do."

The above story is based on a real life experience, I was starting a new job with a large corporation as the company's lead security analyst. I knew that all the Intrusion Detection

Social Engineering

Systems, Firewalls, Video Cameras, proximity locks, and key codes weren't going to be worth a single red cent if the employees were not security-minded and would give out their login ID's and passwords. It's safe to say that things are vastly different today then they were just a little over a year ago when this took place. I had obtained full permission to take ANY and ALL necessary steps to make this "audit" a success by the solicitation of the companies board of directors shortly after the job offer was made. Most everything in the audit relied upon social engineering. Of I had been a malicious hacker or competitor, the damage to the company would have been well into the 10s of millions of dollars if not the 100s of millions. It's important to note that nearly everything