Scam Your Clients for Their Own Good

By Chris Hadnagy

As a professional social engineer, it is beneficial to study the methods of scamming that the bad guys have used in the past, compare it to modern tactics and see what can be learned. Experts have agreed that the motivation for most scams is greed. Although that is true, it is also found that fame, attention or just the need to maliciously hurt and steal from others are strong motivators for scamming people. This month, let’s analyze some old scams, compare them to a modern-day equivalent and see what we can learn as Social Engineering Pentesters.

Although scams have been around since the dawn of man, this one from 1812 is notable. A Philadelphia man name Charles Redheffer claimed that he invented a perpetual motion machine, a theoretical device that, after only one initial input of power, will perpetually continue to generate energy. Even though such a machine would break the laws of thermodynamics, his claim was supposedly backed up by an actual working device. His next desire was to secure government funding to "build a larger version". He actually got the money and built a new machine, but he then fled the city when inspectors found that he had hidden the real power source. Undeterred, he tried the same scam in New York City but was again caught when the inspectors removed a wall of the machine to reveal an old man eating a sandwich and turning a crank. This machine can still be seen today in the Franklin Institute of Philadelphia. In analyzing this scam we can see some basic principles at play here.

Discuss in Forums {mos_smf_discuss:Hadnagy}

Mostly what we can see from this scam is that it is based on greed. People wanted to believe in his invention, as it would have been a significant technological advancement. What's more is that he offered "proof" that his promises were close to completion. This basic scam was based on promising something that people wanted, and that promise would cost them… and it did.

50 Years Later

About 50 years later in 1875 John Ernst Worrell Keely founded the Keely Motor Company. John "invented" another amazing machine, the "vibratory engine." This amazing device could run a fully-loaded train for over 1 hour on only 1 quart of water.

When he displayed this device for investors they were all more than willing to pour money into this invention. 14 years and LOTS and LOTS of money later, poor Keely died. After his death, the machine was inspected to see what it was that all their money should have bought. To their surprise there was an air compressor two floors down that powered the "vibratory engine," and no water was involved.

Another greed-based scam. This scam was based on the same principles as Redheffer's scam… the need for people to believe that this was possible and, with some patience and money, they could not only be a part of history but become wealthy in the process. It plays on greed in two parts. Firstly, the greed of the scammer and how he takes money for something he knows is false. Secondly, the greed of the investors thinking of the promise of the "big payout" they can get if this works.

Bras Are Good

Another scam to analyze focuses on bras. Yes, the story of The Brassiere Brigade takes us to 1950 in Miami, Florida. Police uncovered a crime ring that involved young women working for a local phone company, Southern Bell. The police found that when you mix young women, lingerie and money anything can happen.

These employees had the job of counting the money that came from pay phones. Before the money was officially marked as counted, the girls would stuff $15 rolls of quarters down their bras. They would hide up to 4 or 5 rolls at a time and then excuse themselves to the ladies room. From there a "handler" would take the rolls and smuggle them from the building.

Through a report by one of the girl’s roommates, they were caught and, through an amazing turn of events, they were released and the full amount they stole was never determined.

This scam again feeds off of greed. Different from the last one as it is just off of greed of the scammers. This scam didn't involve actually tricking people into a corner as much as setting up a process to extract and hide the money.

Feeding Off Pain

The previous examples might seem humorous to us, where as this next scam is one that will probably disturb us all. After the attacks in New York City on 9/11/2001 where terrorists took out the Twin Towers killing thousands of innocent people, the pain and suffering wasn't over. Many saw the amazing way in which the whole world came together to support, love and help those who lost loved ones in those attacks. For some, they saw an opportunity to scam people.

Here is a list of just a few accounts:

• A woman from Vancouver, Canada reported that her daughter was killed in the attack. Adding to the sob story to get even more sympathy, she said that bereavement leave from her own employer was denied. Over $2000 was collected from friends, family and even public officials looking to get good press. The truth... the daughter was living in Winnipeg and obviously still alive. Turns out that the mother and daughter hadn't spoken in years.

• Another man claimed that his son died in the World Trade Center. He received $160,000 from the Red Cross on behalf of Wilfred. Because of the topic of this article, it should come as no shock that he didn't have a son named Wilfred. But that didn't stop him from parading around in a shiny new vehicle. This particular stunt was eventually rewarded with a sentenced of 11 out of a possible 33 years.

• A young Moroccan woman reported that her sister had been working in a bond-trading firm inside the WTC. She gained national attention by appearing on the Rosie O'Donnell show. After finding out that she never had a sister living in NY, the woman mysteriously disappeared.

This last scam is a lot different the all the previous ones. Even though in some there was a payout, this scam was based on people’s need for attention. One expert denoted that when the scammer saw and heard of the attention that many of the victim's family was getting, they became jealous. They wanted to feel part of that "love." To get the feelings they craved, they created fake family members that suffered tragic loss.

Unfortunately, it might seem like no one is hurt by this type of scam, but there is some serious damage done. Trust. People are "taught" by this type of scam to be distrusting, and that can affect how others view those in need. Sadly, this can even affect how people treat those who really need help.

What We Can Learn As Social Engineering Professionals

The principles haven’t changed much over the years as greed and sympathy still play on people’s emotions. As social engineers we need to be aware of how these emotions are being used by malicious social engineers and in turn use them in our engagements with clients.

Although covered above, let’s continue with greed. It sounds so much like a movie, but corporate espionage is truly a reality in these times. Often the “marks” or targets within these companies are enticed through greed. To sell company secrets, files or intellectual property a malicious social engineer will find those who are disgruntled with the company or are in financial troubles, and then make them an offer “they can’t refuse.”

As a social engineering pentester, we need to test our clients for this vector of attack. Of course we do not want to commit corporate espionage as a practice, but in one social engineering risk assessment I did for a client, I was asked to look for employees that were on the web complaining about the company, looking for work elsewhere and showed potential risk for being targets by malicious scammers. These are touchy types of tests, but remember our goal is to protect our clients and help them remain secure from threats both inside and out.

Next is sympathy. This one is used with a lot of success in the social engineering world. Psychologically humans have a built-in mechanism to want to help others we see in need. It is why a movie or TV show we know to be fake can move us to real emotional responses. When we see and hear another human in need we instinctively have emotional reactions.

A malicious social engineer can use this on a small scale to get an employee to allow them access and even to give them information they do not deserve. In one test for which I am not particularly proud, we used sympathy by feeding on the CEO’s personal interest in a children’s cancer fund to pull the sympathy card and get him to go to a link and open a file he should not have. Does this mean I promote being cold and not caring? Not at all, what I promote is being more self-aware and thus making the company more secure.

In 2005, a group of researchers (Deborah A. Small, George Loewenstein, and Paul Slovicdid) a study called, “Sympathy and callousness: The impact of deliberative thought on donations to identi able and statistical victims.” This study showed a very interesting piece of research. When a call went out for donations to help “The 10,000 children who will die this year in auto accidents,” the donations were minimal. But when “Baby Jessica” fell into a well over, $700,000 USD was sent to help in her rescue. The study went on to show how, when a personal attachment is made and then sympathy is induced, an emotional response made people part with their hard earned cash. If that is the case, anyone can use a targeted attack, build rapport and then play the sympathy card to get the target to either give information or take an action that would not be in their best interest.

The same rules apply in a pentest. The professional social engineer can use both greed and sympathy during in-person assessments, phone calls and email messages to get a target to click a link, open a file or answer questions giving over valuable information. The main difference between the good guys and the bad guys is that we have permission and eventually help plug the holes in the clients’ defenses.

How Can You Educate Your Clients to Protect Them

Here is a very short list of things to keep in mind to identify modern day scams:

• Double and Triple-check what the caller or email says. If “your account may be compromised” or you are being asked “to donate to help poor Sally,” do a little searching to see if you can find the information online BEFORE you click that link. Verify to protect.

• If it sounds too good to be true, it may be. Sometimes telling a target that they won a prize or an award plays the greed card. They ask for some small bits of info or payment for shipping fees, but in the end it can be a scam.

• Ask for their details before you give yours. What I mean here is to get a callback number, address, name and company, before you tell them anything. Of course all of these details can be spoofed as well, so I promote jumping to #1 before proceeding.

• Learn from Audits. Of course this implies you are getting audits or at least risk assessments from a professional social engineer with experience and a good reputation. When the professional goes through the steps, it can help your company to find the holes, uncover potential threats and then patch them up.

Preparation and education can go a long way in protecting you and your company from falling prey to this type of attack. Simply making your clients and their employees aware that these long-standing types of attacks are being brought into the digital age is enough to prevent most of them from being successful. Of course, nothing beats critical thinking and good old-fashioned common sense.

So go ahead, scam your clients. In the end, they’ll thank you for it!

Until next month…

If you have comments or questions – please feel free to reach out to me at logan@social-engineer.org

Chris Hadnagy, aka loganWHD, has been involved with computers and technology for over 14 years. Presently his focus is on the "human" aspect of technology such as social engineering and physical security. Chris has spent time in providing training in many topics around the globe and also has had many articles published in local, national and international magazines and journals. He is also the lead developer of Social-Engineer.Org as well as the author of the best-selling book, Social Engineering: The Art of Human Hacking.

He has launched a line of professional social engineering training and pen testing services at Social-Engineer.Com. His

goal is to help companies remain secure by educating them on the methods the "bad guys" use. Analyzing, studying, dissecting then performing the very same attacks used by malicious hackers on some of the most recent attacks (i.e. Sony, HB Gary, LockHeed Martin, etc), Chris is able to help companies stay educated and secure. Chris can be found online at http://www.social-engineer.org/, http://www.social-engineer.com/ and twitter as @humanhacker.