Social Engineering in Practice

Jordan Coff
University of Wisconsin-Madison
College of Letters and Science
coff at wisc dot edu

ABSTRACT

Social engineering has been around for centuries and has only grown with internet boom. In this paper I present the findings of my research and experimentation in social engineering principles and techniques. This study was conducted through the lens of cyber crime and in particular, the theft of sensitive data, although this is just a subset of social engineering. It was my belief that using my research of social engineering I could create and conduct a scheme to obtain students' login credentials for both the university student portal, and their email accounts.

Categories and Subject Descriptors

K.6.5 [**Management Of Computing And Information Systems**]: Security and Protection—*Unauthorized access*

General Terms

elicitation, pretexting

Keywords

Social Engineering

1. INTRODUCTION

Worldwide spending on information security is expected to reach $71.1 billion in 2014 [1], but how will that information be kept safe when it's in the minds of companies' human assets?

In 2003 the organizers of security conference, Infosecurity Europe, conducted a study in Waterloo Station in which they asked passers-by to divulge their passwords in exchange for a cheap pen. Although the researchers made no attempt to validate the passwords given to them, 90% of the subjects gave up a password [2]. Have users learned since then? What does it take to achieve similar results? In these more modern times with cyber crime frequently in the headlines[1] , would people be more security aware?

To answer these questions I set out to identify the strategies and principles of social engineering and test their effectiveness on my peers in a controlled experiment. To that end, this paper details the most important of the aforementioned strategies and principles, as well as the experiment that I conducted with the help of an accomplice.

2. EXPERIMENTAL METHOD

First I defined the basic concepts whose effectiveness I'm attempting to measure. Then I describe the broad strokes of my experiment. Finally I break down the design considerations of the experiment and relate each to the basic concepts.

2.1 Basic Concepts

2.1.1 Information Gathering

Know what information you're targeting. Then view every other piece of information you receive as a potential link to your target. For example, professional penetration tester Mati Aharoni was given only the name of a company. He googled the corporate email domain and found that a high executive was using his company email on a stamp collecting forum. Aharoni made a fake stamp sales website with a malicious frame and emailed the executive saying that he saw his posts on the forum and that he was selling his dead father's stamp collection at foobarbaz.com. The executive clicked the frame and control of his computer was given to Aharoni [3].

2.1.2 Elicitation

Elicitation is the act of drawing the mark out, or inciting a certain behaviour in him/her. For example in the Waterloo Station pen study, the social engineers approached people and asked them to participate in a study about security in the workplace (which was ironically true) in exchange for a pen. This act of approaching the subject and convincing them to answer your question is elicitation. If done well, the subject is happy to perform whatever task you ask of them and not at all suspicious [3].

2.1.3 Pretexting

Pretexting is the story that you tell the subject: [3]

> "I'm a guy who's selling my dead father's stamp collection. I saw your post on the stamp collector forum. Click on this link to view them on my website."

2.1.4 Quid Pro Quo

The promise of something in return for their time, information, etc..

[1] http://www.wired.com/2014/12/sony-hack-what-we-know/
http://www.cnn.com/2014/04/08/tech/web/heartbleed-openssl/
http://www.cnn.com/2012/08/06/tech/mobile/icloud-security-hack/

2.2 Experiment Outline

My target for this attack was the usernames and passwords of students at UW-Madison. In particular, their usernames and passwords for the student center portal and their non-university email addresses. The first thing I did was recruit an innocent-looking female accomplice. The two of us went to a library on campus dressed in business casual attire with a laptop computer and a professional-looking portfolio with a note pad. We walked around the library looking for people that either talking to someone, looking at their cell phones, or on FaceBook. We approached with the line:

> "Hi, we work for the company that makes the student center portal and we're doing a usability study to try to improve the system. Do you have a few minutes to talk to us?"

If they agreed we would thank them and sit down across from them. I would then say:

> "Ok so here's the experiment. We want to see how quickly our users can perform a basic task on our system, and compare that time to how long it takes them to use another system such as their email account. So my partner here is going to time how long it takes you to log onto student center and view your current class schedule, then she's going to time how long it takes you to log on to your email account and view an email."

At this point, if they agreed, I would hand them my laptop and say "go". After the subject finished logging onto either system, my partner would report the time to me and I would write it down, smile and make a friendly sarcastic comment like "Wow it's a world record" or a light-hearted sarcastic comment like "Oh boy you're slow!" Then we would remind them to sign out of their accounts and debrief them on how the study they just participated in could have exposed their passwords.

How were their passwords exposed? If I had had a key logger installed on my computer it would have captured their usernames and passwords for both accounts. And so I had achieved my goal of getting their credentials with the added bonus of verifying that they are correct.

I did not actually have the key logger installed and retained no data on my subjects. I gave them a debrief form which explained the experiment, gave tips on avoiding social engineering scams, and provided my information in case they had questions.

2.3 Design Considerations/Motivations

2.3.1 Target Data

According to Microsoft researchers Florêncio and Herley, web users have an average of 6.5 passwords, each of which are shared across 3.9 different sites. This means that if I retrieved two distinct passwords, I would gain access to an average of 7.8 different sites [4]. In this case I'm guaranteed access to two different email accounts, and the student center which has names of family and emergency contacts, addresses, phone numbers, the last four digits of the bank account number and routing number of anyone who has paid tuition on that account.

2.3.2 Accomplice

The accomplice had a huge effect in terms of pretexting. People are more likely to trust two people than one, especially when one is a very friendly looking female.

2.3.3 Location

We chose to perform our experiment at a carefully selected school library for three main reasons

1. It's surrounded by campus buildings
2. It's not open to the public
3. Doesn't check student IDs unless you look suspicious.

The first and second point listed above give the students there a false sense of security, while the third point would grant us admission even if we weren't actually students.

2.3.4 Appearance

Appearance is a colossal part of pretexting, as a faulty first impression could make the subject suspicious throughout the experiment. We chose everything about our appearance with our characters in mind.

2.3.5 Fake Experiment Premise

This worked to our advantage in a few ways.

1. It was our main form of elicitation as it gave us a reason to ask them to log into their systems on my computer.
2. Offered a subtle quid pro quo. Their participation would supposedly lead to the improvement of a notoriously bad service that all students have to use daily.
3. The fact that it was an experiment gave us reason to be stringent with how we wanted things to be done. For example they *had* to use my computer during the study to maintain consistency in the name of the scientific method.

2.3.6 Comments and Conversation

During the experiment we injected as much conversation as possible. This brought us down to the same plane as the subject. We used it to convince the subject that we were just normal students working a job that we weren't too serious about. This helped with pretexting and put them at ease so the experiment (elicitation) could be done without their suspicion.

2.3.7 Miscellaneous

The use of the key logger turned out to be a very key piece in the success of the experiment. If the subject didn't know what a key-logger was, they would think that their accounts were safe as long as they logged out after they were done.

3. RESULTS

Our experiment was extremely successful. We asked 21 people to participate. Of those, 18 agreed to participate. Of those 18, all of them successfully logged in to both of the systems on my computer which we took for granted *could* have had a key-logger installed.

86% participation rate
100% credential theft rate of participants

4. CONCLUSIONS

The principles of social engineering studied and presented in this paper are obviously very potent even in the hands of a novice social engineer. Of those that I used, I found pretexting to be the most crucial. The subjects had full trust that I was who I said I was, and as such they had no reason to suspect anything. I predict with extreme confidence, that using the same (or similar) method I could have gotten any piece of data that I wanted from the subjects.

I can also conclude that people are still susceptible to social engineering attacks even though threats like identity theft and internet fraud are out in the open. By using technology that most subjects were not aware of (key-logger), and providing them with a plausible background story, I was able to steal (or prove that I *could have* stolen) some of their most sensitive data.

5. ACKNOWLEDGMENTS

Thanks to Jamie Kolb, whose experience in experimental psychology helped me plan my experiment to be in accordance with IRB guidelines.

Thanks to Melanie Ginsburg for being my accomplice in the experiment with the utmost professionalism.

6. REFERENCES

[1] Gartner. Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware. Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware. N.p., 22 Aug. 2014. Web. 14 Dec. 2014.

[2] Leyden, John (18 April 2003). ”Office workers give away passwords”. theregister.co.uk. Retrieved December 2014

[3] Hadnagy, Christopher. Social Engineering: The Art of Human Hacking. Indianapolis: Wiley, 2011. Print.

[4] Florencio, Dinei, and Cormac Herley. ”A Large-Scale Study of Web Password Habits.” (n.d.): n. pag. Research.microsoft.com. 2007. Web. 13 Dec. 2014.