Department of CEE/ Computer Science

Defense Against Human Hacking

Austin Huynh, Diana Orea, Marissa Ramirez, Ryan Moffit, Victor Lin

Advisor: Dr. Melissa Danforth Assistant: Alfonso Puga

CSU Bakersfield

Chevron

Research Experience Vitalizing Science — University Program

NSF

Partial support for this work was provided by the National Science Foundation's Federal Cyber Service: Scholarship for Service (SFS) program under Award No. 1241636.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Background

What is social engineering? - "...social engineering is the act of manipulating a person to take an action that may or may not be in the target's best interest." Christopher Hadnagy - Social Engineering: The Art of Human Hacking.

Like regular hacking, social engineers attempt to breach a company's security to gain information for monetary gain or power. While companies may have strong technological security in their security systems, their personnel usually lack strict protocol and proper training to prevent social engineering attacks. Knowing the techniques of social engineers helps with recognizing and defending against social engineering.

Purpose

To research and review case scenarios in order to understand the mind of a social engineer; using that knowledge to develop a list of guidelines to recognize and to shut down attacks from social engineers.

Techniques

Information Gathering:

Information Gathering is crucial to a successful attack because it provides an understanding of the target, which then creates a foundation for possible vectors of attack. Examples of Information Gathering: Conversation, Search Engines, Books, Magazines, News Reports, Background Checks, Blogs, Inside Job, Dumpster Diving, Websites that purchase information from banks, etc. Information Gathering attempts to identify the most direct route to the target.

Real Life Example: Finding out a high ranking CEO of a company used his work email for his stamp hobby collection (This small information could possibly lead a way for the social engineer to compromise the company's security system).

Prevention of Information Gathering:

Train employees on what is sensitive information and how not to reveal it. Employees should also know that work materials should stay at the designated workplace. Employees must know how to properly dispose of important documents to prevent dumpster diving. Restrict the amount of information online about the company to prevent information gathering.

Communication Modeling:

Communication modeling allows the social engineer to get a response from a person, most likely personnel of the target company, to gather specific information in order to "...decide the best method of delivery, the best method for feedback, and the best message to include" in his or her attack. Christopher Hadnagy – Social Engineering: The Art of Human Hacking.

Steps of Communication Modeling -

1. The Source: The social engineer shall be the source of communication to relay the information he or she has gathered.
2. The Channel: By first communicating, the social engineer will decide what is the best way to channel their attacks to the target, whether through email, mail, and etc.
3. The Message: With the information gathered and the best method of channeling the attack decided, the message will contain what the social engineer will say to the receiver (a.k.a. the target).
4. The Receiver: The social engineer will have to decide the best target to receive the message.
5. The Feedback: This is the desired reaction from the target where the compromise in security is successful, or sometimes, unfortunately not.

Real Life Example: The social engineer used the CEO's stamp collecting hobby as his source. Then, using three different channels which contained the message; a phone call was made to tell the CEO that the social engineer had sent an email, which contained a link to a phishing website (malicious website) disguised as a stamp collecting website. The receiver (the CEO) responded in favor to the social engineer's attack by clicking on the link and compromising the company's security; a desirable feedback.

Prevention of Communication Modeling Based Attacks:

Teach all employees to not access personal email in a company workplace or through a company computer/laptop. Properly instruct company personnel about how, why and when should they help strangers or other company employees.

Elicitation:

Elicitation is the method of drawing out a certain conclusion (behavior or truth for example) that the social engineer wants through his or her appearance, attitude, body language, and etc.

Guidelines to elicitation:

1. Be Natural: The social engineer keeps a natural demeanor by talking to the person about a subject either well known to both parties or just the social engineer. This allows for a easier chance to elicit a response from the person.
2. Educating: The social engineer will educate himself on a particular subject before initiating a conversation with the person, which will help with the natural demeanor of the social engineer. This keeps the social engineer from revealing his identity to the person.
3. Limits to greediness: The social engineer will not focus the entire conversation on getting answers and actions out of the person, rather he or she will feel out the conversation and give something that would elicit a feeling of reciprocation from the person. This avoids the target from losing interest, or feeling suspicious. Social engineers will attempt to set up further possible elicitation attacks by setting up further encounters.

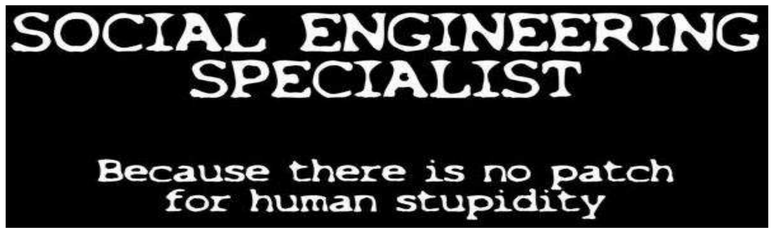
Real Life Example: Using alcohol, and the guidelines for eliciting a response, the CFO of company XYZ spilled sensitive information about his company to the social engineer.

Prevention of Elicitation:

Be careful of what one says, especially while talking to a complete stranger even if they share common interests and/or seem friendly. Avoid the consumption of alcohol when one is around strangers and holding company property. Company information should only be discussed with authorized personnel, no exceptions.

Conclusions

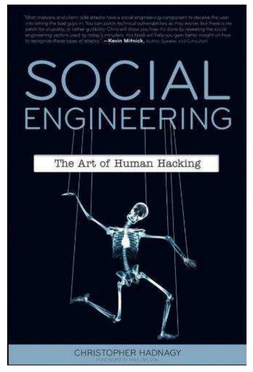
Social Engineers, when targeting large companies through employees, have the ability to cost the company billions of dollars in damages. Through reviews of case studies on attacks by social engineers, we have unanimously decided it critical that employers and employees alike train in recognizing and properly responding to social engineering attacks.



Acknowledgements

- Chevron
- National Science Foundation
- California State University of Bakersfield
- *****Alfonso Puga*****

- Social Engineering: The Art of Human Hacking
- Mindfulsecurity.com (Images 1-3)
- Home.mcafee.com (Image 4)
- Zerosecurity.org (Image 5)
- Social-engineer.org (Image 6)



Fun Facts:

•Kevin Mitnick, arguably one of the most famous social engineers, used his skills at the age of 12 to bypass the punch card system used by the public bus transit in LA, gaining the ability to ride on the buses to any location for free.

•Mitnick later used his skills to access DEC, a computer operating system manufacturer, in order to steal copies of their latest operating system; this crime made him a fugitive from the FBI for over two years.

•Common acts used by magicians, such as Penn and Teller, are closely related to social engineering principles.

•Con men typically use social engineering coupled with a technique called "Sensory Overflow," which overwhelms the target's senses by making them unable to focus on the details of a situation, thus preventing them from noticing what the con man is actually taking from them/cheating them out of, these are supplemental skills for a social engineer.

•Social Engineering is often showcased in Television shows such as the Mentalist, Lie to Me, and White Collar, and in Movies like Sherlock Holmes, Catch Me If You Can, and Sneakers.

•American Security Consultant, Frank William Abagnale Jr, was once one of the most evasive and clever social engineers of his time. He was an amazing imposter, assuming the identity of an airline pilot, a teacher, a doctor, a lawyer, and an agent of the U.S. Bureau of Prisons.