Chapter XIV
Social Engineering and its Countermeasures

Douglas P. Twitchell
Illinois State University, USA

ABSTRACT

This chapter introduces and defines social engineering, a recognized threat to the security of information systems. It also introduces a taxonomy for classifying social engineering attacks along four dimensions: who or what the targets are, what media are used, how the attacks fit in an attack cycle, and the techniques used to execute the attacks. Additionally, the chapter discusses current social engineering countermeasures and how to map attack types to these countermeasures. Finally, the chapter ends with a discussion of future trends and technologies for defending against social engineering attacks. Use of the taxonomy should help security professionals and researchers understand social engineering attacks, and implementation of the discussed current and future countermeasures should help professionals reduce the risks associated with social engineering attacks.

INTRODUCTION

In 1970, Jerry Schneider took part in an early example of social engineering. While dumpster diving the local Pacific Telephone office, Jerry found the procedures for making internal equipment orders and charging them to company accounts. Posing on the phone, or pretexting, as company employees he was able to get the correct account numbers and eventually stole and resold about $250,000 in computer equipment (Whiteside, 1979). Twenty-five years later, in 2005, Hewlett-Packard’s board discovered that sensitive information from a board meeting had been leaked to the media. The chairman of the board decided to determine the culprit and hired a security con-
sulting firm for the job. Private investigators from the firm called the phone company and, posing as the victims, or pretexting, obtained the phone records of members of the media without their knowledge (Kersetter, 2006; Shankland, 2006). Recently, many people with email accounts have been recipients of yet another social engineering attack, phishing, the use of deceptive emails to encourage users to input sensitive identifying data. These three cases are specific examples of a more general information security phenomenon: social engineering.

Social engineering is the use of deception and other non-technical means to gain unauthorized access to information or information systems. Social engineering has been used to describe a number of attacks ranging from widespread phishing for identity information to targeted pretexting for corporate or governmental espionage. Social engineers rely on psychological triggers (e.g., fear, kindness, and greed) and cognitive biases (e.g., truth bias, anchoring, and miscalculation of risk) to gain unauthorized access and evade detection. For the most part, current countermeasures against social engineering attacks rely on people for prevention by educating users through awareness programs and by policy implementation, enforcement and auditing, although new technical countermeasures are emerging.

This chapter has the following objectives:

- Define social engineering
- Provide a taxonomy of social engineering attacks
- Discuss emotional triggers and cognitive biases on which social engineers rely
- Describe current social engineering countermeasures and how they map to techniques
- Discuss future trends in social engineering research and countermeasures

**DEFINITION**

Social engineering has been used to describe a number of attacks ranging from widespread phishing for identity information to narrow pretexting for specific records. It is unclear who first coined the term “social engineering,” but several have attempted to define it. Some definitions are as simple as “the art and science of getting people to comply to your wishes” (Harl, 1997) to much more complex definitions. For the purposes of this chapter, social engineering will be defined as follows:

*Social Engineering is the exploitation of psychological triggers and cognitive biases as a means to gain unauthorized access to information or information systems.*

Phishing and pretexting are only two examples of social engineering attacks that manipulate or deceive targets to obtain information. Table 1 contains some additional examples of social engineering attacks.

The celebrity ex-hacker Kevin Mitnick best described the effectiveness of social engineering to the U.S. Congress in these terms (Mitnick, 2000):

*I was so successful in that line of attack that I rarely had to resort to a technical attack. Companies spend millions of dollars toward technological protections, and that’s wasted if somebody can basically call someone on the telephone and either convince them to do something on the computer that lowers the computer’s defenses or reveals the information they were seeking.*

Attackers with good social skills who don’t have to resort to technical attacks represent a grave and continuing danger to information security. To aid in better understanding them and understand