Chapter II
Why Humans are the Weakest Link

Marcus Nohlberg
School of Humanities and Informatics, University of Skövde, Sweden

ABSTRACT

This chapter introduces the concept of social psychology, and what forms of deception humans are prone to fall for. It presents a background of the area and a thorough description of the most common and important influence techniques. It also gives more practical examples of potential attacks, and what kind of influence techniques they use, as well as a set of recommendations on how to defend against deception, and a discussion on future trends. The author hopes that the understanding of why and how the deceptive techniques work will give the reader new insights into information security in general, and deception in particular. This insight can be used to improve training, to discover influence earlier, or even to gain new powers of influence.

INTRODUCTION

A computer crime starts, and ends, with a human, no matter which method is chosen for the attack. Many successful computer crimes could have been prevented if the people involved had been more vigilant, more security conscious, or aware of their own weaknesses. This chapter deals with human weakness. It can be perceived as a "how-to-manual" for the aspiring attacker, but just as well as a "know-yourself" guide that can be used by both individuals and professionals in order to improve their personal and organizational defenses. It might also give a little more understanding for the victims. When researching successful attacks from the comfortable position of the outside observer, most of us are prone to throw the first stone against what can be seen as gullible humans. The fact is that almost everyone is susceptible to the techniques and weaknesses described in this chapter, simply because the attacks play on human emotion rather than logic.

BACKGROUND

We humans are complicated beings, with some interesting shortcuts in our behavior. In recent years there have been multiple studies on deception in general and influence in particular. These studies have been done in, amongst others, the field of economics and most notably in social psychology. In order to stay as close to the human element as possible, this chapter will focus on the social psychological aspects that can be practically used by the attacker. There are ample theories and work being done in a more theoretical setting, but this chapter will focus on the techniques that the perpetrators might use. Cialdini (2001) has written one of the most influential books in this area, and this chapter will follow his use of the six basic rules of influence, together with some other added aspects of influence. In order to facilitate a better understanding of the concepts, examples will be given, both from the literature and from real life. When applicable, the terms will be tied together with information security as far as possible. Not all the information here will be from research, some will also be added from online sources, guides on what to explore and attack written for the aspiring social engineer. While this information has not been judged against academic standards, it is still relevant, because it is the information attackers will try to use for their attacks and therefore important to know.

Deception is a powerful tool for any attacker, but also for any parent, teacher, salesman, or most of us in our everyday lives. We buy and sell goods, we court romantic interests, and we try to raise our kids in a good way without them loathing us too much when we try to get them to do their chores. In all of these examples, and many more, deception is the key element. Deception can be defined as:

Everything done to manipulate the behavior of the other side, without their knowledge of the friendly intent, for the purpose of achieving and exploiting an advantage is deception. The "what" of deception is the manipulation of behavior. The "why" is to exploit the advantage achieved (Feer, 2004).

There are two different kinds of deception. There is dissimulation, which concerns the hiding of the truth (Bowyer, 2003). The truth can be hidden in three ways. It can be hidden by masking the information, for instance, by hiding nefarious features in a piece of software. It can also be hidden by repackaging the information, for instance, by hiding a Trojan horse in legitimate software. Finally, information can be dissimulated by dazzle, to shock or surprise, for instance, by sending nude pictures in an e-mail. The other kind of deception, simulation, deals with exhibiting false information. Simulation can be done by mimicking, which is spoofing or imitating reality, for instance, as done in a phishing attack. It can also be done by inventing, which is the creation of a new reality, for example, false messages from Microsoft that a certain bug must be patched as soon as possible. The final method of simulation is decoying, where a diversion is done to create a diversion from the real object, such as a false warning of a different attack than the one you are exposed to at the moment.

HUMANS AND DECEPTION

Most of us, and indeed probably you, the reader, consider ourselves exceptionally resistant to manipulation. We are better than the average at detecting lies, and can spot a con a mile away. When asked about our friend's susceptibility to deception, however, we find them to be far more gullible (Levine, 2003). Obviously, we are misjudging our own capacities, as influence in general is highly effective, which is proven by the huge profits it generates for advertisers, corporations, and religious groups, among others, that use these techniques.