Chapter 6
Obtaining Patient's Information from Hospital Employees through Social Engineering Techniques:
An Investigative Study

B. Dawn Medlin
Appalachian State University, USA

Joseph Cazier
Appalachian State University, USA

ABSTRACT

Social engineering can be briefly defined as the obtaining of information through deceptive methods. The intention of the action is to acquire information that will be of use in order to gain access to a system or use of information obtained from the system. There are benefits gained by allowing health care workers access to patient data, but the ability to maintain security of that information may be compromised due to the accessibility. Using methods such as social engineering, health care workers may innocently provide sensitive information without realizing that they have participated in the process of deception. This chapter addresses the issue of social engineering used to obtain health care worker's passwords, as well as the laws that govern health care workers in relation to the privacy and security of confidential patient information.

INTRODUCTION

For most organizations, an employee uses a self-selected username and password as a form of authentication. Even when an organization chooses to enhance security by assigning information used by employees for authentication, social engineers are able to obtain information by using a variety of tricks and techniques (Ciampa, 2005). Social engineering is defined as the "act of manipulating a person or persons into performing some action" (McQuade, 2006). That action may be the "master key" to the health care agency's vault containing patient information.

DOI: 10.4018/978-1-61692-000-5.ch006

Most hackers rely on employees to unknowingly help them attack company networks and systems by simply answering a series of simple questions. Today, most health care agencies have intrusion detection/prevention systems such as firewalls that can be used to alert organizations in the event of a security breach, but these systems cannot prevent employees from inadvertently sharing information with others. Therefore, the question still remains, "how much information might an employee provide to a stranger or to a co-worker?"

The social engineer can, and often does, utilize an arsenal of methods that allow him or her to involve the emotions of a victim to aid in an attack. According to Mitnick & Simon (2002), the social engineer may flirt with the employee in an attempt to trick the individual into releasing information or another approach sometimes taken is to convince the employee that their job depends on supplying the attacker with the requested information. No matter the technique employed, if relevant and meaningful information is supplied, the entire network and all of the information it contains has been placed at risk.

Managers must be vigilant in their efforts to protect patient information as required by several laws. Most recently, on February 17th, 2009, President Obama signed into law the Health Information Technology and Clinical Health Act (HITECH) as part of the American Recovery and Reinvestment Act. The HITECH Act enhances the security and privacy provisions as well as the penalties contained in the Health Insurance Portability and Accountability Act of 1996 (http://www.nixonpeabody.com/publications_detail3.asp?ID=2621). This new law also requires patients be notified in the event of a security breach.

In this study, we simulated how a social engineer might obtain personal information from unsuspecting hospital employees. As previously mentioned, health care agencies and their employees must be especially vigilant in their effort to guard against the sharing of patients personal and/or private information.

BACKGROUND

Social engineers have traditionally used the telephone as the mechanism to obtain information. But today's social engineer is just as likely to approach an employee of an organization and act as though they need to obtain information in order to complete their job. Another method used by social engineers is to present themselves as an employee and act as though they are assisting others. Of course, depending upon the shrewdness and professionalism of the social engineer, not all attempts are successful.

If the social engineer is attempting to find out about one particular patient, they may target that person's medical health record. A patient's medical record may include gender, race, family history, sexual history including types of birth control, sexual activity and treatment, any history or diagnosis of substance abuse, and diagnosis of mental illness. Other medical information, such as HIV status, may also be included. The accessibility of this confidential information may open the door to various forms of discrimination. For instance, chronic diseases such as HIV and AIDS may result in an increase in insurance rates or even denial of coverage, due to the extensive medical treatment usually needed by these patients. Individuals may even be ostracized or stigmatized because of their disease type. Patients expect the information contained in their records to remain secure and private, to be seen only by those individuals whose access is medically or administratively necessary.

Unfortunately, patient's medical records are being illegally accessed and often when a breach occurs, the incident is seen in the news. Table 1 represents recent security breaches of patient information ranging from occurrences that affected individual patients, to an occurrence that wreaked havoc on thousands of patients.

As noted earlier, the HITECH Act includes a series of privacy and security provisions that expand the current requirements under the Health Insurance Portability and Accountability Act

Related Content