Chapter 5
Social Engineering Techniques, Password Selection, and Health Care Legislation:
A Health Care Setting

B. Dawn Medlin
Appalachian State University, USA

Joseph A. Cazier
Appalachian State University, USA

ABSTRACT

Healthcare employees generally have access to view hospital patient's medical records. This access can be simply viewing their chart or reviewing information on a computer screen. With this type of accessibly, hospital employees have the opportunity to view diagnosis, personal medical histories, as well as demographic information such as age and gender. Social engineers can use methods such as familiarity with co-workers for instance to obtain this information from unsuspecting health care workers. In addition, weak password selection can provide opportunities for a wealth of information to be stolen. In this chapter, current security legislation that addresses the security of patient's health care records, social engineering tactics, and passwords are explored.

INTRODUCTION

There are many threats to the privacy of a patient's information, and one of the largest threats is social engineers or the act of social engineering. Social engineering is generally defined to include the use of trickery, personal relationships and trust to obtain information; more specifically, it is the art of deceiving people into giving confidential, private or privileged information or access to a hacker (Gragg, 2007).

Another threat to the privacy of security of patient's information can be the employees themselves. Internal employees actually can pose the largest threat to the security and privacy of information as they can exploit the trust of their

DOI: 10.4018/978-1-4666-7381-6.ch005

co-workers, and they generally are the individuals who have or have had authorized access to the health care organization's network. As well, they are generally familiar with the internal policies and procedures of the organization. Additionally, internal employees can exploit that knowledge to facilitate attacks and even collude with external attackers (http://www.cert.org/insider_threat/).

A patient's personal information, such as address, phone number, and social security number, are all items that may be included and accessible to some or all healthcare employees. PHR (Personal Health Care Records) are available to many who neither touch nor need access to patient's health care information. With the accessibility and sheer volume of patient's data and information patients may be even more vulnerable to security breaches. If the information is not easily accessible, hackers and social engineers have been very successful in founding ways to circumvent networked health data systems by simply asking for the information or by finding weaknesses within the system (Medin & Cazier, 2007).

Due to the number or increase to either losing or sharing information or the severity of these issues, HITECH or the Health Information Technology for Economic and Clinical Health Act of 2009 was enacted. Under Title XIII, HIPPA appears to remain the law that is most discussed in relation to privacy and security within the health care industry. One of the core aspects and a basic goal of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is to provide more electronic medical information. HIPAA addresses security and privacy measures, either directly or indirectly, in the standards related to management processes, user education and training, and access control (http://www.hhs.gov/news/facts/privacy.html). HIPAA regulations were enacted to protect the privacy and security of patients and their medical records; simply put, they make it illegal for unauthorized personnel to access or release information from someone's medical records.

Despite its legal requirements, however, HIPAA standards have been known to be difficult to implement and are not always followed. As required by HIPAA, healthcare institutions are required to provide security methods in order to protect patient's information. One such method is through the authentication of the individual requesting access. Healthcare employees are generally subjected to some type of authentication process. Although there are different ways of authenticating employees, most systems are based on the use of a physical token (something one has), secret knowledge (something one knows) or biometrics (something one is) (Burnett & Kleiman, 2006).

Due to increased regulations and the increased opportunities for exploitation that exist in today's digital world, it is even more important for healthcare providers to keep healthcare records and the information held within, safe and private. Governmental agencies have adopted initiatives that specifically address the issues and rights of healthcare patients. More specifically, the security and privacy of healthcare information is protected by the Health Insurance Portability and Accountability Act (HIPAA), requiring healthcare agencies to do everything possible to protect their information.

In addition to the various security measures discussed above, it is important for security managers and personnel to be familiar with the psychological weapons and motivations behind social engineering and its malicious use. Hasan, Prajapati and Vohara illustrate how social engineers will take advantage of human's innate tendency to trust and be helpful (Hasan et al, 2010). Many social engineers will play to the emotions of the victim by impersonating a staff member who has forgotten a password, thus imploring the victim to help someone in need (Hasan et al, 2010). According to Maan and Sharma there are multiple different types of social engineering (Maan et al, 2012).