Chapter 4
Healthcare Employees and Passwords: An Entry Point for Social Engineering Attacks

B. Dawn Medlin
Appalachian State University, USA

Douglas May
Appalachian State University, USA

Ken Corley
Appalachian State University, USA

ABSTRACT

The healthcare industry has benefitted from its employees’ ability to view patient data, but at the same time, this access allows for patient’s healthcare records to be easily captured or stolen. Although access to and transmission of patient data may improve care, increase delivery time of services, and reduce healthcare costs, security of that information may be jeopardized due to the innocent sharing of personal and non-personal data with the wrong person. Through the tactic of social engineering, hackers are able to obtain information from employees that may allow them access into the hospitals networked information system. In this study, we simulated a social engineering attack in hospitals of varying sizes with the goal of obtaining employees passwords. If employees are willing to share their passwords, serious questions and concerns about the state of employee security awareness within the healthcare system must be raised.

INTRODUCTION

Healthcare records generally include, but are not necessarily limited to, individual patient’s health history, diagnosis, laboratory results, treatments, and the doctor’s progress notes. 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 health-
care employees. These records are vulnerable to security breaches and theft. Both hackers and social engineers have successfully found ways to penetrate networked health data systems by simply asking for the information or by finding weaknesses within the system.

Unfortunately, the largest threat to a healthcare agency’s security may not be outsiders, but rather their own employees. Inside employees actually can pose the largest threat to the security and privacy of information as they can exploit the trust of their co-workers, and they generally are the individuals who have or have had authorized access to the organization’s network and who are familiar with its internal policies, procedures, and technologies. Additionally, internal employees can exploit that knowledge to facilitate attacks and even collude with external attackers (http://www.cert.org/insider_threat/).

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.

There are many threats to the privacy of a patient’s information, and one of the largest threats is 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).

In our study, we simulated how a social engineer might gather information from unsuspecting hospital employees. Healthcare employees must be especially vigilant in their efforts to guard their passwords, as many have access to personal and medical information. HIPAA regulations are very definitive and have specific standards related to security and privacy of information; infractions of those regulations can be costly to the organization and its reputation, as well as devastating to a patient.

**BACKGROUND**

The electronic accumulation and exchange of personal health information has been promoted as significant benefits to healthcare consumers and providers. Many healthcare policy experts believe that broader health information technology adoption may lead to the availability of more complete and transparent information, ultimately helping to contain healthcare costs while simultaneously improving healthcare quality.

But with this availability of information comes the opportunity for more fraudulent activity such as social engineering attacks. According to Thornburough (2004) social engineering has gained profound acceptance in the information technology community as an effective social and psychological tool for exploiting the IT security mechanism of a target organization. For many social engineers the process of obtaining meaningful information may lead to the insight of the organization’s security policy, the countermeasures the organization has put in place and specifics relating to personnel and their level of security privilege.

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,