Social Engineering Techniques and Password Security: Two Issues Relevant in the Case of Health Care Workers

B. Dawn Medlin, Department of Computer Information Systems, Walker College of Business, Appalachian State University, Boone, NC, USA

ABSTRACT

Due to the Internet and applications that can access the Internet, healthcare employees can benefit from the ability to view patient data almost anywhere and at any time. Data and information is also being shared among third party vendors, partners and supplies. With this type of accessibility of information which generally does include very personal information such as diagnosis and social security numbers, data can easily be obtained either through social engineering techniques or weak password usage. In this paper, a presentation of social engineering techniques is explored as well as the password practices of actual health care workers.

Keywords: Authentication, Healthcare Employees, Healthcare Workers, Information, Password Security, Personal Information, Privacy, Social Engineering Techniques

INTRODUCTION

A patient’s personal information, such as address, phone number, and social security number, are all items that may be included and accessible to someone or all healthcare employees. PHR (Personal Health Care Records) are available to many who neither touch or need access to patient’s health care information. Volume of, and access to patient’s health care make them more vulnerable to security breaches, theft, and social engineering attacks. Both hackers and social engineers have successfully found ways to circumvent networked health data systems by simply asking for the information or by finding weaknesses within the system.

Certainly one of the the largest threats to a healthcare systems security may not be outsiders, but rather their own employees. Internal 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 health care organization’s network. As well, they are generally familiar with the internal policies and

DOI: 10.4018/ijcwt.2013040104
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/).

Though in 2009, HITECH or the Health Information Technology for Economic and Clinical Health Act, was enacted under Title XIII, HIPAA appears to remain the law that is most discussed in relation to privacy and security within the health care industry. Both include a patient data breach notification rule, but as noted earlier HITECH is based on HIPPA and relies heavily on its standards related to privacy and security.

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, therefore resulting in more opportunities for cyberthreats. 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.

In relationship to password safety and protection, HIPAA addresses security and privacy measures, either directly or indirectly, in the following standards (http://www.hhs.gov/news/facts/privacy.html). These standards, as listed below, include management processes, user education and training, and access control:

- **Security Management Process** [161.308(a)(1)] Healthcare organizations must show that they have a consistent set of internal processes, with implementation that is widespread and institutionalized. Processes range from establishing criteria for who has access to what, and who can request certain resources; to ensuring that access rights are revoked immediately upon employee termination;

- **Security Awareness and Training** [161.308(a)(5)] HIPAA requires that staff members be trained and educated concerning the proper handling of PHI. This basic-level security training should include measures such as password management;

- **Access Control** [161.312(a)] HIPAA security regulations require a definition of who has access to PHI within the organization, as well as the rules determining an individual’s right of access, and the reasons for denying access to some individuals.

Despite its legal requirements, however, HIPAA standards as well as healthcare security policies are not always followed. As an example, and according to one report, over “870,000 medical records were exposed in data breaches in just the first quarter of 2013. According to this site, medical data breaches have become a source of chronic pain for healthcare organizations” (http://www.experian.com/blogs/data-breach/2013/05/01/medical-data-breaches-a-source-of-chronic-pain).

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 as well as studied the passwords of current health care workers. Healthcare employees must be especially vigilant in their efforts to guard their passwords, as many have access to very sensitive medical information. HIPAA regulations are very
Using Deceptive Information in Computer Security Defenses
www.igi-global.com/article/using-deceptive-information-in-computer-security-defenses/124132?camid=4v1a