Social Engineering: The Neglected Human Factor for Information Security Management

Xin (Robert) Luo, The University of New Mexico, USA
Richard Brody, The University of New Mexico, USA
Alessandro Seazzu, The University of New Mexico, USA
Stephen Burd, The University of New Mexico, USA

ABSTRACT

Effective information systems security management combines technological measures and managerial efforts. Although various technical means have been employed to cope with security threats, human factors have been comparatively neglected. This article examines human factors that can lead to social engineering intrusions. Social engineering is a technique used by malicious attackers to gain access to desired information by exploiting the flaws in human logic known as cognitive biases. Social engineering is a potential threat to information security and should be considered equally important to its technological counterparts. This article unveils various social engineering attacks and their leading human factors, and discusses several ways to defend against social engineering: education, training, procedure, and policy. The authors further introduce possible countermeasures for social engineering attacks. Future analysis is also presented.

Keywords: Human Factors, Information Security, Personality Traits, Security Management, Social Engineering

INTRODUCTION

Information systems (IS) security management depends not only on technological measures but also on managerial endeavors. A plethora of technological methods have been developed to address various security issues but human factors that contribute to significant security breaches have been comparatively neglected. The salient key to derailing potential aggressors is a combination of technical, behavioral, and procedural countermeasures. Imagine receiving a phone call in which someone claiming to work for an official agency suggests that you reveal certain information to help repair an urgent system problem. You willingly help the caller who is, in reality, a fraudster seeking access to private information. The success of this social engineering attack relies on the natural helpfulness of human users, their psychological weaknesses, and their tendencies to be unaware of the value of the information they possess and to be sloppy about shielding their information.

DOI: 10.4018/irmj.2011070101
Within the context of computer and information security, social engineering (SE) is a combination of techniques used to manipulate victims into divulging confidential information or performing actions that compromise security (Mitnick & Simon, 2002). SE attackers, in general, tend to exploit human cognitive biases. SE attacks are non-technical intrusions that rely on human interactions, potentially bypassing technological security mechanisms. Workman (2007) explained that the emotional aspect of the interaction distracts human users and serves to interfere with the potential victim’s ability to carefully analyze the content of the message delivered by social engineers (p. 316). He further indicated that, due to human factors, knowing better but not doing better is one of the key scholarly and practical issues that has not been fully addressed, particularly in the IS security management paradigm (Workman, 2008). SE is undoubtedly one of the weakest links in the domain of IS security management, because it is beyond technological control and subject to human nature.

Prior studies on SE generally tended to focus on technological cues triggering the attacks. Behavioral factors for the SE attacks are not usually described and systematically analyzed. As such, this paper contributes to the literature of IS security by holistically analyzing the human behavioral factors that are associated with SE attacks. In addition to extending previous research on SE, we specifically study behaviors and personality traits that are rooted in social psychology and criminology. We believe that this study can theoretically advance behavioral IS security research in the domain of SE management and control, and could also pragmatically inform organizational decision-makers of how individual employees can deal with the ever increasingly sophisticated SE attacks. It is hoped that this study can offer instrumental insights to the often neglected human aspects of information systems security management.

The remainder of this paper is organized as follows. We first revisit the theoretical bases in social psychology in order to analyze three key aspects related to SE. Then we further draw on criminology and social psychology to discuss the personality traits versus SE attack vulnerabilities. The technical and non-technical means that SE attackers can employ are presented next, followed by a proposed multi-dimensional approach including policies, procedures, standards, employee training and awareness programs, and incident response for more effective and efficient IS security management. The paper concludes with a discussion of future SE analysis and suggestions for future research.

**PSYCHOLOGICAL ASPECTS**

Recent research has discovered that there are certain terms and techniques that are associated with SE and go perhaps far beyond technology and more so into human error and social psychology (Peltier, 2006). Three key aspects of social psychology, alternative routes to persuasion (i.e., central route and peripheral route), attitudes and beliefs that affect human interactions, and techniques for persuasion and influence, could help explain the emotional cues for manipulated SE attacks (Peltier, 2006).

In a central route to persuasion, SE attackers persuade victims to provide desired information by bypassing logical argument and counterargument and seek to trigger intrusion. In the peripheral route to persuasion, the attacker tends to make the intended victim more susceptible to persuasion by triggering strong emotions such as fear or excitement in order to interfere with the victim’s ability to respond. 

Attitudes and beliefs refer to the differences between the victim’s attitude and beliefs about the SE attacker and SE attacker’s attitudes and beliefs about his anticipated or definite victims. Rooted in social psychology, persuasion and influence techniques rely on peripheral routes
Related Content

[www.irma-international.org/chapter/developing-effective-computer-systems-supporting/6367/](www.irma-international.org/chapter/developing-effective-computer-systems-supporting/6367/)

Digital Literacy and the Position of the End-User
[www.irma-international.org/chapter/digital-literacy-position-end-user/13719/](www.irma-international.org/chapter/digital-literacy-position-end-user/13719/)

User Developed Applications and Information Systems Success: A Test of DeLone and McLean’s Model
[www.irma-international.org/article/user-developed-applications-information-systems/1235/](www.irma-international.org/article/user-developed-applications-information-systems/1235/)

Modeling and Analyzing Perspectives to Support Knowledge Management
[www.irma-international.org/chapter/modeling-analyzing-perspectives-support-knowledge/28664/](www.irma-international.org/chapter/modeling-analyzing-perspectives-support-knowledge/28664/)

P2P-Based Management of Collaboration Communication Infrastructures
[www.irma-international.org/chapter/p2p-based-management-collaboration-communication/27803/](www.irma-international.org/chapter/p2p-based-management-collaboration-communication/27803/)