Are Warnings from Online Users Effective? 
An Experimental Study of Malware Warnings Influencing Cyber Behaviour

Wahida Chowdhury, Carleton University, Ottawa, Canada

ABSTRACT

The present research focused on increasing cyber security by reducing users’ likelihood of installing Trojan Horses: malware hiding inside attractive software. Social cognition research suggests that reading online security warnings in software reviews from other users could reduce the likelihood of installing malware. In Study 1, 43 computer users viewed 30 reviews of hypothetical games. Half the reviews were malware warnings. Ratings of the warnings’ strength were used to select strong and weak warnings for Study 2. In Study 2, 45 computer users viewed descriptions and reviews of real computer games. Results indicated that both the number and strength of malware warnings in reviews influenced the likelihood of installing a game: two warnings reduced ratings of installation likelihood more than did one warning; strong warnings reduced the ratings more than did weak ones. Implications and limitations of the findings for social contributions to influencing cyber behaviour are discussed.

Keywords: Cyber Security, Decision Making, Game Reviews, Motivation to Change, Online User Reviews, Secure Behaviour, Security Warnings, Social Influence

INTRODUCTION

A Trojan Horse is an attractive-looking, malicious computer programme that can compromise cyber security. Trojan horses install themselves in the click of a mouse, and the consequences of resulting security problems are often severe, for example, unauthorized access of computers that control a nation’s industrial operations (Cloherty, J. & Thomas, P, 2014). The purpose of this study was to examine how ideas from social cognition might be employed to dissuade computer users from installing Trojan Horses.

A user who installs a Trojan Horse will unknowingly activate the malicious program hiding inside it (e.g., Lavesson, Boldt, Davidsson & Jacobsson, 2011) and compromise his/her computer security. Turing’s (1938) proof of the halting problem suggests it is impossible to detect if a program is or is not malicious while it is running. This implies we have to stop the operation of

DOI: 10.4018/IJCBPL.2015040104
a Trojan Horse before we install it. Currently there are two approaches to dissuade users from installing a Trojan Horse: technical and behavioural.

**Technical Approaches to Prevent Installation of Trojan Horses**

Technical approaches have led to improvements in antivirus software to detect a Trojan Horse (e.g., Gribble, Levy, Moshchuk, & Bragin, 2012), and then warn users of the danger. However, the approaches are often expensive to implement, slow to disperse, and are neither foolproof nor infallible. New Trojan Horses are developed daily, and they often go undetected by security hardware and software for weeks or months required to implement new detection updates (Kephart & Arnold, 1994). During that time, other approaches to limiting the installation of Trojan Horses must be considered.

**Behavioural Approaches to Prevent Installation of Trojan Horses**

Behavioural approaches to prevent users from installing Trojan Horses include user education. Websites such as http://isc.sans.org, http://www.iss.net, and http://www.insecure.org (Dubin, 2008) offer extensive educational materials about how to detect Trojan Horses; www.getcybersafe.gc.ca, a Canadian federal government initiative, offers several webpages describing risks of installing Trojan Horses from email attachments, social network, file sharing, etc., and provide users with tips on how to avoid these risks. Experts in computer security also have published many books and articles giving advice on how to detect and avoid installing Trojan Horses. For example, Cranor and Garfinkel (2005), Pfleeger and Pfleeger (2011), and Rothke (2005) wrote that a computer user could avoid installing malware by following many rules, such as by avoiding phishing emails, and by opening email attachments cautiously. Education, however, is not sufficient for behavioural change. A user must also realize the need for the security information, be motivated to look for it, find it, understand it, and expend time and effort to implement it. Adams and Sasse (1999) argue, “It is important to challenge the view that users are never motivated to behave in a secure manner” (p.45). Still, it is safe to assume that users are not always motivated to behave securely (e.g., Stanton, Caldera, Isaac, Stam & Marcinkowski, 2003).

Forcing users to comply with security guidelines or threatening users with punishment for non-compliance might seem to solve the problem of users’ motivation, and many attempts have been made to influence secure behaviour through rules and regulations tied to rewards or punishments. For example, many work organizations set rules on what can be installed from which websites. However, surveys suggest compliance with security standards is low (Barlette & Fomin, 2009), and most users ignore standards, such as End User License Agreements, that describe before installation what a piece of software does (Chia, Heiner & Asokan, 2012; Thorngate & Tavakoli, 2007). This leaves users still vulnerable to installing Trojan Horses.

**SOCIAL COGNITIVE APPROACH**

Social cognitive theory predicts that human thought, motivation and action could be influenced by communication from others (Bandura, 1986). Classic studies by Asch (1951; see also Bond & Smith, 1996) demonstrate how the opinions and behaviour of others can influence people to conform to these opinions and behaviour. Further, decades of research in advertising show the relative ease of forming and changing attitudes through word-of-mouth communication and testimonials (e.g., Chevalier & Mayzlin, 2003; Kulviwat, Bruner, & Al-Shuridah, 2009). The surfeit of opinions and advice given and sought on the Internet in reviews of books, people, ideas,
Domestication of Smartphones Among Adolescents in Brunei Darussalam
www.igi-global.com/article/domestication-of-smartphones-among-adolescents-in-brunei-darussalam/198335?camid=4v1a

The “Right to be Forgotten” in the Era of Social Media and Cloud Computing
www.igi-global.com/chapter/the-right-to-be-forgotten-in-the-era-of-social-media-and-cloud-computing/107828?camid=4v1a