User Interface Design and E-Commerce Security Perception: An Empirical Study

Faouzi Kamoun, University of Dubai, UAE
Mohanad Halaweh, University of Dubai, UAE

ABSTRACT

In this study, the authors investigate the relationship between human computer interface design and users’ security perception. The authors hypothesize that effective human computer interface design has a positive impact on security perception. To test this hypothesis, they use the seven design elements of the customer interface (7Cs) as a basis of the reference framework for effective interface design. Hypothesis testing was examined through an empirical study involving 247 subjects. Research reveals that human computer interface design significantly affects the perceived security of e-commerce portals. Further analysis of the results highlights that the top HCI factors that influence security perception are permanent working links, demos and online help tools, information accuracy, and easy website navigation. Therefore, this study suggests that applying good user interface design guidelines at the storefront can be an effective technique for enhancing user security perception and increasing trust and purchase intention.

Keywords: E-Commerce Portals, E-Commerce Security, Electronic Commerce, Human Computer Interaction, Human Computer Interface, Security Perception

INTRODUCTION AND RESEARCH BACKGROUND

The emergence of e-commerce as the catalyst for online sales has changed the way consumers shop for goods and services. At the same time, e-commerce provides unprecedented opportunities for many firms to enlarge their customer base and establish competitive business models. A recent Forrester research report predicts that e-commerce sales in the U.S. will keep growing at a 10 percent compound annual growth rate, reaching nearly $250 billion in 2014, up from $155 billion in 2009 (Schonfeld, 2010). Unfortunately, this growth in e-commerce has been accompanied by an increase in the number and sophistication of fraudulent web practices; thus raising consumer concerns about online security (VeriSign, 2009). Recent studies (Abrazhevich, 2004; Kurnia & Benjamin, 2007; Özkan et al., 2010; Dolatabadi & Ebrahimi, 2010; Yulihasri et al., 2011) have

DOI: 10.4018/jebr.2012040102
shown that low perceived security and trust in e-commerce and e-payment systems negatively affects consumers’ intention to purchase online. Further, a Gartner study (Gartner, 2006) reported that US retailers lost near $2 Billion in e-commerce sales because of the security fears of online shoppers. In particular, about half of the $2 Billion losses were due to consumers who avoided sites that they perceived to be less secure, while the remaining losses were attributed to people who, in the first place, were afraid to engage in e-commerce transactions. For most retailers, however, the agony is that the main deriver of consumers’ reluctance to buy online mostly comes from their perception of e-commerce security, rather than from the real lack of security per se. As a result, customers’ positive perception of security is an essential pre-requisite to their willingness to engage in online transactions with a site (Turner, 2003; Zhao-Fu et al., 2010; Fogg et al., 2001). Here we adopt Salisbury (2001) definition of security perception as “the extent to which one believes that the web is secure for transmitting sensitive information” (p. 166).

Understanding the nature of end users’ perception of security and the factors that influence this perception has been the subject of extensive research during the past few years. Most of the earlier contributions have focused on the impact of website security and privacy features on users’ security perception and trust (see e.g., Xiaoyan & Zhiying, 2010; Ally & Toleman, 2005; Yousafzai et al., 2005; Chellappa & Pavlou, 2002).

Online trust is a multi-faceted and context-dependent construct that involves cognitive, behavioral, psychological, cultural, uncertainty and risk factors, among others. Perceived trust can be built and reshaped before, during and after the online transaction (Wang, 2009). The concept can perhaps be better understood by invoking Egger’s (2000) Model of Trust for Electronic Commerce (MoTEC). MoTEC recognizes three main trust - Informational content inducing factors (aka filters) that can potentially convert users into e-commerce customers. These are pre-purchase knowledge, interface properties, and information content.

**Pre-purchase knowledge** captures those external factors that can influence consumer’s initial trust before any online interaction takes place. Among these factors, are the vendor’s brand name and reputation, user’s previous online or offline experience with the vendor, user’s disposition of trust, and input from trusted third parties (including word-of-mouth, media reports). In particular, Radke et al. (2010) conducted a qualitative research that showed that the brand reputation of the company whose website users thought they are browsing is a key perceived intangible security feature. This finding was also confirmed by the earlier empirical work of Turner et al. (2001) and Halaweh and Fidler (2008). Bhattacheree’s (2005) model of trust recognizes that familiarity (knowledge of the trustee based on prior interactions or experiences) can lead to willingness to transact either directly or via the mediation of trust.

**Interface properties** shape two constructs, namely familiarity and attitude. Familiarity refers to the system’s usability (ease-of-use), including learnability, consistency, flexibility and reliability. Ease-of-use is generally perceived as a strong indicator that the company cares for its customers. When first-time visitors access a site for the first time, ease of use, smooth website navigation and pleasurable online experience can potentially affect how much they feel in control of the site (Araujo & Araujo, 2003). To this effect, Church and Whitten (2009) argued that the purpose of computer security is about giving people control over computers and information and this shares one of the goals of Human Computer Interaction. Singh (2002) argued that guided navigation reduces perceived risk for customers originating from high uncertainty avoidance cultures.

Attitude reflects the appeal and first impression the system makes on its users in terms of the visual appearance created by graphic and visual designs, as well as other superficial cues about navigation and reliability of the e-commerce application (Egger, 2001). Wang (2009) found that what consumers see through the HCI
An Agent-Based Architecture for Product Selection and Evaluation under E-Commerce
www.igi-global.com/chapter/agent-based-architecture-product-selection/5209?camid=4v1a