Available online at www.sciencedirect.com

SciVerse ScienceDirect

Int. J. Human-Computer Studies 70 (2012) 364–376

International Journal of Human-Computer Studies

www.elsevier.com/locate/ijhcs

When do online shoppers appreciate security enhancement efforts? Effects of financial risk and security level on evaluations of customer authentication

Jong-Eun Roselyn Lee[a,*], Shailendra Rao[b], Clifford Nass[c], Karin Forssell[d], Jae Min John[e]

[a]Department of Communication, Hope College, 257 Columbia Ave, Holland, MI 49423, USA
[b]Motorola Mobility, Sunnyvale, CA 94089, USA
[c]Department of Communication, Stanford University, Stanford, CA 94305, USA
[d]School of Education, Stanford University, Stanford, CA 94305, USA
[e]Oracle Corp., 500 Oracle Pkwy, Redwood City, CA 94065, USA

Received 15 November 2009; received in revised form 18 November 2011; accepted 16 December 2011
Communicated by A. Cockburn
Available online 20 January 2012

Abstract

As the popularity of online shopping grows, concerns about identity theft and fraud are increasing. While stronger customer authentication procedures may provide greater protection and thus benefit customers and retailers, security is often traded off against convenience. To provide insight into this security-convenience trade-off in customer authentication, we experimentally investigated how levels of authentication security and financial risk factors affect perception and evaluation of authentication systems in two contexts: security questions (Experiment 1) and card security codes (Experiment 2). Experiment 1, which examined the effects of security level and product price as a financial risk factor, showed that authentication procedures based on higher-level security tended to be perceived as significantly less convenient and more frustrating. Interestingly, participants rated the higher-level security system (i.e., asking more demanding challenge questions) as less convenient and more frustrating when the amount involved in the transactions was higher. Experiment 2, which introduced consumer liability for fraudulent activities as an additional financial risk factor, showed that participants gave more positive ratings of the higher-level security system under full liability than under zero liability. Taken together, the present research suggests that patterns of security-convenience trade-offs reflecting consumers' perception and appreciation of authentication technologies may vary depending on the characteristics of financial risk factors involved in the transaction process.

Keywords: Online shopping; Electronic commerce; Online security; Authentication; Security–convenience trade-off

1. Introduction

Online shopping spaces are becoming increasingly attractive to consumers, offering numerous conveniences including 24/7 availability (Hofacker, 2001), time-saving benefits (Childers et al., 2001), and increased product and price research capabilities (Jefferson, 2006). The conveniences of online shopping, however, are accompanied by security threats such as identity theft and fraud (Leggatt, 2009). According to the Pew Internet & American Life Project Report on online shopping (Horrigan, 2008), while 78% of Internet users agree that online shopping is convenient for them, 75% of Internet users also expressed high levels of discomfort about disclosing personal information or payment card information online.

Research on consumer behavior has demonstrated that purchase behaviors are largely determined by the trade-offs between what one gives up and what one gains from it (Dodds et al., 1991; Yadav and Monroe, 1993). In online shopping, such trade-offs tend to occur between security and convenience, as can be witnessed in password access

*Corresponding author. Tel.: +1 616 395 7361; fax: +1 616 395 7937.
E-mail addresses: jroselyn@stanfordalumni.org (J.-E.R. Lee), shailo@stanford.edu (S. Rao), nass@stanford.edu (C. Nass), forssell@stanford.edu (K. Forssell), jaemin.john@oracle.com (J.M. John).

1071-5819/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ijhcs.2011.12.002

systems. For instance, one way to prevent an unauthorized individual from easily guessing or "cracking" a password would be to make the password itself more complicated by requiring users to create a long password (Keith et al., 2007), use system-generated passwords (Adams and Sasse, 1999), or combine numbers or special characters with letters (Nowak et al., 2009). While these measures allow the password system to offer stronger protection against unauthorized access, users frequently find such passwords difficult to remember and inconvenient to use (Nowak et al., 2009).

The dilemma caused by security-convenience trade-offs in online shopping can be even more acute when it comes to customer authentication. To minimize losses for customers and for themselves, many online retailers employ measures for authenticating customer identity. These measures are designed to verify that the person making the purchase is an authorized user of the payment method (Cline, 2004). However, authentication procedures that make the payment process complicated and demanding for stronger fraud protection may hinder users from fully enjoying the convenience of online shopping (Bhatnagar and Ghose, 2004). Hence, increasing levels of security in customer authentication may lead consumers to form a negative perception of the online shopping interface (Odekerken-Schroder and Wetzels, 2003) and may potentially lower their willingness to make purchases.

The present research aims to provide insight into the security-convenience trade-offs concerning customer authentication procedures in online shopping. In particular, we test possible moderation by factors associated with financial risk, investigating whether and how the effects of security levels instantiated by authentication technologies on consumers' evaluation of the systems would depend upon perceived financial risk. In so doing, we examine two different types of authentication procedures: challenge questions (Experiment 1) and card verification codes (Experiment 2).

2. Customer authentication as a human–computer interaction process

Although it may not always seem obvious to consumers, online customer authentication procedures are based on communication and collaboration between human users and computer technology underlying the authentication system. However simple or sophisticated, the process can be broken down into the following five key steps: (1) some information (e.g., answers to security questions, personal identification codes, or credit card verification codes) is shared between the authentication system and the customer (Szabó, 2003); (2) when performing a transaction, the customer is asked by the system to provide the information to complete the purchase; (3) the customer responds to the system's request by providing the solicited information; (4) the system verifies the information provided by the customer; and finally, (5) when the verification is complete, the customer finalizes the transaction. In the process of customer authentication, unless both parties—the customer and the authentication system—"collaborate" with each other, the transaction cannot be completed successfully. Hence, authentication processes may be viewed as an important form of human–computer collaboration.

Authentication procedures demand varying degrees of user effort and inconveniences. Some authentication procedures are relatively simple and thus require minimal effort on the consumers' end, while other procedures involve more complicated and demanding processes, which customers might find burdensome. The latter procedures, intended for higher security levels of anti-fraud protection, may be beneficial to consumers. The problem, however, is that such high-level security procedures may not always be appreciated by consumers because the potential benefit to be gained from higher levels of security can be overshadowed by the lack of convenience. Research has demonstrated that customers are far from being willing to trade usability and convenience for perceived increases in security when it comes to authentication (Weir et al., 2009).

Under what conditions would consumers show more negative reaction to, or show greater appreciation of, more demanding authentication procedures oriented toward high-level security and protection? Research conducted on development of novel authentication procedures has been illuminating (e.g., De Angeli et al., 2005; Kuber and Yu, 2010), but relatively little research has identified factors that shape the security-convenience trade-offs in online customer authentication. As an initial effort, we propose to examine factors associated with financial risk, which play a key role in consumers' decision-making in the context of online shopping (Liebermann and Stashevsky, 2002).

3. The role of financial risk

Financial risk, defined as one's subjective beliefs about suffering a monetary loss while pursuing an outcome one desires (Forsythe and Shi, 2003; Ko et al., 2004; Pavlou, 2003), is considered one of the key elements of perceived risk in electronic commerce (Tan, 1999). Research has shown that perceived financial risk is negatively associated with consumers' intention to engage in online shopping (Kim, 2007; Pavlou, 2003), and this tendency has been found among both novice and experienced consumers (Liang and Jin-Shiang, 1998), particularly when it comes to perceived financial risk that can potentially result in monetary losses (Keating et al., 2009; Ko et al., 2004; Liebermann and Stashevsky, 2002).

In the context of Internet-based commercial transactions, financial risk entails possibilities that one's payment information may be used fraudulently by another (Forsythe and Shi, 2003). Given that authentication systems with higher levels of security tend to be more complicated and are thereby more demanding (or require greater effort) on the consumers' end, the extent to which consumers appreciate (and in turn willingly "collaborate" with) a complicated and demanding authentication system may depend on the extent to which