Int. J. Human-Computer Studies 80 (2015) 36–44

Contents lists available at ScienceDirect

Int. J. Human-Computer Studies

journal homepage: www.elsevier.com/locate/ijhcs

The role of security notices and online consumer behaviour: An empirical study of social networking users ☆

Benson Vladlena [a,*], George Saridakis [a], Hemamali Tennakoon [b], Jean Noel Ezingeard [c]

[a] Kingston University, UK
[b] Asia Pacific Institute of Information Technology, Sri Lanka
[c] Manchester Metropolitan University, UK

ARTICLE INFO

Article history:
Received 19 September 2014
Received in revised form
5 March 2015
Accepted 11 March 2015
Available online 20 March 2015

Keywords:
Social media
Security notices
Security seals
Personal information privacy
Information security
Cybercrime victimisation
Social learning

ABSTRACT

This paper uses a survey of social networking users to empirically explore their perceptions of security notices – independently verified artefacts informing internet site users that security measures are taken by the site owner. We investigate such factors as purchase experience, purchase intention, risk propensity, usage of various social network categories and user victimisation. The results suggest a strong positive link between purchase intention and paying attention to security notices/features on social networks. We find that higher use of narrow-purpose social networking services has a negative association with paying attention to security notices. We also show that users with higher risk propensity pay less attention to security notices/features. Finally, we find no association between purchase experience, user victimisation and perception of security notices/features. Our results provide new, and possibly more refined, evidence of the factors that influence the attention paid to security notices/features by social media users. The results have important implications for theory development, policy and practice.

1. Introduction

The proliferation of social technologies has been seen as a positive shift in the way people communicate, collaborate, share knowledge (Susarla et al., 2013; Hsu et al., 2007), transact online and consume (Aral et al., 2013). Originating largely as a set of leisure applications for connecting with friends and family and as content sharing tools, social networks have naturally evolved into instruments for business, professional and commercial uses (Aral et al., 2013).[1] The delineation between commercial and personal applications of social media is becoming more prominent as the social business models and revenue streams mature.[2] Social media has played a particularly key role in business transformation and has opened new avenues for revenue generation (Agarwal et al., 2008; Bharadwaj et al., 2013; Malthouse et al., 2013). However, Social media security breaches are continually reported in the press, raising concerns about the ability of social networking sites to sustain safe user information management and the provision of appropriate security measures.[3] The growing concern about information security on social networking platforms is hindering business organisations from gaining the full economic benefit of social technologies (Ellison, 2007; Lievrouw and Livingstone, 2002).

Since the early days of ecommerce, information security measures for online consumers have attracted significant research attention (Dhillon and Backhouse, 2001; Liu et al., 2005; Milne and Culnan, 2004; Von Solms, 2001). The area of internet information security is well developed and evolves continuously in response to new threats. A proven, successful online security measure

☆ This paper has been recommended for acceptance by Karen Renaud.

* Corresponding author.
E-mail address: v.besnon@Kingston.ac.uk (B. Vladlena).

[1] Wirtz et al. (2010) argue that the interaction on social networks is the driving force behind its increasing popularity as a business platform. Social networks evolved from being virtual spaces for socialising to instruments for businesses and customers to co-create and reinforce consumption via virtual word-of-mouth (Kozinets, 1999; Wirtz et al., 2010).

[2] In a study conducted in the US, it was found that Fortune 500 companies use popular social media platforms such as Facebook and Twitter to interact with customers, where they could create virtual customer environments (VCEs) (Culnan et al., 2010). According to Mangold and Faulds (2009: 357), social media is the "new hybrid element of the promotion mix". Co-creation (Zwass, 2010), and word-of-mouth (Park et al., 2007; Cheung et al., 2009) are other applications of social media in commercial settings.

[3] Incidents such as the theft of 2 million passwords affecting Facebook, Google, Twitter, Yahoo, and LinkedIn accounts in December 2014 (Andrew, 2014), the Sony PlayStation information security breach (Minihane, 2011), and criticisms against Facebook apps tracking/selling personal information (Hickins, 2012) are just a the few of the social media security breaches reported in the media in recent years.

http://dx.doi.org/10.1016/j.ijhcs.2015.03.004
1071-5819/

was the development of third party security notices or artefacts, informing internet site users that measures are taken by the site owner and are independently verified. The effectiveness of online security notices has been studied for general web users and e-business users (Al-Dwairi, 2013; Belanger et al., 2002; Benassi, 1999; Kim et al., 2008). There is room for further research on the role of security notices in the context of social networking platforms and their perception by social network users. From extant literature, it emerges that the social technology and information security lags behind in the development of appropriate security notices for social media users (Lievrouw and Livingstone, 2002; Campbell et al., 2003; Cavusoglu et al., 2004; Ellison, 2007). This paper empirically examines the link between social media user experience (including past victimisation), attitude and intention and the likelihood of paying attention to security notices online. The paper provides further insights into the existing theory on security notices and informs policy and practice about the importance of security notices to social media users and the affecting factors.

Specifically, the contribution of this paper is threefold. First, we extend the existing literature, which mainly focuses on the role of security notices in e-commerce settings, by turning the research lens towards security notices/features in social media settings. Secondly, we collect rich and original data to allow an empirical investigation of the nature and magnitude of the associations between purchase experience, purchase intention, propensity towards risks, usage of different categories of social networks, user victimisation and the attention paid to security notices. Protecting personal information security in social technologies has been a heated topic for the industry, and in policy debate. This paper sheds more light on the mechanisms and user behaviour traits which can help the social technology industry more effectively protect the personal information of their users and ease concerns over transition into the social commerce era.

The article is organised as follows: in Section 2, we review extant literature on the subject of online information security and security notices, setting forth the research hypotheses. We focus on the security notices, or the security visualisation techniques used on websites, such as security seals (e.g. sign-in seals, VeriSign, TRUSTe), notices (e.g. security policies) and other features (e.g. padlock icon, URL indication, SSL protection) in line with the definition by Dang and Dang (2013). We aim to address the following five important questions. First, does higher usage of social media increase the level of attention paid to security notices? Second, do users with previous purchase experience in a social context pay less attention to security notices/features? Third, does past security victimisation influence user attitudes towards security notices? Fourth, is there a link between security notices and user intention to make a purchase from a social media vendor? Finally, are individuals with high risk propensity less likely to pay attention to security notices? Research design and methodology are discussed in Section 3. Specifically the strategy for data collection from over 500 active social network users[4] is described. Section 4 presents the result and Section 5 discusses their implications for theory and practice. The conclusions of this paper, in Section 6, set an important agenda for social networks supporting business use and commercial transactions, and makes recommendations for the significance of social security notices.

[4] The social network sites used by respondents included Facebook, Twitter, LinkedIn, YouTube, MySpace, Google+, Blogger, Skype, Flickr, and virtual worlds such as Second Life, and World of Warcraft.

2. Existing work and hypotheses development

2.1. Theoretical background

Study of the social media phenomenon has emerged from two dominant areas: while the new medium for content sharing and communication is mainly attributed to the area of communication science, social theory helps explain the social (networking) structures connected via dyadic ties and the behaviour of social actors–individual nodes, groups and networks (e.g. Wasserman and Faust, 1994). Online social networking characteristics are multi-directional, immediate and contingent, which make them different from traditional online and offline communication media (Alba et al., 1997). Peters et al. (2013: 282) define Social Networking Services (SNS) as "communication systems that allow their social actors to communicate along dyadic ties", and emphasises the egalitarian nature of social networking; unlike the widely accepted hierarchal structures, nodes in social networks have equal weight in information communication and authority.

Attempts have been made to classify social networking services according to their purpose, structure, knowledge-sharing direction, and other characteristics. For example, Kaplan and Haenlein (2010) identify six categories of SNS: collective projects (e.g. Wikipedia); blogs and micro-blogging (e.g. Blogger, Twitter); content communities (e.g. Flickr, Youtube); social networking sites (e.g. Facebook, LinkedIn); multiplayer online role-playing games (e.g. World of War Craft) and finally, virtual social worlds (Second Life). This categorisation is rather one-dimensional and application-based, which changes with the evolution of capabilities offered by social media sites. It has been argued that the purpose-based classification approach fails to keep up with the pace of technology and constantly evolving features of social networking services. For example, the functionality of collective projects and content communities is expanding rapidly, and the purposes of the different service categories are starting to converge.

Researchers agree that social media is inherently different from other types of media (Hoffman and Novak, 2012; Rapp et al., 2013). Online social networks are self-developing, dynamic, interconnected and interactive; they are beyond the control of an organisation, with a specific set of metrics for analysis and idiosyncratic management principles. The distinct nature of social media presents a challenge for applying known metrics and values from the traditional online context. Consequently, a new set of principles is required to explain the behaviour of actors in social media, and new tools need to be developed by the parties involved in social transactions to communicate their message of privacy and safety to users.

Extensive studies of behavioural descriptive norms (Cialdini et al., 1990) help explain the behaviour of social actor, the acquisition of privacy safety norms and their dynamics in social networking communities as behaviour predictors. Kashimaa et al. (2013) emphasise the role of descriptive norms – what social media users do in particular settings in terms of their behaviour and decision-making online. Internet users can learn how to behave securely and identify artefacts, such as security notices, which reinforce their perceptions of personal information security measures. These conclusions are very important in the context of online purchase behaviour and social users' perceptions of personal information security. Specifically, social users acquire descriptive norms from others with whom they are connected via social networking ties. These norm acquisition behaviours are either experiential, (i.e. users observe what others do and learn or follow their behaviour, or consequently make decisions according to the norms existing in the social networking community), or conceptual. In the latter case, users learn from what their associates say people do (Kashimaa et al., 2013). This resonates with social learning theory on the role of environmental and cognitive factors in influencing human behaviour (Bandura, 1971,