Computers in Human Behavior 59 (2016) 456–468

Contents lists available at ScienceDirect

Computers in Human Behavior

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

Full length article

From the user's perspective: Perceptions of risk relative to benefit associated with using the Internet

Zinta S. Byrne [a, *], Kyla J. Dvorak [a, 2], Janet M. Peters [a, 1], Indrajit Ray [b], Adele Howe [b], Diana Sanchez [a]

[a] Department of Psychology, Colorado State University, Fort Collins, CO 80523-1876, USA
[b] Department of Computer Science, 1873 Campus Delivery, Colorado State University, Fort Collins, CO 80524, USA

ARTICLE INFO

Article history:
Received 29 May 2015
Received in revised form
28 January 2016
Accepted 6 February 2016
Available online xxx

Keywords:
Internet
Risk-perception
Perceived benefits
Older versus younger users
Risk–gain ratio

ABSTRACT

We departed from existing studies on Internet use by exploring users' perception of their own use of the Internet. Using a mixed-method explanatory sequential design approach, we first asked users to generate lists of actions they take on the Internet and then asked them why they engage in these 35 activities. Using the information gleaned from the interviews, we developed surveys that asked 261 users (ages 19–68) to rate the perceived risk (defined as situations that contain uncertainty regarding outcomes and/or possess the potential for negative consequences) associated with each action, benefits received from each action, frequency with which they engage in the action, and amount of information they are willing to share to engage in the action. We also assessed a number of individual difference characteristics. Our study results (1) provide an Internet Action list usable in future studies; (2) provide an initial understanding that users (to a degree) engage in Internet actions for the benefits they perceive they gain; (3) show that users share little personal information, if any, to get those benefits; and (4) users have little ability to accurately evaluate the true risk (i.e., due to Internet threats) associated with those actions.

Published by Elsevier Ltd.

1. Introduction

As of 2014, 2.92 billion people use the Internet worldwide (Statista, 2015). Using an economical risk-return framework, researchers have suggested the increase in Internet usage is most likely due to the many benefits it provides (e.g., Horrigan, 2008). For example, the Internet facilitates work, social connections, and education. However, along with the many benefits of using the Internet come security and privacy risks.

Given the increasing complexity of computers and sophistication of Internet security threats, we suspect it has become progressively difficult for users to understand what risks they are taking when accessing and using the Internet. In support, despite their reported awareness of possible consequences and self-proclaimed competence as computer users, people still engage in risky online behavior (Aytes & Connolly, 2004). Users report concerns about supplying their personal information online (Cranor, Reagle, & Ackerman, 1999; Horrigan, 2008; Phelps, Nowak, & Ferrell, 2000); however, they continue to do so in exchange for convenience and potential marketing benefits (Horrigan, 2008; Phelps et al., 2000). It is apparent that given their concern yet continued exposure, users are mostly unaware of the risks (i.e., potential consequences; Bauer, 1960) posed by their repeated Internet use.

Furthermore, people become acclimated or insensitive to repeated exposure to risks (Fischhoff, Bostrom, & Quadrel, 1993; Shaklee & Fischhoff, 1990; Slovic, Fischhoff, & Lichtenstein, 1979; Zeckhauser & Viscusi, 1990), which tells us that they will continue to engage in risky Internet use, if not become more emboldened over time. Furthermore, even for those who claim they recognize that risks exist, they tend to believe those risks apply to others rather than to themselves (e.g., Brosius & Engel, 1996; Debatin, Lovejoy, Horn, & Hughes, 2009; Paul, Salwen, & Dupagne, 2000). Given this cumulative evidence, we should conclude that people are poor judges of their own ability to assess risk on the Internet. As of today, there is little empirical evidence to confirm or reject suspicions that users' lack awareness of Internet risks because few have studied users' perceptions of the risks

* Corresponding author. Department of Psychology, 1876 Campus Delivery, Colorado State University, Fort Collins, CO 80523-1876, USA.
E-mail address: Zinta.Byrne@colostate.edu (Z.S. Byrne).
[1] Janet Peters is now at: Department of Psychology, Washington State University (Tri-Cities), Richland, WA 99534.
[2] Dvorak is now Holcombe.

http://dx.doi.org/10.1016/j.chb.2016.02.024
0747-5632/Published by Elsevier Ltd.

inherent in the Internet.

The study of risk perceptions is broad, yet lacks depth in some areas. Defined in multiple ways across a number of domains, risk perceptions are studied in psychology, sociology, political science, and geology, to name a few (Slovic, 1987). In general, the aim of these studies is to stop people from engaging in risky behavior, such as unprotected sex or smoking (e.g., Arnett, 2000; Rolison & Scherman, 2003). Researchers have also examined general perceptions of risky behavior within a number of broad domains such as recreation, finance, and health or safety (e.g., Soane, Dewberry, & Narendran, 2010; Weber, Blais, & Betz, 2002). The intent of this research is to identify people's tendencies towards making risky choices that could be used to predict their subsequent behavior. For instance, within the consumer and marketing literature, perceived risk has been identified as a barrier to electronic commerce (e.g., Lieberman & Strashevsky, 2002) and adoption of technology that leads to more purchases (e.g., Featherman & Pavlou, 2003; Shen & Chiou, 2010). Within the Internet security literature, many have examined methods to encourage secure behavior on the Internet, including password protection, email usage, security notices, and backing up computer files (e.g., Aytes & Connolly, 2004; Davinson & Sillence, 2010; Vladlena, Saridakis, Tennakoon, & Ezingeard, 2015). Researchers in this literature domain focus primarily on how to promote secure behaviors when using the Internet (Davinson & Sillence, 2010; Furnell, Bryant, & Phippen, 2008), alleviate anxiety towards the Internet (Durndell & Haag, 2002), and resolve user ignorance that prevents use of the Internet, such as e-commerce (e.g., Grazioli, 2004).

Although much is understood about users' perceptions of risk when it comes to electronic commerce and securing the Internet, few studies to date provide general insight into what users do with the Internet, how they view the Internet as a medium, or whether they truly perceive the Internet itself as risky. For example, what specific actions do users report that they engage in? How does their view of the Internet shape their regular use of the Internet? Do they perceive those actions as inherently risky?

To explain why people engage in risky behavior on the Internet, some researchers have turned to the theory of planned behavior (Ajzen, 1991; Ajzen & Fishbein, 1973) as an alternative to the economics risk-return framework. The theory of planned behavior suggests that attitudes towards using the Internet (e.g., "is it risky?") determine whether an employee behaves in a manner that increases his or her vulnerability to Internet security threats. Although this theory provides a potentially useful lens through which to study Internet behaviors, and even though researchers have studied Internet use, such as consumer online purchasing (e.g., Harridge-March, 2006; Pires, Stanton, & Eckford, 2004), there is limited information on employees' perceptions of the riskiness of their Internet behavior. Even the consumer research has focused on trustworthiness of online vendors to understand their buying habits (e.g., Harridge-March, 2006), paying no attention to the perceived risk of the Internet itself.

Thus, although research efforts have advanced our understanding of specific uses of the Internet, their narrow focus on a single domain (e.g., shopping, banking, password protection) and reliance on pre-determined lists of general risky actions fail to provide a broad understanding or mechanism for evaluating users' perceptions of the Internet across a variety of domains. Consequently, we depart from existing studies by exploring users' perception of their own Internet use. Using a mixed methods explanatory sequential design approach (i.e., integrating qualitative and quantitative research; Creswell & Clark, 2007), we asked users to generate lists of actions they take on the Internet and then asked why they engaged in these activities. Using the information gleaned from the interviews, we developed surveys that asked users to rate the actions on the perceived risk (defined as situations that contain uncertainty regarding outcomes and/or possess the potential for negative consequences) associated with each action.

Therefore, the focus of our exploratory study was on the user and his or her general perceptions of the Internet. In contrast to extant literature, our focus was driven by how users view the Internet. Our approach is essential for advancing existing literature because knowing the user's perception of risk associated with a specific action is fundamental in applying theories such as the theory of planned behavior (Ajzen, 1991; Ajzen & Fishbein, 1973).

1.1. Psychological risk perception

The objective for studying user perceptions of risk on the Internet is ultimately to design solutions that prevent individuals from increasing their vulnerability to Internet security threats. To achieve this goal, researchers need to understand individuals' perceived level of risk, which according to the theory of planned behavior, may predict Internet behavior (Ajzen, 1985; Ajzen & Fishbein, 1973). Social psychological research in the perception of health-related risky behaviors (e.g., engaging in sex without protection: Weinstein, 1993) and risk of texting while driving (Atchley, Atwood, & Boulton, 2011) indicates, however, that even when individuals hold negative attitudes towards specific behaviors, they engage in them anyway. These findings cast doubt on solely using the theory of planned behavior for explaining behavior resulting from risk perceptions. The key here, according to Weber et al. (2002), is that risk perceptions are not the same as *attitudes* towards risk. Weber et al. argued that attitudes towards risk are stable evaluations of the tradeoff between expected utility of an action and the potential for that action to result in an unfavorable outcome. Those who generally believe they can manage the outcome or are willing to take the chance that the payoff will be favorable hold positive attitudes towards risk; they see the glass as half full. Perceptions of risk, in contrast, are moment-to-moment assessments of the uncertainty and threat a situation or behavior holds at that time. Perceptions of risk are, therefore, dependent on the specific situation.

Findings on risk perception in specific situations, such as health and driving, have alternatively been explained using cognitive dissonance theory (Festinger, 1957). This theory suggests that individuals engaging in negative behaviors reduce their perceptions of the risk associated with those behaviors as a mechanism for resolving the dissonance experienced by knowing the risk, yet still engaging in the behavior. Such an explanation has been put forth for *known* risk perceptions – situations where the risk is known and the consequence has been quantified (e.g., Atchely et al., 2011), such as texting while driving and engaging in unprotected sex. However, even though the study of risk perception has become associated with and defined as a calculated, engineered, or psychometric analysis of an objective outcome, the perception of risk is subjective, where a calculation or probability analysis of consequences is actually not known (Brehmer, 1994). The risk, per se, may or may not actually exist – what is relevant is the *perception* that it exists. Internet threats present a scenario where neither the risk nor the consequence is known or quantifiable.

1.2. Rational choices in risk perception

When studying risk perception, one cannot ignore the body of literature focused on rational decisions under situations of risk or uncertainty (e.g., Kahneman & Tversky, 1982; Slovic, Fischhoff, & Lichtenstein, 1977; Tversky & Kahneman, 1981). This literature focuses on *rational choices* rather than unknown and unquantifiable consequences such as with Internet threats. Specifically, this