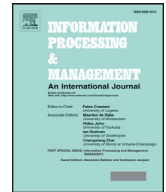


Contents lists available at [ScienceDirect](#)

Information Processing and Management

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

Gender deception in asynchronous online communication: A path analysis

Shuyuan Mary Ho^{a,*}, Paul Benjamin Lowry^b, Merrill Warkentin^c, Yanyun Yang^d, Jonathan M. Hollister^e

^a School of Information, College of Communication and Information, Florida State University, 142 Collegiate Loop, P.O. Box 3062100, Tallahassee, FL 32306-2100, USA

^b Innovation and Information Management, School of Business, Faculty of Business and Economics, The University of Hong Kong, K. K. Leung Building, Hong Kong, China

^c Information Systems, Dept. of Management and Information Systems, College of Business, Mississippi State University, P.O. Box 9581, Mississippi State, MS 39762-9581, USA

^d Department of Educational Psychology & Learning Systems, College of Education, Florida State University, Stone Building 3204 K, P.O. Box 3064450, Tallahassee, FL 32306-4450, USA

^e Information Institute, College of Communication and Information, Florida State University, 142 Collegiate Loop, P.O. Box 3062100, Tallahassee, FL 32306-2100, USA

ARTICLE INFO

Article history:

Received 15 February 2016
Revised 30 April 2016
Accepted 10 June 2016
Available online xxx

Keywords:

Human computer interaction
Computer-mediated deception
Human information behavior
Gender, deception
Online game

ABSTRACT

Gender is a salient feature of identity that is rarely questioned in our physical encounters. We are usually not confused about a person's gender—generally it's male or female. However, as the adoption of computer-mediated communication increases, our social reliance on these technologies has made gender easily disguised online. And yet, the phenomenon of gender deception has not been fully investigated. This study adopts a path analysis to examine interconnected cognitive factors that impact online users' ability to deceive—and detect deception—regarding gender. An asynchronous online game was developed to simulate situations where males were incentivized to communicate like females, and females were incentivized to communicate like males. Twelve hypotheses were tested using path analysis, which resulted in our realization that an actor's true gender can affect the motivation to deceive; males tend to have higher self-efficacy beliefs in gender deception, and females tend to have a higher success rate in detecting gender deception. Our research suggests that the gender of the message recipient could be a significant factor in uncovering gender deception.

© 2016 Elsevier Ltd. All rights reserved.

1. Introduction

Online users must frequently make judgments or decisions based on computer-mediated interaction. It is common for individuals to receive emails with hypertext links or a popup messages from a website, or be asked to confirm or cancel some electronic procedure. Many online users receive phishing emails¹ requesting personal or sensitive information, or seeking a

* Corresponding author. Fax: 850.644.9473, Website: school.cci.fsu.edu.

E-mail addresses: smho@acm.org, smho@fsu.edu (S.M. Ho), Paul.Lowry.PhD@gmail.com (P.B. Lowry), m.warkentin@msstate.edu (M. Warkentin), yyang3@fsu.edu (Y. Yang), jmh09k@my.fsu.edu (J.M. Hollister).

¹ Phishing emails are sent out as one-to-many asynchronous online communication, which is to contrast the synchronous online chat communication.

response (Wright & Marett, 2010). Phishing emails may also induce actions such as answering inquiries about social, financial, or business relationships, or confirming social media friend requests, resulting in online gender fraud (Brady & George, 2013). Repeatedly, online users must determine whether the source of a message is credible and legitimate (Hillgoss & Rieh, 2008; Liu, 2004; Rieh, 2002) in order to maintain privacy and safety (Lopez & Sebe, 2013; Twyman, Lowry, Burgoon, & Nunamaker, 2014).

A rise in the threat of deceptive communications has accompanied the increased reliance of individuals and organizations on computer-mediated communication (CMC²) systems. In a *New York Times* interview, Bruce Schneier, an American cryptographer, states that trust is “the glue that binds our societies” and deceptive communications in the digital age have destroyed this trust (Sengupta, 2012, p.1). Because virtual space lacks traditional face-to-face (FtF) visual cues of deception, it has become easier for online users to misrepresent not only the content of their messages but their identities. As technology changes the way we interact socially, it becomes ever more difficult to discern whether an email from our bank is authentic, and how much we can trust authorities with our online privacy. This threat of deception has been shown to be substantial in various domains and manifests in many ways, such as phishing and “spear phishing” attacks (Wright & Marett, 2010), deception in electronic commerce (Xiao & Benbasat, 2010), deception at workplace (da Cunha, Carugati, & Leclercq-Vandelannoite, 2015), deception in group support systems (George, Marett, & Giordano, 2008), deception in professional virtual communities (Joinson & Dietz-Uhler, 2002), deceptive opinions in online reviews (Fusilier, Montes-y-Gomez, Rosso, & Cabrera, 2015; Ott, Cardie, & Hancock, 2012), deception in 911 calls (Burns & Moffitt, 2014), deception in social media relationships (Hancock, Toma, & Ellison, 2007; Hancock, Woodworth, & Goorha, 2010; Zhou, Burgoon, Twitchell, Qin, & Nunamaker, 2004), deceptive opinions and reviews (Ott, Cardie, & Hancock 2012, 2013; Ott, Choi, Cardie, & Hancock, 2011), deception in story-telling (Rubin, 2010), and fake news (Conroy, Rubin, & Chen 2015). The consequences of successful deception range from harmless inconvenience to significant costs. Such deception can pose a major threat when it drives online transaction fraud (Twyman, Lowry, Burgoon, & Nunamaker, 2014), identity theft, theft of credentials, theft of intellectual property, or threats against national security.

One salient dimension of online deception is users’ misrepresentation of their gender (Ho & Hollister, 2013). One’s gender, which has been traditionally considered binary due to distinct biological differences at birth, has a tendency to be socially reconstructed (Bussey & Bandura, 1999). Bussey and Bandura (1999) suggested that gender roles are constantly being reconstructed by a broad network of peers and societal influences. Gender and gender role development are constantly mixed with experience and motivation. People’s self-development can redefine their gender identity (e.g., recognition or realization of being gay), which eventually contributes to social change (e.g., legalization of gay marriage). Regardless of these social impacts, users’ online identities are continually being constructed by a number of factors, including their redefined gender roles, their motivations, self-efficacy, social interactions with friends and colleagues, as well as personal desires and goals. The binary view of gender creates fundamental representation problems. Rodino (1997), for instance, observed inconsistencies in online chatters’ language and presentation of their gender, and suggested that gender can be “performed” in an online environment. In other words, gender can be made more real and natural in virtual, imaginative communication. Gender, through linguistics, can be socially “constructed,” and online actors may falsify the representation of gender to increase the probability of gaining trust.

Gender can represent a unique feature of online deception in that it can involve fairly nuanced clues and circumstances that one may not normally consider. In asynchronous online communication, individuals may attempt to misrepresent their gender, and recipients of online messaging may lack the ability to identify the gender of their communicators. Regardless of the reasons people may attempt to deceive others about their gender, empirical results show that 18% of males and 11% of females have lied about their gender (Whitty, 2002, p. 348) at some point when engaging in text-based communication. Gender deception can be highly disturbing to both males and females who have been deceived (Stieger, Eichinger, & Honeder 2009). Previous research has found gender-related influences, in the ways males and females communicate—in both FtF and online communication (Herring, 2000; Herring & Martinson, 2004; Savicki, Kelley, & Oesterreich, 1999; Whitty, 2002). Yet, little is understood about the role of gender deception in the complexity of computer-mediated deception. As gender misrepresentation or gender deception has become a major contributing factor in identity fraud, our research intends to explore, describe, and explain different cognitive factors that facilitate gender deception in computer-mediated communication. Our overarching research question is thus set as follows: *How are the cognitive factors of gender deception modeled in asynchronous online communication?*

That said, online users can adapt in ways that extenuate or diminish certain facets of their identities (including their gender) in certain social situations depending on social goals, conversational topics, context, or cultural situations (Herring, 1995, 2000). In other words, depending on the context and topic, it is possible for males to adjust their communication toward female styles, and females can employ communication style more like male utterances in order to disguise their true gender. This paper outlines our investigation to first review deception in FtF interaction as well as online communication when facilitated by computer-mediated technologies. Twelve research hypotheses—examining motivation and self-efficacy of both message senders and receivers that impact the outcome of deception—are discussed within the framework of gender deception. We then discuss our research design and considerations for an experiment deployed in the form of an online

² CMC broadly includes both synchronous (e.g., chat) and asynchronous (e.g., texting, email, etc.) communication.

متن کامل مقاله

دریافت فوری ←

ISIArticles

مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات