Current State of the Digital Deception Studies in IS

Completed Research Paper

Jerry Zhang
University of Texas at San Antonio
Jerry.zhang@utsa.edu

Myung Ko
University of Texas at San Antonio
myung.ko@utsa.edu

ABSTRACT

Digital deceptions exist on the Internet in various forms and for different purposes. The purpose of this study is to understand the current state of the digital deception research in IS discipline. Based on our review and analysis of the selected digital deception articles published in IS journals and conference proceedings, we discussed various perspectives of digital deceptions, such as the media, types of deception, deceivers, motivations, and victims. The results of our study indicate that deception phenomena are severely under-researched in IS discipline. The study provides suggestions for future research.

Keywords

Internet, deception, computer-mediated communication (CMC).

INTRODUCTION

It has been more than twenty years since the Internet was introduced. During these years, people have learned all kinds of ways to gather and exchange information via Internet. Almost any information in this world could be found easily on the Internet, such as friends, products information, and etc. Thus, the Internet has become one of the most important information resources in people's lives, and people can make judgments and decisions based on the information provided online. Facilitated by innovative technologies, the ways we communicate with others and process information have been changed fundamentally in a progressive manner. As a matter of fact, the Internet has created a whole new social environment and a context of information exchange.

Previous studies have suggested that people lie once or twice on the daily basis (DePaulo et al. 1996). Besides harmful lies, deception may be due to avoid conflict or hurting others, or to protect self-image (Guerrero et al. 2010). Since we have started using computer-mediated communication (CMC), do we more likely to lie or get deceived on the Internet? One of the most remarkable characteristics of the Internet is anonymity. If anonymity could provide a user with the opportunities to say anything he or she wants on the Internet without considering any of the consequences (Spears and Lea 1994), then the Internet can be an ideal medium for deception. On the other hand, different from face-to-face (FTF) communication, CMC is only capable of transmitting relatively limited categories of communication cues. Other than verbal cues, some other kind of communication cues such as facial expressions, tones or gestures cannot be sent or observed by communication partners effectively (Daft et al. 1987; DePaulo et al. 1996). Therefore, without such communication cues, it is relatively difficult for people to find out who is the liar and what they are lying about (Daft et al. 1987).

There are some previous studies that have investigated on online deception. These studies describe that people use fake profile pictures or lie about their identity in order to find a romantic partner (Ellison et al. 2006), send phishing messages and build spoof websites to extract users' personal and financial information (Abbasi et al. 2010; Vishwanath et al. 2011), commit auction fraud and review fraud to influence others' decisions (Hu et al. 2011; Porter and Shoham 2005; Xiao and Benbasat 2011), and even lie to protect themselves (Son and Kim 2008).

In IS discipline, online deception is still a relatively new topic comparing to psychology and communication disciplines. The purpose of this study is to provide a literature review on the online deception research published in IS journals and to understand different perspectives and characteristics on this topic. We believe our study provides additional insights on online deception research. In the following sections, we will briefly discuss deception both in general and online context, describe selection process of journals and articles, present a brief literature review on the selected articles, discuss different perspectives and characteristics of digital deception, and provide directions for future research, and then conclude the paper including limitations.

DIGITAL DECEPTION

Among various definitions of deception in traditional communication and psychology, it was believed that definition from Burgoon and Buller (1994, 1996) is the most conclusive one (Hancock 2007). Burgoon and Buller (1996) conceptualize deception as "a message knowingly transmitted by a sender to foster a false belief or conclusion by the receiver", and Hancock

(2007) refers the deception in digital communication context as "digital deception" which is "the intentional control of information in a technologically mediated message to create a false belief in the receiver of the message". According to Hancock (2007), there are three important characteristics of digital deception: first, deception activity must be intentional or deliberate, which means unintentional mistakes or misrepresentations do not count as digital deception; second, the purpose of the deception has to be misleading or creating false beliefs, thus, joke and irony are not considered as deception; third, this is more relevant to digital deception; technologically mediated message has to be the information control mechanism in the deception activities. In other words, the deceptive message must be transmitted through digital media instead of FTF communication. Regarding to the IS discipline identity crisis (Benbasat and Zmud 2003), there might be concerns about the legitimacy of the deception research in IS discipline. We believe that digital deception would fit in one of the recommended IS research parameter since it deals with human behaviors reflected within direct and indirect usage of IT artifacts. In addition, digital deception should belong to the ensemble view of IT artifact, which is one of the metacategories identified by Orlikowski and Iacono (2001).

JOURNAL AND ARTICLE SELECTION

We selected articles focused on the phenomenon that fits Hancock (2007)'s definition of digital deception. Accordingly, the topics regarding financial statement fraud and credit card fraud were not included in this study. On the other hand, some malicious attack methods like phishing and spoofing are included in our research since those attacks are directly relied on the deceptive messages sent to massive Internet users (Vishwanath et al. 2011).

Although it is very clear that digital deception is an interdisciplinary topic involving psychology and communication (Skitka and Sargis 2006), this study focuses on deception research conducted in IS discipline. Thus, we started with the top 10 journals in IS discipline using Rainier and Miller (2005)'s IS journal ranking and added journals recommended as top journals in IS field by the Senior Scholars Consortium of Association of Information Systems (AIS) (Consortium 2011).

Due to the small number of digital deception articles published from these top journals, we expanded our scope to include additional IS journals and conference proceedings that published relevant articles, using key word search, such as "online deception," or "digital deception." At the end, we identified twenty-one articles that focused on digital deception (Table 1). Not surprisingly, the earliest deception research we could find was published in early 2000, indicating that digital deception has only been noticed fairly recent years in IS discipline. Refer to research paradigms (Hevner et al. 2004), most deception research falls under the behavioral research category while only two belongs to design research.

Article	Focus	Paradigm	Type of study
Grazioli and Jarvenpaa (2000)	Fake website	Behavior	Experiment
Grazioli and Wang (2001)	Attitude toward deception	Behavior	Experiment
Burgoon et al. (2003)	Media	Behavior	Experiment
Grazioli and Jarvenpaa (2003)	Deception tactics	Behavior	Content analysis
Zhou et al. (2003)	Text-based CMC	Behavior	Experiment
Carlson and George (2004)	Media	Behavior	Survey
Zhou et al. (2004)	Deception cues and classification models	Design	Experiment
Pavlou and Gefen (2005)	E-commerce	Behavior	Longitudinal
Porter and Shoham (2005)	Auction fraud	Behavior	Econometrics
Tilley et al. (2005)	Online job interview	Behavior	Experiment
Cecil Eng Huang et al. (2007)	Auction fraud	Behavior	Observation
Galanxhi and Nah (2007)	Avatar	Behavior	Experiment
Zhou and Zhang (2007)	Media	Behavior	Experiment
Lewis and George (2008)	Culture	Behavior	Survey
Son and Kim (2008)	Privacy threats	Behavior	Survey
Abbasi et al. (2010)	Fake website	Design	Experiment
Jarvenpaa and Majchrzak (2010)	Knowledge collaboration	Behavior	Discussion
Wright and Marett (2010)	Phishing	Behavior	Field experiment

Hu et al. (2011)	Consumer review	Behavior	Observation
Vishwanath et al. (2011)	Phishing	Behavior	Survey
Xiao and Benbasat (2011)	E-commerce	Behavior	Discussion

Table 1. Selected Articles

LITERATURE REVIEW

A brief review of selected articles is described in the following based on the related subtopic.

E-commerce

Grazioli and Jarvenpaa (2000) investigated consumers' ability of identifying fake shopping websites and found that most subjects who use online shopping still failed to identify the fraudulent cues designed in the forged website and made their purchase decision. Grazioli and Wang (2001) integrated the deception, trust, and risk model (DTR) and the theory of deception to study how online shoppers evaluate the deceptive information and make their purchase decision. Their study suggests that consumers lack the knowledge of online shopping deception. Abbasi et al. (2010) investigated the detection system for fake websites on the Internet, more specifically, the spoof and concocted websites. They proposed a new class of detection system based on statistical learning theory (SLT) and their proposed system outperformed the existing systems.

Pavlou and Gefen (2005) identified deception in online marketplace as one of six key sources of psychological contract violation (PCV), which typically occurs when people believe that they are not getting what they expect from a purchase. They found that PCV can affect buyers' purchasing behavior and perceived risk.

Grazioli and Jarvenpaa (2003) discussed deception tactics on the Internet and identified the most popular tactics used against individuals and organizations on the Internet. The common types of deception in online communities include identity deception, mimicking data and processes, false promise, or some form of fraud. Another study by Xiao and Benbasat (2011) described the types of deceptive information practices that can be used against consumers in e-commerce. The authors developed an integrative model that includes some key factors influencing consumers' responses to the deceptive information in e-commerce.

Consumer Review Fraud

Hu et al. (2011) investigated the existence of online consumer review fraud using data from Amazon.com and Barnes & Noble and found that some publishers, authors, and vendor constantly manipulate online customer reviews. The authors contend that, to certain extent, vendors can control the outcome of the manipulation and consumers will respond to the falsified information.

Culture / Gender

Based on cultural differences, Lewis and George (2008) compared the deceiving behaviors for both Korean and American participants in face-to-face and online social network settings. They found that deceptive behavior was greater for FTF communication than for CMC for both cultural groups but no difference between Korean CMC and American CMC. Using four different electronic communication media - email, Internet relay chat (IRC), IRC with audio, and audio only, Tilley et al. (2005) found that females were significantly better at detecting deceptions than males although there was no significant difference for deception success between genders.

Communication Channels

Burgoon et al. (2003) investigated human deception detections in four different communication channels: FTF, text, audio and audio and video (AV) and found that people tend to detect deception less accurately in visual communication. They also found that people are more likely to detect deception in audio only channel and least likely to detect deception in text-based channel. Zhou et al. (2003) investigated linguistic deceptive cues using emails and they found significant difference in cues between true and deceptive messages.

Carlson and George (2004) studied preferences of media synchronicity and media richness by deceivers and receivers. Both deceivers and receivers felt comfortable using high level synchronicity media to perform deception or detection. The authors also found that receivers had higher confidence of detecting deception when using familiar media. Focusing on deception detection in online IM, Zhou and Zhang (2007) investigated how media modality and media veracity influence human deception detection and found that both modality and veracity of IM influence the process and outcome of human deception detection.

Online Auction

Porter and Shoham (2005) believe that the increased popularity of online auction has made the disadvantage of sealed-bid auction even worse. They analyzed two types of cheating in sealed bid auction and argued that to prevent cheating, more focus on the design of auction should be necessary, possibly using cryptographic methods and digital certificate. Dealing with community crime, Cecil Eng Huang et al. (2007) investigated the Internet users' reaction to online auction fraud using social disorganization theory, and explained how online auction communities deal with this problems and show how they cooperate with the formal authority of auction service providers.

Motivations for Deception

Jarvenpaa and Majchrzak (2010) identified deception, trust asymmetry, and novelty as a three elements of vigilant interactions in online knowledge collaboration. The authors suggest that the purpose of online deception might not exclusively for gain or advantage but for many other reasons such as privacy concern, minimizing conflict, encouraging fun, and etc. Son and Kim (2008) investigated Internet users' responses to privacy threats from online companies and found that besides the refusal to provide personal information, the misrepresentation of personal information is considered to be another protective behavior regarding privacy concern.

Phishing

Wright and Marett (2010) investigated the factors influencing users' susceptibility to potentially malicious phishing messages. Their models contain three experimental factors that include computer self-efficacy, web experience, and security awareness, and three dispositional factors that include disposition to trust, perceived risk, and suspicion of humanity. The result of their study indicated that users' low ratings on experimental factors are more susceptible to phishing messages, and suspicion of humanity decreases the likelihood of being deceived. To provide a comprehensive view of the phishing deception process, Vishwanath et al. (2011) proposed an integrated information processing model of phishing susceptibility based on interpersonal deception theory, theory of deception, and elaboration likelihood model.

Avartar

Galanxhi and Nah (2007) found that deceivers experienced higher anxiety than truth-tellers, but not in the avatar-supported environment. Moreover, deceivers tended to use the avatars different from themselves. For receivers, using avatars did not influence their perception of trustworthiness.

DISCUSSION AND FUTURE RESEARCH DIRECTION

In this section we discuss the reviewed literature from various perspectives, and provide suggestions for future research. Table 2 summarized characteristics of the deception articles selected in this study. To maintain the rigorousness of our study, we left the corresponding cell blank intentionally if not applicable.

Media and deception cues

It is reasonably to believe that deceptive messages can be delivered through any kinds of CMC technologies, such as websites, instant messages (IM), emails, blogs, discussion boards, consumer reviews, or even video chatting. Some of them are richer media, which are capable of transmitting various communication cues, while others are leaner, which can only transmit limited cues such as text-based messages (Daft and Lengel 1983). Based on media richness theory, the richness of communication cues can have direct influence on the efficiency of deception detection (Short et al. 1976). Without having FTF communication, digital communication cues are crucial to deception detection in cyberspace. While sophisticated deception using richer communication cues can get Internet users deceived more easily, it can also be detected by exposing too much leakage cues (Burgoon et al. 2003; Zhou et al. 2004). In the current stage, most of the deception detection studies have concentrated on limited categories of cues such as text-based linguistic cues or website fraud cues (Abbasi et al. 2012; Grazioli and Jarvenpaa 2000; Zhou et al. 2004). Although some studies (Burgoon et al. 2003; Tilley et al. 2005) have reported results of deception detection within different multimedia channels, none of them has addressed multimedia deceptive cues. Since the latest reported IM spoofing has already started to adopt fake videos as one of the supplementary deception methods (Tencent 2011), we suggest that future deception research may include various multimedia communication cues that have not been investigated.

Types of deception

Digital deception can be categorized into two broad types: identity-based digital deception and message-based digital deception (Handcock, 2007). Identity-based digital deception refers to false representation of a person or organization's identity; and message-based digital deception refers to manipulations of message in the communication between two or more agents. However, these two types of digital deception are not mutually exclusive. For instance, in a phishing email, both identity of the sender and the message can be deceptive. Therefore, derived from interpersonal deception theory (Buller and Burgoon 1996), we differentiate digital deceptions by the number of ways of transferring deceptive message: one-way and interactive deceptions. In particular, one-way digital deception refers to the methods by which the deceptive messages were sent or presented to receivers without allowing subsequent modification or interaction according to receivers' reaction. On the other hand, interactive digital deception refers to the methods by which the deceptive messages were sent or presented to receivers several times during the interactions between the senders and receivers, and the deceptive messages are strategically modified by the senders according to the responses of the receivers. Based on our review, most of the deception research have addressed both one-way (Abbasi et al. 2010; Hu et al. 2011; Vishwanath et al. 2011; Zhou et al. 2004) and interactive deception (Burgoon et al. 2003; Galanxhi and Nah 2007; Lewis and George 2008; Tilley et al. 2005; Zhou et al. 2003). However, the research related to interactive deception was either focused on media cues (Burgoon et al. 2003; Zhou et al. 2003), demographic variables (Lewis and George 2008; Tilley et al. 2005), or avatars (Galanxhi and Nah 2007). None of them was concentrating on the behaviors during the information exchange processes. Since Carlson and George (2004) suggested that deceivers tend to use high level synchronicity media to perform deception, the future deception research may look into the reactions of deceivers according to the responses sent by the receivers and how the deceivers modify their messages in order to achieve the ultimate goals.

Deceivers and motivations

The deceptive messages cannot be generated by themselves or by automated systems without human intervention. Thus, the source of deceptive messages, the deceivers, should be investigated. By studying the deceivers we may understand the interested parties behind the deception activities, their motives, and their capabilities to deceive, etc. Most current IS deception studies (Abbasi et al. 2010; Hu et al. 2011; Vishwanath et al. 2011; Xiao and Benbasat 2011) focused on the deceptive activities that are intended to damage or cheat for monetary purposes. However, some studies have investigated other reasons of digital deception. Internet users may deceive or misrepresent themselves for privacy concerns or preventing perceived risks (Jarvenpaa and Majchrzak 2010; Son and Kim 2008). From the perspective of deceivers and their motivations, future IS deception research may focus more on non-monetary motivations such as privacy concerns, protection from perceived threat, interpersonal intimacies (Hancock et al. 2007), or sex crimes (Wolak et al. 2004).

Victimologies

Most of the online deceptions such as auction scams, fake websites, or phishing messages only exhibit a limited number of strategies. These deceptions are crafted for wide audience but not for a particular target. The existing automated systems only have limited capabilities to detect digital deception, leaving much of the responsibilities to end users (Wright and Marett 2010). However, there are only a few studies exploring the individual profile attributes, such as gender and personality traits (Vishwanath et al. 2011). Since there are different types of deceivers and their motivations, the victims also can vary. Besides normal Internet users, online business owners (Grazioli and Jarvenpaa 2003; Porter and Shoham 2005), auction sellers (Porter and Shoham 2005), employers (Tilley et al. 2005), or organizations legally using customer data (Son and Kim 2008) can also become victims of digital deception. We suggest the IS researchers to focus on the traits and attributes, which make these victims vulnerable. Another aspect of victimology of digital deception is the consequences. Cecil Eng Huang et al. (2007) investigated the Internet users' reaction to online auction fraud in the community level, and Pavlou and Gefen (2005) have focused on the individual buyers' responses to fraud in online marketplace. Future research could investigate such digital deception victimologies that can help us better understand why the targeted population is vulnerable, increase victim awareness of such digital deceptions, and develop prevention methods.

Publication	**Communication media**	**Types of deception**	**Motivations**	**Victims**
Grazioli and Jarvenpaa (2000)	Fake website	One-way, identity based and message based	Profit	Buyers
Grazioli and Wang (2001)	Fake website	One-way, identity based and message based	Profit	Buyers
Burgoon et al. (2003)	FTF, text, audio, AV	Interactive, N/A	N/A	Ordinary people
Grazioli and Jarvenpaa (2003)	Internet	N/A	Profit	Consumer and business
Zhou et al. (2003)	Email	Interactive, N/A	N/A	Internet users
Carlson and George (2004)	FTF, phone, voice mail email, fax, letter, memo, hand-written note, video conference, webpage	Interactive, N/A	N/A	Ordinary people
Zhou et al. (2004)	Email	Interactive, message based	N/A	Internet users
Pavlou and Gefen (2005)	E-commerce	One-way, interactive and message based	Profit	Buyers
Porter and Shoham (2005)	Auction website	Interactive, N/A	Profit	Seller or buyer

Tilley et al. (2005)	email, Internet relay chat (IRC), IRC with audio, audio	Interactive, message based	Job opportunities	Employer
Cecil Eng Huang et al. (2007)	Auction website	One-way and interactive	Profit	Buyers and sellers
Galanxhi and Nah (2007)	IM	Interactive, message based	N/A	Internet users
Zhou and Zhang (2007)	IM	Interactive , message based	N/A	Internet users
Lewis and George (2008)	FTF, social network	Interactive, N/A	N/A	Ordinary people
Son and Kim (2008)	E-commerce	One-way, identity based	Self-protection	Businesses
Abbasi et al. (2010)	Fake website	One-way, identity based and message based	Profit	Buyers
Jarvenpaa and Majchrzak (2010)	Online discussion boards, social media sites, etc.	Interactive, message based	Self-protection	Internet users
Wright and Marett (2010)	Phishing email	One-way, identity based and message based	Acquiring sensitive info	Internet users
Hu et al. (2011)	Online consumer review	One-way, message based	Profit	Buyers
Vishwanath et al. (2011)	Phishing email	One-way, identity based and message based	Acquiring sensitive info	Internet users
Xiao and Benbasat (2011)	E-commerce website	Identity based and message based	Profit	Buyers

Table 2. Characteristics of the Selected Deception Research

CONCLUSION AND LIMITATION

Our research is not without limitations. We selected a limited number of articles for the literature review. However, we intended to focus on the deception research exclusively in IS discipline, and we believe that these IS journals and conference proceedings represent the current state of the digital deception research and trend in IS discipline. The characteristics of deception research we discussed might not be exhaustive and there may be some other characteristics that need to be identified. For future studies, selecting additional articles could provide more a comprehensive review on deception research.

In this study, we conducted a literature review of prior deception research published in IS leading journals and conferences. To the best of our knowledge, this is the first study that analyzes the characteristics of deception investigated by the previous studies and also provides suggestions for future research based on the review. The results of our analysis show that although deception is a prevalent phenomenon in cyber space, it is still a relatively new and under- researched topic in IS discipline and thus, further research in this area seems to be promising.

REFERENCES

1. Abbasi, A., Albrecht, C., Vance, A., and Hansen, J. 2012. "Metafraud: A meta learning framework for detecting financial fraud," *MIS Quarterly* (36:4), pp. 1293–A12.
2. Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., and Nunamaker, J. J. F. 2010. "Detecting fake websites: the contribution of statistical learning theory," *MIS Quarterly* (34:3), pp. 435–461.
3. Benbasat, I., and Zmud, R. W. 2003. "The identity crisis within the IS discipline: Defining and communicating the discipline's core properties," *MIS quarterly*JSTOR, pp. 183–194.
4. Buller, D. B., and Burgoon, J. K. 1996. "Interpersonal deception theory," *Communication theory* (6:3)Wiley Online Library, pp. 203–242.
5. Burgoon, J. K., and Buller, D. B. 1994. "Interpersonal deception: III. Effects of deceit on perceived communication and nonverbal behavior dynamics," *Journal of Nonverbal Behavior* (18:2), pp. 155–184.
6. Burgoon, J. K., and Buller, D. B. 1996. "Interpersonal Deception Theory," *Communication Theory* (6:3), pp. 311–328.
7. Burgoon, J. K., Stoner, G., Bonito, J. A., and Dunbar, N. E. 2003. "Trust and deception in mediated communication," In *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on*, pp. 11–pp.
8. Carlson, J. R., and George, J. F. 2004. "Media appropriateness in the conduct and discovery of deceptive communication: The relative influence of richness and synchronicity," *Group Decision and Negotiation* (13:2)Springer, pp. 191–210.

9. Cecil Eng Huang, C., Wareham, J., and Robey, D. 2007. “The role of online trading communities in managing Internet auction fraud,” *MIS Quarterly* (31:4), pp. 759–781.
10. Daft, R. L., and Lengel, R. H. 1983. “Information richness. A new approach to managerial behavior and organization design,”DTIC Document.
11. Daft, R. L., Lengel, R. H., and Trevino, L. K. 1987. “Message equivocality, media selection, and manager performance: Implications for information systems,” *MIS Quarterly*, pp. 355–366.
12. DePaulo, B. M., Kashy, D. A., Kirkendol, S. E., Wyer, M. M., and Epstein, J. A. 1996. “Lying in everyday life,” *Journal of personality and social psychology* (70:5), pp. 979.
13. Ellison, N., Heino, R., and Gibbs, J. 2006. “Managing impressions online: Self-presentation processes in the online dating environment,” *Journal of Computer-Mediated Communication* (11:2), pp. 415–441.
14. Galanxhi, H., and Nah, F. F.-H. 2007. “Deception in cyberspace: A comparison of text-only vs. avatar-supported medium,” *International journal of human-computer studies* (65:9)Elsevier, pp. 770–783.
15. Grazioli, S., and Jarvenpaa, S. L. 2000. “Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers,” *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on* (30:4)IEEE, pp. 395–410.
16. Grazioli, S., and Jarvenpaa, S. L. 2003. “Consumer and business deception on the Internet: Content analysis of documentary evidence,” *International Journal of Electronic Commerce* (7)ME Sharpe, pp. 93–118.
17. Grazioli, S., and Wang, A. 2001. “Looking without seeing: understanding unsophisticated consumers’ success and failure to detect Internet deception,” In *Proceedings of the 22nd International Conference on Information Systems. New Orleans*.
18. Guerrero, L. K., Afifi, W. A., and Andersen, P. A. 2010. *Close encounters: Communication in relationships*, Sage Publications, Incorporated.
19. Hancock, J. T. 2007. “Digital deception: Why, when and how people lie online,” *Oxford handbook of internet psychology*, (Joinson, McKenna, Postines, and Reips, ed.), pp. 289–301.
20. Hancock, J. T., Toma, C., and Ellison, N. 2007. “The truth about lying in online dating profiles,” *Proceedings of the SIGCHI conference on Human factors in computing systems*ACM, pp. 449–452.
21. Hu, N., Liu, L., and Sambamurthy, V. 2011. “Fraud detection in online consumer reviews,” *Decision Support Systems* (50:3), pp. 614–626.
22. Jarvenpaa, S. L., and Majchrzak, A. 2010. “Vigilant Interaction in Knowledge Collaboration: Challenges of Online User Participation Under Ambivalence,” *Information systems research* (21:4), pp. 773–784.
23. Lewis, C. C., and George, J. F. 2008. “Cross-cultural deception in social networking sites and face-to-face communication,” *Computers in Human Behavior* (24:6)Elsevier, pp. 2945–2964.
24. Orlikowski, W. J., and Iacono, C. S. 2001. “Research commentary: Desperately seeking the‘ it’ in it research—a call to theorizing the it artifact,” *Information systems research* (12:2)INFORMS, pp. 121–134.
25. Pavlou, P. A., and Gefen, D. 2005. “Psychological Contract Violation in Online Marketplaces: Antecedents, Consequences, and Moderating Role,” *Information systems research* (16:4), pp. 372–399.
26. Porter, R., and Shoham, Y. 2005. “On cheating in sealed-bid auctions,” *Decision Support Systems* (39:1), pp. 41–54.
27. Short, J., Williams, E., and Christie, B. 1976. “The social psychology of telecommunications,”John Wiley and Sons Ltd.
28. Skitka, L. J., and Sargis, E. G. 2006. “The Internet as psychological laboratory,” *Annu. Rev. Psychol.* (57), pp. 529–555.
29. Son, J.-Y., and Kim, S. S. 2008. “Internet users’ information privacy protective responses: a taxonomy and a nomological model,” *MIS Quarterly* (32:3), pp. 503–529.
30. Spears, R., and Lea, M. 1994. “Panacea or panopticon? The hidden power in computer-mediated communication,” *Communication Research* (21:4), pp. 427–459.
31. Tencent, I. 2011. “Video Spoofing,”.
32. Tilley, P., George, J. F., and Marett, K. 2005. “Gender differences in deception and its detection under varying electronic media conditions,” In *System Sciences, 2005. HICSS’05. Proceedings of the 38th Annual Hawaii International Conference on*, pp. 24b–24b.
33. Vishwanath, A., Herath, T., Chen, R., Wang, J., and Rao, H. R. 2011. “Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model,” *Decision Support Systems* (51:3), pp. 576–586.
34. Wolak, J., Finkelhor, D., and Mitchell, K. 2004. “Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study,” *Journal of Adolescent Health* (35:5), pp. 424. e11–424. e20.
35. Wright, R. T., and Marett, K. 2010. “The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived,” *Journal of Management Information Systems* (27:1), pp. 273–303.
36. Xiao, B., and Benbasat, I. 2011. “Product related deception in E-commerce: A theoretical perspective,” *MIS Quarterly* (35:1), pp. 169–196.

37. Zhou, L., Burgoon, J. K., Twitchell, D. P., Tiantian, Q. I. N., and Nunamaker Jr, J. F. 2004. "A Comparison of Classification Methods for Predicting Deception in Computer-Mediated Communication," *Journal of Management Information Systems* (20:4), pp. 139–165.
38. Zhou, L., Twitchell, D. P., Qin, T., Burgoon, J. K., and Nunamaker Jr, J. F. 2003. "An exploratory study into deception detection in text-based computer-mediated communication," In *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on*, pp. 10–pp.
39. Zhou, L., and Zhang, D. 2007. "Typing or messaging? Modality effect on deception detection in computer-mediated communication," *Decision Support Systems* (44:1), pp. 188–201.