Computers in Human Behavior 72 (2017) 412–421

Contents lists available at ScienceDirect

Computers in Human Behavior

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

Full length article

Individual differences in susceptibility to online influence: A theoretical review

Emma J. Williams [a, *], Amy Beardmore [b], Adam N. Joinson [a]

[a] School of Management, University of Bath, Claverton Down, Bath, BA2 7AY, UK
[b] Faculty of Business and Law, University of the West of England (UWE) - Bristol, Frenchay Campus, Bristol, BS16 1QY, UK

ARTICLE INFO

Article history:
Received 16 April 2016
Received in revised form
27 February 2017
Accepted 1 March 2017
Available online 6 March 2017

Keywords:
Influence
Individual differences
Cyber security
Online scams
Phishing

ABSTRACT

Scams and other malicious attempts to influence people are continuing to proliferate across the globe, aided by the availability of technology that makes it increasingly easy to create communications that appear to come from legitimate sources. The rise in integrated technologies and the connected nature of social communications means that online scams represent a growing issue across society, with scammers successfully persuading people to click on malicious links, make fraudulent payments, or download malicious attachments. However, current understanding of what makes people particularly susceptible to scams in online contexts, and therefore how we can effectively reduce potential vulnerabilities, is relatively poor. So why are online scams so effective? And what makes people particularly susceptible to them? This paper presents a theoretical review of literature relating to individual differences and contextual factors that may impact susceptibility to such forms of malicious influence in online contexts. A holistic approach is then proposed that provides a theoretical foundation for research in this area, focusing on the interaction between the individual, their current context, and the influence message itself, when considering likely response behaviour.

1. Introduction

The rapid expansion of mobile technology and computer-mediated communication in recent years has facilitated greater opportunities for social communication that crosses geographical divides. However, this growth has also increased opportunities for what has been termed 'social engineering' (Anderson, 2008), whereby scammers and other opportunists attempt to influence others to engage in particular behaviours online for financial or other malicious gain. This can range from sending targeted phishing e-mails that encourage recipients to click on links, provide personal information or download malicious software, to engaging in complex online romance scams that persuade targets to transfer large sums of money over a period of time (Atkins & Huang, 2013; Whitty & Buchanan, 2016).

Victims of scams can suffer significant financial and psychological distress (Deem, 2000; Ganzini, McFarland, & Bloom, 1990; OFT, 2006; Pascoe, Owen, Keats, & Gill, 2006; Spalek, 1999; Titus & Gover, 2001), whilst the use of techniques to gain access to corporate information or to disrupt services can have substantial consequences at a wider societal level (The Guardian, 2014; The Washington Post, 2013). In order to counter this threat it is crucial to understand why some people seem to be more susceptible to malevolent influence than others, so that targeted and effective mitigations can be developed. This paper explores the specific influence techniques that are often exploited in such scenarios and the potential impact of a range of individual and contextual factors on susceptibility to these techniques. It then presents an initial model of individual susceptibility that will allow the precise relationship between these factors to be further investigated in the future.

2. Scams in the online environment

The perpetrators of online scams create scenarios in which a target feels sufficiently confident to respond, often using emotionally oriented triggers related to panic, excitement, curiosity or empathy, to encourage errors in judgement and decision making (Langenderfer & Shimp, 2001). Such scenarios can include lottery wins, psychic communicators, the suspension of online accounts and online romance. The growth of the internet has provided a

* Corresponding author.
E-mail address: E.J.Williams@bath.ac.uk (E.J. Williams).

http://dx.doi.org/10.1016/j.chb.2017.03.002

means for scammers to create increasingly elaborate, mass-market approaches, with people who have not traditionally been the target of fraud becoming more accessible despite their geographic distance from the perpetrators location (Button, Nicholls, Kerr, & Owen, 2014).

The relative anonymity provided by online communications means that perpetrators of scams are also able to strategically edit the information that they present, with little chance that their targets will be able to directly verify or challenge this. Such ease of manipulation means that scammers can maximise the likelihood that they will be viewed positively by recipients, and therefore are more likely to be trusted (Walther, 1996). Social media platforms provide extensive opportunities for scammers to identify information regarding individuals' interests, occupation, social networks and geographic location (Hong, 2012), allowing scams to become increasingly personalized and effective (Jagatic, JohnSon, Jakobsson, & Menczer, 2007).

Finally, when people deceive others online, they do not appear to experience the negative emotions associated with face-to-face deception, such as fear or guilt, which has led to the suggestion that differing social norms or ethical judgements govern online interactions (Cromwell, Narvaez, & Gomberg, 2005). This likely contributes to findings that young people who do not appear to be vulnerable offline can become vulnerable in online settings due to increased levels of disclosure and lowered inhibition in online settings (European Online Grooming Project et al., 2012; Suler, 2004).

2.1. Primary mechanisms of online influence

Attempts to influence people online are commonly referred to as 'social engineering' (Atkins & Huang, 2013) and focus on encouraging individuals to perform an unsafe action, such as opening an e-mail attachment containing malware, or persuading people to divulge confidential information, such as user accounts or passwords (Mitnick & Simon, 2006). For example, phishing e-mails contact individuals under the guise of an established and trusted organisation or institution (Greitzer et al., 2014), increasingly featuring logos and website links that appear legitimate (Workman, 2008).

Real world events may be included in the narrative of the message to validate the communication (Freiermuth, 2011) and a number of techniques that exploit social norms and obligations are often present (Button et al., 2014; Cialdini, 2007; Karakasiliotis, Furnell, & Papadaki, 2006; Modic & Lea, 2013; OFT, 2009; Raman, 2008; Rusch, 1999; Stajano & Wilson, 2011) These include the use of *reciprocity* (e.g., providing gifts or favours so that people feel obliged to respond), *conformity* (e.g., referencing the actions and behaviours of peers so that people feel a pressure to conform) or *authority* (e.g., using authority figures that people feel obliged to comply with). Instilling a sense of urgency in respondents is also common, with time-pressured deadlines encouraging people to make decisions quickly rather than systematically considering potential options (Atkins & Huang, 2013; Langenderfer & Shimp, 2001; OFT, 2009). Perpetrators of scams may also evoke feelings of empathy and similarity, which can result in a target believing that they share the same expectations and goals as the person they are interacting with (Cukier, Nesselroth, & Cody, 2007). Specific examples of how such techniques are commonly used in online scams are shown in Table 1.

The Elaboration Likelihood Model (ELM; Petty & Cacioppo, 1986) and the Heuristic-Systematic Model (HSM; Eagly & Chaiken, 1993) both suggest that the effectiveness of persuasive techniques such as those above is likely to depend on the depth of message processing that an individual engages in when a message is encountered. Recent models of phishing susceptibility, such as the Suspicion, Cognition and Automaticity Model (SCAM; Vishwanath, Harrison, & Ng, 2016) and the Integrated Information Processing Model (Vishwanath, Herath, Chen, Wang, & Rao, 2011), highlight the role of individual differences in likely processing depth and the resultant impact on response behaviour. Whether an individual engages in deep, systematic consideration of message content is also likely to be impacted by the design of the message itself (Aditya, 2001; Xiao & Benbasat, 2011).

3. Individual differences: are some people more susceptible?

Research has suggested that a small number of people appear to be at risk of repeat victimisation by fraudsters (Button, Lewis, & Tapley, 2009; OFT, 2009), however, there is a lack of research regarding individual differences in susceptibility to online scams, primarily due to under-reporting, difficulty accessing populations, and little experimental work in this area. Recent research related to phishing emails in particular has suggested that people have a tendency to underestimate their vulnerability to phishing attacks (Halevi, Lewis, & Memon, 2013), with factors such as gender, age, familiarity with the sender, and awareness of phishing risk all being tentatively suggested to impact detection success (Dhamija, Tygar, & Hearst, 2006; Downs, Holbrook, & Cranor, 2006; Jagatic et al., 2007; Jakobsson, Tsow, Shah, Blevis, & Lim, 2007). Vishwanath et al. (2011) argue that both factors related to the phishing message itself and wider individual differences, such as previous experience and beliefs, can impact susceptibility by influencing the information processing strategies that are used. For instance, influence techniques contained within the message, such as urgency cues, can monopolise attentional resources at the expense of other information that may expose the deception, such as the email source or spelling. When individuals demonstrate habitual patterns of e-mail use, this can further increase susceptibility to phishing attempts (Vishwanath, 2015; Vishwanath et al., 2011).

A lack of research regarding individual differences in susceptibility to online scams means that findings from other fields must provide the basis for theoretical development in this area. Research related to consumer behaviour, persuasion and decision making suggest a number of trait and state-induced individual difference factors that may impact susceptibility to malicious influence online. While it is acknowledged that these factors require further investigation in relation to scam responding, they provide an initial framework for discussion and are presented below.

3.1. Self-awareness

Although individuals can be experimentally induced to focus attention on themselves (Duval & Wicklund, 1973), the disposition for self-focused attention is an individual difference factor that has been related to resistance to influence (Fenigstein, Scheier, & Buss, 1975). Individuals high in self-awareness (whether trait or state-induced) have been shown to consider their personal knowledge, internal norms and attitudes to a greater degree when making decisions, leading to increased resistance to social influence and persuasion attempts (Hutton & Baumeister, 1992). However, when individuals perceive themselves as similar to the protagonist within a message, such self-focused attention can also *increase* susceptibility to persuasive charity messages, with individuals showing enhanced resistance only when they consider themselves dissimilar to the message protagonist (Hung & Wyer, 2014).

An awareness of self is a required aspect of self-affirmation, whereby people reflect upon values and attributes that are important to them. In relation to health messages, self-affirmation has been linked with *lower* resistance to threatening health