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
0747-5632/© 2017 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

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

Table 1
Common influence techniques used in online scams.

Influence Technique	Application in Online Scams
Authority	Posing as authority figures or institutions, such as police, banks or senior personnel
Liking	Creating profiles that portray trusted traits or appear friendly
Conformity	Suggesting that other people have benefited from responding
Commitment & Consistency	Requesting a small upfront fee (e.g., advance fee fraud)
Reciprocity	Providing a free gift or favour
Scarcity	Instigating a time-limit in responding
Reward	The promise of rewards, whether monetary or psychological
Loss	Claiming that a failure to respond will lead to a loss of some kind, such as account closure

messages when the threat is considered personally relevant (e.g., smokers who view graphic warnings on cigarette packs; Harris, Mayle, Mabbott, & Napper, 2007). Since Klein and Harris (2009) have shown that individuals who are self-affirmed display an attentional bias toward threat-specific information in such contexts, it may be that self-affirmation prevents the use of denial or other strategies when viewing threatening messages that contradict an individual's current behaviour. This may lead to such individuals actually being more susceptible to online scams that use threat-based influence techniques, such as phishing e-mails focused on the potential suspension of an online account, particularly if they resonate with the individual's current behaviour, such as failing to monitor bank accounts for suspicious transactions.

However, there may be situations in which the wider context makes it difficult for individuals to focus on, or act in relation to, their inherent values and beliefs. Pitesa and Thau (2013) demonstrated that individuals in positions of power within an organisation are able to be more self-focused, more resistant to social influence and thus more likely to act in accordance with their personal preferences than those in less powerful positions, due to decreased dependence on those around them (Guinote, 2007).

3.2. *Self-control*

Resisting influence attempts is a hard task that requires individuals to expend cognitive effort and resources in order to regulate their behaviour (Fransen & Fennis, 2014). A lack of self-control has been associated with compulsive behaviours, such as impulse-buying (Roberts & Manolis, 2012), that are likely to have parallels with susceptibility to scams due to their focus on heuristic processing rather than long-term, systematic evaluation. When people are tired (Welsh, Ellis, Christian, & Mai, 2014), have recently expended cognitive effort by making decisions (Vohs et al., 2008), or lack the motivation or ability to focus on controlling their behaviour, susceptibility to influence is likely to be higher as individuals rely on heuristic, automatic processing mechanisms and social information. A recent study supports the potential relationship between self-control and online influence through the examination of susceptibility to phishing attacks in social media environments. Vishwanath (2015) highlighted that habitual Facebook use, defined as (a) frequent use, (b) maintenance of a large network and (c) deficiency in ability to regulate behaviour, was the single biggest predictor of individual victimisation. However, as suggested by Roberts and Manolis (2012), the lapses in self-control that allow people to fall victim to online scammers are likely to be influenced by a combination of individual motivations (i.e., a desire for money, love or other form of satisfaction) and external stimuli (i.e., a situational opportunity to achieve this, such as a relevant fraudulent communication or relationship interest).

Baumeister (2002) highlighted two main components considered to influence self-control by impacting the degree to which people are able to behave in accordance with their long-term goals – (1) *standards* (an individuals values and ideals) and (2) *monitoring* (awareness and tracking of one's behaviour). This suggests that any relationship between self-control and susceptibility to influence may be mediated by self-awareness. Ego depletion and goal conflicts have also been found to be negatively associated with self-control, such that individuals who do not have clear and consistent goals, are emotionally distressed, or have insufficient mental strength to override impulses are more prone to failures of self-control and susceptibility to influence (Roberts & Manolis, 2012).

3.3. *Self-deception*

The capacity to deceive ourselves and deny information in the surrounding environment has been suggested to provide a self-preservation or self-enhancement function (for review, see von Hippel & Trivers, 2011). For instance, Fein and Spencer (1997) suggest that people derogate others in order to make themselves appear better in their own eyes, whilst eye tracking studies have shown that people orient towards positive information and away from negative information when they are in a bad mood (Isaacowitz, Toner, Goren, & Wilson, 2008). Processes such as retrieval-induced forgetting, whereby continual retrieval of false information from memory can result in individuals consciously ‘forgetting’ that which they know to be true (Price & Phenix, 2015) and replacing it with a new truth based on false or exaggerated information (Arkowitz & Lilienfeld, 2009), may aid the occurrence of self-deception.

Although the link between self-deception and susceptibility to malevolent influence such as scams has not been examined, it is possible that this process is relevant when people who are ordinarily risk-averse take a risk in order to fulfil a current environmental need. For instance, individuals in financial difficulty may respond to a 419 scam, or those who are very ‘emotionally lonely’ may give money to another as part of a ‘romance scam’. In these situations, one means through which people may engage in such behaviour despite potential doubts is via processes of denial and self-deception. To our knowledge, no research has examined this possibility, but such processes could partially explain why people do not discuss their activities with family and friends when they are involved in a potential scam (OFT, 2009).

3.4. *Trust*

The default communicative stance of individuals is generally to trust information in the surrounding environment, with the general population shown to have what has been termed a *truth bias* (Bond & DePaulo, 2006). This truth bias enables people to deal efficiently with the large amounts of information received by the senses every day (Gilbert, 1991). Indeed, if the legitimacy of every piece of incoming information required systematic evaluation, people's limited cognitive resources would quickly be overloaded. When people are more often confronted with honest communications in online settings then they are likely to evaluate future communications in line with these previous occurrences (i.e., as trustworthy). If trustworthy communications are considered to be the “norm”, making a judgement away from this stance will be a cognitively effortful task (Elaad, 2003; Tversky & Kahneman, 1974).

However, there are situations in which people are more aware of the potential for deception, with people becoming more suspicious in situations where deception is considered more likely, such as when judging the messages of salespersons (DePaulo & DePaulo, 1989) or if they operate in environments where deception is more frequently encountered (Garrido, Masip, & Herrero, 2004; Hartwig, Granhag, Strömwall, & Andersson, 2004).

The propensity to trust others has been shown to vary substantially across individuals (Cole, Leets, & Bradac, 2002; Cramer, Brodsky, & DeCoster, 2009; Mayer, Davis, & Schoorman, 1995). In relation to online influence, propensity to trust is likely to vary according to the beliefs that people hold regarding the potential risks of online communications and technology in general (Corritore, Kracher, & Wiedenbeck, 2003; Wang & Emurian, 2005). The perceived anonymity provided by the Internet is likely to contribute to findings that individuals have a tendency to self-disclose more information in online settings compared to face-to-face (Joinson & Paine, 2007) and means that Internet contexts may make people both more susceptible and more vulnerable to influence attempts (Whittle, Hamilton-Giachritsis, Beech, & Collings, 2013).

3.5. Approach to risk

Different individuals have been found to have different propensities for risk (see Mishra, 2014). Although people's approach to risk has been suggested to differ according to the particular situation and domain (i.e., financial vs. recreational) (Ermer, Cosmides, & Tooby, 2008; Weber, Blais, & Betz, 2002), personality traits such as low self-control, sensation seeking and impulsivity have all been associated with risky behaviour across multiple domains (Mishra, 2014). Wider factors have also been shown to influence risk-taking behaviour, such as unpredictable or disruptive social environments (Mishra & Lalumière, 2008; Simpson, Griskevicius, Kuo, Sung, & Collins, 2012) and gender, with men found to engage in more risk-taking behaviour than women (Byrnes, Miller, & Schafer, 1999).

Differences in propensities for risk have been found to relate to the strategies that people use to seek and process risk-related information (Yang, Aloe, & Feeley, 2014). Built upon the sufficiency principle of the HSM (Eagly & Chaiken, 1993) and the subjective norm component of the Theory of Planned Behaviour (TPB; Ajzen, 1991), the Risk Information Seeking and Processing model (RISP; Griffin, Dunwoody, & Neuwirth, 1999) claims that the extent to which an individual systematically seeks and considers risk-related information relates primarily to their psychological need for information sufficiency and informational subjective norms (i.e., social pressures relating to the amount of information that should be acquired when making risk-based decisions).

Engaging in risk-taking behaviour online has been highlighted as a vulnerability factor in relation to susceptibility to online grooming, along with high levels of Internet access and a lack of parental involvement in Internet use (Whittle et al., 2013). The European Online Grooming Project et al. (2012) suggested that victims of online grooming and abuse are likely to be either risk-takers, who are generally confident, outgoing and extraverted, or vulnerable people with low self-esteem and low self-confidence.

3.6. Motivation

Individual differences in motivation are likely to be influenced by both the immediate context that an individual is operating within (i.e., their specific needs, such as a lack of money to pay outstanding bills) and by more stable differences in primary motivators, such as the need for achievement, affiliation or affect (Maio & Esses, 2001; McLelland, 1988). Differences in motivation have been linked to personality characteristics such as conscientiousness, with the characteristic traits of being careful, considered and hard-working also being linked to an achievement-orientation (Barrick & Mount, 1991; Hogan & Holland, 2003). Motivation to engage in complex cognitive activity, shown in the personality trait of need for cognition (Cacioppo & Petty, 1982), has also been linked to a greater resistance to misinformation and decision biases (Carnevale, Inbar, & Lerner, 2011; Hess, Popham, Emery, & Elliott, 2012).

Vishwanath (2015) highlights that the amount of cognitive effort an individual is willing to expend when processing messages may differ according to the degree of attitudinal commitment an individual has to the message sender or subject (Allen & Meyer, 1990). Three components of attitudinal commitment are suggested to influence susceptibility to phishing attacks (Workman, 2008): normative commitment (degree of emotional attachment), affective commitment (extent of fear of loss) and continuance commitment (sense of obligation). Since a number of these factors are likely to be related to susceptibility to various forms of influence, individual differences in motivation may impact susceptibility in a variety of ways according to the particular influence techniques used and scenario that is created. However, the potential role of these factors has yet to be determined.

3.7. Expertise

Individuals have been found to use different information cues when attempting to judge the credibility of a website, potentially due to the degree of expertise they have. For instance, when Dhamija et al. (2006) showed participants a selection of legitimate and fake websites, a quarter of them focused on information within the website itself when judging its credibility (e.g., the presence of logos), whilst neglecting information from other sources, such as the URL. Similarly, Fogg et al. (2002) demonstrated that whilst consumers base their judgements of website credibility on factors such as attractiveness, experts are more influenced by factors related to the content and quality of the information shown.

Such findings suggest that people differ in the extent to which they engage in systematic evaluation when viewing online communications. This can be considered in relation to Sillence, Briggs, Harris, and Fishwick (2006) proposed 3-stage model of website trust, whereby individuals are considered to initially engage in heuristic-based analysis focused on the design and layout of a website (Stage 1), followed by a more systematic analysis of website content (Stage 2) and finally longer-term interaction with, and use of, the site (Stage 3). It is possible that some individuals may jump directly from Stage 1 to Stage 3, leading them to interact with fraudulent sites before their credibility has been systematically evaluated. This jump could be due to a range of factors including distraction, time pressure, misplaced trust, social influence, or overconfidence.

4. The interaction with context

In section 2, a number of influence techniques were discussed that are predominantly designed to influence the extent and type of cognitive processing that an individual engages in when making a decision. By creating a time pressure, or what is perceived to be a time pressure, scammers increase the likelihood that people will use mental shortcuts when making a decision (Stajano & Wilson, 2011). Specifically, this involves exploiting the inherent heuristics and biases that govern what has been termed *System 1* processing (Kahneman, 2011), a rapid and automatic form of information processing that evolved to allow humans to process the vast amounts of information in the surrounding environment quickly and efficiently. When a decision appears complex or a person is overloaded with information, a number of heuristics may be used to make processing more manageable (Muscanell, Guadagno, & Murphy, 2014). In this section, we consider how individuals may be more or less susceptible to these particular heuristics when operating in particular contexts or surroundings.

4.1. Heuristics

If individuals have previous experience of a particular situation, or have been exposed to significant information through the media, their judgements may be biased in relation to a particular outcome (*availability heuristic*; Kahneman, 2011). In relation to online influence attempts, techniques that focus on events that are easily available in memory, either through recent or repeated exposure, may influence an individual's judgement of the likelihood that a message is genuine. For instance, lottery scams have been known to exploit recent media reports of lottery winners so that a lottery win is perceived as more likely, or hackers may repeatedly set-off false alarms in systems so that users ignore genuine alarms, considering them most likely to be continued system malfunction. Alternatively, techniques may focus on activating pre-conceived stereotypes regarding the trustworthiness of a particular individual or message (*representativeness heuristic*; Kahneman, 2011). For instance, online romance scammers may attempt to embody particular characteristics and communication styles that people typically associate with trustworthiness.

Since scams and other online influence attempts are often designed to inspire an emotional response, such as excitement, hope, attachment, desire or even fear, people may base their judgements on emotional responses rather than on systematic consideration of the various risks and benefits (*affect heuristic*). Individuals who are currently experiencing negative emotional states (such as sadness, anxiety or depression) are also more likely to focus on short-term goals related to relieving their distress (Isen & Patrick, 1983), which may make them particularly vulnerable to certain influence attempts.

Confirmation bias and *hindsight bias* have relevance for susceptibility to online scams as they allow the presence of evidence in the environment to be overridden in order to achieve particular goals. Confirmation bias refers to the human tendency to actively search for information that confirms current beliefs and expectations and neglect information that challenges it, whereas hindsight bias refers to the tendency to view previous events as being more predictable than they actually were. If an individual has a strong desire for a person to be trustworthy in order to fulfil a current need, as may occur in online romance scams with individuals who are particularly lonely or strongly desire attachment, then they may be more likely to search for information that confirms this belief and dismiss information that contradicts it. Once individuals have become the victim of a scam, findings of repeat victimisation in the future could also be linked to a hindsight bias, whereby previous scams are dismissed as being different and more predictable than the current proposition. This dismissal of previous experience may represent the reactivation of confirmation bias processes for a second time, with repeat victimisation occurring in a 'confirmation - hindsight bias' cycle.

The influence of cognitive biases and heuristics when making decisions has received substantial support (Kahneman, 2011), impacting a number of the judgements that people make every day. However, of particular concern is the finding that people also show what has been termed *bias blindness*, that is, failing to recognise their own biases and instead claiming that their judgements are relatively objective. This has been shown even when people acknowledge that the judgement strategies that they have used are themselves biased (Hansen, Gerbasi, Todorov, Kruse, & Pronin, 2014). Although such biases can serve a vital function in information processing, they can also lead to inaccurate judgements, errors or seemingly irrational decisions, which people think have been based on objective consideration. Indeed, previous research has suggested an association between susceptibility to phishing attacks and the use of inaccurate heuristics when making decisions (Downs et al., 2006; Hong, 2012).

4.2. Emotions

It is acknowledged that emotions play an important role in the persuasion process (Dillard & Nabi, 2006). However there is still only a limited understanding of why, how, and in what circumstances techniques such as fear appeals are effective (Ruiter, Kessels, Peters, & Kok, 2014). Protection Motivation Theory (PMT; Rogers, 1983) highlights two main processes involved in the processing of fear appeals that have recently been applied to cyber security (Meso, Ding & Xu, 2013) – the extent that any perceived consequences are considered to be a threat (threat appraisal) and the extent that the individual feels able to cope with that threat (coping appraisal). If individuals see a potential response action as something that they are able and willing to do, then they are likely to engage in the recommended behaviour in order to reduce the potential threat (Ruiter et al., 2014). Individuals attempting to influence others take advantage of such approaches by creating a scenario that is interpreted as a threat (such as a security breach on an account) and providing a simple action to reduce this threat (such as clicking a link to verify account details).

The impact of emotions on responding to online scams has largely been neglected, despite the fact that current emotional states may lead individuals to make decisions that are seemingly irrational to an outsider (Mishra, 2014). To achieve more positive emotional states, individuals may be more willing to take risks (e.g., De Vries, Holland, & Witteman, 2008; Fessler, Pillsworth, & Flamson, 2004; Mishra, Morgan, Lalumière, & Williams, 2010), with different emotional states potentially impacting risk-taking to various degrees (Fessler et al., 2004). For instance, fear may heighten threat sensitivity, thereby leading to greater risk aversion (Ohman & Mineka, 2001), whereas anger may result in greater risk-acceptance in order to achieve ones goals (Fessler et al., 2004).

Social isolation, feelings of alienation from peers and emotional loneliness have all been highlighted as risk factors for susceptibility to online grooming, since offenders can exploit the need for attention that accompanies feelings of loneliness (Whittle et al., 2013). This is particularly worrying given that socially vulnerable people may be more likely to use higher-risk communication platforms, such as online chat rooms (Valkenburg & Peter, 2007). When people feel emotionally vulnerable or distressed, they have also been found to have a greater propensity for failures in self-control and a narrower focus of attention (Fredrickson & Branigan, 2005; Tice, Bratslavsky, & Baumeister, 2001).

4.3. Culture

The Needs Opportunities Abilities model (Vlek, 2000) highlights the impact of wider contextual factors such as societal culture, demography and economy on individual decisions and behaviours. It is claimed that such factors influence behaviour by influencing the *abilities* that an individual has and is able to gain, the *opportunities* that are available to them, and their differing *needs* (e.g., wealth, health, attachment).

Culture has been defined as a 'shared system of socially transmitted behaviour that describes, defines, and guides people's way of life, communicated from one generation to the next' (Matsumoto, 2006, p. 220). Differences in propensity to trust across cultures have been primarily considered in relation to the individualism/collectivism component of Hofstede's (2001) model of culture (Jarvenpaa, Tractinsky, & Saarinen, 2000; Weber & Hsee, 1998; Yamagishi & Yamagishi, 1994). Individualistic cultures prioritise independence and the achievement of personal goals whereas collectivist cultures prioritise interdependence, relationships and the needs of the in-group over personal needs. Differences in the trust-building process between these two types of culture have been suggested, with individualistic cultures associated with a more calculative process of trust building based on an evaluation of the costs and benefits to the target (Doney, Cannon, & Mullen, 1998). Individualists are also more likely to seek out previously unknown ‘partners’ according to their reputation, whereas collectivists are more focused on existing relationships in guiding their interactions (Yamagishi & Yamagishi, 1994).

Cross-cultural differences in propensity to trust are particularly relevant when attempting to establish trust between people who are not personally known to each other (termed depersonalized trust), whereby judgements may be based on perceived similarity, group membership and potential connections through mutual acquaintances and existing relationships. Yuki, Maddux, Brewer, and Takemura (2005) explored differences in depersonalized trust between individualist and collectivist cultures and found that Americans were more likely to trust strangers if they shared some form of category group membership, whereas Japanese participants were more likely to trust strangers with whom they shared direct or indirect relationship links.

Finally, traits associated with collectivist cultures have also been associated with a greater tendency to conform to social norms (Iyengar & Lepper, 1999; Kim & Markus, 1999) and to mimic the behaviours of those around them (van Baaren, Maddux, Chartrand, de Bouter, & van Knippenberg, 2003). Given that different influence techniques may differentially exploit links with existing social networks, social norms and in-group category memberships, it is likely that cross-cultural differences in propensity to trust may be reflected in different patterns of susceptibility to online scams.

4.4. Organisation

The norms, habits and values inherent within a workplace are also known to guide behaviour and influence the assumptions that people hold when operating in the workplace (Needle, 2004). If people do not fully understand the potential threats of online communications, or if engaging in secure online behaviour is considered to be difficult, then people may be more vulnerable to engaging in unsecure behaviours, such as clicking on phishing emails (Sasse, Brostoff, & Weirich, 2002; Virginia Tech, 2011), particularly if those around them are considered to engage in similar behaviours.

When people are stressed or under pressure in terms of time or demands (Klein & Calderwood, 1991), overloaded with information (Burke, 2010), heavily focused on a primary task (Mack & Rock, 1998) or are using new, unfamiliar technology, their ability to notice suspicious communications is also likely to be reduced, which may lead to errors in responding (Koumpis et al., 2007). Even if suspicious communications are noticed, individuals may not feel they have sufficient time, resources or means to further investigate these. In such situations, decisions may be made using heuristic processes based on expectations, hindsight and other biases, whereby it becomes normal behaviour to ignore or disregard potential risks. In order to counter such issues, Sasse et al. (2007) highlight the role that system design, organisational behaviour, and security awareness, education and training can have on potential susceptibility to online influence.

5. A holistic theoretical approach

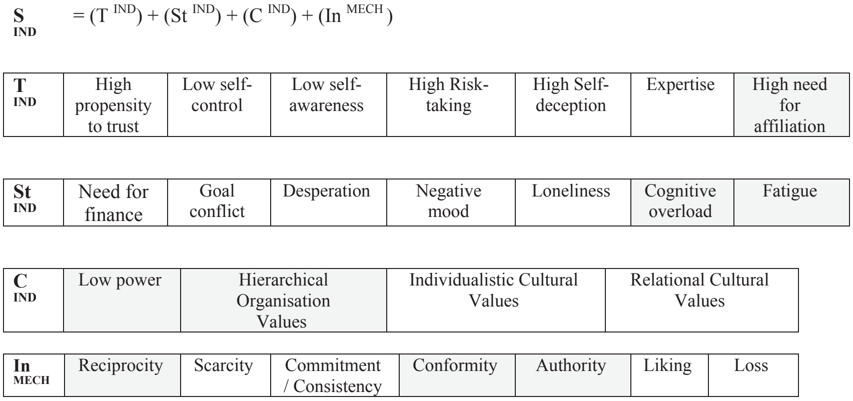
This paper has highlighted a range of individual and contextual factors that may differentially impact susceptibility to various forms of malicious influence employed in online settings. For instance, whilst attempts to extract account details often focus on exploiting time pressure or an essential requirement to complete a work task, lottery or investment scams may target those with a propensity for risk-taking, who are motivated by financial gain, excitement or challenge. Alternatively, being ‘emotionally lonely’ or having a particular desire or other unmet need may lead people to take risks that are counter to their general risk-taking propensity. In such cases, idealism, hope, desperation or a desire to ‘belong’ may lead people to deny doubts through a process of self-deception.

Both Pascoe et al. (2006) and Wright and Marett (2014) have previously proposed frameworks for considering individual differences in susceptibility to phishing or other forms of fraud. However, these are focused on dispositional factors, such as personality, or experiential factors, such as knowledge of security policy, and do not account for the potential impact of context or state-induced factors such as emotional state, cognitive capacity or cultural values. The recently proposed Suspicion, Cognition and Automaticity Model (Vishwanath et al., 2016) attempts to combine concepts related to individual differences in knowledge and cyber risk with those related to habitual and routine behaviours when considering evaluations of phishing e-mails. However, in its present state this does not currently account for how these concepts may interact with influence techniques, or the range of individual factors that may influence susceptibility.

In order to fully understand the potential relationship between individual differences, contextual factors and the influence techniques used that have been identified in this review, a working model of susceptibility to online influence has been developed that provides a foundation for future work. Throughout this paper, influence techniques have been considered to rely on targets engaging in relatively automatic forms of processing, with contextual factors potentially increasing or decreasing susceptibility to influence techniques, whether in combination with, or independently of, individual factors. The extent that individual difference factors may enhance or moderate effects is currently unknown and therefore any potential relationships require exploration. Our intention in formulating this proposed approach is to provide a basis for future experimentation and analysis, in order that a more coherent framework can be developed regarding the interaction between the individual, the context they are operating in, and the influence mechanism used, when considering susceptibility to malicious online influence. Within our model, individual susceptibility to influence (S^{IND}) has been divided into a range of sub-factors that can be grouped according to 4 main levels:

- *The ‘Who’*: Individual traits of the recipient, such as personality and risk-preference (T^{IND});
- *The ‘When’*: The recipients current state, such as their current mood, degree of self-awareness, cognitive pressure, or fatigue (St^{IND});
- *The ‘Where’*: The context an individual is operating in at the time, such as whether they are at home or at work, the communication medium used, and the impact of wider cultural values (C^{IND});
- *The ‘What’*: The influence mechanism that is used, such as invoking compliance with authority, instigating a time pressure or appealing to particular emotions (In^{MECH}).

These factors are conceived as likely to impact individual susceptibility to influence at any given point in time. However, the



$$S_{IND} = (T^{IND}) + (St^{IND}) + (C^{IND}) + (In^{MECH})$$

T_{IND}	High propensity to trust	Low self-control	Low self-awareness	High Risk-taking	High Self-deception	Expertise	High need for affiliation

St_{IND}	Need for finance	Goal conflict	Desperation	Negative mood	Loneliness	Cognitive overload	Fatigue

C_{IND}	Low power	Hierarchical Organisation Values	Individualistic Cultural Values	Relational Cultural Values

In_{MECH}	Reciprocity	Scarcity	Commitment / Consistency	Conformity	Authority	Liking	Loss

Fig. 1. Framework for testing hypotheses based on a holistic individual susceptibility model applied to a workplace phishing attack.

relationship between these factors, and the impact of potential interactions, both across and within each level, is currently unknown. To provide an initial focus for investigation we propose that the presence of vulnerability factors within each level leads to a resultant increase in susceptibility, such that an individual with particular trait vulnerabilities is more susceptible when they are also in a vulnerable context than when they are in a neutral context. Since the influence mechanism is likely to have been designed to exploit particular vulnerabilities at the individual or contextual levels, message factors may then have a greater impact on susceptibility by interacting further with these vulnerabilities. However, alternatively to our proposed hypotheses, it is possible that the presence of additional vulnerability factors does not further increase susceptibility, or that certain combinations of factors have an exponential effect on susceptibility rather than a relatively linear, additive one. The proposed model therefore provides a basis to test these possibilities:

Susceptibility to Influence (S^{IND})= (T^{IND}) + (St^{IND}) + (C^{IND}) + (In^{MECH})

A number of key sub-factors considered to influence susceptibility within each level have been identified and the proposed model can be used and extended to develop and test a range of hypotheses. An example of how these factors may interact using a workplace phishing attack is shown in Fig. 1. For example, an employee with a high need for affiliation may prioritise maintaining harmonious relational ties within the workplace. Scenarios whereby they are fatigued or cognitively overloaded, combined with occupying a position of relatively low power or status within the organisation, may make them particularly susceptible to influence attempts that exploit reciprocity, authority or conformity (see shaded boxes within Fig. 1).

6. Conclusions

In this paper, we have proposed a holistic framework that will allow interactions between individual difference factors, contextual factors, and message factors to be examined and considered in relation to their impact on individual susceptibility to malicious online influence. It is hoped that by further understanding what can make people susceptible to online scams, more effective and targeted mitigations can be developed in the future. We have also highlighted a number of open questions regarding susceptibility to online influence that require further investigation and clarification.

A number of risk factors have been identified that likely increase susceptibility, but the magnitude of the effects of these different factors, and how they interact with other factors, is unknown. For instance, are these factors additive, in that each additional factor leads to a set increase in the degree of susceptibility, or are they multiplicative, in that certain combinations of factors lead to larger effects? If a particular state-induced factor made an individual 3× more susceptible to influence and a particular context factor made an individual 2× more susceptible to influence, would the presence of both of these factors increase susceptibility by 5× or 6×? Or would there be no further increase due to the presence of a relative ceiling of susceptibility?

By understanding the relative contribution of different factors, and combinations of factors, to susceptibility it may be possible to address a second open question emerging from this literature, namely where is the point of intervention that has maximal impact in increasing secure behaviour? A primary aim of research in this field is to enhance online safety for individuals, groups and organisations. Unfortunately current understanding of where best to target future interventions, and the extent to which these factors can be effectively tackled at both the individual and organisational level, is limited and predominantly speculative.

Finally, the relative success of training and education approaches related to online influence would benefit from further exploration in order to understand precisely how and when such techniques work. For instance, do they reduce reliance on heuristic processing, enhance self-awareness and self-control, or increase suspicion? Understanding the mechanisms involved in reducing susceptibility to influence will not only enhance understanding of the processes involved in increasing it, but will also allow particular failures in resistance to be examined, such as how and why suspicious individuals may still succumb to scams.

Acknowledgements

Funding: This work was part funded by the Centre for Research and Evidence on Security Threats (ESRC Award: ES/N009614/1).

References

Aditya, R. M. (2001). The psychology of deception in marketing: A conceptual framework for research and good practice. *Psychology & Marketing, 18*(7), 735–761. http://dx.doi.org/10.5171/2012.712622.

Ajzen, I. (1991). The theory of planned behaviour. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. http://dx.doi.org/10.1016/0749-5978(91)90020-T.

Allen, N. J., & Meyer, J. P. (1990). The measurement and antecedents of affective, continuance and normative commitment to the organization. *Journal of Occupational Psychology, 63*, 1–18. http://dx.doi.org/10.1111/j.2044-8325.1990.tb00506.x.

Anderson, R. (2008). *Security engineering: A guide to building dependable distributed systems* (2nd ed.). Indianapolis, IN: Wiley. ISBN: 978-0-470-06852-6.

Arkowitz, H., & Lilienfeld, S. O. (2009). *Why science tells us not to rely on eyewitness accounts*. Scientific American. Retrieved from http://www.scientificamerican.com/article/do-the-eyes-have-it/. on 15.04.2016.

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences, 1*(03). http://dx.doi.org/10.4236/jss.2013.13004, 23–23.

van Baaren, R. B., Maddux, W. W., Chartrand, T. L., de Bouter, C., & van Knippenberg, A. (2003). It takes two to mimic: Behavioral consequences of self-construals. *Journal of Personality and Social Psychology, 84*(5), 1093–1102. http://dx.doi.org/10.1037/0022-3514.84.5.1093.

Barrick, M. R., & Mount, M. K. (1991). The big five personality dimensions and job performance: A meta-analysis. *Personnel Psychology, 44*, 1–26. http://dx.doi.org/10.1111/j.1744-6570.1991.tb00688.x.

Baumeister, R. F. (2002). Ego depletion and self-control failure: An energy model of the self's executive function. *Self and Identity, 1*(2), 129–136. http://dx.doi.org/10.1080/152988602317319302.

Bond, C. F., & DePaulo, B. M. (2006). Accuracy of deception judgments. *Personality and Social Psychology Review, 10*, 214–234. http://dx.doi.org/10.1207/s15327957pspr1003_2.

Burke, M. (2010). Overcoming challenges of the technological age by teaching information literacy skills. *Community & Junior College Libraries, 16*(4), 247–254. http://dx.doi.org/10.1080/02763915.2010.523327.

Button, M., Lewis, C., & Tapley, J. (2009). *Fraud typologies and the victims of fraud literature review*. National Fraud Authority Report. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118469/fraud-typologies.pdf. on 15.04.2016.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology, 47*(3), 391–408. http://dx.doi.org/10.1177/0004865814521224.

Byrnes, J. P., Miller, D. C., & Schafer, W. D. (1999). Gender differences in risk taking: A meta-analysis. *Psychological Bulletin, 125*, 367–383. http://dx.doi.org/10.1037/0033-2909.125.3.367.

Cacioppo, J. T., & Petty, R. E. (1982). The need for cognition. *Journal of Personality and Social Psychology, 42*, 116–131. http://dx.doi.org/10.1037/0022-3514.42.1.116.

Carnevale, J. J., Inbar, Y., & Lerner, J. S. (2011). Individual differences in need for cognition and decision making competence among leaders. *Personality and Individual Differences, 51*(3), 274–278. http://dx.doi.org/10.3389/fpsyg.2013.00658.

Cialdini, R. (2007). *Influence: The psychology of persuasion*. New York: HarperCollins. ISBN: 978–0061241895.

Cole, T., Leets, L., & Bradac, J. J. (2002). Deceptive message processing: The role of attachment style and verbal intimacy markers in deceptive message judgments. *Communication Studies, 53*, 74–89. http://dx.doi.org/10.1080/10510970209388575.

Corritore, C., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: Concepts, evolving themes, a model. *International Journal of Human Computer Studies, 58*, 737–758. http://dx.doi.org/10.1016/S1071-5819(03)00041-7.

Cramer, R. J., Brodsky, S. L., & DeCoster, J. (2009). Expert witness confidence and juror personality: Their impact on credibility and persuasion in the courtroom. *Journal of the American Academy of Psychiatry and Law, 37*, 63–74. PMID: 19297636.

Cromwell, C. R., Narvaez, D., & Gomberg, A. (2005). Moral psychology and information ethics: The effects of psychological distance on the components of moral behavior in a digital world. In L. A. Freeman, & A. G. Peace (Eds.), *Information ethics: Privacy and intellectual property* (pp. 19–37). Hershey, PA: Idea Group. http://dx.doi.org/10.4018/978-1-59140-491-0.ch002.

Cukier, W. L., Nesselroth, E. J., & Cody, S. (2007). Genre, narrative and the "Nigerian Letter" in electronic mail. In *Proceedings of the 40th annual Hawaii international conference on system sciences* (p. 70).

De Vries, M., Holland, R. W., & Witteman, C. L. (2008). Fitting decisions: Mood and intuitive versus deliberative decision strategies. *Cognition and Emotion, 22*(5), 931–943. http://dx.doi.org/10.1080/02699930701552580.

Deem, D. L. (2000). Notes from the field: Observations in working with the forgotten victims of personal financial crimes. *Journal of Elder Abuse & Neglect, 12*(2), 33–48. http://dx.doi.org/10.1300/J084v12n02_05.

DePaulo, P. J., & DePaulo, B. M. (1989). Can attempted deception by salespersons and customers be detected through nonverbal behavioural cues? *Journal of Applied Social Psychology, 19*, 1552–1577. http://dx.doi.org/10.1111/j.1559-1816.1989.tb01463.x.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 581–590). http://dx.doi.org/10.1145/1124772.1124861.

Dillard, J. P., & Nabi, R. L. (2006). The persuasive influence of emotion in cancer prevention and detection messages. *Journal of Communication, 56*, S123–S139. http://dx.doi.org/10.1111/j.1460-2466.2006.00286.x.

Doney, P. M., Cannon, J. P., & Mullen, M. R. (1998). Understanding the influence of national culture on the development of trust. *Academy of Management Review, 23*(3), 601–620. http://dx.doi.org/10.5465/AMR.1998.926629.

Downs, J., Holbrook, M., & Cranor, L. (2006). Decision strategies and susceptibility to phishing. In *Symposium on Usable Privacy and Security, Pittsburgh, PA*. http://dx.doi.org/10.1145/1143120.1143131.

Duval, T. S., & Wicklund, R. A. (1973). Effects of objective self-awareness on attributions of causality. *Journal of Experimental Social Psychology, 9*, 17–31. http://dx.doi.org/10.1016/0022-1031(73)90059-0.

Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*. Fort Worth, TX: Harcourt. ISBN: 978–0155000971.

Elaad, E. (2003). Effects of feedback on the overestimated capacity to detect lies and the underestimated ability to tell lies. *Applied Cognitive Psychology, 17*, 349–363. http://dx.doi.org/10.1002/acp.871.

Ermer, E., Cosmides, L., & Tooby, J. (2008). Relative status regulates risky decision making about resources in men: Evidence for the co-evolution of motivation and cognition. *Evolution and Human Behavior, 29*, 106–118. http://dx.doi.org/10.1016/j.evolhumbehav.2007.11.002.

European Online Grooming Project, Webster, S., Davidson, J., Bifulco, A., Gottschalk, P., Caretti, V., et al. (2012). *European online grooming project final report*. European Union. Retrieved from http://www.europeanonlinegrooming-project.com/wp-content/file-uploads/European-Online-Grooming-Project-Final-Report.pdf. on 15.04.2016.

Fein, S., & Spencer, S. J. (1997). Prejudice as self-image maintenance: Affirming the self through derogating others. *Journal of Personality and Social Psychology, 73*, 31–44. http://dx.doi.org/10.1037/0022-3514.73.1.31.

Fenigstein, A., Scheier, M. F., & Buss, A. H. (1975). Public and private self-consciousness: Assessment and theory. *Journal of Consulting and Clinical Psychology, 43*, 522–527. http://dx.doi.org/10.1037/h0076760.

Fessler, D. M. T., Pillsworth, E. G., & Flamson, T. J. (2004). Angry men and disgusted women: An evolutionary approach to the influence of emotions on risk taking. *Organizational Behavior and Human Decision Processes, 95*, 107–123. http://dx.doi.org/10.1016/j.obhdp.2004.06.006.

Fogg, B. J., Soohoo, C., Danielson, D., Marable, L., Stanford, T., & Tauber, E. R. (2002). How do users evaluate the credibility of Web sites?. In *Proceedings of the 2003 Conference on Designing for User Experiences* (pp. 1–15). http://dx.doi.org/10.1145/997078.997097.

Fransen, M. L., & Fennis, B. M. (2014). Comparing the impact of explicit and implicit resistance induction strategies on message persuasiveness. *Journal of Communication, 64*(5), 915–934. http://dx.doi.org/10.1111/jcom.12118.

Fredrickson, B. L., & Branigan, C. (2005). Positive emotions broaden the scope of attention and thought-action repertoires. *Cognition and Emotion, 19*(3), 313–332. http://dx.doi.org/10.1080/02699930441000238.

Freiermuth, M. R. (2011). Text, lies and electronic bait: An analysis of email fraud and the decisions of the unsuspecting. *Discourse & Communication, 5*(2), 123–145. http://dx.doi.org/10.1177/1750481310395448.

Ganzini, L., McFarland, B., & Bloom, J. (1990). Victims of fraud: Comparing victims of white collar and violent crime. *Journal of the American Academy of Psychiatry and the Law Online, 18*(1), 55–63. PMID: 2183893.

Garrido, E., Masip, J., & Herrero, C. (2004). Police officers credibility judgements: Accuracy and estimated ability. *International Journal of Psychology, 39*, 254–275. http://dx.doi.org/10.1080/00207590344000411.

Gilbert, D. T. (1991). How mental systems believe. *American Psychologist, 46*, 107–119.

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of unintentional insider threats deriving from social engineering exploits. In *IEEE Security and Privacy Workshops* (pp. 236–250). http://dx.doi.org/10.1109/SPW.2014.39.

Griffin, R. J., Dunwoody, S., & Neuwirth, K. (1999). Proposed model of the relationship of risk information seeking and processing to the development of preventive behaviours. *Environmental Research, 80*(2), S230–S245. http://dx.doi.org/10.1006/enrs.1998.3940.

Guinote, A. (2007). Power affects basic cognition: Increased attentional inhibition and flexibility. *Journal of Experimental Social Psychology, 43*(5), 685–697. http://dx.doi.org/10.1016/j.jesp.2006.06.008.

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. In *Proceedings of the 22nd international conference on World Wide Web companion (WWW)* (pp. 737–744). http://dx.doi.org/10.1145/2487788.2488034.

Hansen, K., Gerbasi, M., Todorov, A., Kruse, E., & Pronin, E. (2014). People claim objectivity after knowingly using biased strategies. *Personality and Social Psychology Bulletin, 40*, 691–699. http://dx.doi.org/10.1177/0146167214523476.

Harris, P. R., Mayle, K., Mabbott, L., & Napper, L. (2007). Self-affirmation reduces smokers' defensiveness to graphic on-pack cigarette warning labels. *Health Psychology, 26*, 437–446. http://dx.doi.org/10.1037/0278-6133.26.4.437.

Hartwig, M., Granhag, P. A., Strömwall, L., & Andersson, L. O. (2004). Suspicious minds: Criminals' ability to detect deception. *Psychology, Crime, & Law, 10*, 83–95. http://dx.doi.org/10.1080/1068316031000095485.

Hess, T. M., Popham, L. E., Emery, L., & Elliott, T. (2012). Mood, motivation and misinformation: Ageing and affective state influences on memory. *Ageing, Neuropsychology & Cognition, 19*(1–2), 13–34. http://dx.doi.org/10.1080/13825585.2011.622740.

von Hippel, W., & Trivers, R. (2011). The evolution and psychology of self-deception. *Behavioural and Brain Sciences, 34*, 1–56. http://dx.doi.org/10.1017/S0140525X10002281.

Hofstede, G. (2001). *Culture's Consequences: Comparing values, behaviors, institutions and organizations across nations*. Thousand Oaks, CA: Sage. ISBN: 9780803973244.

Hogan, J., & Holland, B. (2003). Using theory to evaluate personality and job-performance relations: A socioanalytic perspective. *Journal of Applied Psychology, 88*, 100–112. http://dx.doi.org/10.1037/0021-9010.88.1.100.

Hong, J. (2012). The state of phishing attacks. *Communications of the. ACM, 55*(1), 74–81. http://dx.doi.org/10.1145/2063176.2063197.

Hung, I. W., & Wyer, R. S. (2014). Effects of self-relevant perspective-taking on the impact of persuasive appeals. *Personality and Social Psychology Bulletin, 40*(3), 402–414. http://dx.doi.org/10.1177/0146167213513474.

Hutton, D. G., & Baumeister, R. F. (1992). Self-awareness and attitude change: Seeing oneself on the central route to persuasion. *Personality and Social Psychology Bulletin, 18*, 68–75. http://dx.doi.org/10.1177/0146167292181010.

Isaacowitz, D. M., Toner, K., Goren, D., & Wilson, H. R. (2008). Looking while unhappy: Mood-congruent gaze in young adults, positive gaze in older adults. *Psychological Science, 19*(9), 848–853. http://dx.doi.org/10.1111/j.1467-9280.2008.02167.x.

Isen, A. M., & Patrick, R. (1983). The effect of positive feelings on risk-taking: When the chips are down. *Organizational Behavior and Human Performance, 31*, 194–202. http://dx.doi.org/10.1016/0030-5073(83)90120-4.

Iyengar, S. S., & Lepper, M. R. (1999). Rethinking the value of choice: A cultural perspective on intrinsic motivation. *Journal of Personality and Social Psychology, 76*(3), 349–366. http://dx.doi.org/10.1037/0022-3514.76.3.349.

Jagatic, T., JohnSon, N., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94–100. http://dx.doi.org/10.1145/1290958.1290968.

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., & Lim, Y.-K. (2007). What instills trust? A qualitative study of phishing. *Financial Cryptography & Data Security: Lecture Notes in Computer Science, 4886*, 356–361. http://dx.doi.org/10.1007/978-3-540-77366-5_32.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (2000). Consumer trust in an internet store: A cross-cultural validation. *Information Technology & Management, 1*(1–2), 45–71. http://dx.doi.org/10.1111/j.1083-6101.1999.tb00337.x.

Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the internet. In A. N. Joinson, K. Y. A. McKenna, T. Postmes, & U.-D. Reips (Eds.), *Oxford Handbook of Internet Psychology* (pp. 237–252). Oxford, UK: Oxford University Press. ISBN: 9780199561803.

Kahneman, D. (2011). *Thinking, fast and slow*. London: Penguin. ISBN: 978–0141033570.

Karakasiliotis, A., Furnell, S. M., & Papadaki, M. (2006). Assessing end-user awareness of social engineering and phishing. In *Proceedings of 7th Australian Information Warfare & Security Conference*. Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1011&context=isw. on 15.04.2016.

Kim, H., & Markus, H. R. (1999). Deviance or uniqueness, harmony or conformity? A cultural analysis. *Journal of Personality and Social Psychology, 77*(4), 785–800. http://dx.doi.org/10.1037/0022-3514.77.4.785.

Klein, G. A., & Calderwood, R. (1991). Decision models: Some lessons from the field. *IEEE Transactions on Systems, Man, and Cybernetics, 21*(5), 1018–1026. http://dx.doi.org/10.1109/21.120054.

Klein, W. M., & Harris, P. R. (2009). Self-affirmation enhances attentional bias toward threatening components of a persuasive message. *Psychological Science, 20*, 1463–1467. http://dx.doi.org/10.1111/j.1467-9280.2009.02467.x.

Koumpis, C., Farrell, G., May, A., Mailley, J., Maguire, M., & Sdralia, V. (2007). To err is human, to design-out divine: Reducing human error as a cause of cyber security breaches. In *Human Factors Working Group Complementary White Paper*. Cyber Security Knowledge Transfer Network.

Langenderfer, J., & Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing, 18*(7), 763–783. http://dx.doi.org/10.1002/mar.1029.

Mack, A., & Rock, I. (1998). *Inattentional blindness*. Cambridge, MA: MIT Press. ISBN: 9780262632003.

Maio, G. R., & Esses, V. M. (2001). The need for affect: Individual differences in the motivation to approach or avoid emotions. *Journal of Personality, 69*(4), 583–615. http://dx.doi.org/10.1111/1467-6494.694156.

Matsumoto, D. (2006). Culture and nonverbal behavior. In V. Manusov, & M. L. Patterson (Eds.), *Handbook of nonverbal communication* (pp. 219–236). Thousand Oaks, CA: Sage. ISBN: 978-1412904049.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organisational trust. *Academy of Management Review, 20*(3), 709–734. http://dx.doi.org/10.5465/AMR.1995.9508080335.

McLelland, D. (1988). *Human motivation*. Cambridge, UK: Cambridge University Press. ISBN: 9780521369510.

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security, 9*, 47–67. http://dx.doi.org/10.1080/15536548.2013.10845672.

Mishra, S. (2014). Decision-making under risk: Integrating perspectives from biology, economics, and psychology. *Personality and Social Psychology, 18*(3), 280–307. http://dx.doi.org/10.1177/1088868314530517.

Mishra, S., & Lalumière, M. L. (2008). Risk taking, antisocial behavior, and life histories. In J. Duntley, & T. K. Shackelford (Eds.), *Evolutionary forensic psychology: Darwinian foundations of crime and law* (pp. 176–197). Oxford, UK: Oxford University Press. ISBN: 9780195325188.

Mishra, S., Morgan, M., Lalumière, M. L., & Williams, R. J. (2010). Mood and audience effects on video lottery terminal gambling. *Journal of Gambling Studies, 26*, 373–386. http://dx.doi.org/10.1007/s10899-009-9158-4.

Mitnick, K. D., & Simon, W. L. (2006). *The art of intrusion*. Indiana, US: Wiley. ISBN: 978-0-7645-6959-3.

Modic, D., & Lea, S. E. G. (2013). *Scam compliance and the psychology of persuasion*. Social Science Research Network. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2364464. on 15.04.2016.

Muscanell, N. L., Guadagno, R. E., & Murphy, S. (2014). Weapons of influence misused: A social influence analysis of why people fall prey to internet scams. *Social and Personality Psychology Compass, 8*(7), 388–396. http://dx.doi.org/10.1111/spc3.12115.

Needle, D. (2004). *Business in context: An introduction to business and its environment*. London: Thomson Learning. ISBN: 978–1861529923.

Office of Fair Trading. (2006). *Research on impact of mass marketed scams. A summary of research into the impact of scams on UK consumers*. OFT Report. Retrieved from http://www.icfs.org.uk/~icfs.org.uk/images/pdfs/60.pdf. on 15.04.2016.

Office of Fair Trading. (2009). *The psychology of scams: Provoking and committing errors of judgement*. OFT Report. Retrieved from http://webarchive.nationalarchives.gov.uk/20140402142426/http://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf. on 15.04.2016.

Ohman, A., & Mineka, S. (2001). Fears, phobias, and preparedness: Toward an evolved module of fear and fear learning. *Psychological Review, 108*(3), 483–522. http://dx.doi.org/10.1037//0033-295X.108.3.483.

Pascoe, T., Owen, K., Keats, G., & Gill, M. (2006). *Identity Fraud: What about the victim?* London: CIFAS. Retrieved from https://www.cifas.org.uk/secure/contentPORT/uploads/documents/External-Identity%20Fraud%20-%20What%20About%20the%20Victim%20Research%20Findings.pdf. on 15.04.2016.

Petty, R. E., & Cacioppo, J. T. (1986). *Communication and persuasion: Central and peripheral routes to attitude change*. New York, NY: Springer-Verlag. ISBN: 978–1461293781.

Pitesa, M., & Thau, S. (2013). Compliant sinners, obstinate saints: How power and self-focus determine the effectiveness of social influences in ethical decision making. *Academy of Management Journal, 56*(3), 635–658. http://dx.doi.org/10.5465/amj.2011.0891.

Price, H. L., & Phenix, T. L. (2015). True (but not false) memories are subject to retrieval-induced forgetting in children. *Journal of Experimental Child Psychology, 133*, 1–15. http://dx.doi.org/10.1016/j.jecp.2015.01.009.

Raman, K. (2008, Fall). Ask and you will receive. *Mcafee Security Journal*, 9–12. Retrieved from http://www.wired.com/images_blogs/threatlevel/files/mcafee_security_journal_fall_2008.pdf. on 15.04.2016.

Roberts, J. A., & Manolis, C. (2012). Cooking up a recipe for self-control: The three ingredients of self-control and its impact on impulse buying. *Journal of Marketing Theory and Practice, 20*(2), 173–188. http://dx.doi.org/10.2753/MTP1069-6679200204.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo, & R. Petty (Eds.), *Social Psychophysiology* (pp. 153–177). New York, NY: Guilford Press. ISBN: 978-0898626261.

Ruiter, R. A. C., Kessels, L. T. E., Peters, G. Y., & Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. *International Journal of Psychology, 49*(2), 63–70. http://dx.doi.org/10.1002/ijop.12042.

Rusch, J. J. (1999). *The "social engineering" of internet fraud*. Retrieved from http://www.isoc.org/inet99/proceedings/3g/3g_2.htm. on 15.04.2016.

Sasse, M. A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Fléchais, I., & Kearney, P. (2007). Human vulnerabilities in security systems. In *Human Factors Working Group White Paper*. Cyber Security Knowledge Transfer Network.

Sasse, A. M., Brostoff, S., & Weirich, D. (2002). Transforming the weakest link: A human-computer interaction approach to usable and effective security. In R. Temple, & J. Regnault (Eds.), *Internet and Wireless Security* (pp. 243–258). London, UK: IEE Press. ISBN: 978-0-85296-197-1.

Sillence, E., Briggs, P., Harris, P., & Fishwick, L. A. (2006). Framework for understanding trust factors in web- based health advice. *International Journal of Human-Computer Studies, 64*(8), 697–713. http://dx.doi.org/10.1016/j.ijhcs.2006.02.007.

Simpson, J. A., Griskevicius, V., Kuo, S. I., Sung, S., & Collins, W. A. (2012). Evolution, stress, and sensitive periods: The influence of unpredictability in early versus late childhood on sex and risky behaviour. *Developmental Psychology, 48*(3), 674–686. http://dx.doi.org/10.1037/a0027293.

Spalek, B. (1999). Exploring the impact of financial crime: A study looking into the effects of the maxwell scandal upon the maxwell pensioners. *International Review of Victimology, 6*(3), 213–230. http://dx.doi.org/10.1177/026975809900600304.

Stajano, F., & Wilson, P. (2011). Understanding scam victims: Seven principles for systems security. *Communications of the ACM, 54*(3), 70–75. http://dx.doi.org/10.1145/1897852.1897872.

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior, 7*(3), 321–326. http://dx.doi.org/10.1089/1094931041291295.

The Guardian. (2014). *Sony hack: Sacked employees could be to blame, researchers claim*. Retrieved from http://www.theguardian.com/film/2014/dec/30/sony-hack-researchers-claim-sacked-employees-could-be-to-blame. on 15.04.2016.

The Washington Post. (2013). *Market quavers after fake AP tweet says Obama was hurt in White House explosions*. Retrieved from http://www.washingtonpost.com/business/economy/market-quavers-after-fake-ap-tweet-says-obama-was-hurt-in-white-house-explosions/2013/04/23/d96d2dc6-ac4d-11e2-a8b9-2a63d75b5459_story.html. on 15.04.2016.

Tice, D. M., Bratslavsky, E., & Baumeister, R. F. (2001). Emotional distress regulation takes precedence over impulse control: If you feel bad, do it! *Journal of Personality and Social Psychology, 80*, 53–67. http://dx.doi.org/10.1037//0022-3514.80.1.53.

Titus, R. M., & Gover, A. R. (2001). Personal fraud: The victims and the scams. *Crime Prevention Studies, 12*, 133–152.

Tversky, A., & Kahneman, D. (1974). Judgement under uncertainty: Heuristics and biases. *Science, 185*, 1124–1134. http://dx.doi.org/10.1126/science.185.4157.1124.

Valkenburg, P. M., & Peter, J. (2007). Internet communication and its relation to well-being: Identifying some underlying mechanisms. *Media Psychology, 9*, 43–58. http://dx.doi.org/10.1080/15213260709336802.

Virginia Tech. (2011). *When users resist: How to change management and user resistance to password security*. Pamplin. Retrieved from http://www.magazine.pamplin.vt.edu/fall11/passwordsecurity.html. on 15.04.2016.

Vishwanath, A. (2015). Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication, 20*, 83–98. http://dx.doi.org/10.1111/jcc4.12100.

Vishwanath, A., Harrison, B., & Ng, Y. J. (2016). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, 1–21. http://dx.doi.org/10.1177/0093650215627483. online pre-print.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & 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*, 576–586. http://dx.doi.org/10.1016/j.dss.2011.03.002.

Vlek, C. (2000). Essential psychology for environmental policy making. *International Journal of Psychology, 35*(2), 153–167. http://dx.doi.org/10.1080/002075900399457.

Vohs, K. D., Baumeister, R. F., Schmeichel, B. J., Twenge, J. M., Nelson, N. M., & Tice, D. M. (2008). Making choices impairs subsequent self-control: A limited-resource account of decision making, self-regulation, and active initiative. *Journal of Personality and Social Psychology, 94*(5), 883–898. http://dx.doi.org/10.1037/0022-3514.94.5.883.

Walther, J. B. (1996). Computer-mediated communication: Impersonal, interpersonal, and hyperpersonal interaction. *Communication Research, 23*, 3–43. http://dx.doi.org/10.1177/009365096023001001.

Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behaviour, 21*, 105–125. http://dx.doi.org/10.1016/j.chb.2003.11.008.

Weber, E. U., Blais, A.-R., & Betz, E. (2002). A Domain- specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of Behavioral Decision Making, 15*, 263–290. http://dx.doi.org/10.1002/bdm.414.

Weber, E. U., & Hsee, C. K. (1998). Cross-cultural differences in risk perception, but cross-cultural similarities in attitude towards perceived risk. *Management Science, 44*(9), 1205–1214. http://dx.doi.org/10.1287/mnsc.44.9.1205.

Welsh, D. T., Ellis, A. P. J., Christian, M. S., & Mai, K. M. (2014). Building a self-regulatory model of sleep deprivation and deception: The role of caffeine and social influence. *Journal of Applied Psychology, 99*(6), 1268–1277. http://dx.doi.org/10.1037/a0036202.

Whittle, H. C., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of young people's vulnerabilities to online grooming. *Aggression and Violent Behavior, 18*, 62–70. http://dx.doi.org/10.1016/j.avb.2012.11.008.

Whitty, M., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims. *Criminology & Criminal Justice, 16*(2), 176–194. http://dx.doi.org/10.1177/1748895815603773.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662–674. http://dx.doi.org/10.1002/asi.20779.

Wright, R. T., & Marett, K. (2014). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems, 27*(1), 273–303. http://dx.doi.org/10.2753/MIS0742-1222270111.

Xiao, B., & Benbasat, I. (2011). Product-related deception in e-commerce: A theoretical perspective. *Management Information Systems Quarterly, 35*(1), 169–195. ISSN: 0276-7783.

Yamagishi, T., & Yamagishi, M. (1994). Trust and commitment in the United States and Japan. *Motivation and Emotion, 18*(2), 129–166. http://dx.doi.org/10.1007/BF02249397.

Yang, Z. J., Aloe, A. M., & Feeley, T. H. (2014). Risk information seeking and processing model: A meta-analysis. *Journal of Communication, 64*, 20–41. http://dx.doi.org/10.1111/jcom.12071.

Yuki, M., Maddux, W. W., Brewer, M. B., & Takemura, K. (2005). Cross-cultural differences in relationship- and group-based trust. *Personality and Social Psychology Bulletin, 31*(1), 48–62. http://dx.doi.org/10.1177/0146167204271305.