View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by AIS Electronic Library (AISeL)

Association for Information Systems
AIS Electronic Library (AISeL)

Research Papers | ECIS 2017 Proceedings

Spring 6-10-2017

SAFEGUARDING AGAINST ROMANCE SCAMS – USING PROTECTION MOTIVATION THEORY

Veronica Luu
University of New South Wales, Australia, veronica.luu@unsw.edu.au

Lesley Land
University of New South Wales, Australia, l.land@unsw.edu.au

Wynne Chin
University of Houston, USA, wchin@uh.edu

Follow this and additional works at: http://aisel.aisnet.org/ecis2017_rp

Recommended Citation
Luu, Veronica; Land, Lesley; and Chin, Wynne, (2017). "SAFEGUARDING AGAINST ROMANCE SCAMS – USING PROTECTION MOTIVATION THEORY". In Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal, June 5-10, 2017 (pp. 2429-2444). ISBN 978-989-20-7655-3 Research Papers.
http://aisel.aisnet.org/ecis2017_rp/154

This material is brought to you by the ECIS 2017 Proceedings at AIS Electronic Library (AISeL). It has been accepted for inclusion in Research Papers by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

SAFEGUARDING AGAINST ROMANCE SCAMS – USING PROTECTION MOTIVATION THEORY

Research paper

Luu, Veronica, University of New South Wales, Australia, veronica.luu@unsw.edu.au

Land, Lesley, University of New South Wales, Australia, l.land@unsw.edu.au

Chin, Wynne W., University of Houston, USA, wchin@uh.edu

Abstract

Online dating offers new opportunities for individuals to seek a romantic partner; however, the platform has also been exploited by criminals seeking to perpetrate scams, classified as online dating (romance) fraud. These are arguably one of the most distressing frauds, as victims suffer both financially and emotionally. Thus, this emergent issue has fielded increasing attention from diverse disciplines, though research still remains limited – in particular, investigation of romance fraud from a risk mitigation and information systems (IS) approach has been neglected. This study begins to address these shortfalls by utilising Protection Motivation Theory (PMT) as a framework for understanding the factors and processes underlying intention to use protective tools safeguarding against online dating (OD) scams. The results of Partial Least Squares analysis showed the perceptions and importance of PMT factors differs among protection mechanisms, highlighting the need to better understand and thus enhance the mechanisms based on empirical evidence. Additionally, an online dater's assessment of the protective mechanism (and protective response) generally has a greater influence on adopting protective behaviour, than the evaluation of the scam itself.
Keywords: online dating, romance fraud, Protection Motivation Theory, attitude.

1 Introduction

Humans have long recognised the difficulty in forging romantic relationships, with the involvement of third parties in this endeavour etched in traditions thousands of years old (Coontz, 2005). More contemporary concerns such as time constraints and career aspirations have further increased the difficulty of finding a romantic partner (LaBuda and Kostere, 2012). However, developments in Information Communication Technologies (ICTs) have facilitated the dating process (Lawson and Leck, 2006). A key example being OD services – a relatively inexpensive and practical means to assist individuals in their search for love (Barraket and Henry-Waring, 2008), offering larger pools of potential partners than likely possible in an offline context (Xia et al., 2014; Wiederhold, 2015). The benefits of OD have seen the service proliferate in the last two decades to become a popular and more socially acceptable means of seeking romance (Madden and Lenhart, 2006; Xia et al., 2014).

However, these services aren't limited to those genuinely seeking love, as scammers exploit the platform to perpetrate their crimes on a broader, global scale (Whitty, 2013). The OD platform offers an extension of fraud in the offline world (Cross and Richards, 2015), whilst allowing these scams to be conducted with relative ease, speed, and anonymity (Rege, 2009). Therefore, more people are targeted, on a more frequent basis, with changing – and often innovative – methods of enticing victims (Button, Nicholls, Kerr and Owen, 2014). OD operates from two main platforms – websites and mobile applications. However, we have scoped our study to websites only, as the cost of the fraud is much higher for scams through this medium ($11 million compared to less than $0.5 million (Scamwatch, 2016)).

Notably, OD fraud is distinct from other types of scams due to the 'double hit' victims suffer in not only losing money, yet also what some victims deemed to be the closest relationship in their life

(Whitty and Buchanan, 2012a). Therefore, there is a need to focus on means to better protect users and prevent the financial losses and emotional damage suffered by victims. There exists difficulties in co-ordinating effective and united law enforcement efforts against OD scammers, as they often work within an international criminal network (Whitty and Buchanan, 2012b). In most developed nations, current processes in place to respond to fraud are often disparate and lack co-ordination among the private and public sectors (Smith, 2008). Thus, prevention may be a better tactic than response (e.g. prosecution) for tackling these scams.

Online dating sites themselves offer limited protection. Specialists are employed to review and suspend likely scam profiles (Harrington, 2015); however, such manual checks cannot feasibly investigate all profiles. Where automated detection systems are utilised, they are currently insufficient to protect users (Huang, Stringhini and Yong, 2015). Government bodies, such as the Australian Competition and Consumer Commission, have published best practice guidelines (ACCC, 2015a). However, these guidelines are optional and their effectiveness is untested. Thus, the onus of protection largely lies with the individual when using OD services (Smith, 2005).

Research exploring OD scams is generally limited and restricted to the fields of criminology, psychology, and sociology, which predominantly explore the social engineering involved in the scam (e.g. Rege, 2009; Whitty, 2013; Huang et al., 2015) and the process of fraud (e.g. Whitty and Buchanan, 2012b; Whitty, 2015). However, there is a stark lack of research stemming from the IS discipline. Whitty (2013, p. 682) identifies that it is "important to acknowledge the role of ICTs in creating a close and trusting relationship with the victim". Previous research has also generally adopted a retrospective, rather than a risk mitigation approach. To address this gap, our study seeks to examine the factors and processes leading to the use of *protection mechanisms* – defined here as *tools and techniques used by online daters to safeguard themselves against OD scams*.

The remainder of the paper is organised as follows. Section 2 provides an overview of the current literature on OD scams, as well as the theory relevant for this investigation. Section 3 outlines the research design and model, followed by results and discussion in Section 4, and finally the conclusion in Section 5.

2 Literature Background

Current literature on OD scams relevant to our study examines risk perception and management, the process of romance fraud, as well as characteristics of victims. In addition, we found the PMT to be most suitable for understanding the factors and processes behind protection mechanism adoption. The above areas will be presented in this section.

2.1 Risk Perception and Management

OD inherently entails a number of risks, including the prospect of deceit, the possibility of encountering dangerous and suspect people online, as well as risks of a sexual, emotional, and/or physical nature (Couch, Liamputtong and Pitts, 2012). Such risks are perceived to be a ubiquitous aspect of the online dating experience, though a small proportion of online daters regard using these services as no riskier than other means of meeting people (Couch et al., 2012).

These risks are accepted in the hopes of finding love; consequently, some online daters tend to be proactive, using a range of technology and techniques (e.g. online surveillance) to pragmatically protect themselves against risks (Couch, Liamputtong and Pitts, 2011).

However, these studies examine risk from a broader perspective, in which the 'risk of being scammed' is one of many. No studies have specifically investigated the risk of OD fraud – in terms of its perception by online daters, the techniques used to safeguard against it, and/or how effective these mechanisms are perceived to be.

2.2 Process of Romance Fraud

In first crafting the fake persona, scammers adopt features that are stereotypically attractive, with additional tailoring of personality to match what their victim is seeking (Hickey, 2015). For example, women demonstrate a greater preference for income compared to other traits (Hitsch, Hortaçsu and Ariely, 2010). Therefore, the typical fake male persona will often be a wealthy man with a steady career, in a position of high status. Regardless of gender however, the personas are generally portrayed as vulnerable (Whitty, 2013), carefully designed to elicit empathy and prompt norm activation in the victim (Schwartz, 1977), essentially instilling a sense of obligation to assist their partner.

In almost all situations, the scammer will initiate contact with their target victim (Tracy, 2008). Victims in Whitty's (2013) study all appeared motivated to find the 'right' person, and described the profile of the scammer's persona as depicting such an ideal. In the burgeoning stages of the relationship – generally very early on – the perpetrator declares their love for the victim, and their desire to commit to an exclusive relationship. The scammer will often suggest they move their communication to other modes, such as email or instant messaging (Whitty and Buchanan, 2012b), which are often unmoderated (Pan, Winchester, Land and Watters, 2010).

The grooming stage is the hallmark of OD scams (ACCC, 2015b), where the aim of the criminal is to create an "intense intimate connection" (Garrett and Taylor, 2014, p. 10), priming the victim to comply with demands for finances (Whitty, 2015). This phase generally lasts 6-8 months (Rege, 2009), though can take up to a year (Whitty, 2015). Communication is regular, frequent, and flattering – poetic emails are used to charm the victim, whilst regular instant messages are used to embed the relationship into the victim's daily life (Whitty, 2013). In particular, communicating via ICTs leaves a digital record which the individual can revisit as they wish, reinforcing the notion that the target individual is special, loved, and appreciated (Koon and Yoong, 2013). Thus, ICTs play a key role in strengthening the bond, making it more difficult for the victim to distance themselves from the relationship, with victims describing being fully immersed, and swept up in the process (Whitty, 2013).

The "continuous and progressive exchange of self-disclosure" (Koon and Yoong, 2013, p. 31) occurring in this stage fosters trust and intimacy in the online relationship (McKenna, Green and Gleason, 2002), which is when the scammer begins requesting finances via pretence of a crisis situation, such as a medical emergency (Whitty, 2013). This gives the victim little time to consider the situation beyond their initial instinct, and if the victim fails to acquiesce, the scammers may then threaten the victim with the cessation of the relationship (Whitty, 2013).

The scam continues for however long the victim continues to send funds to the criminal, and ends when the victim is aware they have been scammed and no longer provides money (Garrett and Taylor, 2014). Upon learning they have been a victim of fraud, individuals generally find it highly difficult to relinquish the relationship, with those in denial particularly vulnerable to being scammed again (Whitty, 2015).

While this deep understanding of the process of fraud is useful, it ignores the role that technology plays in terms of risk mitigation. Given that technology is a key enabler of this fraud, it is surprising that IS researchers have not investigated how technology may be able to assist in preventing the scam from progressing, or commencing in the first place.

2.3 Characteristics of Victims

The literature and practitioners have reported a number of interesting (and sometimes conflicting) characteristics of OD victims; these are summarised in Table 1.

Victim Characteristics	Findings from Literature
Age range	The 55-64 age group were over-represented in terms of financial loss, accounting for close to 40% of total money lost to fraud, in contrast to representing only 20%

	of reports made (Scamwatch, 2016)
Gender and impact	Men and women are targeted roughly equally, though women lost more money and were also more emotionally affected than men by the scam (Whitty and Buchanan, 2012b)
Vulnerabilities (past relationships, health, risk taking, self-perceptions, emotions)	• Some female victims were previously in abusive relationships, and some male victims experienced mental health issues (e.g. social anxiety disorder and depression) (Whitty and Buchanan, 2012b) • Risk takers, believers of fate and destiny (Dudley and Shadel, 2015) • High in 'romantic beliefs', high motivation to fall in love (Whitty and Buchanan, 2012b) • Sensitive, and less emotionally intelligent (Tatera, 2016)
Background (occupation, education, and income)	• Range of backgrounds (e.g. professionals, university professors, lawyers) (Scamwatch, 2011; Koon and Yoong, 2013) • Educated (university degrees), and middle to high income earners (Hitsch et al., 2010; Young, 2015)
Fraud Knowledge	Varied, ranging from no knowledge, to being fairly familiar with a number of scam types (Cross and Richards, 2015). However, knowledge of scams did not prevent financial scams; rather Whitty (2013) argues that the more skilful the scammer is at grooming the victim, the more likely the victim will be defrauded.

Table 1. Characteristics of victims

As the Internet becomes increasingly accessible to people of different demographics, and with modern lives potentially making finding partners more difficult, people will continue to use OD platforms to seek romance. As with many technology misuses, scammers also become more persistent and innovative in their tactics, and consequently, we would also expect users of different demographics to be increasingly exposed to OD scams. Undoubtedly, more needs to be done to protect online daters.

2.4 Protection Motivation Theory

In this section, we describe the PMT which is useful for predicting users' behaviour based on their threat and coping appraisals. We summarise the original model and its use in both IS and non-IS fields.

PMT was initially utilised primarily in health and social psychology research (Lee, 2011), though its application has extended beyond this realm to be applied to various disciplines (Milne, Sheeran and Orbell, 2000). In the IS field, the theory's constructs have provided valuable explanatory power in predicting protective security behaviours (e.g. Herath and Rao, 2009; Lee and Larsen, 2009; Anderson and Agarwal, 2010; Johnston and Warkentin, 2010; Liang and Xue, 2010). Johnston and Warkentin (2010, p. 561) believes PMT's "impact within the realm of IS research, particularly information security, is promising". However, the application of PMT in IS is highly limited beyond the security realm. To the best of our knowledge, no other similar predictive or explanatory models have been applied in the domain of OD scams.

PMT was developed by Rogers (1975, 1983) and is a framework examining how an individual's assessment of the threat and coping mechanism influences their intentions and actions to adopt these protective measures (Paravastu and Anandarajan, 2015). PMT is divided into the threat appraisal and coping appraisal, which assist with understanding the manner in which individuals perceive a threat, and consequently 'cope' with it (Hanus and Wu, 2016). Protection motivation elicited is a function of these two appraisals, and is often operationalised as behavioural intention (Rogers, 1983).

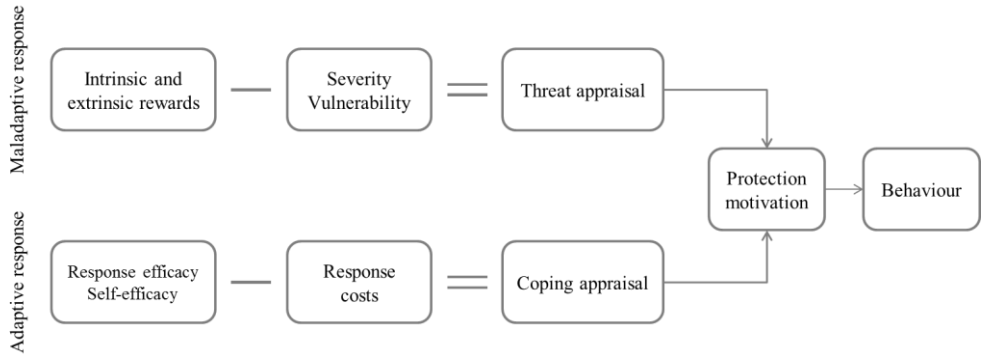

Figure 1. Protection Motivation Theory (Rogers 1983)

The threat appraisal is associated with the maladaptive response, i.e. the undesired response, as the level of fear is decreased, though not the threat itself. As can be seen in Figure 1, the perceived severity (PS) of the threat and perceived vulnerability to personally experiencing the threat (PV) reduce the likelihood of the maladaptive response, whereas extrinsic and intrinsic rewards (e.g. social approval) increase this probability (Rogers, 1983). These are regarded as the sub-constructs of threat appraisal.

The coping appraisal is the process by which the individual assesses their ability to cope with, and mitigate the threat (Rogers, 1983), in terms of the effectiveness of the mechanism (response efficacy, RE), their perceived capability of performing the behaviour (self-efficacy, SE), and an estimation of the costs involved (response cost, RC), such as finances and time (Floyd, Prentice-Dunn and Rogers, 2000). This evaluation influences the adaptive response, i.e. the desired response which assists to reduce the threat (Boss et al., 2015). The sub-constructs RE and SE increase the likelihood of the adaptive response, whereas RC decreases the probability (Figure 1).

PMT provides a valuable framework through which to investigate this area– examining how an individual assesses the threat and the coping mechanism, and how this then influences their intention to engage in protective behaviour. The research questions derived from this objective are:

RQ1: *How do threat appraisals impact users' intention to adopt protection mechanisms when using OD websites?*
RQ2: *How do coping appraisals impact users' intention to adopt protection mechanisms when using OD websites?*

In particular, any difference between mechanisms will be examined.

3 Research Design and Model

In this section, we will describe the design of our research to address the two research questions stated in the previous section, and then explain the research model we developed to conduct our study.

The research design involves two phases. Firstly, we identified the protection mechanisms available to online daters. Since there is no prior categorisation system of OD users' protection mechanisms, web content analysis was performed on the most popular OD websites as identified by Choice (Sheftalovich, 2014). The first author navigated through each identified dating website to search for protection mechanisms and features. These were listed and functionally described in an Excel spreadsheet and then they were further grouped according to similarities in overall functionality. A few iterations of grouping were performed with co-authors to ensure agreement on the final classification scheme. Table 2 shows the categories and the descriptions identified. In this initial study, we decided to focus on two categories only – informational and reporting - which were more common to OD sites.

Category	Example(s)	Description
Informational	Guidelines, FAQs, tips	Content with the aim of providing OD users with information on how to date safely
Reporting	Flag, block, report	OD website features which allow users to flag suspicious members, or to prevent communication from a particular member
External Check	Private investigator, DateSmart.Com	Users pay an external entity to check the background of a given profile
Do-it-yourself (DIY) Check	Searches on Google, TinEye, or social media	Members use their own IT skills to perform background checks on another OD member

Table 2. Categories of protection mechanisms on online dating websites

Secondly, we developed the research model shown in Figure 2, using PMT as the baseline with a few changes summarised below:

1. We added a number of constructs – awareness, attitude, and behavioural expectation - to the basic PMT model, in order to capture as much predictive power as possible (described below).
2. We developed new constructs to capture the overall coping and threat appraisal constructs as specified in Rogers' (1983) update of the original PMT model. To our knowledge, these overall appraisals have not been used in IS studies using PMT. We include them to test their importance in potentially explaining the overall impact of threat/coping appraisals leading to adoption intention.

Awareness plays an important role, serving as a source of information for individuals' appraisal processes (Milne et al., 2000). The importance of IT security awareness has been widely emphasised both from an organisation (Whitman and Mattord, 2010) and an individual (Kritzinger and von Solms, 2010) perspective. Awareness is distinguished in terms of awareness of the protection mechanism itself, and awareness of the threat (i.e. OD scams).

The attitude construct refers to "an individual's positive or negative feeling (evaluative affect) about performing the target behaviour" (Fishbein and Ajzen, 1975, p. 216). Studies exploring IT adoption have neglected the role attitude plays in explaining technology acceptance behaviour; however, as identified by Kim and colleagues (2009), there is considerable support in the social psychology realm suggesting the critical influence of attitude on behaviour, and information processing.

The concepts of behavioural intention (BI) and behavioural expectation (BE) have often been used interchangeably, though are distinct concepts (Warshaw and Davis, 1985b). BI refers to the development of conscious plans to perform a specified future behaviour; on the other hand, BE refers to their perception of the likelihood they actually will act upon this behaviour (Warshaw and Davis, 1985b, p. 4). In essence, BE is a broader construct which is often believed to be superior to BI in predicting the performance of behaviour (Warshaw and Davis, 1985a). (For definitions of the various constructs, please refer to Appendix A – Construct Definitions.)

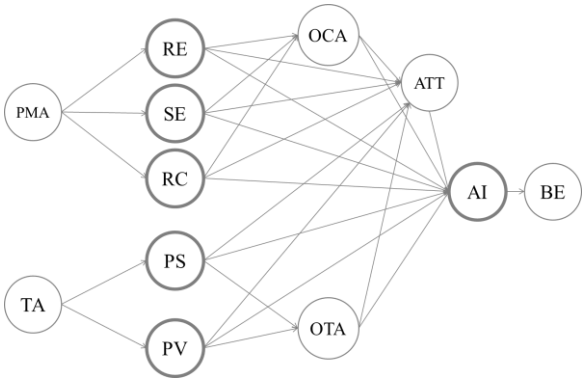

Figure 2. Research model

(*Bolded circles indicate base PMT constructs*; *PMA = protection mechanism awareness, TA = threat awareness, RE = response efficacy, SE = self-efficacy, RC = response cost, OCA = overall coping appraisal, TA = threat awareness, PS = perceived severity, PV = perceived vulnerability, OTA = overall threat appraisal, ATT = attitude, AI = adoption intention, BE = behavioural expectation)*

The research model presented in Figure 2 utilises the core nomology of PMT as defined by Boss and colleagues (2015). This was deemed more appropriate as incorporating fear (including fear appeals) and maladaptive rewards may introduce potential issues associated with their measurement, potentially altering participant reactions in a manner that would not occur outside of the study, and/or sensitising participants to the risk. Therefore, "the core model might provide a safer, more realistic setting for a study in the IS field", though ideally both versions would be investigated (Boss et al., 2015, p. 842).

Hypotheses are not explicitly stated, though all paths are expected to be positive relationships, aside from paths involving RC, which are expected to be negative. Each path modelled was based on the literature, and tested as part of the analysis.

3.1 Survey Instrument Development

A survey, utilising online questionnaires was then developed to investigate the impact of individuals' perceptions of threat and protection mechanisms on their intention to adopt protective measures. Questions were based on the research model, and consistent for the two mechanisms.

For the basic PMT constructs, measurement items were adapted from the studies conducted by Lee and Larsen (2009), Anderson and Agarwal (2010), Crossler (2010), Liang and Xue (2010), Herath and colleagues (2014), Zahedi and colleagues (2015), and Hanus and Wu (2016). Some measurement items were self-developed based on their theoretical definition. Using Boss and colleagues' summary (2015), there are no PMT studies which incorporate the overall appraisal processes within IS. As such, measurement items for these constructs were developed based on their definition, as synthesised from the literature. Three questions were developed and measured on a semantic differential scale.

Awareness of threats and countermeasures was based on those constructed by Zahedi and colleagues (2015), as well as the theoretical definition of awareness as defined by Hanus and Wu (2016). Attitude questions were developed based on those utilised in the study conducted by Yang and Yoo (2004). Five questions were devised and measured on a semantic differential scale. The measurement items for behavioural expectation were derived from Venkatesh and colleagues' study (2008).

Questions were generally measured on a 7-point Likert scale (1 = "Strongly Disagree" to 7 = "Strongly Agree"). The survey was created on Qualtrics and distributed on Amazon Mechanical Turk, which is used to obtain reliable data for social sciences inexpensively and rapidly (Buhrmester, Kwang and Gosling, 2011).

4 Results and Discussion

We used PLS Graph version 3.00 for analysing the data. Partial Least Squares (PLS) places low demands on sample size and measurement scales (Wold, 1985), and is suitable for exploring phenomena which may be relatively new or changing (Chin, 1998). While the underlying PLS algorithm estimates PLS components scores for each construct in our model, we consider all constructs as modelled at the first order level where each block of items are designed to reflect the same underlying construct. The measurement model was first evaluated (in terms of indicator reliability, composite reliability, convergent validity and discriminant validity), followed by the structural model (in terms of path estimates, and the model's explanatory power, R-squared).

A pilot study of 33 data points was first conducted to assess the quality of the measurement items and survey instrument. A number of measurement items were found to have a loading below the 0.70 threshold and cross-loading issues, which were subsequently modified for the main study.

The main study had a sample size of 399 respondents which allowed for statistical power above 0.80. All measurement items met the 0.70 threshold for loadings, aside from four, which fell between 0.40 – 0.70, which is considered acceptable for exploratory research (Bagozzi and Yi, 1988). The composite reliability (CR) of each construct was above the 0.70 threshold. In terms of convergent validity, for all constructs, the average variance extracted (AVE) was above 0.50 as required. Discriminant validity was assessed in terms of the Fornell-Larcker criterion and cross loadings. To meet the Fornell-Larcker criterion (Fornell and Larcker, 1981), the AVE of each construct should be greater than its squared correlation with any other construct, which was true of each construct. For the cross loadings, each item should load highest on its respective construct, which was the case for all measurement items. Therefore, discriminant validity can be ascertained (i.e., each construct is more closely related to its own measures than it is to other constructs).

The R-squared for the informational and reporting models were 45% and 41% (rounded down) respectively. As such, the model holds greater predictive power when attempting to assess an individual's intention to adopt informational mechanisms, in comparison to reporting mechanisms. The path coefficient estimates for the individual mechanism models are presented in Table 3.

Paths	Informational	Reporting
RE→AI	0.242***	0.161***
SE→AI	0.095*	0.174***
RC→AI	-0.083*	N.S
PS→AI	N.S	0.101*
PV→AI	0.177***	0.134**
RE→OCA	0.309***	0.292***
SE→OCA	0.189***	0.203***
RC→OCA	-0.105*	-0.082*
PS→OTA	0.484***	0.483***
PV→OTA	0.224***	0.225***
PMA→RE	0.363***	0.307***
PMA→SE	0.561***	0.638***
PMA→RC	-0.174***	-0.284***
TA→PS	0.401***	0.401***
TA→PV	N.S	N.S
RE→ATT	0.135***	0.092*
SE→ATT	0.079	0.18***
RC→ATT	-0.111***	-0.088**
PS→ATT	0.174***	0.129**
PV→ATT	N.S	N.S
OCA→ATT	0.462***	0.456***
OTA→ATT	N.S	0.099*
OCA→AI	N.S	N.S
OTA→AI	N.S	N.S
ATT→AI	0.386***	0.392***
AI→BE	0.676***	0.697***

*Table 3. Path coefficients (*** p < 0.005, ** p < 0.01, * p < 0.05, N.S = not significant*)

Tests for mediation were also conducted. The path coefficients (direct, indirect, and total) were calculated utilising the percentile bootstrap method outlined by Chin (2010, p. 678). The following tests were conducted: 1) attitude mediating the impact of sub-constructs on adoption intention, 2) overall coping appraisals mediating the impact of sub-constructs on adoption intention, and 3) coping appraisals mediating the impact of sub-constructs on attitude. Attitude was found to be a significant mediating variable, though the overall appraisals only mediated the relationship from sub-construct to attitude, not to adoption intention. The results per mechanism will be discussed, followed by overall findings.

In determining whether or not to adopt informational mechanisms, online daters particularly take into consideration the value of the information provided (in terms of its effectiveness in safeguarding against OD fraud), as well as how personally vulnerable they are to being scammed. Their belief in their ability to understand and utilise the information, as well as the time and effort involved are also factored into their adoption intention. Of note, these effects (of response efficacy, self-efficacy, and response cost) are partially mediated by their attitude towards using protection mechanisms, which itself is the single most important factor in determining an individual's intention to use informational mechanisms. The perceived severity of an OD scam, and the individual's overall assessment of coping with the threat, increases their intention to use informational mechanisms, though only through their sentiment towards using protection mechanisms.

The time and effort required to report another OD member does not factor into the likelihood of an online dater utilising such features. This is likely due to the ease of reporting a user (which often requires simply clicking a button). Instead, their belief in the effectiveness of the reporting tool, and their ability to use reporting features, factor strongly into their adoption intention. Additionally, the more a user believes they are vulnerable to an OD scam, they more inclined they are to use reporting tools. The overall coping and threat appraisals only influence adoption intention through their influence on attitude, with the greater impact stemming from the coping appraisal.

Results for threat awareness were consistent with those of Hanus and Wu's (2016) study on desktop security behaviour. Though threat awareness had a significant impact on how damaging an online dater perceived a scam to be, the results showed that this awareness had no influence on an online dater's assessment of their own vulnerability. It is possible that knowledge of scams leads online daters to recognise that romance fraud does occur, yet they neglect to consider themselves as a potential victim – likely an underestimation of their own vulnerability – a finding which is corroborated by Couch and colleagues' (2012) study on online daters' perceptions of risk. This plausible cognition may signify optimism bias, in which individuals have a tendency to underestimate the probability of negative events affecting them, whilst overestimating the probability of positive events (Sharot, 2011).

Overall, protection mechanism awareness had the strongest influence on self-efficacy. This suggests that the more knowledgeable about protection mechanisms an online dater is, the more they believe they are capable of using it. Awareness of protective tools was also associated with an increased perception of the effectiveness of the mechanism. These findings are akin to those of Hanus and Wu (2016) in their study of desktop security behaviour.

In terms of threat appraisal (RQ1), PV had a direct impact on adoption intention, whereas the impact of PS on adoption intention stemmed from either direct path impact, or through the mediator variable of attitude. PS was either partially or fully mediated by attitude. These results suggest that understanding the harm caused by OD scams helps to motivate the use of these protection mechanisms, as it helps to form a positive attitude towards the use of these protective behaviours.

Overall, the coping appraisal (RQ2) – both in terms of the overall appraisal and the sub-constructs – had a greater impact on adoption intention than the threat appraisal. This finding is consistent with the conclusions drawn by two separate meta-analyses conducted on PMT (Floyd et al., 2000; Milne et al., 2000). Additionally, RE and SE had greater impact on the overall coping appraisal, attitude, and adoption intention than did RC, which was often insignificant. This suggests that greater attention must be paid to improving protection mechanisms, in order to better encourage online daters' protective behaviour. RE was often one of the top most influential variables on its dependent constructs (i.e. OCA,

ATT, and AI), which is consistent with the results of studies using PMT in IS (e.g. Herath and Rao, 2009; Liang and Xue, 2010; Sun, Wang, Guo and Peng, 2013; Johnston, Warkentin and Siponen, 2015; Zahedi, Abbasi and Chen, 2015). Thus, this provides further support for the importance of the perceived effectiveness of the coping response in PMT.

5 Conclusion

This study presents a number of theoretical contributions, both to PMT and to the dearth of research investigating the domain of OD scams. Our study demonstrated that PMT may be enhanced with the inclusion of attitude – a factor which encompasses general feelings and sentiment, distinct from the cognitive thought processes of PMT – and overall coping appraisals. The addition of the attitude construct significantly improved the predictive power of the model, and – in its role/capacity as a mediating variable – helps to elucidate and more precisely explain the process leading to adoption intention. These findings highlight the importance of an individual's sentiment towards using protection mechanisms, as it mediates the influence of both the threat and coping sub-constructs, as well as the overall appraisals on adoption intention.

To the best of our knowledge, no studies utilising PMT have incorporated the overall appraisals. Some studies have included one appraisal – generally the threat appraisal (e.g. Liang and Xue, 2010) – though the majority do not model either of the overall appraisals as specified in Rogers' (1983) updated version of PMT. The inclusion of the overall coping and threat appraisals in the research model may not influence adoption intention directly; however, these appraisals play a valuable role in mediating the path from sub-constructs to attitude, suggesting that individuals integrate their disparate assessments of the various aspects of the threat and coping mechanism, to form an overall evaluation each of the threat and coping mechanism. These higher level appraisals then influence their general feeling towards protection mechanisms. By conducting a more comprehensive examination of the relationships in the research model, the value of the overall appraisals to the PMT model is realised.

This study also contributes to existing literature in proposing a preliminary high-level classification framework of protection mechanisms available to OD users. Previous research identified 'risk management techniques', though these studies examined a broader scope of risks in OD, in which the 'risk of being scammed' was one of many (e.g. Andrejevic, 2002; Couch et al., 2011, 2012). Relevant mechanisms from these studies, in addition to those identified from web content analysis, led to the categorisation of protection mechanisms specific to OD scams. We have only reported on the use of informational and reporting mechanisms in this paper. Future studies can use the full taxonomy for examining the protective behaviour of online daters.

The study also offers a number of implications for the OD industry and the government. Greater understanding around the factors and processes leading to the use of various protection mechanisms can enhance the design of existing mechanisms, inform the design of new mechanisms, and provide an empirical basis for government and/or industry initiatives to combat romance fraud. A summary of some example practical implications is provided in Table 4 below.

Path	Implication
General	
TA→PV	Frame content about scams to place the individual in the position of a victim in order to break down the invulnerability barrier (Witte, Cameron, McKeon and Berkowitz, 1996) and perception that they are invulnerable to being scammed; this is particularly important as PV has a direct impact on adoption intention.
ATT→AI	As attitudes impact adoption intention considerably, and play an important role as mediator, it is important to ensure attitudes towards using protection mechanisms are positive. This could include the publication of success stories of how people were able to avoid losing money or being scammed through the use of protection mechanisms.

Informational mechanisms	
RC→AI	Content should be easy to find (Whitty and Buchanan, 2012b) and presented in a manner which reduces the effort required to understand and digest it. For example, guidelines should be clear and concise; otherwise this may dissuade users from viewing the information.
PV→AI	Information should position the online dater in the narrative (rather than simply as a third party observer), as it is important to break past a sense of invulnerability to ensure they recognise that they aren't "immune to fraud when using online dating" (Cross, 2014, para 29).
Reporting mechanisms	
RE→AI	Implement proper investigative procedures and establish the required transparency to build trust in the effectiveness of the tool; for example, clarifying the process of how the report is followed up, and providing information about whether any actions are taken as a result of a report.
SE→AI	Ensure the tools are easy to locate, and if a form must be completed, this should be relatively simple to answer in order to promote users' perceived ability to use reporting features. Standardisation across sites in regards to the location of the feature would also assist to lower the perceived ability required to use the tool (particularly for those users who may use more than one site, or change the service they use). This is of particular importance as ease of use is an important consideration for potential adopters of a tool (Karahanna, Straub and Chervany, 1999).

Table 4. Practical implication recommendations

Research limitations of the study pertain to the external validity of the results, and the proxy measure of intention. As the questionnaire was disseminated via Amazon Mechanical Turk (AMT), only online daters using the service were able to respond to the survey. Since AMT users cannot be taken to be a representative sample of the population of OD users, the results may not be completely generalisable to the entire OD population. Additionally, in terms of the usage of the various protection mechanisms, our study measured behavioural intention and expectation, and not actual behaviour. Therefore, we cannot ascertain actual adoption of the mechanisms. It should be noted, however, that measuring behaviour in a cyber-security context is difficult (Vroom and von Solms, 2004), particularly given the private nature of OD. Additionally, it has been demonstrated that 'adoption intention' can be useful in predicting actual behaviour, if 1) the behaviour, situation, and object are measured at the same level of specificity, 2) the measure of intention reflects intention at the point in time in which behaviour is measured, and 3) the behaviour is under the volitional control of the individual (Fishbein and Ajzen, 1975). As our measurement items meet these requirements, our results should be valid.

The current study aims to address the issue of OD fraud from an empirical, risk mitigation approach. Utilising PMT as a base framework, we examined the factors and processes leading to adoption intention of protection mechanisms in the OD domain. Our findings show that the coping appraisal process generally has a greater impact on adoption intention than the evaluation of the threat. Attitude was a considerable influencer of adoption intention, and functioned as a mediator, whilst the overall appraisals also played a mediating role in the model, further helping to explicate the process leading to the adoption of protective tools. These results lead to a number of key practical implications for the government and industry to enhance the design of protection mechanisms, and encourage online daters to utilise safeguarding measures against romance fraud. Our study is the first to utilise PMT to investigate OD scams, and one of the first to examine the issue with prevention and mitigation in mind, rather than retrospection. This work will hopefully be built upon by further research in this relatively new and critical area.

Appendix

Appendix A – Construct Definitions

Construct	Definition
Protection mechanism awareness (PMA)	User awareness of protection mechanisms that may assist to prevent or mitigate the threat of OD scams (Hanus and Wu, 2016)

Threat awareness (TA)	User awareness of OD scams (Hanus and Wu, 2016)
Coping appraisal (OCA)	An individual's assessment of his or her ability to use a protection mechanism, and his/her confidence that the protection mechanism will be successful in mitigating or preventing the potential loss or damage resulting from an OD scam, whilst also taking into consideration finances, time, effort, and other costs involved (Crossler, 2010)
Response efficacy (RE)	An individual's confidence that a recommended protection mechanism will effectively prevent or mitigate an OD scam (Witte et al., 1996; Crossler, 2010)
Self-efficacy (SE)	An individual's confidence in his/her ability to use the recommended protection mechanism to prevent or mitigate OD scams (Witte et al., 1996; Crossler, 2010)
Response cost (RC)	The opportunity cost (e.g. time, effort, money) of using the protection mechanism to prevent or mitigate OD scams (Crossler, 2010)
Threat appraisal (OTA)	An individual's assessment of the level of harm posed by an OD scam (Crossler, 2010; Liang and Xue, 2010)
Perceived severity (PS)	An individual's assessment of the degree of harm of the consequences resulting from an OD scam (e.g. amount of money lost, emotional harm) (Crossler, 2010; Johnston and Warkentin, 2010)
Perceived vulnerability (PV)	An individual's subjective assessment of the probability of experiencing an OD scam (provided no adaptive behaviour is performed, and there is no modification to the existing behavioural disposition) (Lee and Larsen, 2009; Crossler, 2010)
Attitude (ATT)	Reflects the individual's positive or negative evaluations about using protection mechanisms to prevent or mitigate an OD scam (Karahanna et al., 1999; Au and Enderwirck, 2000)
Adoption intention (AI)	An individual's conscious plans to use (or not use) protection mechanisms (Warshaw and Davis, 1985b)
Behavioural expectation (BE)	An individual's evaluation of the perceived probability that he/she will actually use protection mechanisms (Warshaw and Davis, 1985b)

Table 5. Definitions of research model constructs

Appendix B – Questionnaire Items

Construct	Survey question
PS	Online dating scams can result in serious harm
	The results of OD scams can be very severe
	Online dating scams can lead to significant negative consequences
	Online dating scams can result in [negligible - very serious] harm
PV	I am a likely target for scammers on OD websites
	There is a slight chance that I may get scammed on OD websites
	There is a possibility that I will fall victim to OD scams
	I am at risk of being a victim of an OD scam
Ta (overall)	Overall, the threats associated with OD is [very low - very high]
	Overall, the threats associated with OD is [non-existent - substantial]
	Overall, the threats associated with OD are [insignificant - significant]
TA	I am conscious of OD scams when I use OD websites
	Online dating scams can occur on OD websites
	I am aware of the OD scams that occur on OD websites
PMA (overall)	Overall, I have knowledge of protection mechanisms when using OD websites
	Overall, I am aware that protection mechanisms are available when using OD websites
	Overall, I am conscious of protection mechanisms being available when using OD websites
	Overall, I understand that protection mechanisms are available when using OD websites

Ca (over all)	Overall, managing the threats associated with OD websites is… - Of little value - valuable - Unhelpful - beneficial - Worthless - worthwhile
PMA	I have knowledge of informational / reporting mechanisms being available on OD websites
	I am aware of informational / reporting mechanisms being available on OD websites
	I am conscious of informational / reporting mechanisms being available on OD websites
RE	Informational / reporting mechanisms are effective in safeguarding against possible OD scams
	Informational / reporting mechanisms are valuable in safeguarding against possible OD scams
	Informational / reporting mechanisms is helpful in safeguarding against possible OD scams
SE	I am confident in using informational / reporting mechanisms on OD websites
	I am capable of using informational / reporting mechanisms on OD websites
	I am competent in using informational / reporting mechanisms on OD websites
RC	Using informational / reporting mechanisms on OD websites is inconvenient
	Using informational / reporting mechanisms on OD websites is time-consuming
	Using informational / reporting mechanisms on OD websites takes significant effort
AI	I plan to adopt informational / reporting mechanisms when I use OD websites.
	My intention to adopt informational / reporting mechanisms on OD websites is: [very low – very high]
	I aim to adopt informational / reporting mechanisms when using OD websites.
BE	Overall, I expect to adopt informational / reporting mechanisms when I use OD websites
	Overall, I will likely use informational / reporting mechanisms when I use OD websites
	Overall, I predict that I will use informational / reporting mechanisms when I use OD sites
ATT	Overall, my attitude towards the use of protection mechanisms during OD is: - Undesirable - desirable - Bad - good - Negative - positive - Foolish - wise - Unhelpful - beneficial

Table 6. Questionnaire items

References

ACCC. (2015a). "Online dating industry report." (A. C. and C. Commission, Ed.). Canberra.

ACCC. (2015b). "Targeting scams: Report of the ACCC on scams activity 2014." (A. C. and C. Commission, Ed.). Canberra.

Anderson, C. L. and R. Agarwal. (2010). "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions." *MIS Q.*, *34*(3), 613–643.

Andrejevic, M. (2002). "The work of watching one another: Lateral surveillance, risk, and governance." *Surveillance & Society*, *2*(4).

Au, A. K. and P. Enderwirck. (2000). "A cognitive model on attitude towards technology adoption." *Journal of Managerial Psychology*, *15*(4), 266–282.

Bagozzi, R. P. and Y. Yi. (1988). "On the evaluation of structural equation models." *Journal of the Academy of Marketing Science*, *16*(1), 74–94.

Barraket, J. and M. S. Henry-Waring. (2008). "Getting it on(line): Sociological perspectives on e-dating." *Journal of Sociology*, *44*(2), 149–165.

Boss, S. R., D. F. Galletta, P. Benjamin Lowry, G. D. Moody and P. Polak. (2015). "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors." *MIS Quarterly*, *39*(4), 837–864.

Buhrmester, M., T. Kwang and S. D. Gosling. (2011). "Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data?" *Perspectives on Psychological Science*, *6*(1), 3–5.

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

Chin, W. W. (1998). "The partial least squares approach to structural equation modeling." *Modern Methods for Business Research*, *295*(2), 295–336.

Chin, W. W. (2010). "How to write up and report PLS analyses." In: *Handbook of partial least squares* (pp. 655–690). Springer.

Coontz, S. (2005). *Marriage, a History: From Obedience to Intimacy, Or how Love Conquered Marriage*. Viking.

Couch, D., P. Liamputtong and M. Pitts. (2011). "Online Daters and the Use of Technology for Surveillance and Risk Management." *International Journal of Emerging Technologies and Society*, *9*(2), 116–134.

Couch, D., P. Liamputtong and M. Pitts. (2012). "What are the real and perceived risks and dangers of online dating? Perspectives from online daters." *Health, Risk & Society*, *14*(7/8), 697–714.

Cross, C. (2014). "Love hurts: the costly reality of online romance fraud." Retrieved from https://theconversation.com/love-hurts-the-costly-reality-of-online-romance-fraud-35263

Cross, C. and K. Richards. (2015). "The 'ACA Effect': Examining How Current Affairs Programs Shape Victim Understandings and Responses to Online Fraud." *Current Issues in Criminal Justice*, *27*(2), 163–178.

Crossler, R. E. (2010). "Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data." In: *System Sciences (HICSS), 2010 43rd Hawaii International Conference on* (pp. 1–10).

Dudley, D. and D. Shadel. (2015). " 'Are You Real?' — Inside an Online Dating Scam." Retrieved from http://www.aarp.org/money/scams-fraud/info-2015/online-dating-scam.html

Fishbein, M. and I. Ajzen. (1975). *Belief, attitude, intention, and behavior: an introduction to theory and research*. Addison-Wesley Pub. Co.

Floyd, D. L., S. Prentice-Dunn and R. W. Rogers. (2000). "A Meta-Analysis of Research on Protection Motivation Theory." *Journal of Applied Social Psychology*, *30*(2), 407–429.

Fornell, C. and D. F. Larcker. (1981). "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error." *Journal of Marketing Research*, *18*(1), 39.

Garrett, E. V. and R. W. Taylor. (2014). *Exploring internet users' vulnerability to online dating fraud: Analysis of routine activities theory factors*. The University of Texas at Dallas, Ann Arbor. Retrieved from http://search.proquest.com/docview/1656449717?accountid=12763

Hanus, B. and Y. "Andy" Wu. (2016). "Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective." *Information Systems Management*, *33*(1), 2–16.

Harrington, R. (2015). "Dating Services Tinker with the Algorithms of Love." Retrieved from https://www.scientificamerican.com/article/dating-services-tinker-with-the-algorithms-of-love/

Herath, T., R. Chen, J. Wang, K. Banjara, J. Wilbur and H. R. Rao. (2014). "Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service." *Information Systems Journal*, *24*(1), 61–84.

Herath, T. and R. H. Rao. (2009). "Protection motivation and deterrence: a framework for security policy compliance in organisations." *European Journal of Information Systems*, *18*(2), 106–125.

Hickey, S. (2015). "Scammers target lonely hearts on dating sites." Retrieved from https://www.theguardian.com/money/2015/aug/14/scammers-target-middle-age-women

Hitsch, G. J., A. Hortaçsu and D. Ariely. (2010). "What makes you click?--Mate preferences in online dating." *Quantitative Marketing and Economics*, *8*(4), 393–427.

Huang, J., G. Stringhini and P. Yong. (2015). "Quit Playing Games with My Heart: Understanding Online Dating Scams." In: M. Almgren, V. Gulisano, & F. Maggi (Eds.), *Detection of Intrusions and Malware, and Vulnerability Assessment: 12th International Conference, DIMVA 2015, Milan, Italy, July 9-10, 2015, Proceedings* (pp. 216–236). Cham: Springer International Publishing.

Johnston, A. C. and M. Warkentin. (2010). "Fear appeals and information security behaviors: an empirical study." *MIS Q.*, *34*(3), 549–566.

Johnston, A. C., M. Warkentin and M. T. Siponen. (2015). "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric." *MIS Quarterly*, *39*(1), 113–134.

Karahanna, E., D. W. Straub and N. L. Chervany. (1999). "Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs." *MIS Quarterly*, *23*(2), 183–213.

Kim, Y. J., J. U. Chun and J. Song. (2009). "Investigating the role of attitude in technology acceptance from an attitude strength perspective." *International Journal of Information Management*, *29*(1), 67–77.

Koon, T. H. and D. Yoong. (2013). "Preying on lonely hearts: A systematic deconstruction of an internet romance scammer's online lover persona." *Journal of Modern Languages*, *23*, 28–40.

Kritzinger, E. and S. H. von Solms. (2010). "Cyber security for home users: A new way of protection through awareness enforcement." *Computers & Security*, *29*(8), 840–847.

LaBuda, M. A. and K. Kostere. (2012). *Individuals involved in online dating sites description of the process of developing a relationship: A grounded theory study*. Capella University, Ann Arbor.

Lawson, H. M. and K. Leck. (2006). "Dynamics of Internet Dating." *Social Science Computer Review*, *24*(2), 189–208.

Lee, Y. (2011). "Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective." *Decis. Support Syst.*, *50*(2), 361–369.

Lee, Y. and R. K. Larsen. (2009). "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software." *European Journal of Information Systems*, *18*(2), 177–187.

Liang, H. and Y. Xue. (2010). "Understanding security behaviors in personal computer usage: A threat avoidance perspective." *Journal of the Association for Information Systems*, *11*(7), 394.

Madden, M. and A. Lenhart. (2006). "Online dating: Americans who are seeking romance use the Internet to help them in their search, but there is still widespread public concern about the safety of online dating." Retrieved from http://www.pewinternet.org/Reports/2006/Online-Dating.aspx

McKenna, K. Y. A., A. S. Green and M. E. J. Gleason. (2002). "Relationship Formation on the Internet: What's the Big Attraction?" *Journal of Social Issues*, *58*(1), 9–31.

Milne, S., P. Sheeran and S. Orbell. (2000). "Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory." *Journal of Applied Social Psychology*, *30*(1), 106–143.

Pan, J., D. Winchester, L. Land and P. Watters. (2010). "Descriptive data mining on fraudulent online dating profiles."

Paravastu, N. and M. Anandarajan. (2015). "Fear Appeals, Threat Perceptions, and Protection Motivation in Information Systems Security."

Rege, A. (2009). "What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud." *International Journal of Cyber Criminology*, *3*(2), 494–512.

Rogers, R. W. (1975). "A Protection Motivation Theory of Fear Appeals and Attitude Change." *Journal of Psychology*, *91*(1), 93.

Rogers, R. W. (1983). "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation." *Social Psychophysiology*, 153–176.

Scamwatch. (2011). "Scams: It's personal." Retrieved from http://www.austlii.edu.au/au/journals/AUCCCUpdate/2011/23.pdf

Scamwatch. (2016). "Scam statistics - Dating & romance for 2014." Retrieved from https://www.scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=13&date=2014

Schwartz, S. H. (1977). "Normative influences on altruism." *Advances in Experimental Social Psychology*, *10*, 221–279.

Sharot, T. (2011). "The optimism bias." *Current Biology*, *21*(23), R941–R945.

Sheftalovich, Z. (2014). "Can you really find true love online?" Retrieved from https://www.choice.com.au/electronics-and-technology/internet/using-online-services/articles/online-dating-sites-review

Smith, A. D. (2005). "Exploring online dating and customer relationship management." *Online Information Review*, *29*(1), 18–33.

Smith, R. (2008). "Coordinating individual and organisational responses to fraud." *Crime, Law & Social Change*, *49*(5), 379–396.

Sun, Y., N. Wang, X. Guo and Z. Peng. (2013). "Understanding the Acceptance of Mobile Health Services: A Comparison and Integration of Alternative Models." *Journal of Electronic Commerce Research*, *14*(2), 183–200.

Tatera, K. (2016). "These Personality Traits Make You Most Vulnerable to Online Dating Scams, Study Finds." Retrieved from http://thescienceexplorer.com/technology/these-personality-traits-make-you-most-vulnerable-online-dating-scams-study-finds

Tracy, J. (2008). "No Title." Retrieved from http://www.onlinedatingmagazine.com/columns/industry/2008/onlinedatingscams.html

Venkatesh, V., S. A. Brown, L. M. Maruping and H. Bala. (2008). "Predicting Different Conceptualizations of System Use: The Competing Roles of Behavioral Intention, Facilitating Conditions, and Behavioral Expectation." *MIS Quarterly*, *32*(3), 483–502.

Vroom, C. and R. von Solms. (2004). "Towards information security behavioural compliance." *Computers & Security*, *23*(3), 191–198.

Warshaw, P. R. and F. D. Davis. (1985a). "Disentangling behavioral intention and behavioral expectation." *Journal of Experimental Social Psychology*, *21*(3), 213–228.

Warshaw, P. R. and F. D. Davis. (1985b). "The Accuracy of Behavioral Intention Versus Behavioral Expectation for Predicting Behavioral Goals." *Journal of Psychology*, *119*(6), 599.

Whitman, M. E. and H. J. Mattord. (2010). *Management of Information Security*. Cengage Learning.

Whitty, M. T. (2013). "The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam." *British Journal of Criminology*, *53*(4), 665–684.

Whitty, M. T. (2015). "Anatomy of the online dating romance scam." *Security Journal*, *28*(4), 443–455.

Whitty, M. T. and T. Buchanan. (2012a). "The Online Romance Scam: A Serious Cybercrime." *Cyberpsychology, Behavior, and Social Networking*, *15*(3), 181–183.

Whitty, M. T. and T. Buchanan. (2012b). "The psychology of the online dating romance scam." *A Report for the ESRC. In*, 23.

Wiederhold, B. K. (2015). "Twenty Years of Online Dating: Current Psychology and Future Prospects." *Cyberpsychology, Behavior, and Social Networking*, *18*(12), 695–696.

Witte, K., K. A. Cameron, J. K. McKeon and J. M. Berkowitz. (1996). "Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale." *Journal of Health Communication*, *1*(4), 317–342.

Wold, H. (1985). "Partial least squares." *Encyclopedia of Statistical Sciences*.

Xia, P., K. Tu, B. Ribeiro, H. Jiang, X. Wang, C. Chen, … D. Towsley. (2014). "Who is dating whom: Characterizing user behaviors of a large online dating site." *arXiv Preprint arXiv:1401.5710*.

Yang, H. and Y. Yoo. (2004). "It's all about attitude: revisiting the technology acceptance model." *Decision Support Systems*, *38*(1), 19–31.

Young, E. (2015). "The surge of romance scams in Australia and who falls victim to them." Retrieved from http://www.watoday.com.au/wa-news/the-surge-of-romance-scams-in-australia-and-who-falls-victim-to-them-20150709-gi8u7m.html

Zahedi, F. M., A. Abbasi and Y. Chen. (2015). "Fake-Website Detection Tools: Identifying Elements that Promote Individuals' Use and Enhance Their Performance." *Journal of the Association for Information Systems*, *16*(6), 448–484.