Emerald Journal of Financial Crime

Who can spot an online romance scam?

Journal:	*Journal of Financial Crime*
Manuscript ID	JFC-06-2018-0053
Manuscript Type:	Scholarly Article
Keywords:	cyber scams, romance scam, fraud, cyber security, human detection

Who can spot an online romance scam?

Abstract

Purpose – This paper examines predictors (personality, belief systems, expertise and response time) of detecting online romance scams.

Design/methodology/approach – The online study asked 261 participants to rate whether a profile was a scam or a genuine profile. Participants were also asked to complete a personality inventory, belief scales, and demographic, descriptive questions. The online study was also designed to measure reponse time.

Findings – It was found that those who scored low in romantic beliefs, high in impulsivity, high in consideration of future consequences, had previously spotted a romance scam, and took longer response times, were more likely to accurately distinguish scams from genuine profiles. Notably, the research also found that it was difficult to detect scams. The research also found that it was important to adapt Whitty's (2013) 'Scammers Persuasuive Techniques Model' to include a stage named: '*human detection of scam versus genuine profiles'*.

Originality/value – This is the first study, to the author's knowledge, that examines predictors of human accuracy in detecting romance scams. Dating sites and government e-safety sites might draw upon these findings to help improve human detection and protect users from this financial and psychologically harmful cyberscam.

Keywords: cyber scams, romance scams, fraud, cyber security, human detection.

Paper type Research paper

1. Introduction

Online romance scams are one of the most common and lucrative (for criminals) cyber-enabled scams (ACCC, 2017; ONS, 2017; Whitty & Buchanan, 2012). In these scams criminals create fake online profiles on dating sites and social networking sites (e.g., Facebook, Skype, LinkedIn) to draw individuals into relationships with the intention to trick them out of money. These fake profiles include stolen photographs (e.g., attractive models, army officers) and the creation of a false identity. Some victims are quite traumatized by the experience, suffering a 'double hit' of financial losses and the loss of a relationship (Whitty & Buchanan, 2016). There is, therefore, an urgent need to protect online daters. Understanding who is more likely to be tricked by a romance scam can potentially help improve guidelines and educational training programmes developed to protect users of these sites.

Previous research has examined the persuasive strategies employed by criminals and the decision-making errors made by victims who are drawn into these scams (Gregory & Bistra, 2012; Whitty, 2013, 2015). Researchers have also examined the psychological characteristics of victims compared with non-victims (Buchanan & Whitty, 2014; Whitty, 2018). Whilst there might be some overlap between victims and those who are unable to identify a scam, to date there is no research on whether psychological characteristics (e.g., personality, belief systems and behaviours) predict who is more likely to recognise an *online dating profile of a romance scammer*. Understanding who is more likely to make errors in judgement when confronted with a scam could be very useful for those developing prevention programmes (e.g., government e-safety websites, online dating sites).

Notably, a few studies have examined the distinguishing personality characteristics of scam victims and those who can detect phishs (e.g., Holtfreter, Reisig & Pratt, 2008; Pattinson, Jerram, Parsons, McCormac & Butavicius, 2012; Welk, Hong, Zielinska, Tembe, Murphy-Hill, Mayhorn, 2015; Wright, Chakraborty, Basoglu, & Marett, 2010; Wright & Marett, 2010). Holtfreter et al., (2008), for example, found that self-control is a significant predictor of scam victimisation. Pattinson et al., (2012) found that more impulsive people were less likely to detect phishing emails. Of further note, a susceptibility to persuasion scale has been developed with the intention to predict likelihood of becoming scammed (Modic, Anderson & Palomäki, 2018). This scale includes the following items: premeditation, consistency, sensation seeking, self-control, social influence, similarity, risk preferences, attitudes towards advertising, need for cognition and uniqueness. In consideration of this previous research, it is therefore worthwhile considering whether personality plays a role when detecting romance scams.

Some researchers have focused more specifically on the psychological and social demographic characteristics that put people at risk of romance scam victimisation (Buchanan & Whitty, 2014; Whitty, 2018). Buchanan and Whitty (2014) found that individuals with a higher tendency towards idealization of romantic partners were more likely to be scammed. Whitty (2018) extended upon this research and found that romance scam victims tended to be middle-aged, well educated women who are more impulsive (scoring high on urgency and sensation seeking), less kind, more trustworthy and have an addictive disposition. Whilst the characteristics these researchers have identified are useful in explaining victimisation, we are yet to

learn their utility in predicting scam detection. Are victims of romance scams tricked because they are unable to distinguish genuine from fake profiles? Does personality and other psychological characteristics play a role in determining victimisation from the get-go?

The relationship between 'routine activities' and cyber-scam victimisation has also been examined by scholars (e.g., Hutchings & Hayes, 2009; Pratt, Holtfreter & Reisig, 2010; Reyns, 2015). Pratt, Holtfreter and Reisig (2010), for example, found that demographic characteristics shape routine online activities and that indicators of routine online activities fully mediate the effect of demographic characteristics on the likelihood of being targeted online for fraud. More recently, Reyns (2015) conducted a study that examined whether online exposure placed users at more risk of online victimisation (phishing, hacking and malware infection) and if online guardianship helped prevent this form of victimisation. He found that individuals who were more likely to make online purchases, engage in social networking and post information online were more likely to be victimised.

With respect to detecting deception researchers have examined whether experts are better at detecting deception compared with novices. Vrij (2004) contends that experts tend to focus on the wrong cues, and as a result are less accurate at detecting deception compared with novices. Vrij and his colleagues have found that this is most likely to occur when experts rely heavily on non-verbal cues in preference to verbal cues (Vrij, 2008; Bogaard, Meijer, Vrij & Merchelbach, 2016). Moreover, research has found that when participants are trained to focus on verbal content cues they are more accurate at detecting deception (Hauch, Sporer, Michael & Meissner, 2016).

We know less about individuals' ability to detect lies in online environments (Whitty & Joinson, 2009), and given that non-verbal cues are often absent we might find very different results when we compare experts versus non-experts in textual environments. Research on phishing detection gives us some clues. For example, it has be found that knowledge and experience with email increased resilience to a phishing attack (Harrison, Svetieva & Vishwanath, 2016; Purkait, 2012).

1.1 Current study

This study attempts to expand on the research that explains why individuals are tricked by online dating romance scams. Research has set out a *stage model* to explain the success of this particular scam, moving from: a) motivations to find the ideal partner, b) the creation of a perfect profile, b) grooming, c) testing the waters, d) 'the sting', e) and finally, in some cases, re-victimisation (Whitty, 2013, 2015). Although this model suggests that victims are susceptible to scams because they are motivated to find an 'ideal partner', this notion has not been empirically tested. Moreover, the model does not consider when individuals are making decisions regarding whether a profile is fake or genuine. The assumption by many is that this is an easy task (Whitty, 2013); however, this assumption is based on public opinion, rather than solid empirical research. Moreover, as highlighted above, we have yet to learn whether psychological characteristics and behaviour play a role at the detection stage. More specifically, this study examined whether psychological characteristics (personality and belief systems), previous experience of spotting a scam, and response time predicted accurate detection of fake from real scams. Understanding the types of people who are more likely to score

low on accuracy of human detection can potentially help in the development of effective education and change behaviour programmes to assist citizens in detecting romance scams and other types of cyber-scams.

With respect to belief systems, previous research has found that romance scam victims score significantly higher on measures of romantic beliefs compared with non-victims (Buchanan & Whitty, 2014). It was decided, therefore, to include a romantic beliefs measure in this study. Akin to Buchanan and Whitty's research, in this study Sprecher and Metts' (1989) Romantic Beliefs Scale was used, which defines romanticism or love as an ideology that is "a relatively coherent individual orientation toward love" that "may function as a cognitive schema for organizing and evaluating one's own behaviour and the behaviour of a potential or actual romantic partner" (p. 388). Those who score high on this scale believe in the notion of romantic destiny. It is therefore plausible to conceive that these romantic notions might influence individuals' accuracy in detection. The first hypothesis is that those who score high on the Romantic Beliefs Scale will be less accurate at detecting fake from genuine profiles (H1).

The personality traits impulsivity and consideration of future consequences were examined in this study. Impulsive individuals are likely to rush through tasks not giving the task their full attention (Gellatly, 1996) and therefore miss key deception indicators. Consequently, they might miss the important cues in a profile that indicate that it is a scam. The second hypothesis is therefore that those who score high on a measure of impulsivity will be less accurate at detecting fake from genuine profiles (H2). Impulsivity was measured using the UPPS-R (Whiteside & Lynam, 2001). Consideration

of Future Consequences is a personality trait defined as the extent to which individuals consider the potential future outcomes of their current behaviour (Strathman, Gliecher, Boninger & Edwards, 1994). Those who score low on this scale may be less motivated to do well on a detection task, given they perceive no immediate benefits from doing well at this task. The third hypothesis is therefore that those who score low on Consideration of Future Consequences will be less accurate at detecting fake from genuine profiles (H3). The Consideration of Future Consequences was measured using the CFC (Strathman et al., 1994).

The behavioural measure of previously spotting a dating scam was also considered – given that rehearsal (Turley-Ames & Whitefield, 2003), and task familiarity (Sarter & Schroeder, 2001) have been found to improve task performance. Moreover, experience in detecting scams might be important given the background of literature which has examined expert and novice detectors (Bogaard et al., 2016; Hauch et al., 2016; Vrij, 2004, 2008;). It was hypothesised that those who had not spotted a scam will be less accurate at detecting fake from genuine profiles (H4). Finally, the amount of time taken up to complete the task (response time) was included as a predictor variable, given that accuracy might be improved when participants read the profile and have more time to notice any anomalies. Moreover, researchers have found that participants who perform better at decision-making tasks take longer to make their decision (Dror, Busemeyer, & Basola, 1999). The fifth and final hypothesis is therefore that those who have a shorter response time will be less accurate at detecting fake from genuine profiles (H5).

2. Method

2.1 Participants

There were 261 participants in final sample, with all participants residing in the UK. According to Green (1991) the minimal effect size needed for a multiple regression with 6 predictors, expecting a medium effect of R^2 = .07; ß = .20 is 110. The sample size was therefore adequate. As a note: during checks and cleaning of the data one participant was removed from the sample due to selecting the same option on the Likert scale for all of the personality questionnaires.

All participants had either used a dating site and/or a social networking site. There were 49% men and 51% women in the sample, with a mean age of 45.47 years (*SD* = 15.10). Education levels achieved included: 4% less than high school; 30% high school (GCSEs), 28% high school (A-levels), 27% undergraduate degree; 9% Masters and 2% PhD. In the final sample 28% of participants believed they had previously spotted a dating scam profile.

2.2 Materials

Data were collected using a questionnaire hosted on the Qualtrics online survey platform. The questionnaire consisted of personality inventories, belief scales, profiles to rate, as well as items devised to measure demographic descriptive data. The questionnaire was also designed to measure response time. Genuine dating profiles and known scammer profiles were collected to be used in this study. The profiles contained an image and written information about the person (see Figure 1 for an example of a scammer profile). They were all formatted in the same style (including font size, borders, sizing). They were collected, with permission, from two public sites operated by the same owner: a) a dating site where each profile is verified and b) a scam profile

website ('scamlist') where known romance scam profiles are recorded by site moderators in order to warn and inform the public of identified scam profiles and techniques. Twenty verified scammer profiles and twenty known real profiles were used. The two sets were matched on gender and age.

INSERT FIGURE 1 ABOUT HERE

Romantic Beliefs was measured using Sprecher and Metts (1989) Romantic Beliefs Scale. The scale demonstrated excellent internal consistency (Cronbach's alpha = .90). Impulsivity was measured using the UPPS-R Impulsivity scale (Whiteside & Lynam, 2001), which also demonstrated excellent internal consistency for both (Cronbach's alpha = .88). The Consideration of Future Consequences was measured using the CFC (Strathman et al., 1994). The scale demonstrated acceptable internal consistency (Cronbach's alpha = .74). Response time was calculated by adding each of the response times calculated on making a decision about whether the scam was real or fake. Accuracy score was calculated by adding the number of profiles the participated scored correctly for both the fake and the real profiles. Participants scored a mean of 6.74 (*SD* = 2.04) on the fake profiles and 6.77 (*SD* = 2.40) on the real profiles, making a total accuracy mean of 13.51 (*SD* = 2.63).

2.3 Procedure

The study was set up on the Qualtrics online survey platform. Qualtrics was also commissioned to recruit a UK representative sample from their online panel. This is a reputable company often used by academics for recruitment and to set up surveys. Progression though the study was controlled by

disabling browser 'back' buttons, and participants were forced to answer each question.

The survey began by asking participants socio-demographic details (age, gender, education) and then provided a definition of the online dating scam followed by 20 randomly presented profiles (10 fake and 10 genuine) for participants to rate as genuine or a scam. Participants where then asked about their use, if any, of dating sites and other online platforms and whether, prior to the survey, they had spotted a dating scam profile. They were then asked to complete the Romantic Beliefs Scale, the UPPS-R Impulsivity scale and the CFC.

3. Results

Prior to conducting the analysis bivariate associations between the independent variables were examined for the predictor variables (see Table 1). Most correlations were low and very few were significant.

INSERT TABLE 1 ABOUT HERE

Forced-entry multiple regressions were run to test the hypotheses (see Table 2). Preliminary analyses were conducted to ensure no violation of the assumptions of normality, linearity, multicollinearity and homoscedasticity. A log 10 transformation was conducted on response time because this variable was was positively skewed. Response time then met the assumption of normality. All other assumptions were met.

The model was significant, $F(5,255) = 7.504$, $p < .001$, with 13% of variance explained by the model. Four of the hypotheses were supported with: those who scored high on romantic beliefs being less accurate (H1), those who scored low on consideration of future consequences being less

accurate (H3), those who had never spotted a scam were less accurate (H4), and those who scored low on response time being less accurate (H5). Impulsivity was also significant (H2); however, not in the direction which was predicted. Of further note is that response time was the strongest unique contribution to explaining the dependent variable.

INSERT TABLE 2 ABOUT HERE

4. Discussion

Cyber-fraud is a crime that is on the increase and has global impact (on the indivuals affected by these crimes as well as nations' economies when money is taken out of countries into the pockets of criminals residing in other countries). The harm for victims is a 'double-hit' of money and the death of a romance – once the scam is realised (Whitty & Buchanan, 2016). Online romance scams are one of the more common cyber-scams impacting individuals around the world (ACCC, 2017; ONS, 2017; Whitty & Buchanan, 2012). They have been around in their online form since about 2007 (Whitty & Buchanan, 2012) and despite the efforts of law enforcement, governments, and intelligence agency, continues to increase (ACCC, 2017; ONS, 2017). There is, therefore, an urgent need to better understand the reasons why victims are drawn into these scams and tricked out of their money. Greater understandings can then be drawn upon to improve detection and prevention techniques and strategies.

The findings from this study demonstrate that personality and behaviour predict accuracy in human detection of dating scams. It is of interest that belief systems can impact, to some extent, individuals' abilities to detect a romance scam – demonstrating that victims of romance scam most

likely have pre-dispositions that make them vulnerable to these scams, even before a criminal begins communicating with the victim.

Response time was the strongest unique contributor, suggesting that the way someone approaches the task is more important than personality or belief systems as a predictor of accuracy. This is an important finding and one that can potentially help protect individuals from becoming scammed. Dating sites might, for example, warn users to take their time when considering profiles and perhaps might draw upon these findings in the design of their sites. Government e-safety websites might also consider highlighting the types of behaviours individuals need to change rather than simply highlight the problem. This is important to consider given that research has found that users who consult information on government e-safety websites and other places are more likely to become scammed compared with those who do not read information about scams (Whitty, in press).

Of further interest, is that having spotted a scam prior to the study predicted better accuracy scores. This too is an important finding and adds to the little of what we know regarding novices versus experts in detecting deception in online environments. These findings might also be used to help protect users. E-safety websites, for example, might provide interactional exercises to train users to detect scams rather than provide screeds of information. Further research might find this a more useful training technique.

Contrary to the hypothesis, high impulsivity predicted greater accuracy. Whilst this was unexpected, perhaps this finding suggests that it is important to go with one's 'initial gut instinct'. Previous qualitative research on romance scams has found that victims report that in the early stages they have an

initial uneasiness about the scammer, but either choose to ignore these feelings or challenged the scammer who convinced them they were genuine (Whitty, 2013, 2015).

These findings add to Whitty's (2013) 'Scammers Persuasive Techniques Model'. In this model it is argued that victims go through a number of stages prior to becoming scammed out of their money. The success of the scam, according to Whitty, is the scammer's skills to persuade and trick the individual (drawing from a variety of techniques), the victims' willingness to believe the scammer and ignore evidence to the contrary (cognitive dissonance), and importantly, the scammers's ability to move the victim from one stage to the next. Whitty argues that some people are more susceptible to the criminal's charms and abilities to deceive, however, she does not consider when individuals make a decision about whether a particular profile is genuine or a scam. It is argued here that it is important to consider this stage in the scam. This stage has been inserted into Whitty's (2013) model after the stage where a person is presented with an ideal profile (see Figure 2). It helps to highlight that an individual might be protected prior to any communication or grooming and that it is important to help users with effective deceiving making when comfronted with potentially deceptive online material. Given that researchers have argued that poor decision-making can place individuals are greater risk of becoming scammed (see for example, Lea, Fisher & Evans, 2009) this research highlights that decision-making errors and the reasons why people make these errors also need to be considered prior to communication between protential victims and scammers.

INSERT FIGURE 2 ABOUT HERE

The accuracy scores also suggest that distinguishing fake from genuine profiles is not a simple task. This contradicts the general publics' view that romance scams are easy to detect, and victims are stupid for being taken in by such scams (Whitty, 2013). However, with training (as with phishing scams) accuracy might be improved – thus helping to protect citizens from this particular financial crime.

In conclusion, to the author's knowledge, this is the first study that has examined predictors of human accuracy in *detecting scammer romance scam profiles*. The study highlights some very important findings. First, that it is difficult for people to detect fake from genuine profiles, suggesting that much work is needed to help protect users of online dating sites. Second, psychological characteristics do, to some extent, predict accuracy in human detection. Whilst personality factors played a role, response time was a stronger predictor of accuracy. Third, the findings here might be used to inform the development of future training programmes.

References

ACCC, (2016), "Australians lose over $229 million to scams in 2015", available at: https://www.accc.gov.au/media-release/australians-lose-over-229-million-to-scams-in-2015.

Buchanan, T. and Whitty, M.T. (2014), "The online dating romance scam: Causes and consequences of victimhood", *Psychology, Crime & Law*, Vol. 20 No. 3, pp. 261-283.

Bogaard, G. Meijer, E.H. Vrij, A. and Merckelbach, H. (2016), "Strong, but wrong: Lay people's and police officers' beliefs about verbal and nonverbal cues to deception", *PLOS ONE,* Vol. 11 No. 6, e0156615.

Gellatly, I.R. (1996), "Conscientiousness and task performance: Test of a cognitive process model", *Journal of Applied Psychology,* Vol. 81 No. 5, pp. 474-482.

Gregory D.W. and Nikiforova, B. (2012), "A sweetheart of a deal: How people get hooked and reeled in by financial scams", *The Journal of Behavioral Finance & Economics*, Vol. 2 No. 2, pp. 96-122.

Green S.B. (1991), "How many subjects does it take to do a regression analysis", *Multivariate Behavioral Research,* Vol. 26 No. 3, pp. 499-510.

Hauch, V. Sporer, S.L. Michael, S.W. and Meissner, A. (2016), "Does training improve the detection of deception? A meta-analysis", *Communication Research,* Vol. 43 No. 3, pp. 283-343.

Harrison, B. Svetieva, E. and Vishwanath, A. (2016), "Individual processing of phising emails: How attention and elaboration protect against phishing", *Online Information Review,* Vol. 40 No. 2, pp. 265-281.

Holtfreter, K. Reisig, M.D. and Pratt, T.C. (2008), "Low Self-control, Routine Activities, and Fraud Victimization. Criminology", Vol. 46 No. 1, pp. 189-220.

Hutchings, A. and Heyes, H. (2009), "Routine activity theory and phishing victimisation: Who gets caught in the 'Net'?", *Current Issues in Criminal Justice,* Vol 20 No. 3, pp. 433-451.

Lea, S. Fisher, P. and Evans, K.M. (2009), "The Economic Psychology of Scams', International Association for Research in Economic Psychology and the Society for the Advancement of Behavioral Economics, Nova Scotia, Canada, July 2009.

Modic, D. Anderson, R. and Palomäki, J. (2018), "We Will Make You Like Our Research: The Development of a Susceptibility-to-Persuasion Scale", *PLOS ONE,* Vol. 13 No. 3, e0194119.

ONS (2016), "Overview of fraud statistics: year ending March 2016", available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016.

Pattinson, M. Jerram, C. Parsons, K. McCormac, A. and Butavicius, M. (2012), "Why do some people manage phishing e-mails better than others?" *Information Management & Computer Security,* Vol 20 No. 1, pp. 18-28.

Pratt, T.C. Holtfreter, K. and Reisig, M.D. (2010), "Routine online activity and Internet fraud targeting: Extending the generality of routine activity theory", *Journal of Research in Crime and Delinquency,* Vol. 47 No. 3, pp. 267-296.

Purkait, S. (2012), "Phishing counter measures and their effectiveness – literature review", *Information Management & Computer Security,* Vol. 20 No. 5, 382-420.

Reyns, B.W. (2015), "A routine activity perspective on online victimisation: Results from the Canadian general social survey, *Journal of Financial Crime,* Vol 22 No. 4, pp. 396-411.

Sarter N.B. and Schroeder, B. (2001), "Supporting decision making and action selection under time pressure and uncertainty: the case of in-flight icing", *Human Factors: The Journal of the Human Factors and Ergonomics Society,* Vol. 43 No. 4, pp. 573-583.

Sprecher, S. and Metts, S. (1989), "Development of the 'romantic beliefs scale' and examination of the effects of gender and gender-role orientation", *Journal of Social and Personal Relationships,* Vol. 6, pp. 387-411.

Strathman A. Gleicher F. Boninger D.S. Edwards C.S. (1994), "The consideration of future consequences: Weighing immediate and distant outcomes of behavior", *Journal of Personality and Social Psychology*, Vol. 66, No. 4, pp. 742-752.

Turley-Ames, K.J. and Whitefield, M.M. (2003). Strategy training and working memory task performance. *Journal of Memory and Language,* Vol. 49 No. 4, pp. 446-468.

Vrij, A. (2004), "Why professionals fail to catch liars and how they can improve", *Legal & Criminological Psychology,* Vol. 9, pp. 159-181.

Vrij, A. (2008*), "Beliefs about nonverbal and verbal cues to deception*". In: Vrij A, Editor. *Detecting lies and deceit*. Chirchester: Wiley, p. 115–40.

Welk, A. K. Hong, K. W. Zielinska, O. A. Rembe, R. Murphy-Hill, E. Mayhorn, C. (2015), "Will the "Phisher-Men" reel you in?: Assessing individual differences in a phishing detecting task", *International Journal of Cyber Behavior, Psychology and Learning*, Vol. 5 No. 4, pp. 1-17.

Whitty, M.T. (in press), "Predicting susceptibility to cyber-fraud victimhood", *Journal of Financial Crime.*

Whitty, M.T. (2018), "Do you love me? Psychological Characteristics of romance scam victims", Cyberpsychology, Behavior and Social Networking Vol. 21 No. 2, pp. 105-109.

Whitty, M.T. (2015b), "Anatomy of the online dating romance scam", *Security Journal,* Vol. 28, pp. 443-455.

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,* Vol. 53 No. 4, pp. 665-684.

Whitty, M.T. and Buchanan, T. (2016), "The online dating romance scam: The psychological impact on victims – both financial and non-financial", *Criminology & Criminal Justice*, Vol. 16 No. 2, pp.176-194.

Whitty, M.T. and Buchanan, T. (2012), "The online dating romance scam: A serious crime", *Cyberpsychology, Behavior, and Social Networking,* Vol. 15 No. 3, pp. 181-183.

Whitty, M.T. and Joinson, A.N. (2009), *Truth, Lies, and Trust on Internet.* London: Routledge, Psychology Press.

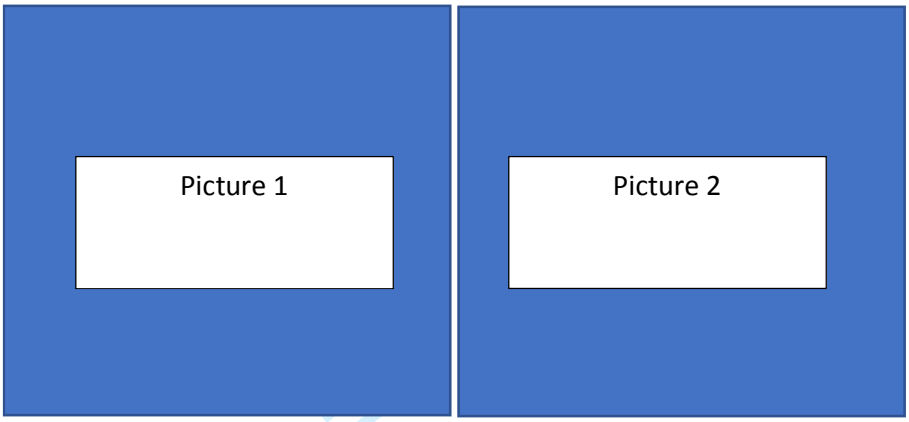
Wright, R.T. Chakraborty, S. Basoglu, A. and Marett, K. (2010), "Where did they go right? Understanding the deception in phishing communications", Group Decision and Negotiation, Vol. 19 No. 4, pp. 391-416.

Wright, R.T. and Marett, K. (2010), "The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived", *Journal of Management Information Systems*, Vol. 27 No. 1, pp. 273-303.

Whiteside, S. and Lynam, D.R. (2001), "The Five Factor Model and Impulsivity: Using a Structural Model of Personality to Understand Impulsivity", *Personality and Individual Differences* Vol. 30 No. 4, pp. 669-689.

Figure 1

Example of a fake profile



Username: Richkid01

Age: 41

Location: Manassas, Virginia, United States

Ethnicity: white

Occupation: contractor

Marital status: divorced

Description: Hey am Moore by name a single father , caring honest kind and loyal resonsible and hardworking man..am out here in seach of my lost ribs. You should feel free to send me mails .i will be glad to reply you.

Table 1

Pearson 1-tailed correlations between predictor variables

	1.	2.	3.	4.	5.
1. Rom. Bel.	1.00	.150**	-.025	-.122*	.044
2. UPPS-R		1.00	-.271**	-.140*	.158**
3. CFC			1.00	.101	.027
4. RT				1.00	-.071
5. Spot scam					1.00

Note: * p<.05, ** p<.01

Table 2

Multiple regression: Predictors of accuracy

Variable	***B***	***SE B***	***β***	***p***
Rom. Bel.	-.023	.011	-.127*	.033
UPPS-R	.025	.011	.140*	.026
CFC	.065	.022	.179**	.004
RT	2.000	.507	.235***	.000
Spot scam	.730	.349	.124*	.037
Constant	4.07	2.29		.077

*p<.05; **p<.01; ***p<.001

R^2 = .128; R^2 Adjusted = .111

Figure 2

Adaptation of Whitty's (2013) 'Scammers Persuasive Techniques Model'