Predicting susceptibility to cyber-fraud victimhood

Monica T. Whitty
*Cyber Security Centre, University of Warwick, Coventry, UK,
and Department of Media and Communication, University of Melbourne,
Carlton, Australia*

Abstract

Purpose – This paper aims to develop a theoretical framework to predict susceptibility to cyber-fraud victimhood.

Design/methodology/approach – A survey was constructed to examine whether personality, socio-demographic characteristics and online routine activities predicted one-off and repeat victimhood of cyber-fraud. Overall, 11,780 participants completed a survey (one-off victims, $N = 728$; repeat victims = 329).

Findings – The final saturated model revealed that psychological and socio-demographic characteristics and online routine activities should be considered when predicting victimhood. Consistent with the hypotheses, victims of cyber-frauds were more likely to be older, score high on impulsivity measures of urgency and sensation seeking, score high on addictive measures and engage in more frequent routine activities that place them at great risk of becoming scammed. There was little distinction between one-off and repeat victims of cyber-frauds.

Originality/value – This work uniquely combines psychological, socio-demographic and online behaviours to develop a comprehensive theoretical framework to predict susceptibility to cyber-frauds. Importantly, the work here challenges the current utility of government websites to protect users from becoming scammed and provides insights into methods that might be used to protect users from becoming scammed.

Keywords Cyber-security, Routine activity theory, Personality, Cyber-fraud, Internet-security, Scams

Paper type Research paper

1. Introduction

Cyber-frauds (also referred to as cyber-scams) are any type of fraud that exploits mass communication technologies (e.g. email, Instant Messenger, social networking sites) to trick people out of money (Whitty, 2015a). Examples include: foreign lotteries and sweepstakes (in which the victim believes they have won money from a lottery and are told to pay a fee to release the funds), 419 scams (advance fee fraud, in which victims believe that for a small amount of money they will make a large fortune) and romance scams (taken in by a fake online dating persona, in which the victim sends the 'fake persona' money). According to governmental and academic reports, the numbers of scam victims appear to be on the

The work reported in this paper was supported by the Engineering and Physical Sciences Research Council [EP/N028112/1].

Journal of Financial Crime
Vol. 26 No. 1, 2019
pp. 277-292
Emerald Publishing Limited
1359-0790
DOI 10.1108/JFC-10-2017-0095

increase on a global scale (ACCC, 2016; NFA, 2013; ONS, 2016a,2016b Whitty, 2015a, Whitty and Buchanan, 2012). In the UK in 2016, it was reported in the England and Wales Crime Survey that citizens are 10 times more likely to be robbed while at their computer by a criminal based overseas than to fall victim of traditional theft (ONS, 2016a). In 2015, Australians lost over AU$229m to scams, with 105,200 scam complaints. This amount was a 15 per cent increase from 2014. The National Fraud Authority (NFA, 2013) in the UK estimated that fraud costs in the UK equate to over £52bn a year.

Of further concern to the numbers of overall victims, is the number of victims who become 'repeat victims' of cyber-frauds. In 2016, the Office for National Statistics reported that in the UK 16 per cent of fraud victims became re-scammed within the same 12-month crime reference period (ONS, 2016a). In a representative sample of 2,000 UK adults, it was found that in 2012, approximately 800,000 UK adults were defrauded by cyber-frauds in the UK and about a quarter (26 per cent) of these victims were repeat victims during their lifetime (Whitty, 2015a). Understanding why people are repeatedly scammed online is critical, given that these victims often suffer both financial and psychological harms (Button, *et al.*, 2014; Whitty, 2015a; Whitty and Buchanan, 2016). By studying one-off and repeat victims of cyber-frauds, we might be able to develop methods to substantially reduce the rates of this particular crime.

The research presented in this paper draws from psychological and criminological theories to examine the predictors of cyber-fraud victimhood. In particular, the research focusses on psychological and socio-demographic characteristics and online behaviours that might place individuals at risk of becoming a victim of a cyber-fraud. In addition, the work examines whether there are dispositional and/or behavioural differences between one-off and repeat victims.

1.1 Victims' psychological profile

There has been some speculation about the distinctive psychological characteristics of fraud victims, in general. Titus and Gover (2001) believe that victims of fraud are more likely to be: co-operative, greedy, gullible/uncritical, careless, susceptible to flattery, easily intimidated, risk takers, generous, hold respect for authority and are good citizens. Fischer, Lea and Evans (2013), found in their survey research that scam victims or near scam victims were more affected by the high values offered in scams and displayed a high degree of trust in the scammers. Holtfreter *et al.* (2008) found that self-control is a significant predictor of victimisation. Buchanan and Whitty (2014) found in their research on romance scams that individuals with a higher tendency towards idealisation of romantic partners were more likely to be scammed. Whitty (2013) has theorised that romance scam victims are addicted to the scam. Whilst more research is needed in this area, the current work suggests some merit in considering whether personal dispositions predict cyber-fraud victimhood. The first hypothesis is as follows:

H1. Victims of cyber-frauds are likely to significantly differ on psychological characteristics compared with non-victims of cyber-frauds.

Drawing from the previous literature on scamming compliance behaviour and the research on behaviours related to certain personality dispositions, the following psychological characteristics were examined: impulsivity, *locus* of control and addictive disposition. Impulsivity was examined given that much of the literature that theorises why individuals become defrauded highlights the use of the scarcity tactic used by criminals and their push for urgency to respond to a crisis (Lea, *et al.*, 2009; Whitty, 2013). Victims of scams, therefore, might be more likely to respond to pushes to respond quickly without checking facts and be pulled into sensational narratives (e.g. handsome military soldiers, stuck in war torn areas). A subset of the first hypothesis is:

H1a. Victims of cyber-frauds are likely to score higher on measures of impulsivity compared with non-victims.

Locus of control refers to an individual's belief about control over his/her environment. People who have an internal *locus* of control have the conviction that events are contingent upon one's behaviour. Those with an external *locus* of control believe that events do not depend upon their actions, but rather upon luck, chance, or fate (Rotter, 1966). If individuals believe that they have little control over events, they might be more likely to comply with a scammer. A subset of the first hypothesis is:

H1b. Victims of cyber-frauds are likely to score higher on measures of external *locus* of control compared with non-victims.

There has been some theorising that individuals get 'caught up in a scam' do so because they are addicted to the scam itself and the visceral response they experience from the involvement in the scam (Whitty, 2013; Whitty, 2015b). Addictive disposition was therefore considered important to investigate in this research. A subset of the first hypothesis is:

H1c. Victims of cyber-frauds are likely to score higher on measures of addiction compared with non-victims.

1.2 Victims' socio-demographic profile

With respect to socio-demographic characteristics, such as age and education of fraud victims, in general, the literature is fairly sketchy, with much of the research focussing on the elderly given that it is presumed they are more at risk (ACCC, 2016; Bolimos and Choo, 2017; James, *et al.*, 2014; Oliver, *et al.*, 2015; ONS, 2016c; Titus and Gover, 2001). Those who report cyber-frauds tend to be older (ACCC, 2016) and there is a view that those who are uneducated are more likely to be scammed (Titus and Gover, 2001), although empirical research is needed to support this belief. The second hypothesis is:

H2. Victims of cyber-frauds are likely to significantly different on the socio-demographic characteristics compared with non-victims of cyber-frauds.

H2a. Older people are more likely to become victims of cyber-frauds compared with younger people.

H2b. Less educated people are more likely to become victims of cyber-frauds compared with more educated people.

1.3 Routine activity theory

The premise of routine activity theory, first proposed by Cohen and Felson (1979), is that crime is unaffected by social causes, such as poverty and inequality. Proponents of this theory argue that individuals become victims of crime because they participate in 'high risk' activities or behaviours in the absence of capable guardianship and in the company of motivated offenders (Farrell, Phillips and Pease, 1995; Turanovic and Pratt, 2014).

According to this theory, opportunity is the root cause of victimisation. Victims of burglary, for instance, are encouraged to change their locks and add alarm systems to decrease their chances of becoming burgled a second time.

There are a few studies that have examined the relationship between online activities and cyber-fraud. Hutchings and Heyes (2009), drawing from a very small sample, found that computer use was a significant predictor of receiving a phishing email. Pratt *et al.* (2010) examined whether demographic characteristics (e.g. age, gender, education, marital status) and online routines (hours spent online and Internet web site purchases) increase people's exposure to scams. They 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. Psychological characteristics, however, were not considered in their study. Moreover, the likelihood that a victim would be taken in by these scams was not considered. In more recent research, 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. He also found that online guardianship was positively related to victimisation but in the opposite direction to what he predicted. For example, Reyns found that individuals who installed anti-virus software where more likely to become a victim of a phishing attack, although he suspects the reason for this finding was a temporal ordering problem (i.e. the participants in his sample may have installed the software as a consequence of being phished). Therefore, although Reyns' results were mixed, the findings suggest there is a need to further investigate the relationship between online behaviours and online victimisation.

Overall, research findings therefore highlight that online routine activities are important to investigate when examining cyber-fraud victimisation. Drawing from previous research the online risky activities this study focussed on included: instant messaging, positing pictures, posting messages, streaming media, online shopping and online banking. It was reasoned that engaging in these activities might increase the likelihood that a user is likely to encounter a scam or provide personal information for scammers to use against that user, thereby increasing a person's chances of being scammed. In addition, an item on online guardianship was included (visiting online sites for consumer advice, e.g. scammer alert advice). The third and fourth hypotheses are:

H3. Victims of cyber-frauds are likely to significantly differ on their frequency in engaging on online activities compared with non-victims of cyber-frauds.

H4. Victims of cyber-frauds are less likely to engage in online guardianship behaviours compared with non-victims of cyber-frauds.

1.4 Repeat victims

There is a body of academic literature on repeat victims, which has mostly focussed on crimes, such as: burglary, theft, domestic violence, and child sexual abuse (Farrell and Pease, 2001; Farrell *et al.*, 1995; Grove *et al.*, 2012). Broadly, theorists argue that repeat victimisation occurs because of one or more of the following: predisposing personal characteristics; situational risk factors; and the criminals or connected co-offenders return to the same victims once learning they are a suitable target (Farrell *et al.*, 1995; Farrell and

Pease, 2001; Lantz and Ruback, 2015). Whitty (2015a) has reported that about a quarter of cyber-fraud victims are scammed at least twice. This proportion of repeat victims suggests an urgent need to also understand why some cyber-fraud victims continue to be victimised by subsequent cyber-frauds. The empirical literature, to date, provides few clues as to why some victims learn their lessons and others move on to become victims of other cyber-frauds. The fifth and final hypothesis is that repeat victims of cyber-frauds are like to significantly differ on psychological and social characteristics, online behaviours and online guardianship behaviours compared with one-off victims.

2. Method

2.1 Participants

Overall, 12,060 participants who resided in the UK were recruited from a random sample from a paid panel organised by Qualtrics (a well-established company, often used by academics to recruit representative samples for online studies). Of these individuals, 11,780 participants remained in the final sample. Individuals who were excluded: failed to complete the survey, provided repetitive or inappropriate responses to attention filler items, completed the survey more than once, or completed the survey in an usually short amount of time. In this final sample 10,723 participants were non-victims, 728 were one-off victims and 329 were repeat victims. All participants stated that they had been exposed to an online scam online. The mean age of the sample was 48.5 years (*SD* = 16.3), ranging from 18-93 years. Overall, 37 per cent of the sample was men and 63 per cent women. With regard to the highest level of education achieved by participants: 1.4 per cent had a doctoral degree, 8.3 per cent had a master’s degree, 29.5 per cent had an undergraduate degree, 29.3 per cent had A levels, 27.6 per cent held GCSE qualification and 3.9 per cent had less than high school qualifications.

2.2 Materials

Data were collected using a questionnaire hosted on the Qualtrics online survey platform. The questionnaire consisted of personality inventories and items devised to measure demographic descriptive data, routine activities and online guardianship behaviours. Those who had been scammed were also asked to describe the type of cyber-fraud/s they has been tricked by and as a consequence lost money. Impulsivity was measured using the UPPS-R Impulsivity Scale (Whiteside and Lynam, 2001). The 45-item scale measures a person’s tendency to act on whim, displaying behaviours characterised by little forethought or consideration of the consequences of their actions. The scale comprises four subscales: lack of premeditation (11 items), urgency (12 items), sensation seeking (12 items) and lack of perseverance (10 items). Possible scores range from 11 to 44 for the lack of premeditation subscale, from 12 to 48 for both the urgency and sensation seeking subscales, and from 10 to 40 for the lack of perseverance subscale. A lower score indicates low impulsivity for that dimension. In the current study, all of the subscales demonstrated good internal consistency (Cronbach’s alpha = 0.86, 0.91, 0.89, 0.83 for lack of premeditation, urgency, sensation seeking and lack of perseverance, respectively).

Locus of control was measured using the Internal-External Locus of Control scale (Rotter, 1966). The 29-item scale measures a person’s general tendency for an internal or external *locus* of control. For each item on the scale, participants indicate which of two statements they agree with most. Possible scores range from 0 to 23, with a lower score indicating a more internal *locus* of control insofar as a participant believes that everyday events are contingent on his or her own behaviour. In the current study, the study demonstrated acceptable internal consistency (Cronbach’s alpha = 0.65).

Addictive disposition was measured using the Eysenk Personality Questionnaire (EPQ-A). Acceptable internal consistency was obtained for this scale (Cronbach's alpha = 0.68). There are 32 dichotomous items in the EPQ-A scale, with possible scores ranging from 0 to 32. A high score equates with high addictive disposition.

Routine activities included items on frequency of the following online activities: Instant messaging, posting pictures, posting messages, streaming media, shopping online and banking online. Participants were also asked a question on online guardianship: how frequently they viewed consumer advice sites, for example, fraud alerts, *Which?* magazine). For each of these items participants were presented with five-point Likert scales with 1 = never and 5 = several times a day. Non-victims were asked to answer these questions considering the past six months, one-off victims were asked to consider six months prior to the scam and repeat victims were asked to answer six months prior to the last scam they were taken in by.

An exploratory Factor Analysis was performed on all routine activities items, except for the online guardianship question. Before subjecting the scale to principle axis factoring the data were assessed to ensure suitability for analysis and it was found that none of the assumptions were violated. The Kaiser-Meyer-Olken measure of sampling adequacy was 0.75 which exceeded the recommended lowest value of 0.6. The Barlett's Test of Sphericity also reached statistical significance, supporting the factorability of the correlation matrix. Principal axis factoring revealed the presence of two components with eigenvalues exceeding 1. Together they accounted for 60.71 per cent of the total variance (42.86 per cent and 17.85 per cent, respectively). Inspection of the scree plot confirmed two factors. Direct Oblimin separated these components obliquely, which allows for the possibility of intercorrelation among factors. All items exceeded loadings of 0.4, and therefore, they were all considered for further analysis. The rotated factor solution took four iterations to produce and is reported in Table I. Factor 1 was labelled *Exposing online activities* and Factor 2 was labelled *Risky online spaces*. Factor-based scales were generated by obtained regression scores.

2.3 Procedure

Participants were recruited via a Qualtrics online panel. Qualtrics recruited a random sample from its large panel of UK participants. Participants were asked to complete a series of socio-demographic questions (e.g. age, gender, education), personality items (e.g. impulsivity, *locus* of control, addiction disposition) and whether they had been scammed by a cyber-fraud. Participants were all asked a series of questions about routine activities and whether they had ever come across a cyber-scam. They were also asked if they had been

Table I.
Factor pattern matrix

Items	Factor 1 (eigenvalue) Exposing online activities (2.571)	Factor 2 (eigenvalue) Risky online spaces (1.071)
How often do you use Instant messaging	*0.819*	−0.145
How often do you post pictures online	*0.807*	0.005
How often do you stream media (movies, music, etc.)	*0.507*	0.125
How often do you post messages online	*0.416*	0.176
How often do you shop online	−0.024	*0.737*
How often do you conduct online banking	0.042	*0.422*

defrauded by more than one cyber-fraud. They were also asked questions about the type of cyber-fraud.

3. Results

3.1 Bivariate associations

Bivariate associations between the independent variables were first examined (see Table II). Most correlations were moderate to low. Correlations of note include those between: age and exposure online (Pearson's $r = -0.533$), urgency and addiction (Pearson's $r = 0.497$), exposure online activities and risky online spaces (Pearson's $r = 0.617$), and risky online spaces and online guardianship (Pearson's $r = 0.433$). Unsurprisingly, many of the correlations between subsets of impulsivity were moderate and ranged from Pearson's $r = -0.290$ to 0.497.

3.2 Relationship between personality and socio-demographic characteristics with routine activities

First, statistically significant relationships between personality (impulsivity, *locus* of control and addictive disposition) and socio-demographic characteristics (age, gender and education) with routine activities (exposing online activities, risky online places and online guardianship) were investigated.

Prior to running the analysis it was found that the assumptions were met to run simultaneous forced entry multiple regressions. It is also noted that there were no issues with multicollinearity given that VIF levels were less than 2. The total variance of the model examining exposing online activities was 34.5 per cent, $F(9, 11700) = 689.54$, $p < 0.001$ (see Table III). The total variance of the model explaining risky online spaces was 15.1 per cent, $F(9, 11700) = 232.08$, $p < 0.001$ (Table IV). The total variance of the model explaining 'online guardianship' was 7 per cent, $F(9, 11700) = 99.524$, $p < 0.001$ (Table V).

As shown in the tables these findings demonstrate that psychological and socio-demographic characteristics are associated with routine activities. Notably, younger people were more likely to engage in routine activities that potentially expose them to cyber-frauds and older people were more likely to engage in online guardianship behaviours. Educated people were more likely to engage in routine activities that potentially expose them to cyber-frauds and were more likely to engage in online guardianship behaviours. Those who scored higher on the impulsivity sub-scales urgency and sensation seeking, and high on addiction were more likely to engage in routine activities that potentially expose them to cyber-frauds and were more likely to engage in online guardianship behaviours. In contrast, those who scored low on the impulsivity subscale, lack of perseverance, and low on external *locus* of control were more likely to engage in routine activities that potentially expose them to cyber-frauds and were more likely to engage in online guardianship behaviours.

3.3 Predictors of cyber-fraud victimhood

H1-4 were next examined. Given that a statistical relationship was revealed for personality, socio-demographic variables and routine activities, these were initially considered in separate models before considering them in a combined model. Three binary logistic regressions models were therefore conducted (Tables VI-VIII). Given gender was found to be a weak predictor of routine activities and there were no gender hypotheses developed to predict victimhood, gender was not examined in these models. Model 1 examined the psychological characteristics examined in the previous regression analyses with the exception of gender. Model 2 examined the routine activities examined in the previous

Table II.
Pearson two-tailed correlations between predictor variables

	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.
1. Age	1.00	−0.156**	−0.075**	−0.290**	−0.355**	−0.119**	−0.133**	−0.311**	−0.533**	−0.288**	−0.044**
2. Education		1.00	−0.045**	−0.048**	0.169**	−0.081**	−0.112**	−0.068**	0.145**	0.202**	0.174**
3. Lack of premed.			1.00	0.317**	0.128**	0.486**	0.090**	0.052**	0.091**	0.016	−0.021*
4. Urgency				1.00	0.232**	0.338**	0.241**	0.497**	0.305**	0.206**	0.104**
5. Sensation seeking					1.00	−0.103**	−0.112**	0.097**	0.358**	0.253**	0.181**
6. Lack of persev.						1.00	0.228**	0.159**	0.051**	−0.018**	−0.044**
7. Locus of control							1.00	0.287**	0.022*	−0.024**	−0.078**
8. Addiction								1.00	0.272**	0.142**	0.023*
9. Exposure online									1.00	0.617**	0.287**
10. Risky places										1.00	0.433**
11. Guardianship											1.00

Notes: *$p < 0.05$; **$p < 0.01$

regression analyses. Model 3 was the saturated model, which included both psychological characteristics and routine activities.

Model 1 was significant, with a good fit to the data, [χ^2(8, N = 11,780) = 536.90, $p <$ 0.001] (Nagelkerke R^2 = 0.098). Model 2 was significant, with a good fit to the data [χ^2(3, N = 11,780) = 395.80, p < 0.001] (Nagelkerke R^2 = 0.073). Model 3 was significant, with an improved fit to the data [χ^2(11, N = 11,780) = 685.05, p <0.001] (Nagelkerke R^2 = 0.125). Notably, all predicator variables were significant in all models, with the exception of lack of perseverance. The saturated model was a better fit and none of the psychological characteristics dropped out of the model. Furthermore, although the predictors, education, lack of perseverance, *locus* of control and guardianship were significant, they were in the opposite direction to what was hypothesised.

Finally, any differences between one-off victimhood and repeat victimhood were examined. This was carried out using a multinominal logistic regression, including both psychological characteristics and routine activities in the model, with one-off victimhood as the reference category (Table IX). The model was significant, χ^2(22, N = 11,780) = 727.28, p < 0.001), (Nagelkerke R^2 = 0.117). When considering non-victims and one-off victims, most of the predictor variables were significant with the exception of lack of perseverance. Furthermore, although the predictors, education, lack of premeditation, *locus* of control and online guardianship were significant, they were in the opposite direction to what was

Variables	*B*	*SE*	*β*	*t*	*p*
Constant	0.004	0.069		0.051	0.959
Age	−0.023	0.000	−0.413	−46.744***	0.000
Gender	−0.030	0.015	−0.016	−1.992*	0.046
Education	0.048	0.006	0.057	7.413***	0.000
Lack of premed.	0.003	0.002	0.016	1.818	0.069
Urgency	0.017	0.001	0.130	13.552***	0.000
Sensation seeking	0.018	0.001	0.155	17.380***	0.000
Lack of persev.	−0.006	0.002	−0.029	−3.091**	0.002
Locus of control	−0.013	0.002	−0.061	−7.508***	0.000
Addiction	0.016	0.002	0.077	8.444***	0.000

Notes: *p < 0.05; **p < 0.01; ***p < 0.001

Table III. Predictors of ‘exposing online activities’

Variables	*B*	*SE*	*β*	*t*	*p*
Constant	−4.23	0.069		−6.106***	0.000
Age	−0.009	0.000	−0.185	−18.422***	0.000
Gender	0.021	0.015	0.013	1.420	0.156
Education	0.112	0.006	0.153	17.384***	0.000
Lack of premed.	−0.005	0.002	−0.029	−2.804**	0.005
Urgency	0.018	0.001	0.158	14.493***	0.000
Sensation seeking	0.012	0.001	0.114	11.203***	0.000
Lack of persev.	−0.009	0.002	−0.049	−4.609***	0.000
Locus of control	−0.009	0.002	−0.049	−5.284***	0.000
Addiction	0.005	0.002	0.027	2.633**	0.008

Notes: *p < 0.05; **p < 0.01; ***p < 0.001

Table IV. Predictors of ‘risky online spaces’

hypothesised. When considering one-off victims and repeat victims very little separated these groups, except for online guardianship, which was in the opposite direction to what was predicted.

4. Discussion

Cyber-fraud is a crime that is on the increase, and one that affects digital technology users across the globe. This research found that all participants in this sample had been exposed to a cyber-fraud at some point in their lives and 7 per cent of the sample had lost money to a cyber-fraud – giving weight to the importance of this investigation. There is a scant amount

Table V. Predictors of 'online guardianship'

Variables	*B*	*SE*	*β*	*t*	*p*
Constant	1.16	0.096		12.133***	0.000
Age	0.003	0.001	0.052	4.964***	0.000
Gender	0.014	0.021	0.006	0.664	0.506
Education	0.149	0.009	0.154	16.719***	0.000
Lack of premed.	−0.013	0.002	−0.059	−5.532***	0.000
Urgency	0.020	0.002	0.135	11.842***	0.000
Sensation seeking	0.019	0.001	0.142	13.350	0.000
Lack of persev.	−0.003	0.003	−0.013	−1.196	0.232
Locus of control	−0.015	0.002	−0.060	−6.157***	0.000
Addiction	−0.002	0.003	−0.007	−0.625	0.532

Notes: $*p < 0.05$; $**p < 0.01$; $***p < 0.001$

Table VI. Model 1: Binary logistic regression for psychological characteristics and victimhood

Variable	*β*	SE	Wald	df	*p*	Exp *β*
Constant	−6.58	0.350	352.49***	1	0.000	0.001
Age	0.012	0.002	24.89***	1	0.000	1.012
Education	0.227	0.031	52.53***	1	0.000	1.255
Lack of premed.	−0.036	0.008	19.71***	1	0.000	0.965
Urgency	0.057	0.006	94.82***	1	0.000	1.059
Sensation seeking	0.042	0.005	77.14***	1	0.000	1.043
Lack of persev.	0.014	0.009	2.354	1	0.125	1.014
Locus of control	−0.038	0.009	18.70***	1	0.000	0.962
Addiction	0.071	0.009	56.17***	1	0.000	1.073

Notes: $*p < 0.05$; $**p < 0.01$; $***p < 0.001$

Table VII. Model 2: Binary logistic regression for routine activities and victimhood

Variable	*β*	SE	Wald	df	*p*	Exp *β*
Constant	−3.119	0.093	1122.78***	1	0.000	
Exposure online	0.329	0.047	47.94***	1	0.000	1.389
Risky places	0.245	0.057	18.64***	1	0.000	1.278
Guardianship	0.277	0.034	66.081***	1	0.000	1.319

Notes: $*p < 0.05$; $**p < 0.01$; $***p < 0.001$

of available literature that has examined who is more likely to be taken in by cyber-frauds and which online behaviours (if any) might place individuals at greater risk of becoming scammed. This paper moves the research forward by developing a susceptibility theoretical framework based on empirical research that uncovers key findings into the psychological and socio-demographic characteristics and online behaviours of cyber-fraud victims.

4.1 Susceptibility theoretical framework

Much of the previous research on cyber-fraud (of which there are still few studies) has focussed on the types of people and the routine activities of those who are *targeted* (Pratt *et al.*, 2010). Research that has examined predictors of victimhood has typically considered personal dispositions (Buchanan and Whitty, 2014) or routine activities (Reyns, 2015) in isolation. The work here demonstrates that a susceptibility to cyber-fraud framework needs to include: personality and socio-demographic characteristics, exposing online activities, risky online spaces and online guardianship behaviours. Combining psychological theories of individuals' differences and criminological theories of routine activities is essential if scholars are to further their understandings of why individuals are tricked by cyber-scams as well is in the development of methodologies to prevent these types of crimes.

This study found that most of the psychological characteristics predicted online routine activities – both risky activities and online guardianship activities. However, although certain types of people are more likely to place themselves at risk and protect themselves (which in itself is important to understand), the saturated model found that both psychological characteristics and routine activities are important to consider when predicting victimhood. Therefore, it is proposed here that a predictive model for cyber-fraud victimhood needs to include socio-demographic characteristics, personality traits and online routine behaviours.

Most of the predictor variables proposed in this study were significant; however, they were not all significant in the direction hypothesised. The research supported the hypotheses that age, some of the impulsive sub-categories (urgency and sensation seeking), addiction and the risky online behaviours (exposure and risky places) significantly predicted victimhood. Significant predictors in the opposite direction to what was predicted included: education, lack of premeditation, *locus* of control and online guardianship behaviours.

Table VIII.
Model 3: Saturated binary logistic regression for psychological characteristics, routine activities and victimhood

Variable	β	SE	Wald	df	p	Exp β
Constant	−6.779	0.359	356.65***	1	0.000	0.001
Age	0.018	0.003	48.34***	1	0.000	1.019
Education	0.165	0.032	25.91***	1	0.000	1.179
Lack of premed.	−0.030	0.008	13.89***	1	0.000	0.970
Urgency	0.045	0.006	56.05***	1	0.000	1.046
Sensation seeking	0.031	0.005	37.97***	1	0.000	1.031
Lack of persev.	0.017	0.009	3.608	1	0.058	1.017
Locus of control	−0.029	0.009	10.54**	1	0.001	0.971
Addiction	0.064	0.010	44.91***	1	0.000	1.066
Exposure online	0.269	0.055	23.54***	1	0.000	1.309
Risky places	0.133	0.058	5.25*	1	0.022	1.142
Guardianship	0.207	0.035	34.13***	1	0.000	1.230

Notes: *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$

Table IX. Multinominal logistic regression: Reference group = one-off victim

Variable	β	SE	Wald	df	p	Exp β
Repeat						
Intercept	−2.289	0.717	10.187***	1	0.001	
Age	−0.004	0.005	0.678	1	0.410	0.996
Education	−0.020	0.065	0.098	1	0.754	0.980
Lack of premed.	−0.002	0.016	0.011	1	0.916	0.998
Urgency	0.019	0.012	2.394	1	0.122	1.019
Sensation seeking	0.014	0.010	1.938	1	0.164	1.014
Lack of persev.	0.015	0.018	0.715	1	0.398	1.015
Locus of control	−0.015	0.018	0.680	1	0.410	0.985
Addiction	0.002	0.019	0.012	1	0.911	1.002
Exposure online	0.214	0.114	3.510	1	0.061	1.238
Risky places	−0.181	0.113	2.587	1	0.108	0.834
Guardianship	0.208	0.072	8.298***	1	0.004	1.232
Non-victim						
Intercept	6.720	0.415	261.753***	1	0.000	
Age	−0.020	0.003	40.560***	1	0.000	0.981
Education	−0.170	0.037	20.703***	1	0.000	0.843
Lack of premed.	0.029	0.010	9.474**	1	0.002	1.030
Urgency	−0.040	0.007	31.685***	1	0.000	0.961
Sensation seeking	−0.026	0.006	20.800***	1	0.000	0.974
Lack of persev.	−0.012	0.011	1.394	1	0.238	0.988
Locus of control	0.024	0.010	5.481*	1	0.019	1.025
Addiction	−0.063	0.011	32.220***	1	0.000	0.939
Exposure online	−0.208	0.065	10.344**	1	0.001	0.813
Risky places	−0.182	0.067	7.322**	1	0.007	0.833
Guardianship	−0.145	0.041	12.362***	1	0.000	0.865

Notes: *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$

The explanation for why educated people are more likely to be scammed by these types of scams might be explained in a number of ways. Although education was significant in the saturated model where routine activities were also included (meaning that education still made a significant contribution to the model in spite of this variable significantly predicting routine activities) it might be that there are other online routine activities that educated people engage in that place them at risk that were not considered in the research (van Deursen and Dijk, 2014; Estacio *et al.*, 2017, in press, for a discussion on how educated people use the Internet differently compared with less educated people). An alternative explanation can be offered by drawing from the work of Lea *et al.* (2009). Lea and colleagues theorised that overconfidence in the ability to recognise scams places people at greater risk of becoming scammed as they hold a ‘belief of invulnerability’. Educated people might be more likely to be more likely to hold the view that they can spot a scam, and thereby spend less efforts seeking out persuasion and deception cues.

Counter to the hypotheses, those who were more likely to be premeditative and have a high internal *locus* of control were more likely to be scammed. Although this finding is counter-intuitive, this suggests that cyber-fraud victims do not recognise the control others might have over them and as a consequence are pulled into a scam – with the false belief that they are in control. These findings might also suggest that spending time considering one’s actions online is not, in itself, protective. Further research might consider which cues individuals' believe signal a scam and whether individuals are able to correctly discern authentic material from scammer material (e.g. profiles, advertisements, emails).

Perhaps the most interesting and important finding here is that online guardianship behaviours did not protect individuals from becoming scammed. In fact, the opposite finding was revealed in this study with one-off victims more likely to engage in online guardianship behaviours compared with non-victims and repeat victims more likely to engage in guardianship behaviours compared with one-off victims. The finding might be interpreted in a number of ways. Engaging in online guardianship behaviours might be exposing individuals more to scams/scammers and/or the sites that present information on how to protect individuals from scams does not communicate this information effectively. This final point is not trivial, given the criticisms that are often made of fraud information sites. As Sasse and Smith (2016) contend, useful cybersecurity advice needs to be both correct and actionable. Moreover, given that, as this study found, victims are typically impulsive, information might need to be written succinctly so that users can easily and quickly digest the details needed to change their behaviours. It might be useful to provide more engaging and interactive advice to capture and hold users' attention.

When considering repeat victimisation it is noteworthy that there were no significant distinguishing psychological or socio-demographic characteristics between one-off victims and repeat victims. In this sample, 45 per cent of cyber-fraud victims were repeat victims. This finding highlights an urgent need to develop effective preventative strategies for this group. Alarmingly, the only variable that predicted whether someone was a repeat or a one-off victim was their likelihood to read e-safety websites. Although more research is needed to understand this finding – at face value, at least, this suggests that e-safety websites need to improve on the content and possibly presenting of information placed on these sites.

5. Conclusion

The findings in this paper provide new insights into the types of people and routine behaviours that place individuals at greater risk of becoming scammed. The work here suggests that any approach to preventing scam victimhood needs to consider: socio-demographic, personality and routine activities together and that a routine activity approach or personality approach alone is not sufficient.

The work here has implications for the design of websites (e.g. shopping sites, dating sites etc.). Given that victims tend to be those who score high on urgency and sensation seeking – safer guards might be built into the design where users are forced to carry out their own checks (and/or the sites carry out further checks) prior to: engaging with someone on the site to date, discuss a job opportunity, purchase an item, etc. Moreover, advice on these sites needs to be upfront, easily accessible and provide useful and correct advice.

There are some important policy implications that governments should consider as a result of this study. The findings here suggest that government and other educational sites built to prevent scams are a hindrance rather than helpful. As previous research has found (Junger *et al.*, 2017), priming and warnings are not also effective to prevent social engineering attacks and so work is urgently needed on how to improve cyber security educational websites. Developers need to be mindful that their cites need to cater for a range of different types of users, using effective messaging and visualisations (Moreno-Fernández *et al.*, 2017). Moreover, given that impulsive individuals are more susceptible to becoming scammed, information needs to be concise, easily accessible, engaging and actionable. Simply informing users that particular scams exist might not change cybersecurity behaviour and instead sites might give practical advice on what users need to do to protect themselves, which cues to pay attention to that might indicate a scam, what checks are required and how to go about conducting these checks.

In conclusion, this research provides important evidence that supports the notion that socio-demographics and psychological characteristics and routine activities predict victimhood. Future research might examine routine activities in greater detail and might examine the ways individuals go about discerning between authentic and disingenuous scammer content.

References

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

Bolimos, I.A. and Choo, K.-K.R. (2017), "Online fraud offending within an Australian jurisdiction", *Journal of Financial Crime*, Vol. 24 No. 2, pp. 277-308.

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

Button, M., Lewis, C. and Tapley, J. (2014), "Not a victimless crime: the impact of fraud on individual victims and their families", *Security Journal*, Vol. 27 No. 1, pp. 36-54.

Cohen, L. and Felson, M. (1979), "Social change and crime rate trends: a routine activity approach", *American Sociological Review*, Vol. 44 No. 4, pp. 588-608.

Estacio, E.V., Whittle, R. and Protheroe, J. (2017), in press, "The digital divide: examining the socio-demographic factors associated with health, literacy, access and use of the internet to seek health information", *Journal of Health Behavior*.

Farrell, G. and Pease, K. (2001), "Editors' introduction: why repeat victimization matters", in Farrell G. and Pease K. (Eds), *Repeat Victimisation: Crime Prevention Studies*, Criminal Justice Press, Vol. 12, No. 14, pp. 1-4.

Farrell, G., Phillips, C. and Pease, K. (1995), "Like taking candy: why does repeat victimization occur?", *The British Journal of Criminology*, Vol. 35 No. 3, pp. 384-399.

Fischer, P., Lea, S.E.G. and Evans, K.M. (2013), "Why do individuals respond to fraudulent scam communication and lose money? The psychological determinants of scam compliance", *Journal of Applied Social Psychology*, Vol. 43 No. 10, pp. 2060-2072.

Grove, L., Farrell, G., Farrington, D.P. and Johnson, S.D. (2012), "Preventing repeat victimization: a systematic review", Brottsförebyggande Rådet/The Swedish National Council for Crime Prevention.

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.

James, B.D., Boyle, P.A. and Bennett, D.A. (2014), "Correlates of susceptibility to scams in older adults without dementia", *Journal of Elder Abuse and Neglect*, Vol. 26, pp. 107-122.

Junger, M., Montoya, L. and Overink, F.J. (2017), "Priming and warnings are not effective to prevent social engineering attacks", *Computers in Human Behavior*, Vol. 66, pp. 75-87.

Lantz, B. and Ruback, B. (2015), "A networked boost: burglary co-offending and repeat victimization using a network approach", *Crime and Delinquency*, Vol. 63 No. 9, pp. 1066-1090.

Lea, S.E.G. Fischer, P. and Evans, K.M. (2009), "The psychology of scams: provoking and committing errors of judgement, report for the office of fair trading", available at: www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf

Moreno-Fernández, M.M., Blanco, F., Garaizar, P. and Matute, H. (2017), "Fishing for phishers. Improving internet users' sensitivity to visual deception cues to prevent electronic fraud", *Computers in Human Behaviour*, Vol. 69, pp. 421-436.

NFA (2013), "Annual fraud indicator", available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf

Oliver, S., Burls, T., Fenge, L. and Brown, K. (2015), "'Winning and losing'": vulnerability to mass marketing fraud", *The Journal of Adult Protection*, Vol. 17 No. 6, pp. 360-350.

ONS (Office for National Statistics) (2014), "Highest levels of qualification across England and Wales", available at: http://webarchive.nationalarchives.gov.uk/20160105160709/http://www.ons.gov.uk/ons/rel/census/2011-census-analysis/local-area-analysis-of-qualifications-across-england-and-wales/info-highest-qualifications.html

ONS (Office for National Statistics) (2016a), "Overview of fraud statistics: year ending march 2016", available at: www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016

ONS (Office for National Statistics) (2016b), "Percentage of incidents of fraud and computer misuse reported to action fraud, and reasons for not reporting incidents to action fraud, year ending september 2016 CSEW (Experimental statistics)", available at: www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/adhocs/006626percentageofincidentsoffraudandcomputermisusereportedtoactionfraudandreasonsfornotreportingincidentstoactionfraudyearendingseptember2016csewexperimentalstatistics

ONS (Office for National Statistics) (2016c), "Overview of the UK population: February 2016", available at: www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/articles/overviewoftheukpopulation/february2016

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.

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.

Rotter, J.B. (1966), "Generalized expectancies for internal versus external control of reinforcements", *Psychological Monographs*, Vol. 80 No. 1, pp. 1-28.

Sasse, A. and Smith, M. (2016), "The security-usability tradeoff myth", *IEEE Security and Privacy*, Vol. 14 No. 5, pp. 11-13.

Titus, R.M. and Gover, A.R. (2001), "Personal fraud: the victims and the scams", in Farrell G. and Pease K. (Eds), *Repeat Victimisation: Crime Prevention Studies*, Criminal Justice Press, Vol. 12, pp. 133-151.

Turanovic, J.J. and Pratt, T.C. (2014), "Can't stop, won't stop: self-control, risky lifestyles, and repeat victimization", *Journal of Quantitative Criminology*, Vol. 30 No. 1, pp. 29-56.

van Deursen, A.J.A.M. and van Dijk, J.A.G.M. (2014), "The digital divide shifts to differences in usage", *New Media and Society*, Vol. 16 No. 3, pp. 507-526.

Whiteside, S.P. 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.

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. (2015a), "Mass-marketing fraud: a growing concern", *IEEE Security and Privacy*, Vol. 13 No. 4, pp. 84-87.

Whitty, M.T. (2015b), "Anatomy of the online dating romance scam", *Security Journal*, Vol. 28 No. 4, pp. 443-455.

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

About the author

Professor Monica T. Whitty holds two Chairs in Human Factors in CyberSecurity (The University of Melbourne and The University of Warwick). She is the author of over 100 publications, including *Cyberpsychology: the study of individuals, society and digital technologies* (2017, Wiley). She is a psychologist and her work focusses on cyber crime and cyber security. In the past 15 years, examples of her projects include DAPM: Detecting and Preventing Mass-Marketing Fraud (EPSRC); UNDERWARE: UNDERstanding West African culture to pRevent CybercrimEs (NSCS); Cyber Insider Threat Detection (GCPD); An examination of the online romance scam (ESRC); and An exploration of Superidentity (EPSRC). Monica T Whitty can be contacted at: monica.whitty@unimelb.edu.au