International Journal of Future Generation Communication and Networking
Vol. 13, No. 2, (2020), pp. 32 - 44

An Analysis of Psychology of Advance Fee Fraud Victimization – A Systematic Overview

Jalindar R. Gandal

Asst.Professor, Dr. D.Y.Patil School of MCA -Pune-05,

Dr. R.G.Pawar

Principal, SVPM's College of Commerce, Science & Computer Education,

Malegaon, Tal - Baramati, Dist – Pune

Abstract

Now a day's advance fee fraud on the internet is a current widespread that degenerates in hundreds of millions of dollars per year. Existing theories of fraud provides how criminals target and exploit people in the online environment .Systematic review will provide a timely mixture of the psychologically based literature to establish the key theories and experiential research that promise to impact on advance fee fraud policies and operations.

Researcher findings have been listed that there is still lack of studies in the present literature about the information security in Cyber Crime environment .There is still an increasing need for comprehensive but specific approaches to cyber security aspects for effective management of information and low. Researcher has concluded that due to rapid advancement of e-commerce occurrences of advance fee fraud are increasing dramatically due to exposure of security weaknesses in traditional scam finding processing systems resulting in loss of billions of money every year. Researcher are also able to identify specific psychological processes associated with increased susceptibility to online fraud victimization was limited. Suggestions for future research and practical interventions are discussed.

Keywords – *Victimization, Phishing, Advance Fee Scam, Security Risks, Scam baiting.*

1. INTRODUCTION

Existing theories of fraud provide some insight into how criminals target and exploit people in the online environment .This systematic review will provide a timely synthesis of the leading psychologically based literature to establish the key theories and empirical research that promise to impact on advance fee fraud policies and operations. Relevant databases and websites were searched using terms related to psychology and fraud victimization. Despite a growing body of research, the total number of studies able to identify specific psychological processes associated with increased vulnerability to online fraud or advance fee fraud victimization was limited.

The FBI's Internet Crime Complaint Center (IC3) recently reported figures that show Internetenabled advance fee fraud and misuse being responsible for $2.7 billion in financial losses in 2019 (FBI 2019). The annual Internet Crime Report shows that IC3 received 451,936 complaints last year nearly 1200 per day. The most financially costly were matrimonial, lottery, business email compromise, romance or confidence fraud, and investment scams. Advance fee fraud also call as Internet-based fraud was the fastest growing crime in the India in 2015–2016, with 3.25 million victims each year and annual combined loss of £3.6

ISSN: 2233-7857 IJFGCN

billion (2016). Estimates indicate 4.7 million incidents of fraud and computer misuse were experienced by adults aged 16. Researcher provide a summary on the rising role of technology in perpetuating these crimes: It is estimated globally there are 29 billion spam emails daily and that the email virus rate is 1 in 196 and phishing emails are 1 in 392.

However, despite current efforts to teach individuals on the way in which criminals operate online, millions of these AFS activities from phishing attempts to 'lonely hearts' scams are responded to each year. For example, priming individuals with images of money has been shown to reduce helpfulness towards others and increase isolation in tasks involving new acquaintances. Similarly, financial decisions cause different structures to similar non-financial rewards (Knutson et al. 2000).When considering the committers of fraud, there is only limited data available. Even the law enforcement community does not always know the background of the perpetrators. Significantly, the existing fraud literature is limited in scope in terms of exploring the 'how' and the 'why' in precisely what way they influence individual decision-making processes? Thus, this systematic review aims to connect some of these methodological and conceptual links to establish how experiential and dispositional factors may influence an individual's cognitive processing associated.

1.1 PREVIOUS REVIEWS

There are a number of reviews in the wider online/consumer fraud area, although the focus for many is age as a risk factor. Nigerian Prince" scams are also known as "419 scams," a reference to the Nigerian penal code designed to deal with them. They are particularly difficult to prosecute for both Nigerian and foreign authorities. Victims are often too ashamed to pursue the case, and even when they do, the trail quickly goes cold.

In its earliest personifications, the scam involved someone claiming to be a Nigerian prince sending a target an email saying he desperately needed help smuggling wealth out of his country. All the target needed to do was provide a bank account number or send a foreign processing fee to help the prince out of a jam, and then he would show his gratitude with a generous kickback.

These scams really do appear to have begun in Nigeria, but they can now come from almost anywhere people posing as Syrian government officials is one the current favorites. Nevertheless, the "Nigerian Prince" moniker persists.

But today's 419 scams can involve dating websites, like the one that ensnared Maria Grette.

Wealthy orphans claiming to need an adult sponsor, lottery winners saying they're required to share their winnings with others, and inheritances trapped in banks due to civil war are also common ploys.

Reporter Erika Eichel berger spent time with Nigerian scam artists in 2017. She found them to be surprisingly forthcoming. She reported that most scammers tended to be ordinary people, such as university students or people working low-paying jobs, who discovered that they could make fabulously more money as much as $60,000 per year scamming. These scammers are sometimes referred to as "Yahoo Boys," because so many of them are young males and, at least in the early days, they frequently worked through Yahoo accounts.

In most cases, after establishing a connection and cultivating a relationship, the Yahoo Boys eventually get around to persuading their targets to provide their bank account or credit card information. They prefer to

ISSN: 2233-7857 IJFGCN

pursue 45-to-75-year-old widowed men and women. The thinking goes that this demographic is most likely to have money and be lonely – in other words, easy marks.

2. THEROTICAL CONCEPTS AND ISSUES

The majority of previous research conducted in this area predominantly focus on the credible influence of the scam message employed by the fraudster. The purpose of this systematic review is to extend that focus to integrate variables related to individual psychological differences, i.e. those which make people more vulnerable to be deceived by fraudulent communications (see Judges et al. 2017). Research by Modic and colleagues has highlighted individual differences to scam compliance through the lens of vulnerability to persuasion and wider theoretical links with social influence .The development of the Susceptibility to Persuasion scale has demonstrated good construct validity in relation to self-report scam acceptability across large samples. The second iteration measuring individual differences in a range of mechanisms, including impression seeking, risk preferences, and social impact.

Dispositional factors currently evaluated in the literature predominantly focus on demographic factors, such as age, gender, income, and education (Purkait et al. 2014), in conjunction with individual characteristics, such as low self-control. The application of Petty and Cacioppo's (1986) elaboration likelihood model (ELM) to explain how psychological mechanisms impact is common although few have applied this theoretical model to explore how dispositional factors influence an individual's cognitive processing associated with victimization. Similarly, there are a limited number of experimental designs or use of large secondary data sets in this field, both of which would provide the dynamic understanding of 'how' these influences occur. Literature exploring dispositional factors and vulnerability to fraud is limited in scope in terms of understanding the psychological mechanisms that lead people to become victims of these Advance Fee Scams. The aim of this systematic review is to collate and analyze the key research in relation to the psychology of Advance Fee Fraud to ascertain the baseline theoretical and research knowledge in this growing area, focusing on established psychological theories and empirically based methodologies.

3. METHODOLOGY

To scrutinize the level to which psychological theories have been empirically tested to explain Advance Fee Fraud victimization through a systematic review of the literature. The primary focus is upon understanding the literature which relates to how victims respond to fraudulent communications as opposed to the offender. However, as Button, Lewis, and Tapley note growing literature upon different types of fraud provides much information on the techniques of fraudsters.

These diverse range of tactics can be considered under three sub-headings, victim selection techniques, perpetration strategies and finally detection avoiding strategies

4. OBJECTIVES

1. Victim Selection concern the strategies that fraudsters use to contact their victims, e.g. email, Phishing, fake calls, Lottery Win, Matrimonial Sites ,Identity Theft etc.
2. Perpetration strategies: once the victim has been identified, these are the techniques used by fraudsters to secure money or identity, e.g. legitimate appearance of an email.

ISSN: 2233-7857 IJFGCN

3. Detection avoidance techniques: techniques used by fraudsters that would minimize their risk of getting caught, e.g. making reporting unlikely if ask for a small sum of money.
4. Primarily the aim is to consolidate our understanding of the psychological mechanisms by which offender (message) and victim (respondent) interact.

5. SYSTEMATIC REVIEW TECHNICAL DATA

Following flow diagram outlining the search and exclusion process conforming to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines (Moher et al. 2009).

Following are the full technical data for the systematic review: 1.

Review title: Psychology, fraud, and risk

2. Review question :

   How have psychological mechanisms been applied to help understand the individual determinants of consumer susceptibility to online fraud victimization?

3. Search terms
   a. Offence type: fraud ,scam, phishing, advance fee
   b. Offence subtype: consumer, online ,internet ,cyber ,telephone and email
   c. Focus on victim not offender: victim; victimization ,susceptibility; risk
   d. Psychology: decision-making, attention, social-engineering,judgement, influence, personality, psychology, cognition

ISSN: 2233-7857 IJFGCN

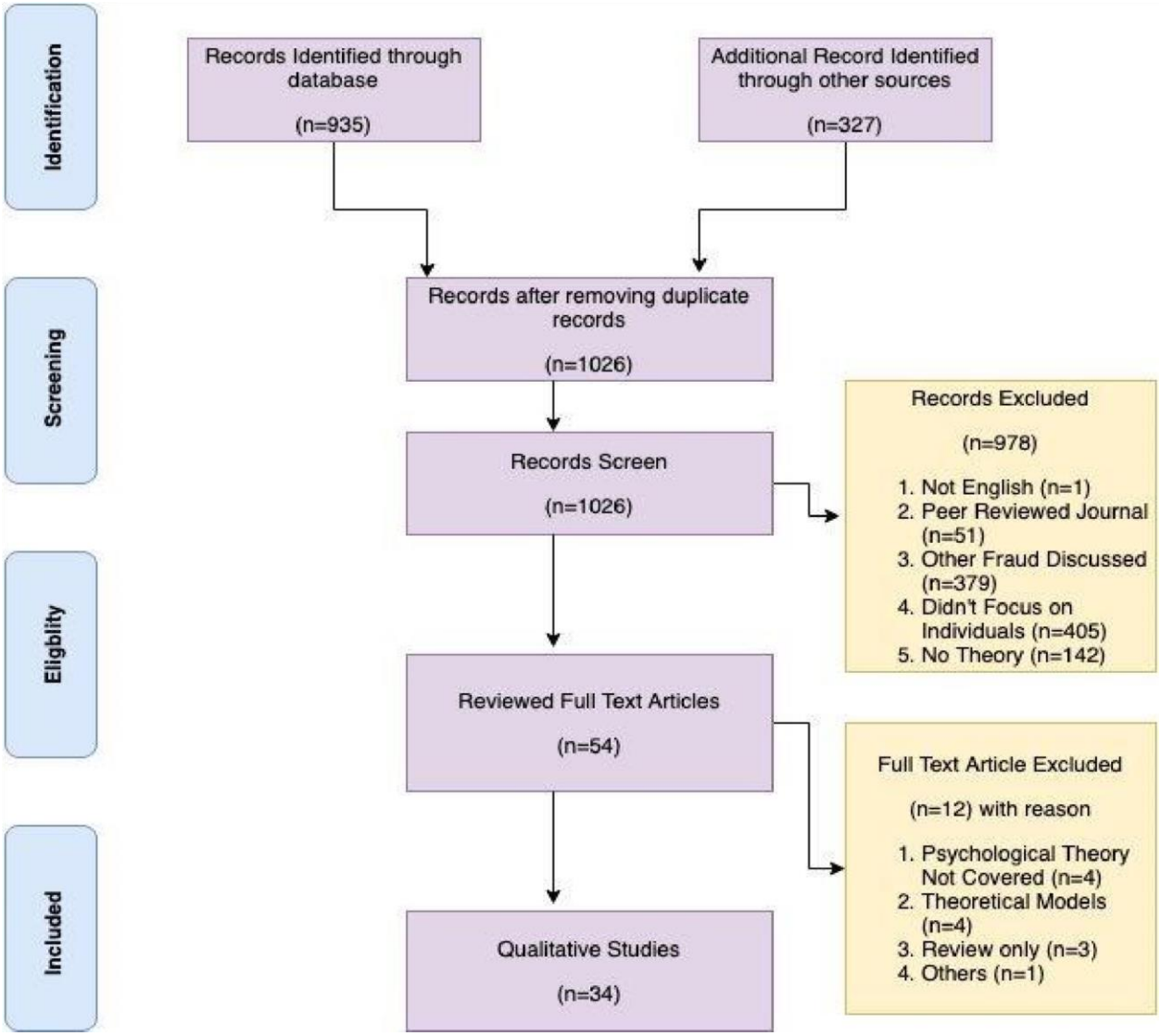

Fig. 1 flow diagram for identifying psychologically based studies into Internet-based fraud

5.1 Inclusion Criteria

The key inclusion criteria were that the paper should be and consider psychological theory related with advance fee fraud. In order to minimize more general observation and published articles, we restricted our search criteria to peer-reviewed journal articles, conference presentations, and book chapters in English. Both quantitative and qualitative studies were acceptable.

5.2 Exclusion Criteria

There were a large number of articles extracted and screened full text article before being rejected as not fulfilling the inclusion criteria ($n = 1026$). The majority of these articles purported to include psychological theories. Additional exclusions included other fraud types (e.g. Matrimonial and social cause fraud), those not focusing on the individual factors

ISSN: 2233-7857 IJFGCN

6. DATA COLLECTION AND ANALYSYS

Result

A total of around 1000 initial papers were extracted, 44 papers were included in the final search after the exclusion criteria were applied and an additional 10 equivocal items also added ($n = 54$) (see Fig. 1). from this, a further 20 were excluded by a Second author due to not including an established psychological theory and/or were theoretical models or existing reviews (i.e. not empirical studies). The final number of reviewed articles was 34.

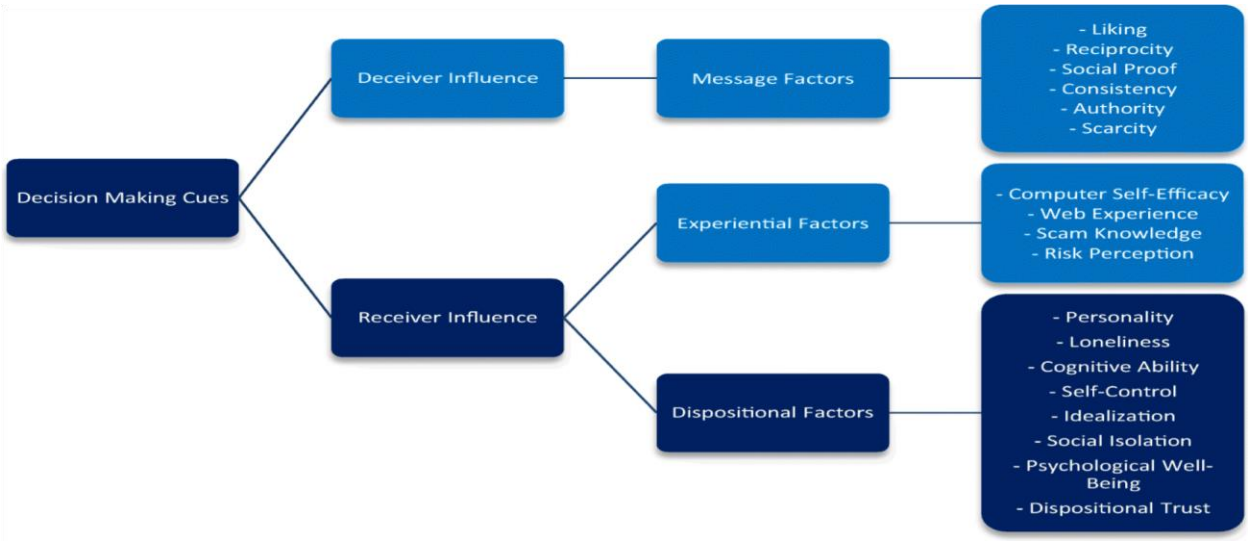

Fig. 2 variables and processes which influence an individual's ability to correctly identify advance fee fraud communication

6.1 Summary of Studies

Modic and Lea regard Internet fraud as a process, involving interaction with a fraudster. The review highlighted some broad groupings under which the empirical research in this area has been targeted. The key variables associated with decisions as to whether or not to decide whether information via the internet is believable can be divided into two categories.

These categories represent both the *content* and the way in which it *interacts* with the target. The receiver characteristics can also be further divided into two distinct elements: *experiential* and *dispositional* factors. Experiential factors relate to the person's knowledge and experience of computers and knowledge of fraudulent activity. Dispositional factors include personality, heuristics, and cognitive ability.

6.2 Message Factors

The 4 papers classified into this category primarily focused on how the fraudulent message was framed in order to maximize the potential for tempting a victim (Table 1). In these articles, only limited mapping onto demographic or individual factors was made. Experimental designs included

'fake' phishing emails sent out to university staff and students purporting to be from 'Information Services' requesting account verification.

ISSN: 2233-7857 IJFGCN

Table 1: Summary table of articles focusing on message factors (n = 4)

Authors	Year	Location	Theory	Method	Sample	Key findings
Luo, Zhang, Burd, and Seazzu	2013	USA	Information processing; heuristics	Experimental	University staff and faculty	Phishing attacks benefit from high source credibility.
Vishwanath	2016	USA	Cognitive, heuristics	Experimental	University students	Mobile devices lead to more phishing attack.
Fisher, Lea, and Evans	2013	UK	Heuristics, social influence, individual differences	Crosssectional survey	Community research panel and community	Size of reward can (negatively) impact on decisionmaking; cues of trust and authority predicted scam compliance.
Wang, Herath et al.	2012	USA	Cognitive (ELM); attention	Experimental	University students	Time limitation increase responding; deception indicators (e.g. grammar) increase attention and limit responding

Fischer et al. suggest that this could be in some way linked to 'self-confidence' and an increased belief in one's ability to detect scams. Scam compliance was linked to decision-making errors and hence limits the exploration of message factors alone as explanation of fraud. It appears that individual differences are more relevant to understanding the way messages are constructed and what processes they are likely to deed.

ISSN: 2233-7857 IJFGCN

Author extends this perspective to the use of smartphones as a means of reducing cognitive involvement in email fishing, alongside usage variables such as familiarization. Responding to fraudulent messages on smartphones was found to be more probable, potentially due to increased cognitive demands and further impacted by the presentation on smaller screens. Certainly fraudulent responding on smartphones is one potential additional variable to be included in future research.

6.3 Experiential Factors:

A total of 5 papers were classified into the experiential category, focusing primarily on the experience and expertise of the end-user (Table 2). Knowledge of internet scams was one way in which people showed some resilience to victimization. However, Internet use itself was not a protective factor; for some, usage patterns predicted whether they were likely to respond to fraudulent requests, with those people dealing with significantly high email traffic more likely to respond to messages (van Wilsem 2011; see also Vishwanath 2015).Interestingly, Vishwanath (2015) proposes that email behavior is linked to low social and emotional control and predictive of increased likelihood to respond to phishing emails.

Table 2: Summary table of articles focusing on experiential factors (n = 5)

Authors	Year	Location	Theory	Method	Sample	Key findings
Moody and Galleta	2011	USA	Individual differences: trust, boredom proneness, risk	Experimental	College students	Internet experience and risk tendency (lower financial risk takers) most of phishing responses
Harrison, Vishwanath , and Rao	2016	USA	Heuristics (GCS)	Experimental	University students	Individuals with high general communicativ e suspicion (GCS) less likely to be phishing victim
van Wilsem	2011	Netherland s	Self-control and rational choice	Crosssectional survey	Secondary data: largescale	Low selfcontrol leads to higher fraud victimization;

ISSN: 2233-7857 IJFGCN

Vishwanath	2015	USA	Personality, heuristics	Experimental	University students	Reliable and habitual email responders more likely to respond to phishing requests
Wright and Marett	2010	USA	Interpersonal deception theory	Experimental	University students ($n = 446$)	Experience and training led to reduced phishing susceptibility

Hence, a person's own competency with Internet safety cannot alone explain how they become victims of web-based fraud. Rather, it is an interaction between their ability and usage of the web and general dispositional factors, such as more controlled information processing, which are possibly more fruitful of future research in this domain.

6.4 Dispositional Factors

In reviewing the literature in the previous sections, it becomes seeming that this process of social engineering as techniques used to manipulate people into performing actions. Subsequently, the key mediating factor between the messages and whether experience/expertise in detecting fraud is likely to be practical are individual and personality variables.

Although not focused solely on Internet-based fraud, it nonetheless identifies the influences that make individuals susceptible to scams, through a process that reduces the intellectual deliberation when faced with a message. Theory of persuasion: the elaboration likelihood model (ELM). In essence, ELM suggests that individuals who are motivated to respond to the content contained in a fraudulent message are likely to focus and be persuaded by the key messages. On the other hand, those less motivated by the content are more likely to be influenced by peripheral cues. Hence, motivation is likely to be negatively correlated with scam victimization. The higher the level of motivation, the more likely attention will be expended upon aspects of the message and cues to deception identified.

Table 3: Summary table of articles focusing on dispositional factors (n = 15)

Authors	**Year**	**Location**	**Theory**	**Method**	**Sample**	**Key findings**
Chuchen and Chanvarasuth	2015	Thailand	Personality (DISC model)	Crosssectional survey	Convenience community sample	Influence and steadiness personalities more prone to phishing; all personalities equal in response to link manipulation

ISSN: 2233-7857 IJFGCN

Judges, Gallant, Yang, and Lee	2017	Canada	Personality , cognitive ability, and trust	Crosssectional survey	Older adults - victims and nonvictims	Victims lower scores on: cognitive ability, honestyhumility
Pattinson, Jerram et al.	2011	Australia	Personality , cognitive impulsivity	Experimen tal	University students	High extraversion and openness, and lower impulsiveness
						less susceptible to phishing
Chang	2008	Australia	Elaboration likelihood model	Interpretati ve	Case study	Advance fee fraud exploit automatic behavior through authority, urgency, and legitimacy
Chang and Chong	2010	Australia	Cognitive, heuristics	Qualitative	Content analysis of phishing emails	Time limitation increase responding; autonomous and heuristic thinking styles likely to increase victimization
Chen, Beaudoin, and Hong	2017	USA	Selfcontrol and rational choice	Crosssectional survey	Public panel survey (n = 11,534)	Willingness to make risky investments predicted internet fraud victimization
Buchanan and Whitty	2013	UK	Personality (sensation seeking, romance beliefs)	Crosssectional survey	University students (n = 853); victim support (n = 397)	High scores on idealization led to romance scam victimization; low openness a protective factor

ISSN: 2233-7857 IJFGCN

Alseadoon, Chan et al.	2012	Australia/ Saudi Arabia	Theory of deception (MDD); personality	Experimental	University students ($n = 200$)	Low email use and submissive personality less likely to suspect phishing; extraversion and openness likely to respond more
Iuga, Nurse, and Erola	2016	UK	Heuristics securing	Experimental	Web community sample ($n = 382$)	Real initial pages on fake website led to anchoring towards later 'real' website not phishing site
Sun, Yu, Lin, and Tseng	2016	Taiwan	Selfefficacy	Crosssectional survey	University students ($n = 411$)	No gender differences in self-efficacy and antiphishing behavior
James, Boyle, and Bennett	2014	USA	Cognition; well-being	Longitudinal survey	Community panel survey ($n = 639$)	Susceptibility to fraud linked to low income, cognitive ability, wellbeing and social-support,
Alseadoon, Chan et al.	2012	Australia/ Saudi Arabia	Theory of deception (MDD); personality	Experimental	University students ($n = 200$)	Low email use and submissive personality less likely to suspect phishing; extraversion and openness likely to respond more

ISSN: 2233-7857 IJFGCN

Lichtenberg, Stickney, and Paulson	2013	USA	Health and cognitive functioning	Longitudin al survey	Public panel survey ($n = 4461$)	Depression and social needs related to victimization in older adults
Iuga, Nurse, and Erola	2016	UK	Heuristics — anchoring	Experimen tal	Web community sample ($n = 382$)	Real initial pages on fake website led to anchoring towards later 'real' website not phishing site
Sun, Yu, Lin, and Tseng	2016	Taiwan	Selfefficacy	Crosssectional survey	University students ($n = 411$)	No gender differences in self-efficacy and antiphishing behavior

However, there was only a small relationship; generally speaking, less impulsive respondents are more able to manage potentially fraudulent messages. Some small links with potential to increase victimization and personality factors emerge from these and other studies for example, victims have lower scores lead caution that given the wide range of phishing and fraudulent message content no one personality feature is likely to predict susceptibility in isolation that there is relatively little information about the relationship between personality types and phishing techniques.

7. METHODOLOGICAL LIMITATIONS

A number of papers were rejected, most notably through the stipulation that there be an established psychological theory. There are also some methodological considerations to be accounted for in regard to the studies themselves and in particular their ecological validity in respects to accounting for behavior in the real world. Role play scenarios, in which participants are asked to access the account of a character and decide how they would deal with a number of emails, may suffer from expectancy/observer effects. Hence, although many studies suffer from a potential lack of environmental validity and generalizability, there is a growing corpus of studies which at the very least recognize the limitations inherent in this research domain.

8. CONCLUSION

The purpose of this systematic review was to examine the range of psychological factors associated with Advance Fee Fraud victimization to identify the way in which Internet scams exploit inherently compromised human decision-making. The majority of the studies reviewed focused on 'phishing' and examined a range of factors from personality through to heuristics. The majority of evidence and subsequent beliefs we have regarding the psychological factors associated with vulnerability to online fraud are at best

ISSN: 2233-7857 IJFGCN

circumstantial and at worst in danger of creating misleading .Policies designed to limit the extent and impact of advance fee fraud should clearly recognize the universal nature of compliance. Advance fee fraud is relatively unique in that examples of potential criminal activity are openly available. Seemingly we are unable to stop this onslaught, but we can limit their effectiveness by increasing awareness and understanding. Through gaining an insight into how they work and with whom, the potential for law enforcement to create general and targeted crime prevention initiatives is enhanced.

REFRENCES

1. Alseadoon IM, Othman MFI, Foo E, Chan T (2013) Typology of phishing email victims based on their behavioral response. AMCIS 2013: Anything, anywhere, anytime:

   Proceedings of the 19th Americas Conference on Information Systems, 5, 37163624Google Scholar

2. Chen H, Beaudoin CE, Hong T (2017) Securing online privacy: an empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. Comput Hum Behav 70:291–302CrossRefGoogle Scholar

3. Buchanan T, Whitty MT (2014) the online dating romance scam: causes and consequences of victimhood. Psychol Crime Law 20(3):261–283CrossRefGoogle Scholar

4. Burnes D, Henderson CR, Sheppard C, Zhao R, Pillemer K, Lachs MS (2017) Prevalence of financial fraud and scams among older adults in the United States: a systematic review and meta-analysis. Am J Public Health 107(8):13–21CrossRefGoogle Scholar

5. Button M, Cross C (2017) Technology and fraud: the 'Fraud genic' consequences of the internet revolution. In: McGuire M, Holt T The Rutledge handbook of technology, crime and justice. Routledge, London, pp 1–5Google Scholar

6. Alseadoon I, Chan T, Foo E, Gonzales Nieto J (2012) Who is more susceptible to phishing emails?: a Saudi Arabian study. ACIS 2012: Location, location, location: Proceedings of the 23rd Australasian Conference on Information Systems 2012 (pp. 1–11). ACIS Google Scholar

7. Button M, Lewis C, Tapley J (2009) Fraud typologies and the victims of fraud: literature review. National Fraud Authority, London Google Scholar

8. Button M, Lewis C, Tapley J (2016) Fraud typologies and victims of fraud. National Fraud

   Authority, London Google Scholar

9. Chang JJ (2008) an analysis of advance fee fraud on the internet. J Finance Crime 15(1):71–81CrossRefGoogle Scholar

10. Chang JJ, Chong MD (2010) Psychological influences in e-mail fraud. J Finance Crime

    17(3):337–350CrossRefGoogle Scholar

ISSN: 2233-7857 IJFGCN