International Journal of Cyber Behavior, Psychology and Learning

July-September 2015, Vol. 5, No. 3

Table of Contents

Research Articles

The *International Journal of Cyber Behavior, Psychology and Learning* is indexed or listed in the following: ACM Digital Library; Bacon's Media Directory; Cabell's Directories; DBLP; Google Scholar; INSPEC; JournalTOCs; MediaFinder; ProQuest Advanced Technologies & Aerospace Journals; ProQuest Computer Science Journals; ProQuest Illustrata: Technology; ProQuest SciTech Journals; ProQuest Technology Journals; PsycINFO®; SCOPUS; The Standard Periodical Directory; Ulrich's Periodicals Directory

Susceptibility to Email Fraud: A Review of Psychological Perspectives, Data-Collection Methods, and Ethical Considerations

Helen S. Jones, Department of Psychology, Lancaster University, Lancaster, UK

John N. Towse, Department of Psychology, Lancaster University, Lancaster, UK

Nicholas Race, School of Computing and Communications, Lancaster University, Lancaster, UK

ABSTRACT

The authors review the existing literature on the psychology of email fraud, and attempt to integrate the small but burgeoning set of research findings. They show that research has adopted a variety of methodologies and taken a number of conceptual positions in the attempt to throw light on decisions about emails that may be in best-case scenarios, sub-optimal, or in the worst-case scenarios, catastrophic. They point to the potential from cognitive science and social psychology to inform the field, and attempt to identify the opportunities and limitations from researcher's design decisions. The study of email decision-making is an important topic in its own right, but also has the potential to inform about general cognitive processes too.

Keywords: Cyberpsychology, Decision-Making, Fraud Victimisation, Online, Phishing

INTRODUCTION

The continued expansion of the internet provides a valuable source of entertainment, communication, and commerce. However, along with this comes the ever more sophisticated threat of online fraud, with reports that there are more than one million victims of consumer cybercrime every day (Norton Cybercrime report, 2013). Such fraud has obvious implications on a personal and commercial level, as well as within the criminal justice system. However, psychologically, it also offers an intriguing arena for the understanding of decision-making processes leading to online fraud victimisation, alongside a valuable environment within which to apply and test theoretical predictions for such behaviour. In this article, we attempt to map out some key contemporary issues for researchers, as well as potential directions for future work.

DOI: 10.4018/IJCBPL.2015070102

In order to keep the commentary concise and manageable, we restrict our remit to one specific aspect of online fraud; that of decision-making surrounding email management and phishing. A definition of phishing is not straightforward given the multitude of formats that these communications can take. Nonetheless, one broad and useful description is offered by Myers (2007):

Phishing: A form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organisation in an automated fashion. (p. 1)

Most of these email communications are sent out to thousands of internet users, with only a small response rate necessary to make it worthwhile (economically) for the attacker. On average, successful phishing attempts have around a five percent response rate (Norton, 2014). This makes phishing a potentially more sustainable fraud than more costly and time-consuming traditional formats, such as postal and telephone fraud.

Computer science research is continually developing more advanced algorithms to detect phishing emails before they reach the user's inbox in both traditional network-based systems (e.g. Fette, Sadeh, & Tomasic, 2007; Bergholz et al., 2010; Islam, & Abawajy, 2013), but also more recently in cloud-based systems which aim to detect phishing attacks in the cloud before they even reach the network (Salah, Alcaraz Calero, Zeadally, Al-Mulla, & Alzaabi, 2013). However, the simultaneous increased sophistication of the emails themselves means that the benefits of these newly developed approaches are often short-lived; advances in the technology developed to detect phishing attacks are often quickly mirrored in the methods used by the fraudsters to circumvent such detection algorithms. Similarly, efforts to block the phishing websites that emails direct users to, through automated heuristic filters which detect machine learned patterns (e.g. in words used on the webpage - Abu-Nimeh, Nappa, Wang, & Nair, 2007; or in URLs - Garera, Provos, Chew, & Rubin, 2007), or through manual blacklisting, face the same issues with continual technological advancement on the part of the fraudsters in line with that of the researchers. Moreover, there may be a risk that users develop a false sense of security: if they believe (erroneously) that software can capture phish, then they may treat all messages that reach their inbox undetected, and accessible linked websites, as being genuine. The inaccuracy in these filtering efforts means that it is left to the user to recognise and manage potential phishing attempts.

The biases in human decision-making which cause some people to respond to phishing emails lead us to consider why certain people make these poor decisions, whilst thousands of others can receive the same email and ignore it or delete it straight away. Is this just the luck of the draw, or is the division somewhat systematic? There is a common assumption that demographic factors, especially age, are influential upon vulnerability, when in fact the research surrounding this is inconclusive. Some research supports this assumption, demonstrating that the average age of fraud victims is significantly higher than the general population (Pak & Shadel, 2011; Shadel & Pak, 2007). However, contradictory research has demonstrated that older internet users are actually less vulnerable than younger users (Titus, Heinzelmann, & Boyle, 1995; Kerley & Copes, 2002; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010). The National Fraud Authority (2011) produced a report which outlines key demographics for different victim typologies, demonstrating that victims come from a range of age groups and backgrounds, and that we cannot necessarily focus attention on one particular demographic when considering vulnerability.

This review attempts to integrate psychological research from a disparate literature, exploring issues that have previously been considered in isolation. Where feasible, we seek to highlight the theoretical context and consider the implications this has for future research. An additional

objective is to take stock of the methodological approaches that might be used to investigate behavioural responses to phishing, and some of the limitations that might arise from research design choices. We feel this is important and timely because, as a result of its status as a relatively new topic in psychology, online decision-making and victimisation lacks both a clearly defined methodology for measuring susceptibility, and an overarching conceptual theory to guide the development of empirical research.

As this paper will go on to explain, perspectives from social psychology have suggested that poor decisions result from processes of persuasion from *the sender*, i.e. the perpetrator. On the other hand, cognitive approaches naturally focus on the fallible mental architecture of *the recipient*, i.e. the victim. Although this review will focus on the psychological perspectives, it is worth noting that approaches from computer science have considered human-computer interaction (HCI) and the influences that can increase or decrease users' trust in online systems and communications. These influences include the appearance of the email or website, the perceived quality of information provided, and the degree of transparency with regard to how information will be used once shared (Karat, Karat, & Brodie, 2009). One of our core conclusions is that, ultimately, we will need to understand the medium and the processes on *both* sides of the interaction. Indeed, there may be emergent properties from the dynamic that exists between message content and message interpreter that are important in the outcome of the email response decision-making process (see Figure 1 for a simple process-based framework of email decision-making process).

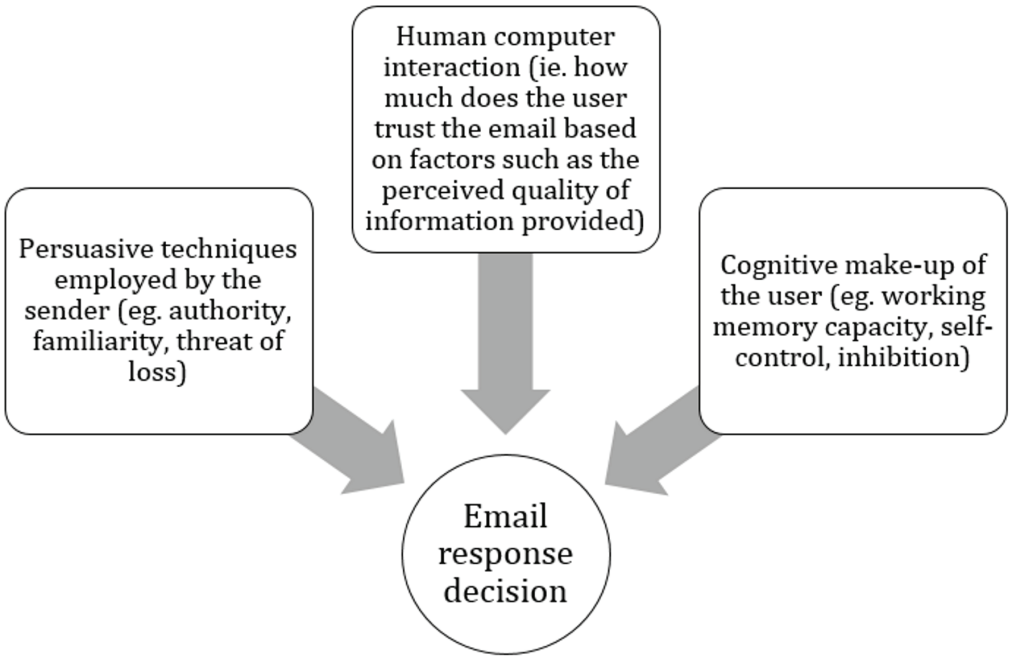
THEORETICAL PERSPECTIVES

Psychology of Persuasion

Theoretical work surrounding persuasion techniques in general, as represented in the leftmost arm of Figure 1, suggests the relevance of factors such as authority, scarcity, and social conformity (Cialdini, 1993). These persuasive influences can be present in fraudulent communications (as well as benign messages) and have been shown to result in more successful phishing attempts. For example, spear phishing is a technique that may use social engineering techniques to collect personal information about the victim to make the communications more personal and thus more plausible. Work by Jagatic, Johnson, Jakobsson, and Menczer (2005) showed that, unsurprisingly, participants were more likely to respond to an email communication purporting to be from a friend than an email which came from an unknown sender, thus supporting the influence of a more personal, targeted message. Further to this, the level of authority in an email seems to be an important factor in persuading the user to respond. Historically, ground-breaking research such as that conducted by Stanley Milgram in the 1960s has shown how, regardless of the severity of the consequences, people are generally submissive to the instructions of an authority figure. Guéguen and Jacob (2002) demonstrated that participants were much more likely to respond to an email asking users to complete a survey when the sender was a scientific researcher - labelled by the researchers as the more authoritative figure - in comparison to the same email when it came from an undergraduate student. There may be a number of factors (such as history of past messages, awareness of what to expect from the sender, etc.) that are potentially influencing this variation in response likelihood, but regardless, the effect is noteworthy.

Other visceral influences may also be manipulated by fraudsters to increase the persuasive power of an email communication. Such influences include greed and fear, for example via offers of money, or threat of loss (e.g. access to online accounts, or impending fines) as part of the email message. Higher levels of visceral influence are thought to lead users to overlook the importance of cues that might otherwise trigger suspicion (Langenderfer & Shimp, 2001).

Figure 1. Diagram to demonstrate the proposed theoretical influences upon the email decision-making process



Cognitive Processing

In this section, we discuss the central and rightmost arms of Figure 1, focusing on individual characteristics, capacities and processes that might affect decision-making. Dual system theories of reasoning (such as that proposed by Stanovich, 1999; Kahneman, 2000; and Evans, 2003) propose two psychological systems for generating behavioural responses, the deployment of which depends on the nature of the individual situation. System 1 uses intuitive, immediate, and emotional responses to make decisions, while system 2 uses more analytic, and deliberate processes. In the context of the current discussion, when faced with the need for immediate solutions – such as deciding how to respond to an email – with constraints such as a time limit on response, or threat of loss, users are potentially liable to make intuitive and less reasoned decisions. These are often portrayed by the perpetrator as the rational solution but are actually poor decisions (Dong, Clarke, & Jacob, 2008). Yan and Gozu (2012) support the relevance of this idea when comparing susceptibility to email fraud victimisation between rational and intuitive decision-making strategies. Participants were told to either give rapid responses upon a first look at the email (intuitive), or told to take their time, and read the email carefully before deciding on their final response (rational). In the rational decision-making condition, participants correctly identified more emails as scams than when intuitive decision-making was employed. This supports the importance of utilising system 2 thought processes when managing emails, or alternatively the notion of training system 1 thought processes to pick up on appropriate cues.

This theory is also associated with work looking at risky decision-making more generally, and can be related to the central channel of interest in Figure 1. Such work has yet to be directly linked to online fraud victimisation, but we see strong parallels in both fraud detection and gam-

bling risk / payoff scenarios. The prevalent methodologies in such research are described in more detail below, but all rely on the same basic principle of exploring whether people would take a gamble or not. In employing system 1, intuitive, decision-making processes, a person would likely choose the option which gave them the biggest reward, rather than thinking through the decision in terms of the long term benefits or risks. If the same processes are in fact employed in online decision-making, then it is likely that psychological variables found to influence risky decision-making in these gambling scenarios will also influence decisions surrounding email management.

As well as situational factors, individual differences in variables such as working memory capacity have also been shown to influence the reasoning process, which in turn may reflect in email management scenarios. Limitations in working memory span can affect a wide variety of cognitive situations, such as the ability to maintain multiple interpretations of ambiguous sentences (e.g. Miyake, Just, & Carpenter, 1994). By analogy, it is also possible that processing the content of an email and simultaneously assessing its veracity may be cognitively taxing. As a result, it may be difficult for a person to think rationally, and engage system 2 processes, when cognitive load is increased. This means that when put in situations where cognitive load is high people tend to fall back on impulsive, system 1, decision-making strategies. In addition, it may be that individual differences in a construct such as working memory capacity affect the propensity of individuals to process emails sub-optimally. That is, working memory demands can vary by situation for a person, but working memory capacity may differ across individuals too (Conway, Jarrold, Kane, Miyake, & Towse, 2007).

In this regard, Cokely and Kelley (2009) found that participants who demonstrated a higher working memory span were less likely to engage in risk taking behaviour, which is likely to be because they were able to engage in more rational decision-making strategies than those participants with lower working memory spans (see also Moore, Clark & Kane, 2008, for a discussion of how this might play out in a very different scenario). An alternative explanation of this is that those with higher working memory spans perform better under cognitive load, as they are better able to efficiently divide their attention. Theories of divided attention suggest that individual differences, in factors such as working memory capacity, and situational factors can influence how well a person is able to perform multiple tasks at once (Kane, Bleckley, Conway & Engle, 2001). Colflesh and Conway (2007) demonstrated that participants with a higher working memory capacity performed better on a selective attention, dichotic listening task (participants must concentrate on a task based on an auditory stimulus, whilst simultaneously listening to another different auditory stimulus) than those with a lower working memory capacity. In relation to online decision-making, it may be that a person's ability to detect phishing emails is, in part, influenced by any other tasks requiring their attention at the same time, along with their ability to effectively divide attention. In real life email management, there are often times when users need to respond to emails whilst preoccupied with other tasks, such as getting ready in the morning, or a deadline at work.

Divided attention is often measured using dual-task paradigms, in which participants are given a primary task to complete, whilst simultaneously completing a secondary task that adds to their cognitive load, such as counting out loud, or remembering a letter string. More recent literature using these types of tasks has looked at participants' attention to driving when using a mobile phone. Beede and Kass (2006) gave participants a simulated driving task, whilst engaging in a conversation on a hands-free mobile device and found that driving performance was negatively affected by simultaneous use of a mobile device. The dual-task paradigm is easily transferable to situations involving email management, whereby a participant would complete an email judgement task whilst simultaneously completing another task to establish whether divid-

ing attention is detrimental to the decision-making process. In addition, the effect of different types of secondary tasks could be measured, including both domain-specific (e.g. trying to meet a deadline on another piece of work whilst also keeping an eye on incoming emails), as well as more experimental tasks (e.g. an Operation Span task – see Conway et al, 2005, for example).

Cognitive Make-Up

Whilst we have already mentioned individual differences in working memory capacity as a potentially influential factor in the online decision-making process, there are also other psychological variables that have been examined as potential signals of fraud susceptibility, including personality and self-control. A combination of these factors may contribute to a sort of 'cognitive profile', representative of those users who are most at risk to online fraud victimisation.

Modic and Lea (2011) demonstrated that higher levels of agreeableness and lower levels of extraversion, measured using the International Personality Item Pool (IPIP; Goldberg, 1999), were associated with higher levels of vulnerability to fraud victimisation, as measured by self-reports of personal experience. They suggest that users who show higher levels of agreeableness are likely to be more trusting generally and so believe what they are told by those they are communicating with online, whilst those who show lower levels of extraversion are likely to seek and build stronger relationships online than they are in person as they are not as comfortable in offline social situations, which again may lead them to be more trusting of people who they are interacting with online.

Research into offline fraud victimisation has demonstrated that lower levels of self-control are linked to increased vulnerability to fraud victimisation (Holtfreter, Reisig, Piquero, & Piquero, 2010). Users with lower levels of self-control are thought to engage in intuitive, rather than rational, decision-making processes (see comments above about dual-process cognitive styles), as they are less likely to consider the negative consequences of their actions and instead will make immediate decisions based on the proximity of gain or loss.

In conclusion, it is clear that there are a number of different theoretical approaches to be considered in addressing the issues surrounding susceptibility to fraud victimisation. The relative novelty of this research area means that a clear and comprehensive theoretical model is yet to be established, as the research is still in an exploratory stage. In the same sense, the methods most effective at measuring vulnerability are also yet to be refined. Below we discuss the various approaches that researchers have taken to date, with most focused around the same concept of judging emails or communication scenarios.

METHODOLOGICAL APPROACHES

Whilst the psychological variables which we want to measure, such as personality, self-control, and working memory, can be assessing using reliable, well-specified measures, and the persuasive techniques manipulated through content shown to participants, the methods used so far to assess susceptibility are less clear-cut. Whilst each of the following methods has practical benefits, none have been extensively replicated to assess reliability, nor compared to real life vulnerability, as a way of assessing validity. Here we will discuss each methodology we are aware of in related research and comment on how we can build on these to maximise their validity. Although we will not explicitly discuss the detailed data analysis methods adopted for each of these methodologies, all will elicit a performance-based score that can be used to compare levels of susceptibility between participants.

It is also worth noting that those studies using email stimuli - either in a lab setting or in a simulated phishing scenario - to measure susceptibility run the risk of becoming out-dated within the space of a couple of years from publication. It may be the case that these studies are no longer representative of the kinds of phishing emails that users encounter on a daily basis. Constant technological advancements mean that the fraudulent emails are becoming ever more sophisticated and difficult to detect. Classically, users were told that cues such as spelling and grammar mistakes were a key giveaway for a phishing email, whereas contemporary phishing attempts rarely contain such superficial cues and instead rely on the user's ability to detect more subtle cues, such as the likelihood that a company would ask for the details requested in the email, or the legitimacy of the email address which appears in the 'from' field of the email.

Risky Decision-Making Research

In addition to the variables that have been linked directly to fraud victimisation, there are also potentially relevant constructs from broader, analogous topics. Risky decision-making behaviour has been associated with working memory (Hinson, Jameson, & Whitney, 2003), personality (Lauriola & Levin, 2001), and time pressure (Ordóñez & Benson III, 1997). All of these studies share a key feature – participants assess the attractiveness of a gamble. Ordóñez and Benson III asked participants exactly that; given a set of gambles they were asked to rate the attractiveness of each and state the maximum amount they would pay to play the gamble. Both Lauriola and Levin, and Hinson, Jameson, and Whitney used a binary response task in which participants were asked to select either a safe, immediate outcome, or choose either a more risky option which involved a gamble (Lauriola & Levin) or a delay in pay-out (Hinson, Jameson, & Whitney), but would result in a larger pay-out. Some phishing emails may involve such a gamble – the chance to win money traded off against a self-recognised risk of fraud. However, it is not clear that this is true in all cases – we should not assume that people are making a conscious decision to choose between the 'safe' and 'risky' options. Since many recipients genuinely believe an email *is* from the company that it purports to be from –the decision to respond to that email would not be considered a risk at the time.

Measuring Risky Decision-Making in Email Management

Scale Measures

Modic and Anderson (2014) have recently developed a self-report scale measure of susceptibility to persuasion. This incorporates psychological mechanisms from a range of contexts, with a focus on measuring factors that influence scam compliance. Example items from the scale include: *'It is important to me that those who know me can predict what I will do'*, *'I have a hard time breaking bad habits'*, and *'In general, I work better when I'm under pressure'*. Validity testing on an earlier version of the scale (Modic & Lea, 2013) found the factors measured in the scale, such as self-control and sensation seeking, were all related to vulnerability. However, since developing the second version of the scale, and including a number of added variables, this validity testing does not seem to have been repeated so we cannot know for sure that this updated scale is actually measuring susceptibility. In addition to this, as with all self-report measures, this scale may be subject to demand characteristics, i.e. the participant responds to the scale in a way that they think is socially acceptable rather than responding truthfully.

Email Legitimacy Tasks

A more commonly used measure of vulnerability involves asking participants to rate their likelihood to respond in given situations. This method has been used in research looking at both online (see below) and offline fraud (e.g. Holtfreter, Reisig, Piquero, & Piquero, 2012), but we will focus here on those studies that have investigated online fraud.

Yan and Gozu (2012) used this method with email screenshots, showing participants either the subject line of an email or the entire body of text, as a measure of the importance of availability of information. Overall, there were 36 emails in this task, which were all unsolicited scam emails that had been circulated to internet users. Participants correctly identified significantly more emails when they were shown the entire body of text, as opposed to when they saw only the subject line of an email. Whilst this kind of task seems more reliable as a measure of vulnerability than the questionnaire approach, as it is measuring actual behaviour, this behaviour is still laboratory based and participants are unlikely to be reading and managing emails in the same way as they would were they to receive the given emails to their own inbox. The lab setting may induce cautious, system 2 thinking while participants responses are being monitored, whilst in the moment decisions in a real life decision-making setting may induce more intuitive, system 1 thinking. In addition, Yan and Gozu's task uses only phishing emails as stimuli, which may influence participants' responses. To the extent that participants expect to differentiate between a mixture of phishing and legitimate emails when they are being asked to rate their likelihood to respond, decisions may not mirror real-life performance exactly.

Variations of this type of methodology have used 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 in the inbox of this account. Downs, Holbrook, and Cranor (2007) employed this method when assessing how knowledge of cues, such as security icons, affected phishing susceptibility. Participants, in the role of the fictional 'Pat Jones' were asked how they would respond to each of five emails, each of which contained a URL link -with no mention that the study looked at ability to detect phishing emails. Possible response options for each email included, *'reply by email'*, *'click on the link'*, and *'type the URL into a browser window'*. Those who indicated that they would click on the link were then shown the linked webpage and asked how they would respond faced with this. Participants who could correctly define 'phishing' and recognised incorrect security lock images showed lower susceptibility to phishing, whilst knowledge of other risks such as spyware and viruses did not affect susceptibility. This type of task is informative in the sense that it can assess susceptibility in a lab based setting whilst not alerting participants to the nature of the task, thus eliminating expectancy effects. However, the way in which these types of tasks are constructed may still prompt socially desirable responses. For example when given the option *'type the URL into a browser window'*, this may alert participants that this is the most sensible option compared to the other options such as *'click on the link'*. Parsons, McCormac, Pattinson, Butavicius, and Jerram (2015) demonstrated, using a role-play task as a measure of susceptibility, that knowledge of the nature of the study affected behaviour. Participants identified phishing emails more successfully when they had been alerted to look out for them. Such subject expectancy effects might affect the integrity of a study even more than any socially desirable response bias.

These email legitimacy tasks are potentially further constrained, as participants do not have anything to risk in their participation. If participants were to judge these emails in their own inboxes then it would be their information or money at stake if they chose to reply, whereas in the lab situation, participants have nothing to lose whether they perform well or not. In order to encourage participants to perform realistically, it would be necessary to provide them with some

incentive such as a prize for the participant who performs best. Whilst this may encourage participants to put more effort into the task, it is still not representative of the risk that they face when managing phishing emails in real life. As yet, it is unclear how much this affects study validity.

Modic and Lea (2011) gave participants written descriptions of fraudulent communications, both online and offline, but instead of asking their likelihood to respond, they asked participants whether they had ever responded to such a communication and only used those participants who reported being victimised in the past in further analysis. Of 506 initial participants, only 67 claimed to have responded to a fraudulent offer like those described, meaning that the sample size used in the remainder of the analysis was drastically reduced. Once these participants have identified themselves as victims of fraudulent communications then working with them generates the same issues as described below in relation to research that directly samples victims. Whilst real-life victimisation does provide a more realistic measure of vulnerability, this task generates an element of self-report bias. Participants may interpret the written descriptions differently depending upon their own experiences and they may be embarrassed to admit that they responded to the communications. In addition to this, the task measures victimisation rather than vulnerability - just because a person has never responded to a phishing email does not mean that they are not vulnerable, as it may be that they have simply not received a sufficiently convincing email yet.

Working with Past Victims

Given the uncertain validity of lab-based simulations of online phishing scenarios for real-world behaviour, an alternative approach is to study past victims of fraud. On one hand, victims form a sample population who have self-evidently demonstrated vulnerability to online fraud attempts in a real-world setting. However, there are still a number of challenges faced in using such a sample for this kind of research. One of these is that, of course, fraud victimisation is a quasi-experimental variable; such individuals have not been assigned at random to a 'victim' group, meaning that the contextual circumstances surrounding their victimisation need to be established. Being a past event outside of experimental control, this can be difficult as we are reliant upon the victim's own recall of the context surrounding the event. The likelihood of a victim being able to recall their mental state upon receiving the email and as a consequence of reading it – were they tired, distracted, anxious, excited – is minimal. It is also quite possible that the individual who has been a victim will have changed as a result of the incident; after all, they may have been financially ruined, they may be embarrassed by what now appears to them to be gullibility. They may also have read about the scam or other similar scams, and may have been part of training programmes with respect to online security. As a result, the responses they give to questions and psychological measures may differ from the way they would have responded prior to victimisation.

In addition, this method relies on the researcher's ability to establish a comparable control group so that differences can be measured between the vulnerable group and a group of users who do not demonstrate vulnerability. This may prove challenging for a number of reasons – the most significant being establishing who is not vulnerable. It may be the case that a user has never responded to a fraudulent email communication, but this may be because they have not received a sufficiently convincing phishing email. Control group participants and past victims can be matched on their demographic characteristics (age, gender, educational background), their internet experience, and their email usage habits, but unfortunately it is not realistic to establish the exact emails which participants have received in their time as internet users, so is not possible to know whether members of the control group are less vulnerable or whether they have simply not received the same phishing emails as victims.

Nonetheless, this method has been used by a number of researchers as it can be seen to carry more face validity as a measure of vulnerability than the email legitimacy tasks mentioned above. Whitty and Buchanan (2012) compared performance measures of loneliness, extraversion, agreeableness, neuroticism, romantic beliefs, and sensation seeking, between victims of online romance scams and a control group to establish any differences. The only significant finding in this study was that victims were more inclined to idealise romantic partners. This work looks solely at victims of online romance scams though, which is a specific focus and it cannot be assumed that findings would generalise to victims of other types of scams online.

Shadel and Pak (2007) also worked with past victims, looking at differences in demographic, and psychological characteristics - such as impulsivity, self-reliance, and optimism - between offline fraud victims and a control group. These victims were grouped depending on the type of fraud of which they were victim, in this case either lottery, or investment victims. Some differences were found between victims and controls on demographic factors such as gender, age, marital status, and religious beliefs. Further to this, differences were found between the victim and the control groups. For example, lottery victims were found to demonstrate higher impulsivity than both investment victims and the control group, whilst the victim group as a whole demonstrated more self-reliance than the control group. However, each of the variables discussed in this study was only measured by one question, meaning that the accuracy of these in measuring the variables described may be fairly limited.

Although prior victimisation does demonstrate a clear vulnerability, we must also consider differences that may be apparent as a result of the severity of the victim's experience (i.e. how much money was lost), and the extent of their vulnerability (i.e. how long the scam went on, how convinced they were that the scam was legitimate). For this reason it would be necessary to take such information into account when working with victims, which neither of the above studies report doing. The method of recruitment for work with past victims may also influence the validity of the data as cybercrime goes heavily underreported, with substantially lower reporting rates than other crimes (Copes, Kerley, Mason, & Van Wyk, 2001), so there may be some bias in the sample of victims who are willing to participate in research relating to their experiences. They may not report their victimisation due to embarrassment or lack of belief that it will help in any way, so it is unlikely that these people will be willing to discuss their experiences with a researcher either. Even of those who have reported their experiences, it is unlikely that all will be inclined to participate in research about their experience, which may further bias the sample. We must also not ignore the issue that obtaining access to a sample of past victims in itself produces a challenge for the researcher, as does obtaining a comparable control group in terms of the demographic make-up of the participants.

Simulated Phishing Attacks

Possibly the experimental assessment of vulnerability with the highest face validity, but clearly also the most ethically challenging, would be to simulate a genuine phishing attack by sending a fake phishing email to participants and recording whether or not they respond. Jagatic, Johnson, Jakobsson, and Menczer (2005) used this method to establish whether there was a difference in response rate when the participant received an email purporting to be from someone within their social group compared to a control email which came from a stranger, unknown to the participant. They found a significantly higher response rate to the emails that came from senders familiar to the participant. For this study, Jagatic et al. recruited participants from Indiana University based on social networking information publicly available about them on the internet, which represents the ease of a genuine spear phishing attack being targeted at them. The email which

participants received, either purporting to be from a friend or from a stranger to the recipient, linked to a website which had no reference to Indiana University in the URL but asked them to enter their University network information (i.e. username and password). Although the research found a relatively high response rate for emails from familiar senders, the premise of a friend/peer sending an email that asks you to input University log in credentials may not be realistic. It may have been more appropriate to send these emails from a lecturer/known administrator at the University who the student participants would also have been familiar with and would be more used to receiving such emails from. In addition, the level of authority of the sender of an email asking about University credentials may influence the response rate in addition to familiarity with the sender, as demonstrated by Guéguen and Jacob (2002).

Guéguen and Jacob (2002) used a similar method to measure the influence of information about social status on likelihood to respond. They sent a simulated email containing a HTML form for a survey on food habits, which purported to be from either a scientific researcher, who was deemed to be of higher social status, or from an undergraduate student, who was deemed to be of lower social status. This data came from two separate samples, the first of which targeted students at the University of Bretagne-Sud who were logged into workstations at the university at the time the phishing attack was to be sent. The second sample was randomly selected from a list of email addresses taken from software designed to procure this kind of information from the internet. Emails sent from the scientific researcher gained a higher response rate from both samples (sample 1: 97.5%, sample 2: 54.70%) than the emails from an undergraduate student (sample 1: 65%, sample 2: 6.98%). The content of the email is likely to have been more relevant to the student sample, as they are more likely to have received similar emails previously, which may explain their higher response rate. Unlike Jagatic et al.'s work, in which participants were asked for personal information, this email containing a link to a questionnaire about food habits does not pose any particular risk to the participant. It is not necessarily representative of a phishing attack in which the fraudster would attempt to elicit personal information such as log in credentials or bank details, and the lack of personal context (e.g. needing to update their personal information on a site to avoid losing access) means that there is no incentive for the participant to respond. In addition to this, Guéguen and Jacob suggest that the lack of geographical proximity between those in the second sample and the sender of the email (who is based at the University) may have made them more likely to refuse / ignore the request for participation, as there would be no chance of future interactions between the recipient and sender.

Another example of this methodology comes from Wright and Marett (2010) who measured the importance of different behavioural factors to recipients' likelihood to respond to a simulated phishing email. In this study, participants signed up to take part in research with the generic title 'security research' and were then given a unique ID code, which they were told was to be used to access course materials, assessments, and grades. The participants were also told not to disclose the code to anybody and signed a nondisclosure agreement. These students then studied a module on internet security and privacy as part of their course, which lasted for eight weeks and completed a number of questionnaires assessing web experience and risk taking behaviour during this time. After this, the simulated phishing attack occurred, asking students to disclose their unique ID code due to lost information within the information technology database. Of the 299 participants included in the final analyses, 32% of these responded to the email and it was reported that success of the phishing attack was related to less web experience, less security knowledge, less suspicion of humanity, and lower computer self-efficacy.

However, one potentially problematic aspect of this experiment was that since starting their course, all students at the University were subject to a genuine phishing attack, which may have raised awareness of the issue, as a follow-up email was sent around from administrators warn-

ing students not to respond to such emails. The fact that the students had just studied a module on internet security may also have made them more wary of such attacks and may have led to a reduced response rate. Further to this, the participants had agreed to participate in a study concerning 'security research' and even though they had not been told they would receive a phishing email, they may have been more suspicious of such security breaches occurring.

All of these examples have the same fundamental problems that the likelihood of participants responding to an email is highly dependent on the content of the email itself and the context in which the email is received. The content can be manipulated by the researcher, however this would likely require a between subjects design, whereby each participant would only receive one email manipulation, as issues may arise from sending multiple email manipulations to the same participant. Even if they were unfamiliar with the research they would undoubtedly become suspicious and be less likely to respond upon receipt of numerous simulated emails. It is clear though that there are individual differences in response rates to phishing emails, so a between subjects design is not ideal, as this would require a large sample size to account for such individual differences. In addition, the context in which a participant receives or reads a simulated email cannot be manipulated in this situation, which would mean that the researcher would be reliant upon the participant to recall the situation they were in when they read the email. If a person chooses to respond and is told straight away about the purpose of the research then this is a legitimate option. However if a participant does not respond and is contacted with a follow-up questionnaire at a later date then it is unlikely they will remember what device they were using, what they were doing when they read the email, or how they felt at the time. In addition to this there are ethical issues surrounding sending fake phishing emails to un-informed participants and gaining post-consent, which are discussed in more detail below. Assuming that it were plausible to address these issues then email simulation would be the most reliable measure of susceptibility, however the difficulties involved in field research mean that this is challenging for the researcher, both ethically and practically.

ETHICAL CONSIDERATIONS

As with any research area surrounding criminal behaviour, this is a sensitive topic and victimisation could be an embarrassing and traumatising experience. From a research planning and implementation perspective, ethical considerations affect the feasibility or appropriateness of designing and carrying out studies that might illuminate any aspect of the decision-making process (ie. all sources of influence for Figure 1). Whilst lab-based email judgement tasks ought to be relatively straightforward ethically, and unlikely to negatively affect participants, there is evidence (Parsons et al., 2015) that the effects measured in such studies are more reliable when participants are unaware of the nature of the study. This means that a certain level of deception –withholding of research intentions - may be necessary, although given the controlled environment in which these studies are conducted, the type of task involved, and the opportunity for immediate debriefing at the conclusion of a session - the impact should be constrained to the task session alone. However, both work with past victims and simulation studies do elicit some further ethical concerns. In working with past victims of fraud, it is important for the researcher to remain sensitive to the traumatic experience that the user has been through. Reliving the experience may be difficult for some victims, especially those who lost substantial amounts of money, so it is important that the voluntary nature of their participation is emphasised. In addition to this, it is important to ensure that victims receive detailed information about where they can seek support for their victimisation in case reliving their experience has brought up negative emotions.

When using simulated phishing studies, there is a chance that those participants who chose to respond to the emails will feel embarrassed and upset that they have demonstrated such vulnerability in the same way that real life victims might. One suggested approach to deal with these ethical challenges is to invite participants to take part in a study in which they will receive a phishing email at some point in the near future. This way, participants are giving informed consent to participate and should be less negatively affected when they realise that the 'phishing' email they received is part of the study that they signed up to. However, the logic of taking this approach is that participants may forget that they have signed up to the study in the first place and so will respond to the email in the same way they would if it was a genuine email in their inbox. If this is the case, then this approach yields the same ethical issues as if the participants were not expected the email in the first place. If this is not the case, then the expected receipt of the email eradicates all validity from the method, as the participants will not manage the email in the same way as they would if it had been unexpected. Indeed, work in our lab suggests that informed consent prior to a phishing attack can reduce a user's likelihood to respond relative to post-event informed consent (Mack, 2014), which means informed consent can compromise, or at least affect, task validity. In all variations of this task, it would be crucial that participants are fully debriefed as soon as possible as to the true purpose of the study, and ideally be educated about the cues that they missed and how they might avoid falling for similar phishing attacks in the future. Finn and Jakobsson (2007) report that in their 2005 study, Jagatic et al. received only 30 complaints from over 1700 participants, and only 7 requested their data be removed from the study. Given the large sample size involved, and the deceptive nature of the study, these figures seem low, providing some reassurance that most participants are not commonly distressed or angered as a result of being deceived.

CONCLUSION AND RECOMMENDATIONS

All of the methodological approaches above would allow for manipulations of the email content to measure the influence of factors such as authority, familiarity, and quality of information – which are discussed above in relation to the theoretical approaches to this topic. However, the most realistic approaches that reflect real life situations are the most valuable methods, which in this case would be simulated phishing studies. As is the case in a lot of research though, this method is also the most ethically problematic, time consuming and research intensive. From an ethical perspective, asking participants to judge emails in a lab based setting with no deception is a relatively simple approach, and even minor deception about the nature of the study in this situation poses little ethical issue. However this provides limited insight into how users manage their own emails on a daily basis, when their own money and personal information is at risk.

Working with past victims seems to offer a balance between these two methods and their constraints, as the participants have demonstrated real life vulnerability. However the major concern in working with this kind of sample is that, depending on the source of the sample, victimisation is likely to have occurred some time ago, and it is possible that the victims have changed in terms of how they would respond to the assessments which you are supplying them with. This may be as a result of the victimisation, which may have changed their perspective on things, or it may just be a change that has occurred over time. Either way, any measures that researchers are trying to associate with victimisation may no longer be present in victims even if they were at the time of victimisation.

From a methodological perspective, sending out 'phishing' emails and assessing response is the only truly valid measure of susceptibility at the time of the study, and this is only valid if

the participant is not expecting the email. With the right approach, and close consideration of the ethical challenges, there is no reason that this should not be a plausible approach to assessing the psychology of scam victimisation. However, in situations where this is not an appropriate approach, researchers must use the resources available to best replicate a situation in which a participant is managing their own emails, with consideration of factors such as the relevance of the content of the emails to the user, and the context in which they are received.

Future research in this field would benefit from initial focus on how we can most accurately and effectively measure susceptibility under the constraints, both ethically and methodologically, which are commonly faced in empirical research. Only when such measures are recognised as having credibility and validity can we go on to explore the effects that factors, such as increased cognitive load, authority level of the sender, and working memory capacity, have on an individual's susceptibility to email fraud. In most of the studies cited here, there are evident differences in email management performance between participants, but whether this is due to susceptibility or due to each participant's interpretation of the task and the study environment, is yet to be evidenced.

ACKNOWLEDGMENT

This review stems from a project that is funded by the Ministry of Defence through the Defence Science and Technology Laboratory (Dstl) under the National PhD scheme. The authors would like to thank Timothy Harrison for his helpful comments on the review as it developed.

REFERENCES

Abu-Nimeh, S., Nappa, D., Wang, X., & Nair, S. (2007). A comparison of machine learning techniques for phishing detection. In *Proceedings of The Anti-Phishing Working Group's Second Annual eCrime Researchers Summit*, 60-69. ACM. doi:10.1145/1299015.1299021 doi:10.1145/1299015.1299021

Beede, K. E., & Kass, S. J. (2006). Engrossed in conversation: The impact of cell phones on simulated driving performance. Accident; Analysis and Prevention, 38(2), 415–421. doi:10.1016/j.aap.2005.10.015 PubMed doi:10.1016/j.aap.2005.10.015 PMID:16310750

Bergholz, A., De Beer, J., Glahn, S., Moens, M. F., Paaß, G., & Strobel, S. (2010). New filtering approaches for phishing email. Journal of Computer Security, 18, 7–35.

Cialdini, R. B. (1993). Influence: The Psychology of Persuasion. New York: Quill William Morrow.

Cokely, E. T., & Kelley, C. M. (2009). Cognitive abilities and superior decision making under risk: A protocol analysis and process model evaluation. Judgment and Decision Making, 4(1), 20–33.

Colflesh, C. J., & Conway, A. R. (2007). Individual differences in working memory capacity and divided attention in dichotic listening. Psychonomic Bulletin & Review, 14(4), 699–703. doi:10.3758/BF03196824 PubMed doi:10.3758/BF03196824 PMID:17972736

Conway, A. R., Jarrold, C., Kane, M., Miyake, A., & Towse, J. N. (Eds.). (2007). Variation in Working Memory. New York: Oxford University Press.

Conway, A. R. A., Kane, M. J., Bunting, M. F., Hambrick, D. Z., Wilhelm, O., & Engle, R. W. (2005). Working memory span tasks: A methodological review and user's guide. Psychonomic Bulletin & Review, 12(5), 769–786. doi:10.3758/BF03196772 PubMed doi:10.3758/BF03196772 PMID:16523997

Copes, H., Kerley, K. R., Mason, K. A., & Van Wyk, J. (2001). Reporting behavior of fraud victims and Black's theory of law: An empirical assessment. Justice Quarterly, 18(2), 343–363. doi:10.1080/07418820100094931 doi:10.1080/07418820100094931

Dong, X., Clarke, J. A., & Jacob, J. (2008). Modelling user-phishing interaction. In Proceedings of Human System Interaction, 627-632. IEEE.

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioural response to phishing risk. In *Proceedings of the Anti-Phishing Working Groups Second Annual eCrime Researchers Summit*, 37-44. ACM. doi:10.1145/1299015.1299019 doi:10.1145/1299015.1299019

Egelman, S., Cranor, L. F., & Hong, J. (2008). You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1065-1074. ACM.

Evans, J. B. T. (2003). In two minds: Dual-process accounts of reasoning. Trends in Cognitive Sciences, 7(10), 454–459. doi:10.1016/j.tics.2003.08.012 PubMed doi:10.1016/j.tics.2003.08.012 PMID:14550493

Fette, I., Sadeh, N., & Tomasic, A. (2007). Learning to detect phishing emails. In *Proceedings of the 16th International World Wide Web Conference*, 649-656. ACM. doi:10.1145/1242572.1242660 doi:10.1145/1242572.1242660

Finn, P., & Jakobsson, M. (2007). Designing ethical phishing experiments. Technology and Society Magazine, IEEE, 26(1), 46–58. doi:10.1109/MTAS.2007.335565 doi:10.1109/MTAS.2007.335565

Garera, S., Provos, N., Chew, M., & Rubin, A. D. (2007). A framework for detection and measurement of phishing attacks. In *Proceedings of the 2007 ACM Workshop on Recurring Malcode*, 1-8. ACM. doi:10.1145/1314389.1314391 doi:10.1145/1314389.1314391

Goldberg, L. R. (1999). A broad-bandwidth, public domain, personality inventory measuring the lower-level facets of several five-factor models. In I. Mervielde, I. Deary, F. De Fruyt, & F. Ostendorf (Eds.), Personality Psychology in Europe, 7, 7- 28. Tilburg, The Netherlands: Tilburg University Press.

Guéguen, N., & Jacob, C. (2002). Solicitation by e-mail and solicitor's status: A field study of social influence on the web. CyberPsychology & Behaviour, 5(4), 377–383. doi:10.1089/109493102760275626 PubMed doi:10.1089/109493102760275626 PMID:12216702

Hinson, J. M., Jameson, T. L., & Whitney, P. (2003). Impulsive decision making and working memory. Journal of Experimental Psychology. Learning, Memory, and Cognition, 29(2), 298–306. doi:10.1037/0278-7393.29.2.298 PubMed doi:10.1037/0278-7393.29.2.298 PMID:12696817

Holtfreter, K., Reisig, M. D., Piquero, N. L., & Piquero, A. R. (2010). Low self-control and fraud offending, victimization, and their overlap. Criminal Justice and Behavior, 37(2), 188–203. doi:10.1177/0093854809354977 doi:10.1177/0093854809354977

Islam, R., & Abawajy, J. (2013). A multi-tier phishing detection and filtering approach. Journal of Network and Computer Applications, 36(1), 324–335. doi:10.1016/j.jnca.2012.05.009 doi:10.1016/j.jnca.2012.05.009

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2005). Social phishing. Communications of the ACM, 50(10), 94–100. doi:10.1145/1290958.1290968 doi:10.1145/1290958.1290968

Kahneman, D. (2000). A psychological point of view: Violations of rational rules as a diagnostic of mental processes. Behavioral and Brain Sciences, 23(5), 681–683. doi:10.1017/S0140525X00403432 doi:10.1017/S0140525X00403432

Kane, M. J., Bleckley, M. K., Conway, A. R. A., & Engle, R. W. (2001). A controlled- attention view of working-memory capacity. Journal of Experimental Psychology. General, 130(2), 169–183. doi:10.1037/0096-3445.130.2.169 PubMed doi:10.1037/0096-3445.130.2.169 PMID:11409097

Karat, J., Karat, C., & Brodie, C. (2009). Human-computer interaction viewed from the intersection of privacy, security, and trust. In A. Sears, and J. A. Jacko (Eds.), Human-Computer Interaction: Design Issues, Solutions, and Applications, 311-330. Boca Raton, FL: CRC Press. doi:10.1201/9781420088861.ch16 doi:10.1201/9781420088861.ch16

Kerley, K. R., & Copes, H. (2002). Personal fraud victims and their official responses to victimization. Journal of Police and Criminal Psychology, 17(1), 19–35. doi:10.1007/BF02802859 doi:10.1007/BF02802859

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

Lauriola, M., & Levin, I. P. (2001). Personality traits and risky decision-making in a controlled experimental task: An exploratory study. Personality and Individual Differences, 31(2), 215–226. doi:10.1016/S0191-8869(00)00130-6 doi:10.1016/S0191-8869(00)00130-6

Mack, S. (2014). Reasoning and judgements made in an online capacity. An exploration of how phishing emails influence decision making strategies (Unpublished dissertation). Lancaster University, Lancaster, UK.

Miyake, A., Just, M. A., & Carpenter, P. A. (1994). Working memory constraints on the resolution of lexical ambiguity: Maintaining multiple interpretations in neutral contexts. Journal of Memory and Language, 33(2), 175–202. doi:10.1006/jmla.1994.1009 doi:10.1006/jmla.1994.1009

Modic, D., & Anderson, R. J. (2014). We will make you like our research: The development of a susceptibility-to-persuasion scale. *Social Sciences Research Network*. Retrieved from http://ssrn.com/abstract=2446971 [16/07/14].

Modic, D., & Lea, S. E. G. (2011). *How neurotic are scam victims, really? The big five and Internet scams*. Paper presented at the 2011 Conference of the International Confederation for the Advancement of Behavioral Economics and Economic Psychology, Exeter: UK.

Modic, D., & Lea, S. E. G. (2013). Scam compliance and the psychology of persuasion. *Social Sciences Research Network*. Retrieved at http://ssrn.com/abstract=2364464 [16/07/14].

Moore, A. B., Clark, B. A., & Kane, M. J. (2008). Who shalt not kill? Individual differences in working memory capacity, executive control, and moral judgement. Psychological Science, 19(6), 549–557. doi:10.1111/j.1467-9280.2008.02122.x PubMed doi:10.1111/j.1467-9280.2008.02122.x PMID:18578844

Myers, S. (2007). Introduction to phishing. In M. Jakobsson & S. Myers (Eds.), Phishing and Countermeasures (pp. 1–29). New Jersey: John Wiley & Sons, Inc.

National Fraud Authority. (2011). A quantitative segmentation of the UK population. Helping to determine how, why and when citizens become victims of fraud. Accessed at: https://www.gov.uk/government/uploads/system/uploads/ attachment_data/file/118481/national-fraud-segmentation.pdf [accessed 08/07/2013].

Norton (2014). Online fraud: Phishing. Retrieved from http://uk.norton.com/cybercrime- phishing [12/07/14].

Norton Cybercrime Report. (2013). Retrieved from http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid =norton- report-2013 [11/01/13].

Ordóñez, L., and Benson III, L. (1997). Decisions under time pressure: How time constraint affects risky decision making. *Organizational Behaviour and Human Decision Processes, 71* (2), 121-140.

Pak, K. B. S., & Shadel, D. P. (2011). AARP Foundation National Fraud Victim Study. Retrieved from http://assets.aarp.org/rgcenter/econ/fraud-victims-11.pdf [05/09/13].

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (in press). The design of phishing studies: Challenges for researchers. Computers & Security.

Salah, K., Alcaraz Calero, J. M., Zeadally, S., Al-Mulla, S., & Alzaabi, M. (2013). Using cloud computing to implement a security overlay network. IEEE Security and Privacy, 11(1), 44–53.

Shadel, D. P., & Pak, K. B. S. (2007). *The Psychology of Consumer Fraud*. (Unpublished doctoral thesis). Tilburg University, Netherlands.

Sheng, S., Holbrook, M. B., Kumaraguru, P., Cranor, L. F., & Downs, J. S. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 373-382. ACM.

Stanovich, K. E. (1999). Who is rational? Studies of individual differences in reasoning. Mahwah, NJ: Erlbaum.

Tangney, J. P., Baumeister, R. F., & Boone, A. L. (2004). High self-control predicts good adjustment, less pathology, better grades, and interpersonal success. Journal of Personality, 72(2), 271–324. doi:10.1111/j.0022-3506.2004.00263.x PubMed doi:10.1111/j.0022-3506.2004.00263.x PMID:15016066

Titus, R. M., Heinzelmann, F., & Boyle, J. M. (1995). Victimization of persons by fraud. Crime and Delinquency, 41(1), 54–72. doi:10.1177/0011128795041001004 doi:10.1177/0011128795041001004

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. Cyberpsychology, Behavior, and Social Networking, 15(3), 181–183. doi:10.1089/cyber.2011.0352 PubMed doi:10.1089/cyber.2011.0352 PMID:22304401

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. Journal of Management Information Systems, 27(1), 273–303. doi:10.2753/MIS0742-1222270111 doi:10.2753/MIS0742-1222270111

Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI conference on Human Factors in computing systems,* 601-610. ACM. doi:10.1145/1124772.1124863 doi:10.1145/1124772.1124863

Yan, Z., & Gozu, H. Y. (2012). Online Decision-Making in Receiving Spam Emails Among College Students. [IJCBPL]. International Journal of Cyber Behavior, Psychology and Learning, 2(1), 1–12. doi:10.4018/ijcbpl.2012010101 doi:10.4018/ijcbpl.2012010101

CALL FOR ARTICLES

International Journal of Cyber Behavior, Psychology and Learning

An official publication of the Information Resources Management Association

MISSION:

The mission of the **International Journal of Cyber Behavior, Psychology and Learning (IJCBPL)** is to identify learners' online behavior based on the theories in human psychology, define online education phenomena as explained by the social and cognitive learning theories and principles, and interpret the complexity of cyber learning. IJCBPL offers a multi-disciplinary approach that incorporates the findings from brain research, biology, psychology, human cognition, developmental theory, sociology, motivation theory, and social behavior. This journal welcomes both quantitative and qualitative studies using experimental design, as well as ethnographic methods to understand the dynamics of cyber learning. Impacting multiple areas of research and practices, including secondary and higher education, professional training, Web-based design and development, media learning, adolescent education, school and community, and social communication, IJCBPL targets school teachers, counselors, researchers, and online designers.

ISSN 2155-7136
eISSN2155-7144
Published quarterly

COVERAGE/MAJOR TOPICS:

- Cognitive and information processing related to online learning including cognitive architecture and online information processing
- Motivation
- Online behavior such as online gaming, online addiction, and Internet predation
- Online training, online instructional design, and development with a focus on cognitive and psychological processes
- Psychological aspects of online learning and instruction, including individual differences and psychological and personal traits
- Social aspects of online learning including online social communication and relationship formation

All inquiries regarding IJCBPL should be directed to the attention of:
Robert K. Atkinson (ijcbpl@igi-global.com), Editor-in-Chief
<a href="mailto:zyan@albany.edu">
All manuscript submissions to IJCBPL should be sent through the online submission system:
http://www.igi-global.com/authorseditors/titlesubmission/newproject.aspx

Ideas for Special Theme Issues may be submitted to the Editor-in-Chief.

Please recommend this publication to your librarian. For a convenient easy-to-use library recommendation form, please visit:
http://www.igi-global.com/IJCBPL