

## Aberystwyth University

### *Personality, emotion, and individual differences in response to online fraud*

Norris, Gareth; Brookes, Alexandra

*Published in:*

Personality and Individual Differences

*DOI:*

[10.1016/j.paid.2020.109847](https://doi.org/10.1016/j.paid.2020.109847)

*Publication date:*

2021

*Citation for published version (APA):*

Norris, G., & Brookes, A. (2021). Personality, emotion, and individual differences in response to online fraud. *Personality and Individual Differences*, 169, Article 109847. <https://doi.org/10.1016/j.paid.2020.109847>

#### **Document License** CC BY-NC-ND

#### **General rights**

Copyright and moral rights for the publications made accessible in the Aberystwyth Research Portal (the Institutional Repository) are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the Aberystwyth Research Portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the Aberystwyth Research Portal

#### **Take down policy**

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

tel: +44 1970 62 2400  
email: [is@aber.ac.uk](mailto:is@aber.ac.uk)

Manuscript Number:

Title: Personality, emotion and individual differences in response to online fraud.

Article Type: SI: PAID40 (Invited)

Section/Category: Review Article (<10,000 words)

Keywords: emotion, personality, decision making, fraud, internet

Corresponding Author: Dr. Gareth Norris, Ph.D

Corresponding Author's Institution: Aberystwyth University

First Author: Gareth Norris, Ph.D

Order of Authors: Gareth Norris, Ph.D; Alexandra Brookes

Abstract: The growth in social communication facilitated by technology mean that online scams represent a growing societal issue, with perpetrators successfully persuading people to make fraudulent payments or download malicious attachments. Incidents of online scams have continued to increase across the world, aided by technology that allows fraudsters to mimic communications so as to appear to come from legitimate sources. Much of the previous literature has focused on dispositional factors, such as personality, alongside experiential factors, such as knowledge of security policy; there is limited examination of the context or state induced factors, such as emotional state of the individual, and, importantly, how that may impact upon their decision making process. This paper reviews and applies the literature exploring the role of emotions in decision making to understand how individuals may be susceptible to scams in online contexts. The mood maintenance/mood-repair view is proposed as an appropriate theoretical foundation for research in this area; it provides the focus on the interaction between the individuals current emotional state and the emotional appeals embedded in any message, and what the likely response will be.

Dr Gareth Norris\*

Alexandra Brookes

Department of Psychology  
Aberystwyth University  
Penglais Campus  
Aberystwyth  
SY23 3UX

\*corresponding author (ggn@aber.ac.uk)

# Personality, emotion and individual differences in response to online fraud.

## Abstract

The growth in social communication facilitated by technology mean that online scams represent a growing societal issue, with perpetrators successfully persuading people to make fraudulent payments or download malicious attachments. Incidents of online scams have continued to increase across the world, aided by technology that allows fraudsters to mimic communications so as to appear to come from legitimate sources. Much of the previous literature has focused on dispositional factors, such as personality, alongside experiential factors, such as knowledge of security policy; there is limited examination of the context or state induced factors, such as emotional state of the individual, and, importantly, how that may impact upon their decision making process. This paper reviews and applies the literature exploring the role of emotions in decision making to understand how individuals may be susceptible to scams in online contexts. The mood maintenance/mood-repair view is proposed as an appropriate theoretical foundation for research in this area; it provides the focus on the interaction between the individuals current emotional state and the emotional appeals embedded in any message, and what the likely response will be.

## Introduction

Psychological research has been applied to a range of critical behavioural issues such as responses to climate change and global health challenges. Psychological models provide a valuable way to demonstrate the processes which underlie behavioural decisions, for example, recycling (Poškus & Žukauskienė, 2017) and smoking cessation (Sharma, Khubchandani & Nahar, 2017). Consistently we witness seemingly irrational behaviour in light of overriding scientific evidence. The ability to detect fraudulent communications is another example of how a seemingly rational decision maker can be easily deceived. The rapid development of technology in recent years has facilitated more opportunities for computer-mediated communication that crosses geographical divides (Williams, Beardmore & Joinson, 2017). However, this growth in technology enhanced communication has also increased opportunities for individuals to engage in behaviours online for illegitimate financial or other malicious gain (for example, non-financially motivated blackmail). These processes are generally referred to as ‘social engineering’ (Anderson, 2008), and, specifically, are online influence attempts often involving ‘phishing’ emails. Phishing emails frequently persuade recipients to click on links to spoof websites or include an attachment that would download malicious spyware to data-mine the victim’s computer for passwords, usernames and credit card information. Indeed, it is estimated globally that 29 billion phishing emails are sent daily with the aim of victimising unsuspecting individuals (Button & Cross, 2017, p 23). Victims of these scams frequently suffer substantial psychological and financial distress (Pascoe, Owen, Keats & Gill, 2006; Titus & Gover, 2001), whilst the use of technologies to gain access to corporate information can disrupt services and have wider societal consequences (BBC, 2017). In order to counter this global threat, there is an increasing need to understand why certain people fall victim to online fraud, so that effective mitigation methods may be developed. Thus, this review aims to identify fruitful avenues for future study to encourage a more comprehensive understanding of how individuals might be susceptible to scams in online contexts.

## Individual Differences: are some people more susceptible?

Any attempt to mitigate the threat posed by online scams requires an understanding of why some individuals appear to be more susceptible to malicious influence attempts than others. The outcomes can be used to develop targeted consumer education measures, for example, or to curtail the activities of particular fraudulent websites/organisations. Research examining online deception has demonstrated that scammers aim to target and exploit both the social and technical vulnerabilities of individuals (Jagatic, Johnson, Jakobson & Menczer, 2007). Much of this previous research has focused upon demographic factors, such as age, gender, income and education (e.g. Purkait, Kumar,

& Suar, 2014), although results are equivocal and some variables such as age actually proving protective factors (i.e. many older people don't use the Web for banking or shopping; Hussain, Ross & Bednar, 2018). In a recent report of fraud typologies and victims published by the UK National Fraud Authority (NFA), Button, Lewis & Tapley (2016) caution that: "[...] what is striking about the scams is that the profiles cover almost everybody; hence almost anyone could become a victim of a scam" (p.24). Therefore, although the literature reports some small variations in demographics of fraud victims (e.g. age and gender), these findings do not provide a strong foundation on which to develop targeted consumer protection efforts (Correia, 2019). This is suggested as successful mitigation methods cannot be developed from inconclusive or unclear findings associating demographic factors with susceptibility to online scams.

Recognising this issue, recent research refocuses on the importance understanding the individual cognitive and psychological factors that lead people to enact erroneous decision process when responding to fraudulent online messages (Harrison, Svetieva & Vishwanath, 2015; Norris, Brookes & Dowell, 2019). One promising body of research has found that victimised individuals often fail to recognise deception cues within fraudulent communications due to psychological factors (e.g. personality, low self-control, impulsivity and need for cognition), and this may reflect the amount of cognitive effort they expend when processing any message (Holtfreter, Reisig, & Pratt, 2008; Harrison, Vishwanath, Ng & Rao, 2015; Modic, Anderson & Palomaki, 2018; Pattinson et al. 2011; Vishwanath, Herath, Chen, Wang & Rao, 2011). Cognitive/psychological models suggest that upon being exposed to deceptive communications, individuals who hold such psychological characteristics associated with victimisation have an increased tendency to utilise heuristics to make quick – often erroneous – decisions (Vishwanath et al. 2011). Individual differences in information processing lead some people to focus on specific elements in the fraudulent communication, such as warnings of bank account closure, while ignoring other message features, such as grammatical errors or incorrect logos, that might expose potential deception.

Additional models of phishing susceptibility, such as the Integrated Information Processing Model (IIPM; Vishwanath et al., 2011) and the Suspicion, Cognition and Automaticity Model (SCAM; Vishwanath, Harrison, & Ng, 2018), takes this research a step further and engage with the wider persuasion literature by applying dual process models, including the Elaboration Likelihood Model (ELM; Petty & Cacioppo, 1986) and Heuristic-Systematic Model (HSM; Eagly & Chaiken, 1993). These models support the findings of more general studies on fraud by highlighting the role of individual differences in the depth of processing that a person engages in when encountering a potential scam message. However, although these models have incorporated individual variables, such as personality, existent research in this area has largely ignored the potential impact of context or state-induced factors, such as an individual's integral or incidental emotional state at the time of receiving the deceptive message. In a recently published review of the literature, Williams et al. (2017) reasoned that the impact of emotions on responding to online scams ought to be a pressing area of future study, suggesting that an individual's current emotional state shapes their decisions by moderating attention, perception and depth of information processing. Thus, it appears that a consideration of the emotions experienced by an individual at the time of receiving a fraudulent message, may help to answer the central research question: 'what makes certain people more susceptible to fall victim to online fraud than others?'

In the sections that follow, we delve further into theoretical evidence of how an individual's emotional state could influence online scam victimisation through its influence on information processing. A lack of research regarding the role of emotions in susceptibility to online scams necessitates findings from other fields provide the basis for hypothesis development in this area. For example, research aiming to understand the effects of emotion on the persuasiveness of advertisements (e.g. Kircanski et al, 2018) can be applied to postulate an interaction between emotion and the persuasiveness of scam emails, as both advertisements and scam emails are types of persuasive messages that aim to convince the individual to take specific actions. One consistently cited model in this field is the ELM (Petty & Cacioppo, 1986); research employing the ELM to study consumer behavior and persuasion suggests two key processes in which emotional arousal may impact upon susceptibility to online influence: the central and peripheral processing routes. As such, this review first briefly outlines the ELM, followed by an exploration of how *integral* emotion (i.e. an emotional state directly triggered by an appeal embedded in the scam message, such as a fear appeal)

and *incidental* emotion (i.e. an individual's mood at the time of receiving the scam message not relevant for deciding, such as feeling fear about giving a speech at work when choosing to respond to a phishing email) may influence an individual's decision making process when exposed to a deceptive message. Finally, the review concludes by focusing on the possible interaction between incidental and integral emotion when considering the likely response behaviour of the individual to a scam message and proposes the mood maintenance/mood repair view (e.g. Isen & Geva, 1987; Wegener & Petty, 1994) as the most promising theoretical foundation for research in this area.

## The Elaboration Likelihood Model: the importance of emotion in attention and elaboration

In the persuasion and decision-making literature, the term emotion is often broadly employed to refer to specific affect states such as sadness or happiness (e.g. Ekman, 1972), as well as more general states that are often referred to as moods (e.g. Forgas, 1995). The research available suggests that a person's emotions, whether stemming from the persuasive message (e.g. fear appeals) or incidental factors (e.g. feeling fear about giving a speech at work) can influence their evaluative judgements through differing cognitive and meta-cognitive processes (Petty & Brinol, 2015). In order to provide a general framework to understand the effects that emotion can produce on judgements, much of the work in this area has been conducted using the ELM of persuasion (Petty & Cacioppo, 1986).

ELM is a dual-process model that distinguishes between two ways in which individuals process available information. The central route involves careful scrutiny of the information presented in the message and cross referencing with prior knowledge, contrasting with the peripheral processing route which relies on simple cues to make decisions regarding message legitimacy. The latter sacrifices consideration of all the elements of the message in exchange for expediency and/or reduced resource expenditure. The ability to process information in different ways can affect an individual's attitudes, judgements and behaviors towards any message, subsequently resulting in differing levels of susceptibility to the persuasive stimuli (Petty & Cacioppo, 1986). When an individual uses the central route to process a message, such as a phishing email, they engage in two sub-processes referred to as attention and elaboration. The degree of attention paid by an individual is set by the amount of mental focus they give to certain elements of the message. The subsequent elaboration process occurs when the individual makes connections between these elements and their prior knowledge.

ELM provides a convenient theoretical framework for understanding the process of scam compliance, because it enables an examination of how attention to message cues and elaboration of scam messages can result in victimisation (Harrison et al, 2015). Alongside attention, it also provides a general theoretical premise to examine how focusing upon certain cues in a scam message can influence both the nature and extent of elaboration. For example, upon receiving a phishing email an individual might read the sender's email address, name, and/or the subject line before actually opening the email (in essence what ELM deems 'attention'). This initial consideration may compel the receiver to search for further cues in the message (the ELM process of 'elaboration'), connecting them to their existing knowledge and potentially reaching the conclusion the email is fraudulent. However, individuals who do not closely attend to the same email details, could neglect to elaborate on the message and judge the email as legitimate and relevant (Harrison et al, 2015; Vishwanath et al., 2011). In essence, ELM suggests that differences in processing in terms of an individual's attention and elaboration of the message ultimately lead to differences in susceptibility to falling victim to scams.

Additionally, ELM also suggests processing is heavily contingent on the information presented in the persuasive message (e.g. message cues, such as fear appeals) and individual differences (e.g. individuals mood at the time of receiving the message), as these variables can moderate the route of persuasion taken by an individual (Petty & Cacioppo, 1986). Research examining the impact of emotion on the persuasiveness of a message has increased greatly in recent years (Lerner, Li, Valdesolo & Kassam, 2015). In a recent review of this body of literature, Petty and Brinol (2015) argue that emotions can have a pervasive impact on persuasion: "[...]affecting the direction of thoughts that come to mind (i.e. bias thinking) or even by determining whether people use their thoughts or not [...] emotions can also influence judgements by determining the amount of

processing that takes place (i.e. the amount of attention and elaboration given to a message)” (p.2). Hence, we need to expand our exploration by examining the integral emotional factors embedded *within* scam messages and how they might influence information processing.

## Integral Emotion as a Fraud Tactic

In the context of online scam communications, the perpetrator attempts to persuade the victim into disclosing personal details by developing a message that encourages attention to certain message cues, whilst simultaneously reducing any elaboration that might result in deception detection (Gragg, 2003; Rush, 1999). Interestingly, Workman (2008) argues that online scammers specifically craft phishing emails so that they decrease the amount of cognitive processing (i.e. attention and elaboration) of a message. For example, the message argument developed in a phishing email tends to be brief and often relies on urgency cues, employing words such as “warning” or “deadline”, alongside phrases implying a loss, such as “imminent account closure” (Harrison et al, 2015). Scammers intend for these phrases to cause ‘emotional reactions’ and lead receivers to act quickly, bypassing their central more rational decision-making processes and ignoring other cues that might highlight the message to be illegitimate (Harrison et al., 2016; Vishwanath et al., 2011).

The emotion phrases cited are examples of a scammer incorporating an element of threat or fear into the message (e.g. by suggesting that a bank account is about to be closed or implying that it has otherwise been compromised). A content analysis study revealed that this fear inducing tactic is used by scammers in over 60% of phishing emails (Kim & Kim, 2013). Such fear arousing content in a scam message is commonly referred to as a ‘fear appeal’ (Petty & Brinol, 2015), and could lead to increased acceptance of deceptive messages due to the specific effect on information processing. Fear appeals are one of the most studied methods of inciting attitude change in the wider persuasion literature (Wegener & Petty, 2001). For example, fear appeal research has been practically applied by policy makers to motivate individuals to cease smoking by the wide-scale implementation of health warnings on cigarette packages (Ruiter, Kessels, Peters & Kok, 2014). When very strong negative consequences (e.g. loss of personal details or money) are implied if an advocacy is not adopted (i.e. a fear appeal is being attempted), this can often result in a negatively valenced emotional state being experienced by the recipient of the message (Petty, Desteno, & Rucker, 2001). This negative state motivates the individual to engage in precautionary and self-protective behaviors, which encourages agreement with the message to avert the negative consequences it presents (Fishbein & Ajzen, 1975). Thus, it can be argued that fear appeals are effective because they present extremely negative consequences as being likely to occur unless the recipient agrees with the message. In fact, a meta-analysis of the fear appeal literature indicated that increasing fear is associated with an increase in persuasion (Boster & Mongeau, 1984) due to high-fear messages encouraging a more peripheral route of processing (Hale, Lemieux & Mongeau, 1995).

The dominant theoretical perspective in the literature focusing on the conditions needed for fear appeals to be successful is Rodgers’ (1983) Protection Motivation Theory. This model suggests that fear appeals will be effective to the extent that the message convinces the recipient that the consequences are highly undesirable and likely to occur if the proposed action is not taken. Importantly, this model also holds that effective fear appeals should also convey that the negative consequences can be avoided if the proposed action is followed and that the recipient also has the correct skills to be able to complete the recommended action. Extensive literature supports these predictions and has shown that if an individual does not believe that they can cope effectively with a threat, then increasing the threat tends to elicit a ‘boomerang effect’ (Petty, Desteno, & Rucker, 2001, p. 218), potentially as a consequence of trying to restore control and/or reduce fear. Applying this model in the context of online influence, protection motivation theory suggests that fear could be one effective method used by scammers. However, to be effective the negative consequences embedded in the scam message (i.e. phishing email) must enhance the realization that some consequence (e.g. bank account closure) is severe and likely but can be prevented by following the actions suggested (e.g. providing personal details or money).

While many scam messages aim to incite fear, others attempt to persuade individuals by creating a reward-based argument, whereby the scammer offers them something (i.e. goods or money)

of value (Gragg, 2003; Horvitz & Pratkanis, 2002; Rush, 1999). The notorious Nigerian '419' scam provides a useful example of how a widely successful phishing attack can be based on the assurance of an alluring reward (Harrison et al., 2016). These scams and others like them, encourage individuals to provide bank account and personal details by promising that they will receive a significant percentage of money from a multimillion-pound bank account in return for assistance in transferring this large amount of money out of Nigeria [and other countries] (Harrison et al., 2016). Despite the apparent risks, significant numbers of seemingly rational individuals parted with their savings. Over three decades of research on fear appeals and framing effects (not just in relation to Internet fraud) have demonstrated that negative, fear inciting information (i.e. threats, warnings and deadlines), is more salient during information processing than positive, reward-based information (O'Keefe & Jensen, 2008). Such a finding is primarily supported by research on the phenomenon of negativity bias, in essence the heightened impact of and sensitivity to negative information (Cacioppo, Gardner, & Berntson, 1997). Negative stimuli are preferentially detected at lower levels of exposure than positive stimuli (Dijksterhuis & Aarts, 2003) and also evoke stronger or faster reactions than do positive events (O'Keefe & Jensen, 2008). Taken together, negativity bias suggests that fear-based scam messages are more likely to result in victimisation than a positive or reward-based message, largely due to fear appeals reducing the amount of attention and elaboration an individual is likely to exert when receiving the scam message.

Although many studies (e.g. Ferreira & Teles, 2019) have noted the presence of these emotional appeals in scam messages, limited research has directly examined if these appeals affect an individual's decision-making process at the time of receiving a scam message (Goel, Williams & Dincelli, 2017; Harrison et al., 2015; Williams & Polage, 2019). A recent laboratory experiment conducted by Williams & Polage (2019) goes some way to address this issue. In this study, the authors manipulated the scam emails according to whether they contained fear or reward-based influence techniques. The reward based emails offered recipients with a reward for responding (e.g. Just click HERE to be in with a chance to win!), whereas the fear based email suggested to the recipient that they would lose access to something if they failed to respond (e.g. Your internet banking has been temporarily suspended...Click HERE to reinstate your account). The results suggest that individuals are more likely to judge fear based phishing emails as trustworthy than reward-based phishing emails. Similarly, fear based phishing emails were more likely to be rated by participants as 'respond' than reward based phishing emails, which were often rated 'ignore'. While further empirical research is needed to support and clarify these results, this initial research supports the notion that individuals may base their judgements on their emotional response to the content of a scam message (e.g. excitement or fear) rather than on systematic consideration of the various risks and benefits of the proposed actions.

## Incidental Emotion and Scam Compliance

In the research on affect laden messages and fear appeals reviewed above, emotion is induced by - and is part of - the persuasive communication itself. In other research, effects of incidental emotions are more explicitly examined. For example, in a classic experimental study, Petty, Cacioppo & Schumann (1993) made participants feel happy by watching an enjoyable film prior to the presentation of the persuasive message on an unrelated topic [to the induced affect]. This approach enabled the researchers to study and measure the impact of general positive mood on persuasion likelihood (Petty, Cacioppo & Schumann, 1993). The effects of incidental emotions have also been applied in areas closely related to online fraud. Research by Kircanski et al (2018) outlines the significant interaction between emotional state of an individual and the persuasiveness of misleading advertisements. Throughout the majority of the affect-cognition literature using ELM as a general framework, findings often suggest two cognitive mechanisms responsible for moods effect on judgements: (1) *informational effects* (influencing the content and valence of thinking under high and low elaboration conditions), and, (2) *processing effects* (influencing the process of thinking under unconstrained elaboration conditions; Forgas, 2017). The potential effect of incidental emotion on vulnerability to online scam messages will be discussed in this review using these two cognitive mechanisms as a guide. This will effectively organize the mechanisms by which emotions can



produce their effects on an individual's attitudes and judgements concerning the legitimacy of email communications.

### **Informational effects.**

Incidental emotions may influence legitimacy judgements of scam messages by biasing thoughts relating to the message (Petty & Brinol, 2015). The idea that an individual's mood state can bias cognition stems from associative network theories of memory, which suggest that emotions enhance the retrieval of emotionally congruent information and inhibit the retrieval of emotionally unrelated information (Bower, 1981). Stated simply, when in a positive (negative) mood a heightened accessibility of memories associated with positive (negative) events will prime the individual's assessment of the information presented. This then can lead to positive (negative) events to be seen as more likely (Johnson & Tversky, 1983) or desirable (Petty & Wegener, 1991). Thus, in the context of deceptive scam messages received online, a positive mood should prime a more positive, trusting, evaluation of a message (i.e. phishing email), whereas a negative mood should prime greater skepticism and rejection.

Recent theories of affect and cognition, such as the Affect Infusion Model (AIM; Forgas, 1995, 2002) specifically predict that this mood congruent bias should occur when individuals engage in high levels of elaboration (i.e. they are motivated and able to process the message). However, there will be situations when scam messages are received by individuals who are not motivated (e.g. the individual has low personal responsibility for the consequences) or cognitively capable (i.e. a distraction is present) to think carefully about the influence attempt. In this instance we may, for example, think of a phishing email targeting a business that is received by a tired or busy employee on their work computer. In this context, persuasion relevant variables, such as incidental emotion, can have an impact on judgments through relatively low effort and peripheral route processes. Specifically, in low effort situations, incidental emotions influence attitudes in accord with their valence (Petty & Brinol, 2015). That is, if the message is associated with a positive emotional state (e.g. happiness), the arguments presented will be liked more and seen as more trustworthy or desirable than if associated with a negative emotional state (e.g. fear). While these effects may appear similar to mood congruent bias discussed above, the underlying process of how this judgment is reached under low elaboration conditions differs significantly.

A number of low effort psychological processes have been suggested to explain how incidental emotions can influence judgements when cognitive effort is low, including emotion-based heuristics (Schwartz & Clore, 1983), classical conditioning (Staats & Staats, 1958), misattribution of an emotional state to the attitude object (Jones Fazio & Olson, 2009) and direct transfer of affect (Payne, 2005). Although the various individual accounts differ in certain ways, they all hold that incidental emotion is automatically or purposely misattributed to one's attitude (i.e. my positive mood reflects my positive attitude), the message (i.e. my positive feeling means I agree with the message), or object (i.e. I feel good, so I must like the object; Petty & Brinol, 2015). Hence, these findings may be applied to understand how an individual holding low motivation may respond to a scam message (e.g. phishing email). In these conditions, emotion may be misattributed as their attitude towards the email (i.e. I feel positive so I will agree with the message) or potentially convey the trustworthiness of the message source (i.e. I feel positive so I must trust the message). Importantly, this process underlying the impact of incidental emotion on scam likelihood would differ to that of mood congruent bias, as it does not require significant input in the way of cognitive motivation or capacity on behalf of the receiver.

### **Processing effects.**

As detailed at the outset of this section, when applying dual-process theories (ELM; Petty & Cacioppo, 1986), it can be hypothesized that incidental emotions may influence someone to respond to a potentially fraudulent communication online in several ways. In some situations, emotions may exert influence by biasing initial thoughts, whereas at other times invoke peripheral processes (i.e. be used as a heuristic). In addition to these mood-congruent informational effects discussed above, incidental emotions can also impact the extent of the processing a scam message receives. Therefore,

in instances whereby the level of elaboration a scam message receives is not set by other variables (i.e. personal relevance) to be high or low, an individual's emotional state could determine whether to think carefully or not about the deceptive message (Petty & Brinol, 2015).

The majority of research in this area suggests a general pattern. Individuals experiencing a positive mood state are typically less likely to engage in effortful processing of the persuasive appeal in comparison to those experiencing a negative mood state and are therefore more likely to be persuaded by its arguments (Bless, Bohner, Schwarz & Strack, 1990; Bohner, Crow, Erb, & Schwarz, 1992; Mackie & Worth, 1989). There are a number of theoretical accounts of how these emotional states influence thinking. According to Worth & Mackie (1987), the presence of a positive mood state limits individuals' cognitive capacities and, thereby, inhibits their ability to effortfully process information. However, currently one of the most accepted theoretical explanations for the effect of incidental emotion on the level of processing is the feelings-as-information or cognitive tuning account (Schwarz, Bless & Bohner, 1991; Schwarz & Clore, 1983). The basic assumption of this approach is that negative states indicate that the current environment is problematic, motivating a high level of effortful processing; positive states indicate that the current environment is safe, suggesting that only a low level of cognitive effort is needed. More recently, Tiedens and Linton (2001) came to a similar conclusion based on appraisal theory of emotion (Ellsworth & Smith, 1988), whereby positive moods are associated with confidence and negative mood states more with doubt. It is because of this confidence associated with positive emotional states that people subsequently think there is less of a need to process the message than when they are feeling more doubtful (i.e. when in a negative mood), warranting further information. Extrapolating from this evidence, it is likely that a negative mood state would improve recipients' sensitivity to detect scam messages by promoting a more careful, systematic and central route processing style. Thus, adopting a more central route to processing in a negative mood would increase the likelihood that an individual would scrutinize all aspects the fraudulent communication, including those which might expose the deception (e.g. grammatical errors), before choosing to respond. Interestingly, the opposite might be hypothesized for individuals experiencing a positive mood state as they may be less likely to effortfully process the message, meaning they may not notice the cues to deception in the fraudulent email.

To our knowledge, the effects produced by incidental emotions have not yet been applied to study variables that may affect an individual's susceptibility to online scam messages. While related literature (Kircanski et al, 2018) suggests this may be a fruitful avenue of study, research is needed to clarify whether emotions have an effect in this online context and, if so, through what mechanisms they produce their effects on an individual's judgement concerning the legitimacy of email communications.

## Theorising the Interaction Between Integral and Incidental Emotion in Scam Compliance

The majority of the affect-cognition literature does not consider how integral emotion (i.e. positive or negative message framing) may interact with an individual's incidental emotion or prior affective state to affect their decision-making process. However, this interaction may be of particular interest for research aiming to understand the factors that could make an individual more susceptible to fall victim to fraudulent communications; in many situations, the presence of both incidental and integral emotion feasibly coexists. To provide context, a scam message, which is likely to contain an a positively or negatively framed emotional appeal (e.g. warnings of financial losses or promises of financial gains), will be received by an individual who is already experiencing either a positive or negative mood state. Importantly, the mood-maintenance/mood-repair view suggests that people in either a positive or negative mood will differ in their response to positive and negatively framed messages. The three main theories holding this view suggest that the effects of emotion on cognition and behavior stem, at least in part, from our motivation to maintain positive moods and/or elevate negative ones (Aspinwall, 1998). Generally, these theories predict that individuals in a positive mood may in some situations avoid taking risks or thinking about negative information to preserve their positive emotional state (*mood maintenance*), whereas individuals in a negative mood may seek

positive opportunities or information to improve their emotional state (*mood repair*; see Schaller & Cialdini, 1990 for a review).

According to the Negative State Relief Model (NSR; Cialdini, Darby & Vincent, 1973), a negative mood is accompanied by an intrinsic drive to alleviate such negative feelings (Mitchell, Brown, Morris-Villagran, & Villagran, 2001). As people generally do not seek to maintain a negative mood state, they strive towards moving back to their baseline. Individuals are motivated to distract themselves from their unpleasant mood by engaging in mood enhancing activities, such as reading a positively framed persuasive message (Isen & Simmonds, 1978). Drawing on this work, Lassiter, Koenig & Apple (1996) suggested that individuals experiencing a negative emotional state may evoke a cognitive strategy where they are more motivated to effortfully process positive information (i.e. mood-elevating) but not neutral or negative information. Thus, they may be more likely to scrutinize a positively framed persuasive message and elaborate its message content. In accordance with the NSR model, some consumer marketing literature suggests that people in a negative mood report more favorable attitudes and purchase intentions when presented with positively-framed persuasive advertisements (Martin & Lawson, 1998). Thus, in the context of responding to deceptive scam messages online, it could be assumed that the NSR model implies that individuals in a negative mood state would be more likely to respond to positively framed scam messages (i.e. emphasizing a potential financial gain) in order to relieve their negative mood.

Similar to the NSR model, the Hedonic Contingency Hypothesis (HCH) suggests that people in a positive mood will be motivated to process uplifting messages and avoid depressing or negative information (Wegener & Petty, 1994). Consistent with this view, Wegener, Petty and Klein (1994) found that people experiencing a happy or positive emotional state were more persuaded by positively framed arguments than negatively framed arguments advocating students be allowed to work-part time for the university in exchange for tuition cuts. However, the HCH also suggests that individuals in a positive mood are more sensitive to the mood-altering or hedonic consequences of their actions than are people in a neutral or negative mood. In other words, in comparison to people in a positive mood, people in a negative mood do not care as much about how the information will alter their mood because they are already in a negative emotional state. Hence, the HCH corresponds with the mood consistency expectations of the NSR model by predicting that people in a positive mood will be more motivated to exert cognitive effort in processing positively framed than negatively framed messages. However, the HCH differs in its predictions to the NSR model when proposing that framing effects are weaker in people in a negative mood. Specifically, this is as the HCH states that people in a negative mood will not care as much about how the information will alter their mood as they are already feeling negative (meaning they are no more persuaded by negative or positively framed arguments), whereas the NSR model predicts that people in a negative mood will be more persuaded by positively framed arguments in order to relieve their negative mood.

Although the HCH can inform predictions on the relationship between incidental and integral emotion, several reasons indicate that this explanation may not fully generalize to the context in which we are interested. In contrast to the context of online fraud, in which an individual may believe that they will lose a substantial amount of money if they fail to respond, the loss experienced by individuals when testing the HCH in Wegener, Petty and Klein's (1994) study was arguably not as meaningful. For example, in the negative message condition, participants lost the opportunity to enroll on a hypothetical university part-time program. Also, as Petty and Brinol (2015) acknowledge, the HCH may not apply when people in a positive emotional state are motivated to serve long-term mood management goals (e.g. if the negative message discusses actions that a person could take to keep an undesirable event from occurring in the future). To illustrate, an individual may respond quickly to a phishing email by providing their personal details to prevent the long-term financial stress that would occur if their bank account were to close. Furthermore, the predictions of the HCH are not fully supported in the negative mood condition (Wegener, Petty, & Klein, 1994). Specifically, significant framing effects in the negative mood condition of their study imply that participants in positive and negative mood treatments may be equally aware of the hedonic consequences of their behavior.

Given our interest in online scam messages, which often contain arguments emphasizing a meaningful loss or gain (e.g. financial), we chose to also consider a third theory that focuses on the role of incidental emotion in the context of significant losses and gains. Isen and colleagues (Arkes, Herren, & Isen, 1988; Isen & Patrick, 1983; Kahn & Isen, 1993) provide convincing evidence that

individuals in a positive mood effortfully consider negative information if it is urgent or essential (i.e. if a real loss is possible). Specifically, they find that people in positive moods sensibly avoid large risks in several studies of risk taking and gambling (Isen & Geva, 1987; Isen, Nygren, & Ashby, 1988). Of particular importance with respect to the question of how people in a positive mood maintain their positive state, these studies also find that people in a positive mood report more, rather than fewer, thoughts about losses. Such a finding is inconsistent with the idea that people in a positive mood are motivated to avoid negative information. Considering the framework proposed by Isen (1993), Wegener, Petty, and Smith (1995) suggest that loss framed messages persuade people in a positive mood if they are more concerned about maintaining their affective state in the long run rather than just their immediate positive state.

Together these findings suggest that a scam message framed as a loss would be more persuasive to those in a positive state than would a positively framed message emphasizing a gain. This may occur because after the affect induction, people in a positive state are more concerned about losses because they have more to lose; so, for example, receiving a negatively framed phishing email stressing an imminent bank account closure would be more consistent with the thoughts of a person in a positive mood (Isen & Geva, 1987). People in a positive state might also be more receptive to a fear inducing scam message if they are motivated to maintain control over their long-term positive affect rather than worry about dampening their current positive mood. For example, in our context of responding to deceptive messages online, the loss frame may be interpreted as a person will be unhappy in the longer-term future if they do not prevent their bank account from closing.

While this may be the case, it is important to consider that the predictions discussed above based on the mood-maintenance/mood-repair literature could be incomplete in this instance. Unlike the persuasion research outlined previously that provides respondents with *legitimate* message content, online scams contain *illegitimate* content that aims to deceive the individual who receives the message. Hence, the additional attention to positive or negative messages dependent on one's mood may be hypothesized to create a reverse effect on a respondent behavior. To explain this issue, it is important to return to the predictions provided by the dual process theories (e.g. ELM; Petty & Cacioppo, 1986) of persuasion outlined previously in this review. The ELM holds that attention and motivation moderate whether people use peripheral or central routes to process a message. If a person lacks attention or motivation, the likelihood of peripheral route processing increases. If both motivation and attention are high, the probability of central route processing increases. While greater attention and motivation to process a persuasive message may provide more enduring attitude change in support of a legitimate argument, it may elicit higher levels of deception detection in the context of receiving online fraudulent communications. This is supported by previous research, which found that those who were engaged in central route or systematic processing of scam communications were more likely to notice message factors, such as grammatical errors, that expose the deception (Harrison et al, 2015; Vishwanath et al., 2011). Thus, this may have important implications for the proposed interaction between integral and incidental emotion in scam compliance. If we utilize the predictions of the NSR model as an example [which suggests that individuals in a negative mood are more motivated to effortfully process positive information (i.e. mood-elevating) but not neutral or negative information], we may witness a reverse effect. Rather than eliciting a higher level of scam compliance to positively framed scam messages, those individuals in a negative mood may in fact be more likely to notice cues to deception due to their use of a more systematic and central route processing style and, thus, be less likely to respond. Applying the predictions of the NSR model to individuals experiencing a positive mood, this reverse effect may also be predicted to take place. As this model suggests that individuals experiencing a positive mood are more motivated to effortfully process positive information (but not negative or neutral information), they may similarly be more likely to notice the cues to deception within a fraudulent email. Therefore, we may witness findings which suggest individuals in both positive and negative moods may be more likely to respond to negatively framed scam emails (e.g. warning of financial losses), than they are to positively framed scam email (e.g. promising financial gains) due to an increased likelihood of using a peripheral route of processing when responding to the message. As we can do no more than theorize this interaction, future research is needed to clarify whether integral emotion (i.e. positive or negative message framing) interacts with an individual's incidental emotion to affect their decision-making process in the context of responding to fraudulent communications online.

## Conclusion

In this review, we have explored some of the ways that emotions may influence an individual's susceptibility to forms of malicious influence online. A key point was that the influence of emotional factors, whether integral or incidental to the scam message, can occur through different primary mechanisms and in different contexts. That is, emotion may serve multiple roles and the effects of emotional factors in scam compliance could be diverse. Emotions can influence attitudes by peripheral mechanisms (such as heuristics), serve as an item of issue relevant information, bias message scrutiny, and even determine the extent of message processing. The ELM provides a useful organising framework to understand the effects of emotion on scam compliance, additional theoretical developments further complement ELM by specifying which processes enable certain variables to affect judgements within each level of elaboration likelihood. Particularly, we suggest that future research ought to adopt the mood-maintenance/mood-repair view as a theoretical foundation when aiming to explore the potential link between emotions and susceptibility to fall victim to scams online. Importantly, this theoretical foundation would enable researchers to focus on the interaction between the individuals current emotional state and emotional appeals embedded in the influence message itself when considering their likely response behaviour.

## References

- Aarts, H., & Dijksterhuis, A. (2003). The silence of the library: environment, situational norm, and social behavior. *Journal of personality and social psychology*, 84(1), 18.
- Anderson, R. (2008). Security engineering: A guide to building dependable distributed systems (2nd ed.). Indianapolis, IN: Wiley. ISBN: 978-0-470-06852-6.
- Arkes, H. R., Herren, L.T. & Isen, A.M. (1988), The Role of Potential Loss in the Influence of Affect on Risk-Taking Behavior, *Organizational Behavior and Human Decision Processes*, 42 (2), 181–94.
- Aspinwall, L. G. (1998). Rethinking the role of positive affect in self-regulation. *Motivation and emotion*, 22(1), 1-32
- BBC (2017, May 13), NHS services hit by cyber-attack, Retrieved from <https://www.bbc.co.uk/news/health-39899646>
- Bless, H., Bohner, G., Schwarz, N., & Strack, F. (1990). Mood and persuasion: A cognitive response analysis. *Personality and social psychology bulletin*, 16(2), 331-345.
- Bohner, G., Crow, K., Erb, H. P., & Schwarz, N. (1992). Affect and persuasion: Mood effects on the processing of message content and context cues and on subsequent behaviour. *European Journal of Social Psychology*, 22(6), 511-530.
- Boster, F. J., & Mongeau, P. (1984). Fear-arousing persuasive messages. *Annals of the International communication Association*, 8(1), 330-375.
- Bower, G. H. (1981). Mood and memory. *American psychologist*, 36(2), 129.
- Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge.
- Button, M., Lewis, C., & Tapley, J. (2016). *Fraud typologies and victims of fraud*. London: National Fraud Authority.
- Cacioppo, J. T., Gardner, W. L., & Berntson, G. G. (1997). Beyond bipolar conceptualizations and measures: The case of attitudes and evaluative space. *Personality and Social Psychology Review*, 1(1), 3-25.
- Cialdini, R. B., Darby, B. L., & Vincent, J. E. (1973). Transgression and altruism: A case for hedonism. *Journal of Experimental Social Psychology*, 9(6), 502-516.
- Correia, S. G. (2019). Responding to victimisation in a digital word: a case study of fraud and computer misuse reported in Wales. *Crime Science*, 8(1), 4.
- Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*. Harcourt Brace Jovanovich College Publishers.
- Ekman, P. (1993). Facial expression and emotion. *American psychologist*, 48(4), 384.
- Ellsworth, P. C., & Smith, C. A. (1988). From appraisal to emotion: Differences among unpleasant feelings. *Motivation and Emotion*, 12, 271–302.
- Ferreira, A., & Teles, S. (2019). Persuasion: How phishing emails can influence users and bypass security measures. *International Journal of Human-Computer Studies*, 125, 19-31.
- Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behaviour: An introduction to theory and research. Reading, MA: Addison-Wesley.
- Forgas, J. P. (1995). Mood and judgment: the affect infusion model (AIM). *Psychological bulletin*, 117(1), 39.
- Forgas, J. P. (1995). Mood and judgment: the affect infusion model (AIM). *Psychological bulletin*, 117(1), 39.
- Forgas, J. P. (2002). Feeling and doing: Affective influences on interpersonal behavior. *Psychological inquiry*, 13(1), 1-28.
- Forgas, J. P. (2017). Mood effects on cognition: Affective influences on the content and process of information processing and behavior. In *Emotions and affect in human factors and human-computer interaction* (pp. 89-122). Academic Press.
- Geva, N. (1987), The Influence of Positive Affect on Acceptable Levels of Risk: The Person with a Large Canoe Has a Large Worry, *Organizational Behavior and Human Decision Processes*, 39 (2), 145–54.
- Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, 18(1), 2.

- Gragg, D. (2003). A Multi-Level Defence Against Social Engineering. Bethesda, MD: SANS Institute.
- Hale, J. L., Lemieux, R., & Mongeau, P. A. (1995). Cognitive processing of fear-arousing message content. *Communication Research*, 22(4), 459-474.
- Harrison, B., Svetieva, E. & Vishwanath, A. (2016). Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online information Review*, 40 (2), 265-281.
- Harrison, B., Vishwanath, A., Ng, Y. J., & Rao, R. (2015, January). Examining the impact of presence on individual phishing victimization. In *2015 48th Hawaii International Conference on System Sciences* (pp. 3483-3489). IEEE.
- Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities and fraud victimisation, *Criminology*, 46 (1), 189-220.
- Horvitz, T., & Pratkanis, A. R. (2002). A Laboratory Demonstration of the Fraudulent Telemarketers' 1- in- 5 Prize Tactic 1. *Journal of Applied Social Psychology*, 32(2), 310-317.
- Hussain, D., Ross, P., & Bednar, P. (2018). The perception of the benefits and drawbacks of Internet usage by the elderly people. In *Digital Technology and Organizational Change* (pp. 199-212). Springer, Cham.
- Isen, A. M. (1993), Positive Affect and Decision Making, in *Handbook of Emotions*, Michael Lewis and Jeanette M. Haviland, eds. New York: Guilford, 261-77.
- Isen, A. M. (1993). Positive affect and decision making. In M. Lewis & J. M. Haviland (Eds.), *Handbook of emotions* (pp. 261-277). New York, NY, US: Guilford Press
- Isen, A. M., & Patrick, R. (1983). The effect of positive feelings on risk taking: When the chips are down. *Organizational behavior and human performance*, 31(2), 194-202.
- Isen, A. M., & Simmonds, S. F. (1978). The effect of feeling good on a helping task that is incompatible with good mood. *Social Psychology*, 346-349.
- Isen, A. M., Nygren, T. E., & Ashby, F. G. (1988). Influence of positive affect on the subjective utility of gains and losses: it is just not worth the risk. *Journal of personality and Social Psychology*, 55(5), 710.
- Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10), 94-100.
- Johnson, E. J., & Tversky, A. (1983). Affect, generalization, and the perception of risk. *Journal of personality and social psychology*, 45(1), 20.
- Jones, C. R., Fazio, R. H., & Olson, M. A. (2009). Implicit misattribution as a mechanism underlying evaluative conditioning. *Journal of Personality and Social Psychology*, 96, 933-948
- Kahn, B. E., & Isen, A. M. (1993). The influence of positive affect on variety seeking among safe, enjoyable products. *Journal of Consumer Research*, 20(2), 257-270.
- Kim, D., & Kim, J. (2013). Understanding persuasive elements in phishing e-mails: A categorical content and semantic network analysis. *Online Information Review*, 37(6), 835-850.
- Kircanski, K., Notthoff, N., DeLiema, M., Samanez-Larkin, G. R., Shadel, D., Mottola, G., ... & Gotlib, I. H. (2018). Emotional arousal may increase susceptibility to fraud in older and younger adults. *Psychology and aging*, 33(2), 325.
- Lassiter, G. D., Koenig, L. J., & Apple, K. J. (1996). Mood and behavior perception: Dysphoria can increase and decrease effortful processing of information. *Personality and Social Psychology Bulletin*, 22(8), 794-810.
- Lerner, J. S., Li, Y., Valdesolo, P., & Kassam, K. S. (2015). Emotion and decision making. *Annual review of psychology*, 66, 799-823.
- Mackie, D. M., & Worth, L. T. (1989). Processing deficits and the mediation of positive affect in persuasion. *Journal of personality and social psychology*, 57(1), 27.
- Martin, B., & Lawson, R. (1998). Mood and framing effects in advertising. *Australasian Marketing Journal (AMJ)*, 6(1), 35-50.
- Mitchell, M., Brown, K., Morris-Villagran, M., & Villagran, P. (2001). The effects of anger, sadness and happiness on persuasive message processing: A test of the negative state relief model. *Communication Monographs*, 68(4), 347-359.



- Modic, D., Anderson, R., & Palomäki, J. (2018). We will make you like our research: The development of a susceptibility-to-persuasion scale. *PloS one*, 13(3): e0194119. <https://doi.org/10.1371/journal.pone.0194119>
- Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimization: a Systematic Review. *Journal of Police and Criminal Psychology*, 1-15.
- O'Keefe, D. J., & Jensen, J. D. (2008). Do loss-framed persuasive messages engender greater message processing than do gain-framed messages? A meta-analytic review. *Communication Studies*, 59(1), 51-67.
- Ofstad, S., Tobolova, M., Nayum, A., & Klöckner, C. (2017). Understanding the mechanisms behind changing people's recycling behavior at work by applying a comprehensive action determination model. *Sustainability*, 9(2), 204.
- Pascoe, T., Owen, K., Keats, G., & Gill, M. (2006). Identity fraud: What about the victim. *London: CIFAS*.
- Pattinson, M. R., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. A. (2011). Managing Phishing Emails: A Scenario-Based Experiment. *Paper Presented at the Proceedings of the Fifth International Symposium on Human Aspects of the Information Security & Assurance HAISA*, (pp. 74-85).
- Payne, B. K. (2005). Conceptualizing control in social cognition: How executive control modulates the expression of automatic stereotyping. *Journal of Personality and Social Psychology*, 89, 488-503.
- Petty R.E., DeSteno D., Rucker D.D. (2001) The Role of Affect in Attitude Change. In Forgas, J.P. (Ed) *Handbook of Affect and Social Cognition* (pp 121-236). Lawrence Erlbaum Associates: Mahwah.
- Petty, R. E., & Briñol, P. (2015). Emotion and persuasion: Cognitive and meta-cognitive processes impact attitudes. *Cognition and Emotion*, 29(1), 1-26.
- Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. In *Communication and persuasion* (pp. 1-24). Springer, New York, NY.
- Petty, R. E., Cacioppo, J. T., & Schumann, D. (1983). Central and peripheral routes to advertising effectiveness: The moderating role of involvement. *Journal of consumer research*, 10(2), 135-146.
- Petty, R.E., & Wegener, D.T. (1991). Thought Systems, argument quality, and persuasion. In R.S. Wyer & T.K. Srull (Eds.), *Advances in social cognition*, Vol. 4 (pp. 143-161). Hillsdale, NJ: Lawrence Erlbaum Associates.
- Purkait, S., Kumar De, S., & Suar, D. (2014). An empirical investigation of the factors that influence Internet user's ability to correctly identify a phishing website. *Information Management & Computer Security*, 22(3), 194-234.
- Rodgers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation, In J.T. Cacioppo & R.E. Petty (Eds.), *Social Psychophysiology: A source book* (pp. 153-176). New York: Guilford Press.
- Ruiter, R. A., Kessels, L. T., Peters, G. J. Y., & Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. *International journal of psychology*, 49(2), 63-70.
- Rusch, J. (1999). The Social Engineering of Internet Fraud. Paper presented at the INET'99 Conference, San Jose, CA.
- Schaller, M., & Cialdini, R. B. (1990). Happiness, sadness, and helping: A motivational integration. In E. T. Higgins & R. M. Sorrentino (Eds.), *Handbook of motivation and cognition: Foundations of social behavior*, Vol. 2, pp. 265-296). New York, NY, US: The Guilford Press.
- Schwarz, N., & Clore, G. L. (1983). Mood, misattribution, and judgments of well-being: informative and directive functions of affective states. *Journal of personality and social psychology*, 45(3), 513.
- Schwarz, N., Bless, H., & Bohner, G. (1991). Mood and persuasion: Affective states influence the processing of persuasive communications. In *Advances in experimental social psychology* (Vol. 24, pp. 161-199). Academic Press.



- Sharma, M., Khubchandani, J., & Nahar, V. K. (2017). Applying a new theory to smoking cessation: case of multi-theory model (MTM) for health behavior change. *Health promotion perspectives*, 7(2), 102.
- Staats, A. W., & Staats, C. K. (1958). Attitudes established by classical conditioning. *The Journal of Abnormal and Social Psychology*, 57(1), 37.
- Tiedens, L. Z., & Linton, S. (2001). Judgment under emotional certainty and uncertainty: The effects of specific emotions on information processing. *Journal of Personality and Social Psychology*, 81, 973–988.
- Titus, R. M., & Gover, A. R. (2001). Personal fraud: The victims and the scams. *Crime Prevention Studies*, 12, 133-152.
- Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, 45(8), 1146-1166.
- Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51(3), 576-586.
- Wegener D.T. & Petty R. E. (2001) Understanding the effects of mood through the Elaboration Likelihood and Flexible correction models. In Martin, L. L., & Clore, G. L. (2001). *Theories of mood and cognition: A user's guidebook* (pp. 177-210). Psychology Press.
- Wegener, D. T., & Petty, R. E. (1994). Mood management across affective states: The hedonic contingency hypothesis. *Journal of personality and social psychology*, 66(6), 1034.
- Wegener, D. T., & Petty, R. E. (1994). Mood management across affective states: The hedonic contingency hypothesis. *Journal of personality and social psychology*, 66(6), 1034.
- Wegener, D. T., Petty, R. E., & Klein, D. J. (1994). Effects of mood on high elaboration attitude change: The mediating role of likelihood judgments. *European journal of social psychology*, 24(1), 25-43.
- Wegener, D. T., Petty, R. E., & Smith, S. M. (1995). Positive mood can increase or decrease message scrutiny: the hedonic contingency view of mood and message processing. *Journal of personality and social psychology*, 69(1), 5-15.
- Williams, E. J., & Polage, D. (2019). How persuasive is phishing email? The role of authentic design, influence and current events in email judgements. *Behaviour & Information Technology*, 38(2), 184-197.
- Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72, 412-421.
- Workman, M. (2008), A test of intervention for security threats from social engineering, *Information Management & Computer Security*, Vol. 16 No. 5, pp. 463-483.
- Worth, L. T., & Mackie, D. M. (1987). Cognitive mediation of positive affect in persuasion. *Social cognition*, 5(1), 76-94.