TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Department of Software Science

Running Head: Dark Triad in Central Route to Persuasion

Ivo Malve 178184IVCM

DARK TRIAD IN CENTRAL ROUTE TO PERSUASION: A PERSONALITY-BASED PHISHING SUSCEPTIBILITY STUDY

Master's thesis

Supervisor 1: Kieren Nicolas Lovell
LT CDR (RNORN)
RTD

Supervisor 2: David Modic
Ph.D.

Tallinn 2020

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Tarkvarateaduse instituut

Jooksev Päis: Dark Triad in Central Route to Persuasion

Ivo Malve 178184IVCM

TUME KOLMIK JA TSENTRAALNE MÕJUTUSTEE: ISIKUOMADUSTEL PÕHINEV ANDMEPÜÜGI UURING

Magistritöö

Juhendaja 1: Kieren Nicolas Lovell
LT CDR (RNORN)
RTD

Juhendaja 2: David Modic
Ph.D.

Tallinn 2020

Tallinn 2020

Author's Declaration of Originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Ivo Malve

06.12.2020

Abstract

There is a general consensus in phishing susceptibility research, that the decisive factor in responding to phishing e-mails is attention allocation. If the reader pays attention to the elements raising suspicion on the authenticity of the e-mail, they are less likely to fall victim, than if they focused attention on visceral cues inducing rash decisions. While this wisdom helps us recognize a generic phishing e-mail as fraud, it fails to address spear-phishing, which often relies on contextually relevant text-based messages for persuasion. Current literature lacks an insight into the factors motivating people to react to text-based messages, which is necessary to effectively address the threat of spear-phishing.

In my Thesis, I addressed this research gap by exploring the relationship between personality and the appealing elements in text-based phishing messages. I relied on the theoretical premises of the Elaboration Likelihood Model (ELM), which distinguishes two modes of persuasion – peripheral and central. While untargeted phishing (98-99% of all phishing e-mails) seeks to employ the peripheral mode, central route to persuasion is preferred in spear-phishing. Therefore, I designed an experiment to examine the influence of personality on phishing susceptibility in central route to persuasion.

I conducted two surveys to measure the HEXACO and Dark Triad personality domains along with relevant psychometric constructs indicating susceptibility to persuasion in a sample of 200 participants. While there is ample literature available on the relationship between phishing susceptibility and the HEXACO traits in peripheral mode, I was interested in these relationships in central mode. Because Dark Triad traits have been shown to be associated with amoral motivations and desires, I imagined scoring

high on any of the Dark Triad traits could positively influence finding certain persuasive messages more appealing, hence motivating the reader to respond. To explore any relationships between personality and responding to e-mails appealing to different emotional and motivational categories, I measured the likelihood of responding to phishing e-mails designed to induce the central route to persuasion.

The participants were divided into two groups, based on whether or not they admitted having been scammed in near past. I assumed peripheral route to persuasion in cases where the participants had fallen victim in the past, given the prevalent use of peripheral persuasion mode in phishing. Comparing the personality of victims of the two persuasion modes revealed, that past victims were consistently more likely to respond to the e-mails in my experiment, than the control group. I found this *repeat-clicking* tendency to be best explained by the Conscientiousness and Avoidance of Similarity domains, and *repeat-clicking* was the best predictor of overall susceptibility in both central and peripheral routes to persuasion. While *repeat-clicking* has been previously examined in general phishing susceptibility, my findings are the first to highlight the importance of *repeat-clicking* in central information processing mode (i.e., spear-phishing).

While past victimisation was the best positive indicator of susceptibility in central mode, I found a difference in the personality of victims in central and peripheral modes: there is more variance in the predictive power of specific traits in central, than in peripheral mode. This means, that the traits Conscientiousness and Avoidance of Similarity seem to be more important in peripheral, than in central route to persuasion. Furthermore, I found that if an individual was not a *repeat-clicker,* four specific personality domains were better indicators of susceptibility. In particular, scoring high on Social Influence, Sensation Seeking and Honesty-Humility seems to increase and Need

for Consistency decrease the likelihood of responding. This indicates that if a person is prone to *repeat-clicking*, Conscientiousness and Avoidance of Similarity are the best indicators of susceptibility in central mode. Whereas if an individual is not a *repeat-clicker*, Social Influence, Honesty-Humility, Sensation Seeking and Need for Consistency are the best predictors.

Finally, I hypothesized that the Dark Triad personality domains are associated with the appeal categories each e-mail presents. While I found differences in how well specific personality traits predicted responding to certain e-mails, I did not confirm any of my hypotheses, which proposed relationships between Psychopathy and a message indicating chance of romance, Machiavellianism and a chance to earn easy money at the expense of a gullible person, and Narcissism and an e-mail insulting one's ego. Some theoretical and practical implications of my findings are discussed along with areas for further research.

This thesis is written in English and is 82 pages long, including 5 chapters, 11 figures and 3 tables.

Annotatsioon

Tume kolmik ja tsentraalne mõjutustee: isikuomadustel põhinev andmepüügi uuring

Andmepüügi valdkonnas on üldlevinud tõekspidamine, et ohvriks langemisel on määrav tähtsus lugeja tähelepanu juhtimisel. Õngitsuskirja kahtlustäratavate omaduste märkamine ja äratundmine vähendab ning veenvatele elementidele keskendumine soodustab oluliselt ohvriks langemist. Kuigi see teadmine võimaldab meil tuvastada enamlevinud suunamata kirju, on sellest vähe abi suunatud õngitsuskirjade (spear-phishing) tuvastamisel, kuivõrd suunatud kirjad tuginevad sageli tekstis esitatavatele argumentidele lugeja mõjutamiseks. Olemasolev kirjandus ei seleta, kuidas toimub otsustusprotsess õngitsuskirjale vastamisel tsentraalse mõjutustee puhul. Selle teadmuse omandamine võimaldaks sihitud õngitsuskirjade (*spear-phishing*) eest inimesi paremini kaitsta.

Uurisin oma magistritöö raames isikuomaduste ja levinumate tekstisiseste argumentide vahelisi seoseid, toetudes süvenemise tõenäosuse mudeli (ELM mudel) teoreetilistele põhimõtetele. Selleks viisin läbi eksperimendi, milles osalejad pidid lugema e-kirju, mille hulgas oli ka õngitsuskirju. Tekstisisesed argumendid ehk petuskeemid olid kujundatud motiveerima lugejat kirjadele vastama. Osalejad valisid iga kirja puhul ühe viiest vastusevariandist, kuidas nad seda käitleksid (nt. vastaksin kirjale, kustutaksin kirja või blokeeriksin kirja saatja).

Seejärel võrdlesin eksperimendis osalenute tulemusi minevikus petuskeemide ohvriks langenute andmetega, et uurida erisusi kahe ELM mudeli mõjutustee vahel.

Lisaks huvitas mind, kas mõnel tumeda kolmiku isikuomadusel on oluline seos mõne kindla petuskeemiga. Kvantitatiivse analüüsi tulemused näitasid, et olulised erisused mineviku ohvrite ja eksperimendis osalenud vastajate isikuomadustes puuduvad. Lisaks sellele leidsin, et eri isikuomadused olid seotud eri petuskeemide ohvriks langemisega. Lõpetuseks selgitan võimalusi oma leidude praktikas ning tulevases teadustöös rakendamiseks.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 82 leheküljel, 5 peatükki, 11 joonist, 3 tabelit.

List of Abbreviations and Terms

TLD	Top Level Domain
RQ	Research Question
H	Hypothesis
ELM	Elaboration Likelihood Model
CRP	Central Route to Persuasion
PRP	Peripheral Route to Persuasion
DMARC	Domain-based Message Authentication, Reporting & Conformance
DKIM	DomainKeys Identified Mail
SPF	Sender Policy Framework
mTurk	Amazon Mechanical Turk
HEXACO	Honesty-Humility, Extraversion, Agreeableness, Conscientiousness, Openness to experience
IV	Independent Variable
DV	Dependent Variable
CV	Control Variable
MLR	Multiple Linear Regression
VIF	Variable Inflation Factor
GLM	Generalized Linear Model
PII	Personal Involvement Inventory
MCAR	Missing Completely at Random
HSM	Heuristic-Systematic Model

Table of contents

List of figures

1 Introduction

Information security policies and procedures have become commonplace among organizations and IT service providers (Cezar, Cavusoglu, & Raghunathan, 2017). Technological advances allow us to better detect and respond to threats, but relying solely on automation often provides sub-optimal results (Ben-Asher & Gonzalez, 2015). While advanced threat actors exploit vulnerabilities using malware, others have opted for social engineering: the art of manipulating a person into giving information to the social engineer (Krombholz, Hobel, Huber, & Weippl, 2015). This study explores one of the most common tools used by social engineers, phishing (Cho, Cam, & Oltramari, 2016).

Phishing is a form of deception in which a social engineer attempts to acquire sensitive information (Kleitman, Law, & Kay, 2018) or to make the target individual act in a desired way (Krombholz, Hobel, Huber, & Weippl, 2015). While these results can be achieved over any communication medium, this study focuses on e-mail, the most common channel for phishing (Ferreira & Teles, 2019; Krombholz et al., 2015). The abundance of phishing e-mails could explain why most of the phishing susceptibility research has been focusing on e-mail based scams. (Vishwanath, Herath, Chen, Wang, & Rao, 2011; Wang, Herath, Chen, Vishwanath, & Rao, 2012)

1.1 The Phishing E-mail Problem

Phishing presents the problem of telling authentic e-mails from frauds. Wang, Herath, Chen, Vishwanath, & Rao, (2012) divide reading an e-mail into three consecutive stages: message involvement, cognitive effort and response likelihood. Message

involvement is defined as the degree to which a recipient perceives the e-mail to be pertinent to his or her needs, goals, interests and values (Zaichkowsky, 2014). Recognizing relevant information, individuals are motivated to expend cognitive effort on evaluation of the e-mail, thereby forming a judgement on its authenticity and deciding on future action (in case of phishing, forming the likelihood to respond; Wang et al., 2012).

Phishing e-mails often employ persuasive elements, that lower the suspicion concerning the authenticity of the e-mail and persuade the recipient to comply with the request (Alseadoon, 2014). Such manipulations are known as visceral triggers (e.g., stressing the urgency to respond, signatures and pictures expressing authenticity; Wang et al., 2012) and the suspicion-raising features of a phishing e-mail are referred to as deception indicators (e.g., unfamiliar e-mail sender address, foreign language and faulty grammar; Wang & Chen, 2009). An e-mail reader can recognize a phishing e-mail when paying attention to deception indicators (Vishwanath et al., 2011), whereas visceral triggers aim to induce judgment errors by suppressing recipients' cognitive effort and provoking intuitive reactions (Wang et al., 2012).

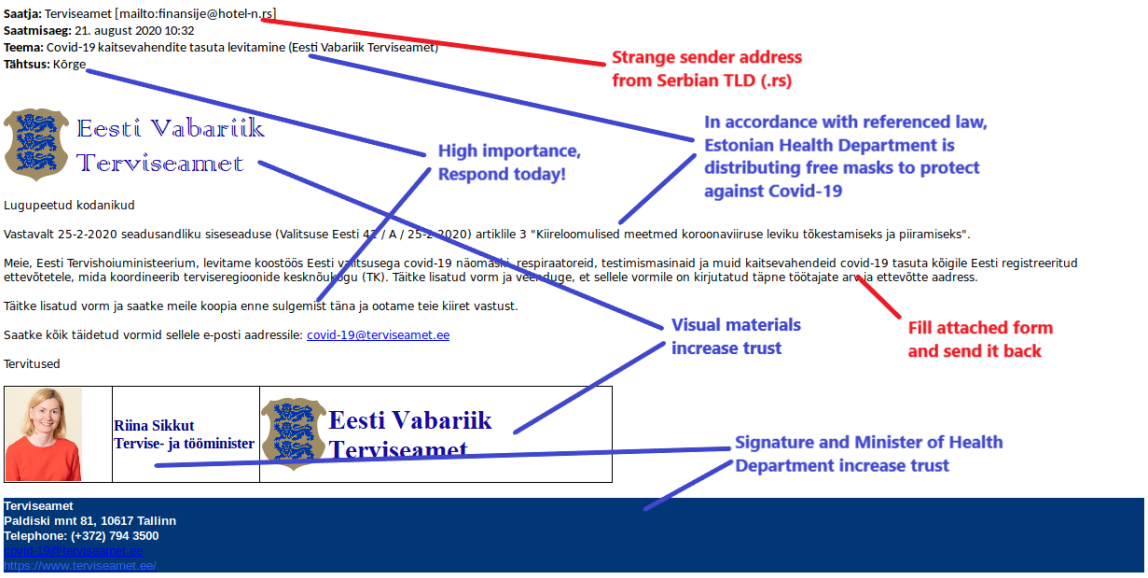


Figure 1. An example of a phishing e-mail from an Estonian phishing e-mail campaign containing common visceral triggers and deception indicators.

Source. CERT-EE Twitter channel (https://twitter.com/cert_ee).

In August of 2020, organisations in Estonia were targeted by several phishing campaigns employing the COVID-19 pandemic theme. Figure 1 presents an example of these e-mails, which served the purpose of delivering malware. These e-mails had an attachment, which the message in the e-mail suggested was a form needing to be filled and returned. Instead, the attachment contained an executable file (.exe) installing Trojan-type malware upon opening. This e-mail employs persuasive elements to lead the reader to believe the Ministry of Health was gathering information to distribute self-protection equipment for organizations, hence getting the reader to open the attachment. Visceral triggers are described in blue and deception indicators in red font.

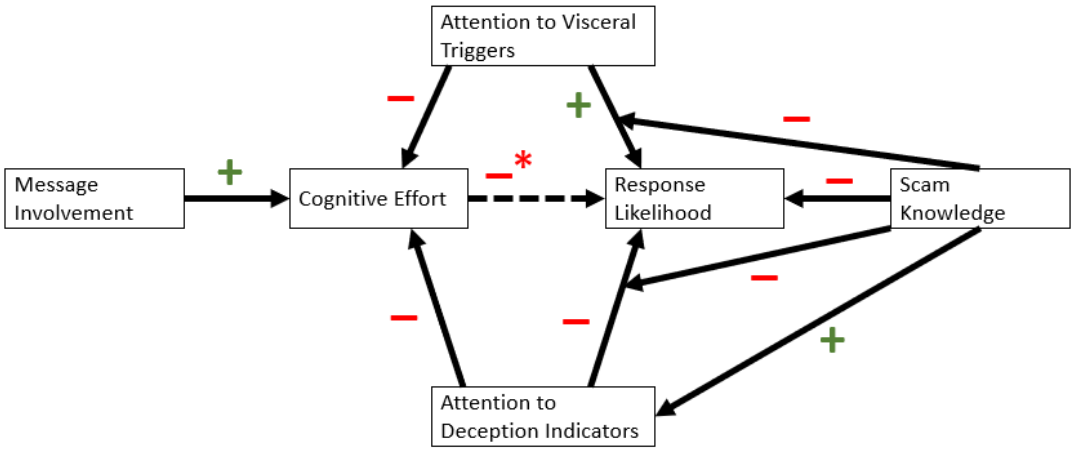


Figure 2. An example of a phishing e-mail processing model.

In an attempt to explain, how we decide upon responding to phishing e-mails, Figure 2 presents the research model and illustrates the results of Wang et al., (2012). Each rectangle on the image represents a factor contributing to the likelihood of responding to a phishing e-mail. These factors may have a positive influence (indicated with a '+' sign) on another factor or a relationship between two factors, or a negative one ('-' sign). Note, that solid lines indicate significant relationships and the dotted line indicates an insignificant relationship.

The model of Wang et al., (2012) suggests, that the level of involvement a reader feels significantly increases their cognitive effort spent on elaboration. And the amount of cognitive effort spent has little effect on deciding, whether or not to respond to a phishing e-mail. Attending to deception indicators and visceral triggers supress cognitive effort while focusing on visceral triggers increases it. Being able to identify a deception indicator decreases response likelihood. Knowledge of scams lowers response likelihood through better detection of deception indicators and decreased attention on visceral triggers. This model suggests that attention allocation and scam knowledge are the more significant predictors of response likelihood. As Wang et al., (2012) concluded:

"Our study suggests that visceral triggers and deception indicators are the two main aspects influencing an individual's response to a phishing email. "

A shortcoming of this model is that it does not accommodate personality as a factor influencing susceptibility. Although Kleitman et al., (2018) and Janczewski, Wolfe, & Shenoi, (2013) found low correlations between personality and phishing susceptibility, several researchers have found that scoring high on Conscientiousness negatively influences, while Agreeableness and Extraversion positively influence the likelihood of responding to phishing e-mails (Albladi & George, 2018; Modic & Lea, 2014; Alseadoon, 2014; Halevi, Memon, & Nov, 2015).

Furthermore, behavioural research in the last two decades suggests that three personality domains in particular – Narcissism, Machiavellianism and Psychopathy, commonly referred to as the Dark Triad, are associated with amoral motivations and desires, which is why individuals scoring high in any of these traits have been shown to be more prone to participate in risky or unethical endeavours (Nie, Zhang, & Song, 2018). According to Paulhus & Williams, (2002), the construct of Narcissism describes grandiosity, entitlement, dominance and superiority. Machiavellianism represents manipulative personality and Psychopathy is characterised by high impulsivity and thrill-seeking along with low empathy and anxiety (Paulhus & Williams, 2002).

Regarding literature on the relationship between the Dark Triad traits and phishing susceptibility, the only article I could find was Curtis et al., (2018), who found Narcissism to correlate positively with phishing susceptibility. Phishing e-mails present offers or demands, that are rationally, emotionally or motivationally appealing for the recipient (Kim & Kim, 2013). Since there is a considerable body of literature to support the importance of personality in phishing susceptibility, it is possible that the Dark Triad

could explain, what motivates people to participate in the scenarios proposed in text-based phishing e-mails.

1.2 Research Motivation

The model of Wang et al., (2012) discussed in the previous chapter represents a general trend in phishing susceptibility research, namely solving the problem of distinguishing between authentic and non-authentic e-mails through peripheral processing (i.e., the peripheral route to persuasion; PRP; Vishwanath, 2015; Vishwanath et al., 2011). This trend can be explained to the extent, that an overwhelming majority of phishing e-mails are untargeted, hence relying heavily on visceral triggers for success (Herley, 2010). Only a percent or two of phishing e-mails are targeted (i.e., spear-phishing; Halevi, Memon, & Nov, 2015; Herley, 2010), able to use contextually significant text-based messages for persuasion (i.e., target the central route to persuasion; CRP; Wang et al., 2012).

Peripheral and central routes are the two ways people process information, according to the Elaboration Likelihood Model (ELM; Petty & Cacioppo, 1986). Rooted in consumer behavioural theory, ELM was first developed to explain how consumers respond and process stimuli, such as advertising messages (Vishwanath et al., 2011). When processing information peripherally, individuals focus attention on simple cues in the persuasion context and deception indicators, rather than diligently considering the information cues based on their merits and comparisons to prior beliefs (Petty & Cacioppo, 1986). Under conditions of low involvement, peripheral cues are more important than issue-relevant argumentation, but under high involvement, the opposite is true (Petty, Cacioppo, & Schumann, 1983). While the research models used to examine peripheral route are mainly based on fraud detection theories (e.g., Theory of Deception;

Johnson, Grazioli, Jamal, & Zualkernan, 1992), the central route has been studied using behavioural models, such as the O-S-I-R and ELM (e.g., Alseadoon, 2014; Wang & Chen, 2009; Vishwanath et al., 2011; Williams, Beardmore, & Joinson, 2017).

Untargeted phishing is attractive for scammers, because it is scalable, automated and costs nothing to try. However, it suffers a major disadvantage of a one-size-fits-all design: these e-mails are generic (Butavicius et al., 2017; Steven Furnell, 2013). Scalable attacks are also addressed first in security investment strategies (Herley, 2010), rendering them ineffective with technical interventions, such as blacklists, security protocols (e.g., SPF, DKIM and DMARC) and antivirus software (Moody, Galletta, & Dunn, 2017). Targeted phishing, however, is difficult to protect against using technical measures (Alseadoon, 2014; Steven Furnell, 2013; Jagatic, Johnson, Jakobsson, & Menczer, 2007) and experiments comparing the success rates of untargeted and spear-phishing campaigns indicate a higher success rate among the latter (Goel, Williams, & Dincelli, 2017; Jagatic et al., 2007). On the contrary, dependence on technical solutions for protection can encourage users to trust the emails arriving in their inbox (Alseadoon, 2014), increasing the probability of success for spear-phishing.

The motivation behind untargeted phishing is primarily financial (e.g., banking and financially oriented messages; Steven Furnell, 2013), while targeted phishing is often the stepping-stone for more serious ends, such as malware delivery, cyber warfare and espionage (Steven Furnell, 2013). The fact that message involvement is a key component of targeted phishing (Halevi et al., 2015), yet its influence of message involvement on phishing susceptibility remains undetermined (Vishwanath et al., 2011), indicates a research gap regarding the factors influencing the likelihood of responding to spear-phishing. This statement is supported by several researchers, who have suggested a strong need to conduct further research relating personality-based factors to security-related

behavioural intentions (e.g. Alseadoon, 2014; Wang et al., 2012). In particular, Moody, Galletta, & Dunn, (2017) has recently called for an investigation into the appeals phishing e-mails make, and how personality-related frameworks, such as the Dark Triad personality traits addressed in my research, could enable researchers to understand more about how personality affects users' security-related behaviour.

This thesis complements the work of Wang et al., (2012), challenging their conclusion as cited in Section 1.1 from the aspect of information processing mode. The spear-phishing emails used in the experiment of Wang et al., (2012) were riddled with visceral triggers. Therefore, it is likely that the majority of the participants of the experiment assessed the e-mail peripherally, meaning the experiment did not involve central route processing of phishing e-mails. My study investigated response likelihood in a CRP setting, enabling discussion on whether the conclusion by Wang et al., (2012) is only true for PRP.

1.3 Goals and Research Questions

This study examined the effect of message appeal on phishing susceptibility from the perspective of personality traits. Using psychometric tools, I analysed the impact of personality traits on response likelihood in CRP. The salient traits would give an insight into central route processing of phishing e-mails. To the best of my knowledge, this research is the first one to study central route processing of phishing e-mails.

The novelty of my research is three-fold. First, it examined the psychometric profile of phishing victims in central route information processing. Research has shown most phishing e-mails are processed peripherally (Workman, 2008). Since these phishing e-mails often make use of visceral triggers inducing PRP, I assumed the majority of

participants had been phished in the past via PRP (e.g., untargeted phishing campaigns). Therefore, the first research question was:

(RQ1) Does the personality of the phishing victims in central mode differ from the personality of victims in peripheral mode?

Second, I examined the relationship between response likelihood and personality traits in central route information processing. Thereby raising the second research question:

(RQ2) Which personality traits stand out as predictors of phishing susceptibility in central mode?

And third, as an extensive literature study yielded no similar works, this study is the first one to examine the relationship between message appeal and the Dark Triad personality traits in CRP.

(RQ3) Does any Dark Triad trait increase susceptibility in central processing of a message with a certain emotional or motivational appeal?

This study aims to improve our understanding of the psychological motivators driving phishing victims to participate in phishing scenarios. The results of this study have implications for understanding the human aspects of cybersecurity and could be used as an input for developing phishing susceptibility forecasting abilities.

1.4 Hypotheses

I assumed, that most past victims participating in this experiment had been persuaded through the peripheral route. Since my experiment sought to induce central route information processing, my first hypothesis was:

(H1) Reported personality scores will reveal significant differences between victims phished in the past and the phishing victims of this experiment.

Given that a) message appeal contributes to felt message involvement, b) message involvement induces central route processing and c) stronger message involvement contributes to higher phishing success rate, I predicted that a message, inducing central route processing and having a specific appeal, shows a higher victimization rate among individuals scoring higher in a specific Dark Triad trait. For example, narcissists are egoistic and overconfident in their judgements (Curtis et al., 2018). Therefore:

(H2) Scoring high on Narcissism will increase the response likelihood to a message targeting the ego.

Furthermore, individuals scoring high on Machiavellianism seek personal advantage regardless of other people's losses (McNamara, 2018). Therefore:

(H3) Scoring high on Machiavellianism will increase the response likelihood to a message proposing an opportunity to benefit at the expense of the sender.

Psychopaths are characterized by high sensation seeking and impulsivity along with callous affect and low empathy (Bicer, 2019). Whitty, (2018) found less kind individuals to be more likely to fall for romance scams. Therefore:

(H4) Scoring high on Psychopathy will increase the response likelihood to a message indicating a chance of romance.

2 Methods

I performed quantitative statistical analyses to determine the strength, significance, and direction of relationships between personality traits and susceptibility to each appeal category represented in each phishing e-mail. The evaluation based on data gathered from participants of two surveys. This chapter outlines the design of the experiment and provides the reasoning for the choice of the used methods.

2.1 Experimental Design

My research model involved research constructs, namely psychometric scales, requiring quantitative data to test the hypotheses. There were several ways these data could be gathered. The solution to the problem of gathering personality data was straight-forward: I used psychometric scales that measure the personality domains of interest. However, the problem of gathering accurate data on responding to phishing e-mails proved more challenging. Fortunately, Finn & Jakobsson, (2007) have written a thorough (though somewhat outdated) paper on the available options when designing phishing experiments. I discuss these options in the following paragraphs and provide the reasoning behind my choice of phishing susceptibility assessment method.

2.1.1 Self-reporting Past Events

The method of self-reporting past events is commonly used in behavioural studies (Rosenman, Tennekoon, & Hill, 2011). Participants of the experiment would report information on events during a given (fairly recent, hence memorable) time-frame - 3

years for example. In phishing context, these events could involve conversations with frauds, participating in scams or having lost utility. The nature of the scams participants have related with would enable categorical assessment, allowing studying message appeal. The strength of this approach lies in the simplicity of the design – a set of straight-forward questions on scams one has related with, and their outcomes.

However, this method had three serious drawbacks: first and foremost, it assumes the experimental group members have been knowingly victimized in the past, which in itself is a low probability scenario (Herley & Florêncio, 2009). This results in a needle-in-a-haystack scenario - in order to gather a representative sample of, for example romance scam victims, one would have to filter through an enormous population. Second, this method fails to accommodate victims unaware of their past reactions to scams and potential phishing victims, therefore likely underestimating the damages (Finn & Jakobsson, 2007). Third, it relies on the memories and interpretations of the reporter, introducing errors in recalling past events (i.e., recall bias; Althubaiti, 2016). In summary, I rejected this method because of its data reliability issues and the requirement of a large sample of respondents.

2.1.2 Mimicking Real Phishing Attacks

Another method commonly used in phishing susceptibility studies is phishing simulation, and it involves phishing the participants of the experiment (Finn & Jakobsson, 2007). Real phishing e-mails, delivering links and attachments, are used to measure the actions of the receiver. This design can include forensic tools (or malware), such as scripts and code, executed on the respondent's device post-mortem[1]. Such techniques

[1] An investigation into the causes of a security incident, which has already taken place.

would enable accurate observation of the participants' actions after and before receiving the e-mail. If such techniques are undesirable or -achievable, less invasive techniques, such as read-receipts and webhooks can be used to similar, yet more limited ends.

A successful application of this method is highly complex and requires outstanding technical and organizational skills. While this method would likely provide the most accurate data on phishing susceptibility, it raises ethical complications met by several researchers in the past. For example, despite the efforts of the authors to use an *ethical phishing* technique, Jagatic, Johnson, Jakobsson, & Menczer, (2007) reported criticism from the participants of their experiment after conducting a spear-phishing attack on university students.

While deception is a necessity in some types of studies on human subjects (Finn & Jakobsson, 2007), it is usually avoided to the extent it is possible, and is typically only allowed by institutional review boards only when the expected benefits of the study outweigh the anticipated risks, and the study meets certain conditions outlined in the regulations governing human subjects research (Finn & Jakobsson, 2007). Here, the risk included any potential psychological harm that may be associated with being deceived.

With regards to the context of this study, the research questions and hypotheses required assessment data on a number of e-mails. Thus, using this method, a single user would have been targeted on several separate occasions with phishing attacks, amplifying the risk of psychological harm and conflict. I ended up rejecting this method due to the complexity and unresolved ethical questions of this design.

2.1.3 Phishing E-mail Assessment

Unable to use aforementioned methods for this experiment, I opted for the so-called lab experiment method, also used by Janczewski, Wolfe, & Shenoi, (2013). Using this method, I had participants read specifically designed phishing e-mails and self-report their reactions to these messages. This method came with several advantages and limitations.

As it involves self-reported data, it suffers from ecological validity issues similar to the *self-reporting past events* method. It is unlikely, that respondents would lie about their demographics (Chan, 2009) and the personality inventories used in this experiment have been shown to produce reliable data. However, self-assessing hypothetical actions or decisions in a simulated environment could produce unreliable data (especially on cases concerning social desirability; Devaux & Sassi, 2016). Social desirability bias may occur when questions concern private or sensitive topics, such as drug use, income, diet etc. (Althubaiti, 2016). The e-mails designed for this experiment make appealing offers, preying on the emotions and desires of the readers. Therefore, it is reasonable to assume, that the responses could be prone to social desirability bias. To negate this bias, I assured the respondents on the anonymity of their responses. Furthermore, I encouraged them to answer truthfully, ensuring no one would be judging their decisions. These assurances have been recommended by several researchers as measures against the effects of social desirability bias (Althubaiti, 2016; Warner et al., 2011).

Another drawback of the method is the *knowledge of the existence* of the study, which could bias the outcome of the study (Finn & Jakobsson, 2007). To minimize the effects of this drawback, I did not alert the participants of the experiment, that their ability

to categorize phishing e-mails was being assessed. The limitations of this method are further discussed in Section 4.1, where I discuss the limitations of this study.

Now to the strengths of this method. It incorporates the strength of the *mimicking phishing attacks* method - immediate assessment of an e-mail and following action - without sacrificing ethical integrity. While an element of deception was still necessary within the experiment, I estimated any psychological harm caused to participants to be less likely and severe. The ethical considerations of this experiment are further discussed in Section 2.1.5.

This design was moderately complex to implement and easy to follow for the participant. What's more, it allowed the participant to assess several e-mails, meeting the contextual requirement of the experiment. Self-reporting the data over the internet was not an issue, as it has been shown to be as reliable as traditional pen-and-paper methods (Kalimeri, Beiró, Bonanomi, Rosina, & Cattuto, 2020). Furthermore, self-reports for specific content (such as this study) have been shown to be more accurate and less consistently biased, than reports of generic frequency or duration of actions (Scharkow, 2016). This finding is supported by Workman, (2008), who conducted a similar experiment to mine, only examining PRP in phishing susceptibility. They utilized observational measures to address the limitation caused by self-reported data and they reported good congruence between their self-report subjective measures and observational measures. This report provides evidence to assume congruency between the responses and real-life actions within my experiment as well.

In conclusion, immediate assessment of phishing e-mails gives this *phishing e-mail assessment* method an advantage in accuracy over the *self-reported past events* method. Therefore, I ended up choosing this method due to its simplicity, good expected

data quality and ethical advantages. I addressed the limitations of this method where possible and in ways recommended in relevant literature.

2.1.4 Designing the Experiment

The participants of the experiment were presented with pictures of received e-mails in a Google Gmail inbox. I designed these e-mails for the purpose of this experiment. Each participant was asked to assess 8 e-mails. For each e-mail, participants were asked to respond to the question "How would you manage this e-mail?" with one of the five options:

a) Reply to the e-mail;

b) Leave the e-mail in the inbox and flag for follow up;

c) Leave the e-mail in the inbox;

d) Delete the e-mail;

e) Delete the e-mail and block the sender.

The 8 e-mails used in the experiment were tested and selected from a larger set of e-mails, being most successful in each appeal category response rate wise. 6 of these e-mails were recognizable as phishing e-mails for an experienced eye, while I designed the remaining 2 to seem authentic and believable, absent any deception indicators. The images of all of the e-mails along with their original message source code can be found in Appendix 11.

Including the authentic-looking e-mails was necessary to avoid the formation of confirmation bias among the e-mail readers. For example, if a participant had finished assessing the first 4 e-mails and they all seemed suspicious to them, they could become biased to reject the next e-mails based on the preconceptions formed during assessing the

previous e-mails. Encountering an authentic-looking e-mail among the first few e-mails assessed could provide evidence contradicting this preconception, hence encouraging to evaluate each e-mail objectively (Althubaiti, 2016).

Each e-mail in the experiment targeted an emotional or motivational message appeal, as categorized by Kim & Hyun Kim, (2013). There is a third category of rational appeals, but since my emphasis was on the Dark Triad traits, I decided to focus on the categories more likely to relate with these traits. Table 1 presents these appeal categories and the e-mails applying them.

Table 1

Message Appeals and Corresponding E-mails

Category	Element	Label of the DV (e-mail)	Persuasion theme
Rational appeals	Reasoning from cause	REA1	Information regarding a conference you are expected to attend
	Reasoning from sign	REA2	A friend of a friend asking for help
	Reasoning from analogy	*Not applied*	
Emotional appeals	Fear	THR	Notification of an upcoming account closure
	Affection	ROM, ROF	Chance of romance (Male/Female)
	Happy	MON	Easy monetary gain
Motivational appeals	Safety	THR	Notification of an upcoming account closure
	Self-esteem	EGO	Negative feedback regarding a social media post
	Belongingness/love	CHA	Fundraising for hurricane victims

It is important to note, that I designed all of the e-mails to induce central route processing. According to the principles of ELM, this could be achieved in phishing by bringing the relevance of deception indicators to a minimum and maximizing the relevance of the argument in the text message. While I deliberately avoided the use of common deception indicators (i.e., message structure, time pressure, semantic manipulation; Kim & Hyun Kim, 2013), deception indicators could not be eliminated entirely. The participants had to assess phishing e-mails, so it was necessary to include the element of deception. Note, that this introduced ethical considerations further discussed in Section 2.1.5.

Each of the phishing e-mails had only one common deception indicator present – an unfamiliar sender domain address (also seen in the example brought in Figure 1). This

deception indicator seldom catches the eye of an inexperienced reader, but can lower the credibility of the e-mail among participants experienced with e-mail fraud (Vishwanath et al., 2011). Although I made up the fake domain addresses, sometimes deriving them from widely known existing service providers, I designed the displayed name of the sender was to seem credible. Note, that the authentic-looking e-mails were seemingly received from the widely known hotmail.com domain. What's more, I crafted the messages to seem congruent with the perceived source's self-interests, as incongruency would further lower source credibility (Walster, Aronson, & Abrahams, 1966).

I made an exception in the 'benefit-at-the-expense-of-the-sender' bait (see Figure 3), which I designed to be more appealing for people scoring high on Machiavellianism. I designed this e-mail to look as one written by an unskilled, rich and elderly e-mail user persona, easily taken advantage of. I sought to make this impression by use of sincere wording and capital letters throughout the message body.

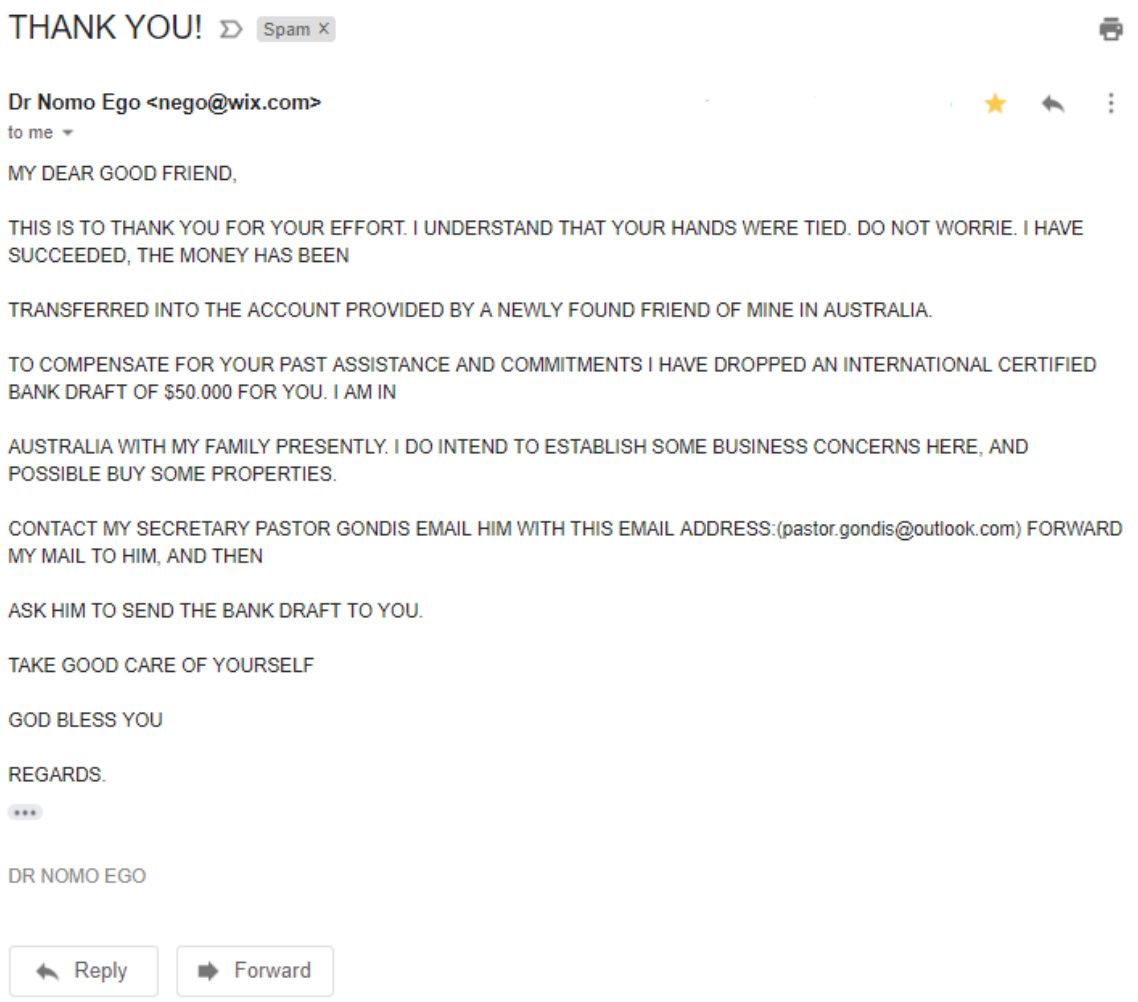


Figure 3. A phishing e-mail with a happiness appeal (label: MON)

Regarding phishing e-mails indicating a chance of romance, I assumed normal orientation, hence the participant was presented with an e-mail from a persona of opposite sex. On cases where no gender was given, orientation could not be assumed. Therefore, these participants were presented with both romance scenarios.

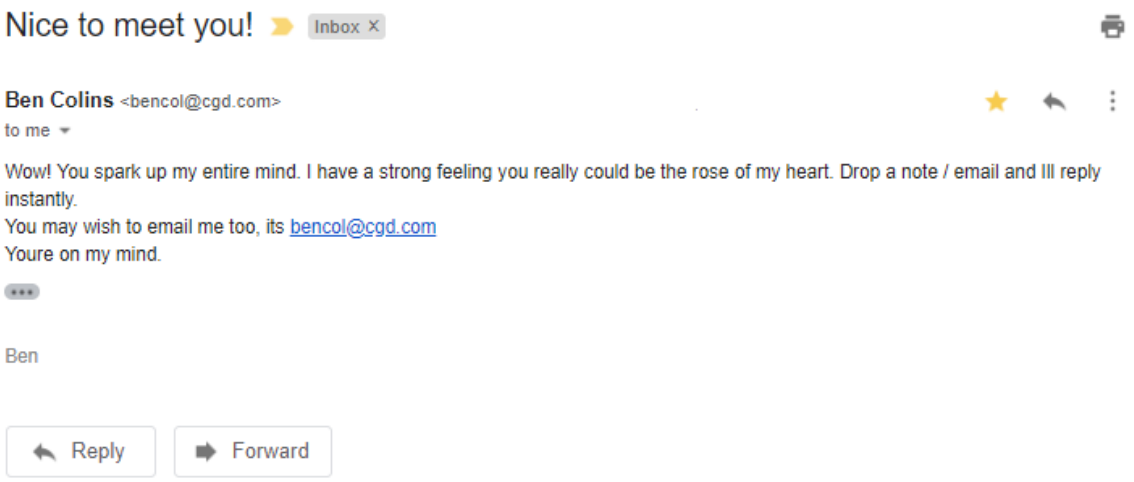


Figure 4. A phishing e-mail with an affection appeal (label: ROM)

2.1.5 Ethical Considerations

This experiment involved human subjects, which means it was subject to common conventions of scientific practice regarding human research. These conventions promote ethical research with the aim of minimizing potential harm of human research and protecting the rights of the participants (World Medical Association, 2013). The potential harm associated with my experiment was any potential psychological harm due to deception. This section describes the common conventions I followed in designing my experiment, in order to ensure the rights of the participants and avoid harm.

There were two ethical issues with my experiment, both coming from the necessity to temporarily withhold information from the participants regarding the true objectives of the experiment. The participants had to be kept unaware that most of the e-mails they assessed were phishing e-mails. Otherwise they would have been biased to reject the offers or demands made in the messages. However, ethical principles of research state that any misleading and deceiving of the participants must be avoided (Bell & Bryman, 2007). While information was temporarily withheld, I did not deceive the participants with misleading information at any point in the experiment. From an ethical

standpoint, the latter approach would have been the worse method. Therefore, I see no ethical issues regarding withholding information.

Furthermore, a fully informed consent of the participants of the experiment should be obtained prior to the study (Bell & Bryman, 2007), which I was unable to obtain. While the participation was voluntary and the participants gave their consent to participate, I was unable to reveal it was a phishing experiment. Instead, in the introduction to the first survey, I notified the participants their IT experience and online communication preferences would be assessed. In the follow-up survey, the participants were informed that their personality was being assessed with regards to how they manage different e-mails. In the end of the follow-up survey, there was a debriefing section explaining the true purpose of the experiment. The participants were informed, that 6 of the e-mails they assessed were phishing e-mails and that the purpose of the experiment was to research security behaviour. While I had to violate this convention, my experiment arguably caused less harm than a simulated phishing attack would. No participants filed complaints or gave negative feedback after the experiment. Therefore, I conclude informed consent was not a significant ethical issue within my experiment.

Concerning other common ethical conventions, I ensured the participants on the anonymity of their answers and did not gather data (on Limesurvey nor mTurk), which would enable identification of participants. The confidentiality of the research data was ensured, as the surveys were hosted and the data stored on a private web server with limited access. The participants were informed prior to the experiment, that the gathered data would be used in a master's thesis and the only affiliation of this study was with Tallinn University of Technology.

2.2 Measures

2.2.1 Dependent Variables

There were two dependent variables (DV) in the experiment:

(DV1) 'PHISHED' – This is a two-outcome categorical variable. I consider a survey participant to have been successfully phished if they admit responding to an unsolicited e-mail during the last six months and/or having responded to a fraudulent e-mail during the last three years.

(DV2) 'APPEAL' – This is an ordinal 5 - level categorical variable group, consisting 8 variables, each representing the likelihood of responding to an assessed e-mail.

2.2.2 Independent Variables

There were a total of 20 independent variables (IV) divided into 3 groups in the experiment. Table 2 presents all of the IV-s and the personality domains they measure. The 3 IV groups were:

(IV1) Independent variable group 1 comprised the mean scores of the 3 Dark Triad subscales. The SD3 domains are Machiavellianism, Psychopathy and Narcissism (Paulhus & Williams, 2002).

(IV2) Independent variable group 2 comprised the mean scores of the 6 subscales measuring HEXACO personality domains. The HEXACO domains are: Honesty-Humility, Emotionality, Extraversion, Agreeableness, Conscientiousness, Openness to Experience (Ashton & Lee, 2009).

(IV3) Independent variable group 3 comprised 11 IV-s: the score means of 10 subscales and the overall StP-II scale score. The Susceptibility to Persuasion domains are Premeditation, Consistency, Sensation Seeking, Self-control, Social Influence, Avoidance of Similarity, Risk Preferences, Attitudes to Advertising, Need for Cognition and Unique Choice (Modic et al., 2018).

Table 2

Independent Variables and Corresponding Personality Domains

IV Group	Scale	Label of the IV	Personality Domain
IV1	SD3	SDT_MACH	Machiavellianism
		SDT_NAR	Narcissism
		SDT_PSY	Psychopathy
IV2	HEXACO	HEX_HH	Honesty-Humility
		HEX_EM	Emotionality
		HEX_X	Extraversion
		HEX_A	Agreeableness
		HEX_C	Conscientiousness
		HEX_O	Openness to Experience
IV3	StP-II	STP2_PRE	Premeditation
		STP2_CON	Consistency
		STP2_SSI	Sensation Seeking
		STP2_SCN	Self-control
		STP2_SI	Social Influence
		STP2_SIM	Avoidance of Similarity
		STP2_RI	Risk Preferences
		STP2_ATA	Attitude to Advertising
		STP2_COG	Need for Cognition
		STP2_UNI	Unique Choice
		STP2_OVERALL	Overall Susceptibility to Persuasion

2.2.3 Control Variables

In addition to the psychometric scales, I gathered context-relevant demographic data during the data-collection process. These data were used as control variables to see, whether demographic factors had any effect on the results of the analyses. Most of these variables were categorical, requiring recoding prior to submission into the regression models discussed in Chapter 3. Table 3 presents the control variables along with the demographic information they measured. All of these control variables were used in the regression models when analysing each DV.

Table 3

Control Variables Used in the Analyses

Label of the CV	Demographic information
AGE	What is your age?
SEX	Please, tell us your gender.
EDU	What is the highest level of education you have completed?
INET	How internet savvy would you describe yourself to be?
MAR	What is your marital status?
LIV	What are your living accommodations?
OCCUP	What is your occupational status?
CORES	What is your country of residence?
CORLE	How long have you lived in your country of residence?

2.3 Data-Collection Process

I used data from two consecutive surveys in this study. The first survey was a short pilot survey, serving the purpose of selecting participants for the second survey. Selected participants were offered to participate in a follow-up survey. In the follow-up survey, data was collected in 5 question groups – demographics, the phishing e-mail assessment group and 3 psychometric scales - in respective order.

2.3.1 Participants

I hosted both surveys on a Limesurvey instance, for which I recruited 530 total workers[1] via the Amazon Mechanical Turk (mTurk) service. Among the 200 participants of the main experiment, the average age group of the respondent was 31-40 and 53% of

[1] Amazon refers to mTurk users performing intellectual tasks as Workers.

the respondents were female. This section presents the demographics of the participants of the experiment.

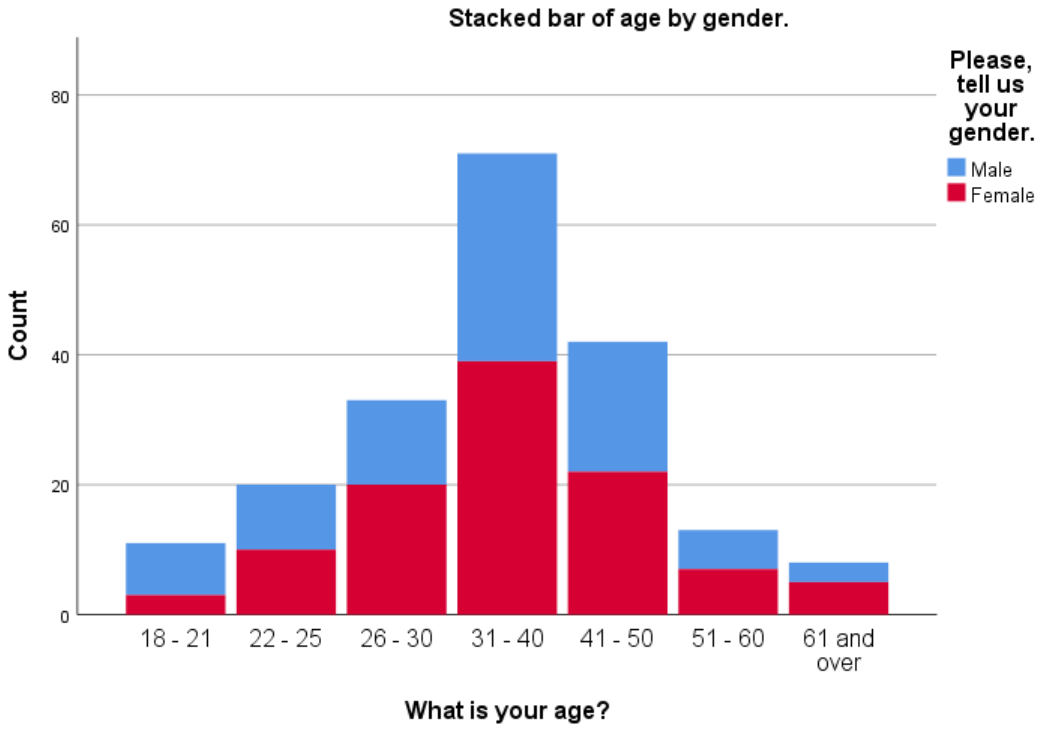


Figure 5. Participants' age stacked by gender.

Based on the workers' self-reported demographics, which they submit upon Amazon account registration, non-random purposive sampling was used to select adults (18 and older) living in Europe or Northern-America. The age requirement was necessary to screen out minors, whose inclusion in the research would demand specific requirements, whereas I set the regional requirement to achieve a representative sample of first world Western individuals.

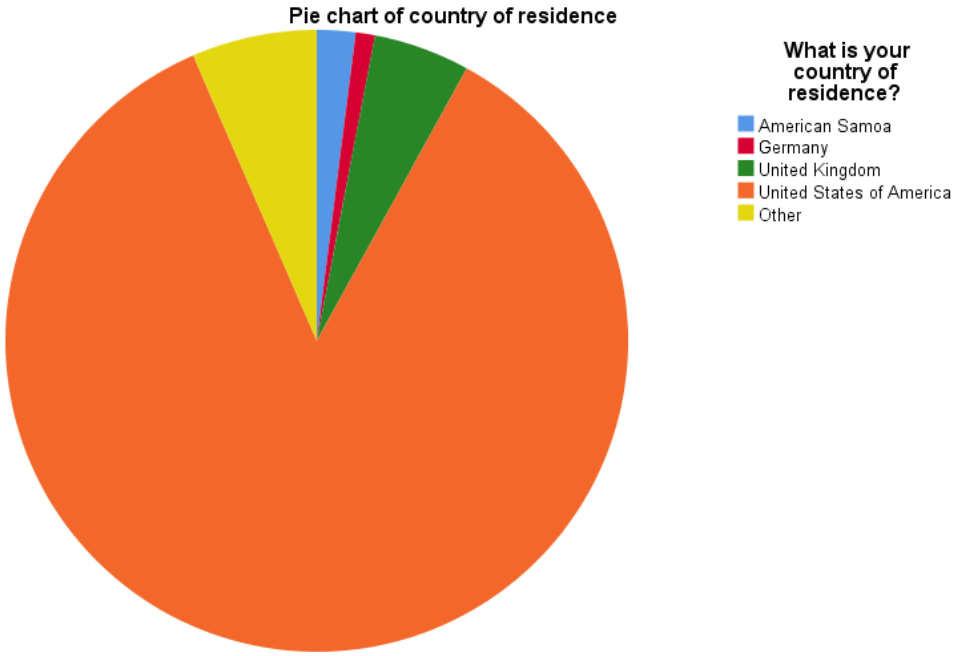


Figure 6. Participants' country of residence.

While participants living in 16 countries were represented, 89% of the participants were American. Additionally, 84% of the participants had lived in their country of residence more than 5 years, while 12% had lived in theirs' for less than a year.

To summarize, I sought demographic homogeny within the participant sample in order to minimize the influence of demographic differences on the data (Vishwanath, 2015). Additionally, as both surveys were in English, I expected workers with this demographic profile to be most likely able to understand and answer the items of the surveys accurately. Given, that the distribution of age, gender and education followed a normal Gaussian curve, and that the majority of the participants had a single English-speaking country of residence, I was satisfied with the demographic profile of the participants of the experiment.

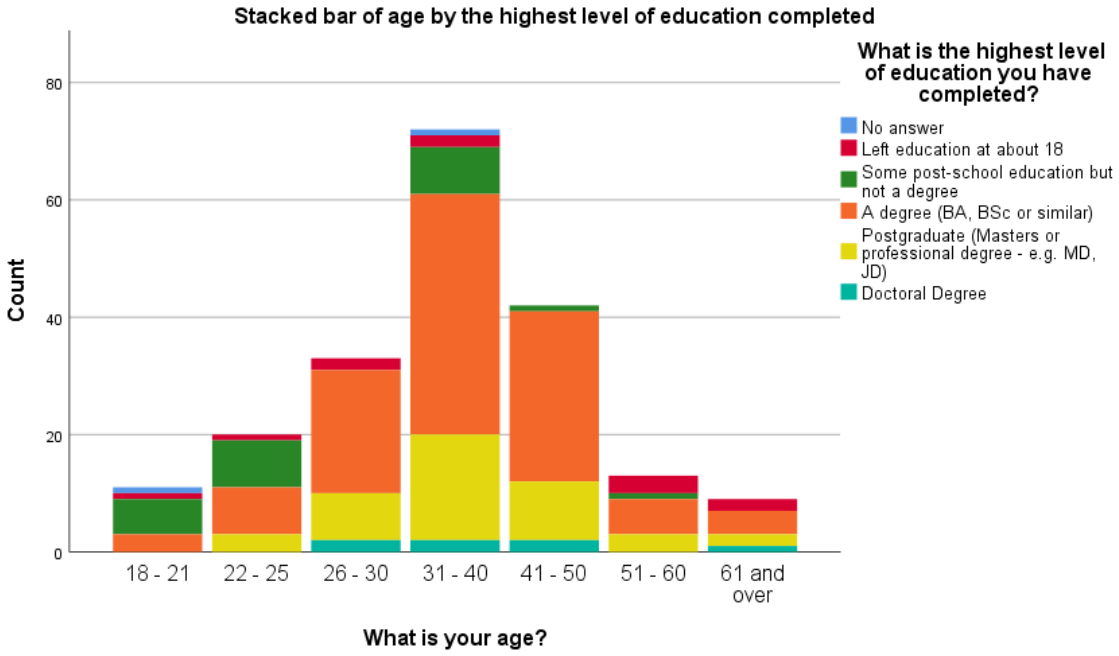


Figure 7. Participants' age stacked by highest level of education completed.

The motivation of mTurk workers is primarily monetary, which is why I employed a reward scheme encouraging complete and accurate answer sets: if the submitted data were incomplete or random, participants would only receive 0,05$ worker fee for their completed task. For a complete and accurate answer set a worker earned a bonus of 0,4$, totalling a 0,45$ in reward for the task.

2.3.2 Personality Data

After submitting demographics and assessing the e-mails, I had participants self-report their personality using 3 consecutive psychometric tests. I used the 27-item Short Dark Triad scale (SD3) to measure Dark Triad domains and the 60-item version of the HEXACO-PI-R to measure HEXACO personality domains (Group, 2009; Jones & Paulhus, 2014). To accommodate other psychometric factors shown to play a role in compliance with fraudulent offers (i.e., scam compliance; Modic, Anderson, & Palomäki, 2018), I used the 54-item Susceptibility to Persuasion-II (StP-II) scale.

Both surveys had an introduction to the experiment and a debriefing. The introduction described the experiment, provided an assurance of anonymity and requested permission to use the data in the analysis. Participants were not informed they would be evaluating phishing e-mails prior to the final debriefing, as they would otherwise have been biased and significantly better at recognizing phishing e-mails (Janczewski et al., 2013). The debriefing section explained the experiment and gave the reasoning for the question groups and phishing scenarios.

2.3.3 Experimental and Control Groups

In addition to selecting participants for the follow-up survey, the first survey served the purpose of dividing the participants into experimental and control groups (past victims and non-victims). Out of the 530 recruited workers, 230 were selected to take the main survey. The participants of the main survey were divided into the experimental and control group, 115 equally to each group. Considering a 10% buffer, I was aiming for 100 usable datapoints in each group to satisfy the assumption on minimum data amount for the analyses (Tabachnick & Fidell, 2012). The criterion for selection into the experimental group was answering 'Yes' to either of these questions indicating potential phishing victimization in near past:

- Have you responded to any emails that (you suspect, or know for sure) were fraudulent in the last three years?

- Have you responded to any unsolicited e-mails in the last six months?

The opportunity to participate in the follow-up survey in the control group was offered randomly to every third non-victim participant. As Limesurvey lacked the functionality to control the flow of participants into experimental and control groups, as

well as cap the groups once desired group sizes were met, an external web server provided the means whereby necessary branch logic could be applied. Data cleaning, after removing the responses with severe missing data, resulted in 200 datapoints used in the analyses – 98 in the experimental and 102 in the control group.

3 Analyses and Results

In this chapter, I present the results of the data analyses. There were a total of 9 outcome, 20 predictor and 10 control variables in the analyses. For both DV1 and DV2 group, I used hierarchical regression models, meaning I entered the predictor variables into the regression model in 4 consecutive blocks – CV, IV1, IV2 and IV3 (see group compositions in Tables 2 and 3). I used the hierarchical approach in order to see, whether adding the variables of an IV group significantly improved the model's ability to predict the outcome variable. I entered IV1 first after the CV block, so that the effect of the SD3 domains could be examined prior to expanding the models with IV2 and IV3. Note that within this chapter, I use the terms significant ($p < 0,05$), highly significant ($p < 0,01$) and extremely significant ($p < 0,001$) when describing the strength of relationship between variables.

3.1 Analysing DV1

I analysed the categorical dependent variable (DV1)] in a binary logistic regression model. [PHISHED] was a dichotomic variable, meaning it had a value of 1 or 0. There were 98 past scam victims in the experimental (PHISHED = 1) and 102 non-victims (PHISHED = 0) in the control group. Appendix 2 shows the results of DV1 analysis.

Regarding logistic regression model assumptions, the Hosmer-Lemeshow Test showed a non-significant result, indicating that the model was a good fit. Analysing the missing data of psychometric scales with Little's MCAR test showed, that missing data was distributed randomly. Therefore, these missing values were replaced with mean values in the analysis.

3.1.1 Analysing Control Variables

Analysis of the demographic variables showed that the CV block extremely significantly influenced the prediction of past phishing victimisation ($p < 0,001$), explaining 25% of the variance (Nagelkerke R^2). The CV block as a whole had a considerable impact on DV1 ($X^2_2 = 41,123$, $p < 0,001$), yet none of the CV-s had a significant influence in the overall predictive model. The most significant control variable in block 1 was time spent living in country of residence [CORLE] ($\sigma = 1,396$; unstandardised β weight = -0,634). The only other significant control variable in block 1 was living accommodations [LIV] ($\sigma = 2,126$; unstandardised β weight = 0,457).

3.1.2 Analysing Independent Variables

The SD3 scale (IV1; block 2) explained 25,4% of the variance and had an extremely significant influence on past phishing victimisation ($X^2_2 = 52,894$, $p < 0,001$). Note, that the Hosmer-Lemeshow test for the block 2 model failed ($p < 0,05$), meaning this model was prone to Type II errors. Since I was interested in examining differences in how individual SD3 traits influence past victimisation and response likelihood within the current experiment, I needed to compare the -2LL and R^2 values for models with each of the individual SD3 variables. However, as all of the SD3 domains had insignificant influence on past victimisation in the overall models, I could not examine each of these IV-s separately from the rest of the IV-s, as this would create an omitted variable bias.

The HEXACO scale (IV2; block 3) added 9,9% of the explained variance, extremely significantly impacting the DV ($X^2_2 = 25,276$; $p < 0,001$). Note, that the Hosmer-Lemeshow test for this model failed as well. Lastly, the STP2 scale (IV3; block 4) explained another 5,4% of the variance but did not show a statistically significant

impact on the DV (X^2_2 = 15,156; p = 0,126) using a cut-off of p < 0,05. However, the overall model passed the Hosmer-Lemeshow test.

Out of the individual independent variables, two IV-s stood out as significant (p < 0,05) predictors of past victimisation: the HEXACO domain Conscientiousness [HEX_C] had a significant negative influence on past victimisation (σ = 0,707; unstandardised β weight = -1,017) and the STP2 domain Avoidance of Similarity [STP2_SIM] had a significant positive influence on past victimisation (σ = 1,665; unstandardised β weight = 1,077).

3.1.3 Model Summary

After adding all the psychometric scales to the regression, the overall model was able to explain 65,7% of variance in past victimization while extremely significantly impacting the DV (X^2_2 = 134,45, p < 0,001). Note, that personality traits accounted for 40,7% of the variance and control variables for 25% of the variance (Nagelkerke R^2 change), meaning personality traits were more important predictors than control variables. Overall goodness of fit for the model is 85,9%, meaning this model with these regressors covers approximately 86% of variance in past victimisation. This means, that we are able to predict whether someone has been phished in the past in 85,9% of the cases when considering these IV-s.

3.2 Analysing DV2

The categorical dependent variable group (DV2) ’APPEAL’ comprised 8 individual variables, each representing the decision of the reader for each assessed e-mail. A total of 1367 answers were collected for the 8 e-mails and 33 answers were missing.

3.2.1 Descriptive Statistics

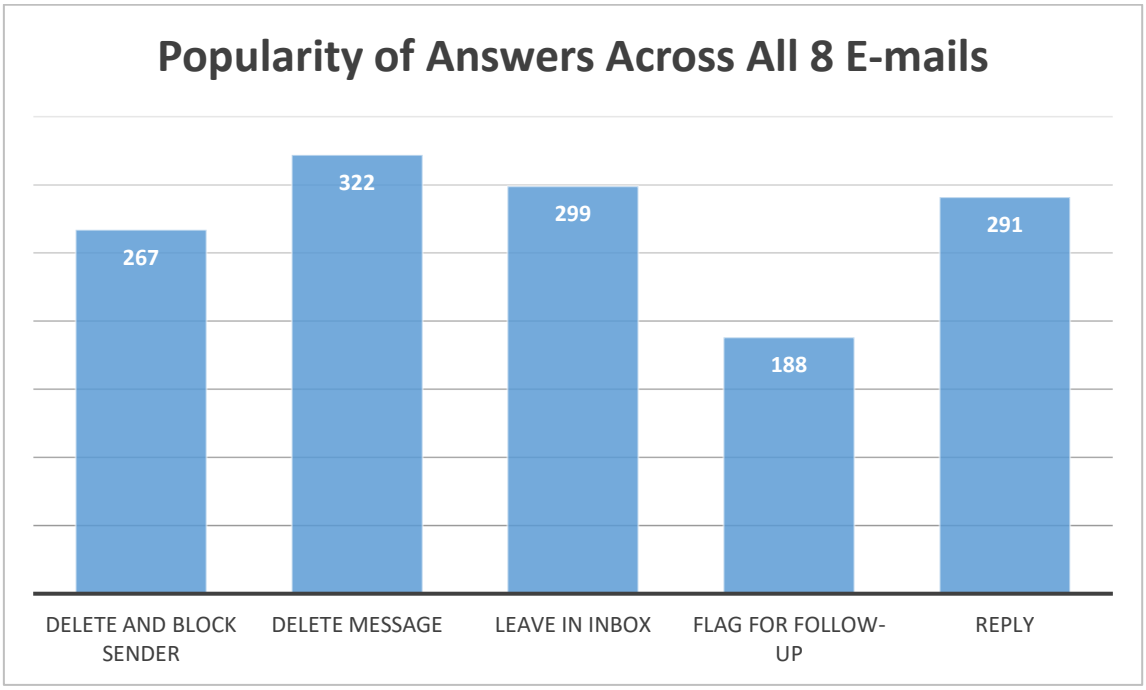


Figure 8. Popularity of answers across all 8 e-mails.

Popularity of each answer is displayed in Figure 8, revealing 291 total cases of successful phishing, forming 21% of all decisions. Each of the 5 decisions was omitted a score of 1-5 on an ordinal scale, representing the response likelihood score. The answer ’Delete the e-mail and block the sender’ would score the lowest possible 1, while ’Reply to this e-mail’ would score the highest possible 5 on the response likelihood scale.

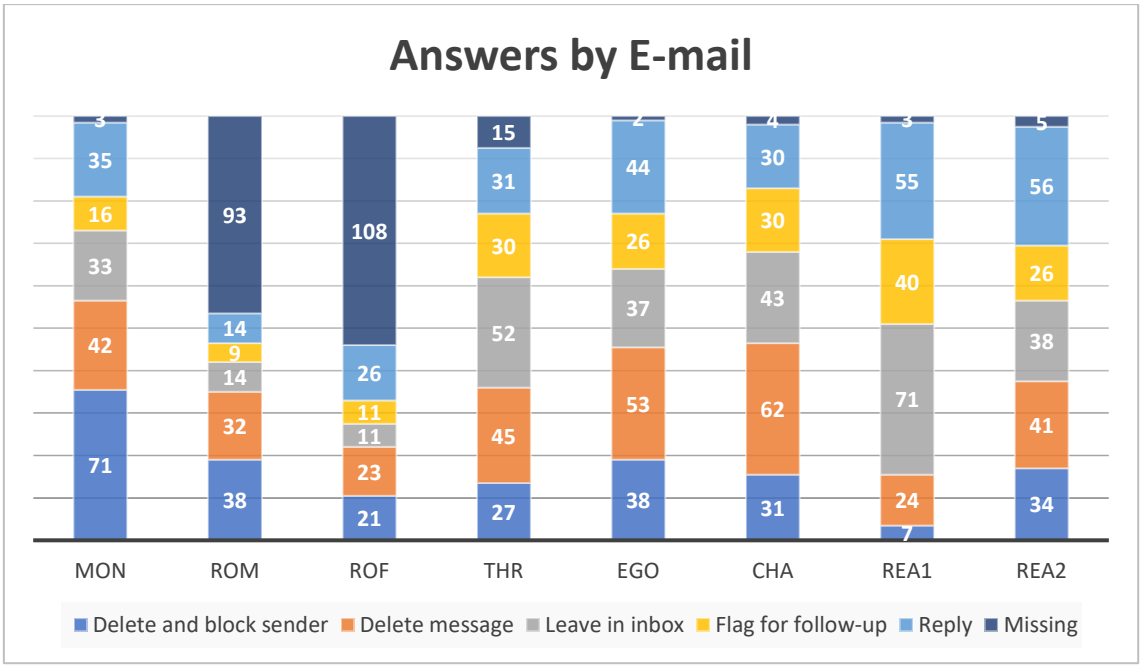


Figure 9. Participants' answers stacked by response items.

Figure 9 presents the answers for each of the 8 e-mails. As can be seen, the stacked bars are consistent with Figure 8, showing fairly equal distribution among all 5 decisions. An inconsistency can be spotted regarding missing answers on [ROM] and [ROF]. This inconsistency was expected, as [ROM] and [ROF] indicate a chance of romance for the opposite gender. Thus, the [ROM] e-mail was assessed only by women and the [ROF] e-mail only by men. Although these two e-mails received least 'Reply' answers, their success rates should be assessed proportionally, given that other e-mails were assessed twice as many times. Unsurprisingly, the authentic-looking [REA1] and [REA2] were the most accepted e-mails with 27,5% response rate. These e-mails were followed closely by [ROF] and [EGO].

The least successful e-mails were [THR], [CHA], [ROF] and [MON], averaging around 31 replies and a 15,5% success rate. What's more, [MON] was most frequently categorized as a scam, showing almost twice as many 'Delete the e-mail and block the sender' responses as the runners-up [ROM] and [EGO]. This was expected, as [MON]

was written in capital letters (see Figure 3) for reasons explained in Section 2.1.4. Note, that when adjusting for the missing answers, [ROM] would likely be most frequently categorized as a scam instead.

3.2.2 Building the Regression Model

Each dependent variable in DV2 group was analysed in a hierarchical MLR model. The control and independent variables were entered into regression in 5 blocks using enter procedure. The first block comprised the 9 control variables described in Table 3. The second block added only the variable past victimisation [PHISHED] into the model. Lastly, blocks 3-5 entered the IV1-3 groups described in Table 2, in corresponding order, into the regression models. The results of the analyses for each DV are presented in Appendixes 3 – 10.

Note, that each DV2 variable was also controlled for the influence of past victimisation [PHISHED]. Controlling for the effect of [PHISHED] enabled to see, whether past victimisation had a significant influence on response likelihood within this experiment. As further explained under Section 3.2.5, past victimisation had a significant influence on several DV-s.

I considered analysing the datapoints of control and experimental groups separately (i.e., using the stratification method; Pourhoseingholi, Baghestani, & Vahedi, 2012) to account for the effect of past victimisation, but research supports adjusting the model to any significant confounding variables in quantitative statistical models (McNamee, 2005; Pourhoseingholi et al., 2012). Therefore, [PHISHED] was included in the regression model as a control variable. I decided to enter [PHISHED] in a separate block, so that its influence would be isolated from the effect of the demographic variables.

Having learned about the influence of past victimisation in my models, I became interested if there were any personality trait differences between the two groups. This insight could be given by stratification. Therefore, in addition to the regression model described in previous paragraphs, I used stratification, but only to examine the differences in personality among control and experimental groups. This means, that each DV2 variable was analysed with two sets of data, selected for the two possible values 0 and 1 of [PHISHED]. The results of stratification are described in Appendix 1 and discussed under Section 3.2.4 and Chapter 43.2.7.

3.2.3 Testing Assumptions

Regarding GLM assumptions, the regression models showed a linear relationship between outcome and predictor variables in all cases. Distribution of residuals was normal, indicating no presence of heteroskedasticity. The variable inflation factor (VIF) remained between 1 and 10 in all cases, indicating no multicollinearity issues within the models and the Durbin-Watson statistic was between 1,5 and 2,5 in all cases, meaning the data was not autocorrelated. Considering the sufficient sample size of 200 (100 for [ROM] and [ROF]) datapoints per model, I conclude, that all of the regression models met GLM assumptions. Predictor variables were entered in 5 consecutive blocks using enter method. The following paragraphs summarize the results of the analyses of each of the variables in DV2 group.

3.2.4 Analysing Variance

Analyses of variance (ANOVA) revealed personality traits had a significant influence on all of the DV-s. The overall models were good fit, meaning these models significantly predict their proportion of variance in response likelihood. This means, that personality traits were good predictors of response likelihood in this experiment.

When using stratification, the models were able to predict response likelihood less accurately. This was expected, as the models no longer accommodated the significant predictor variable [PHISHED]. The results revealed personality traits had a more significant impact among the control group. Among the experimental group, none of the overall models were able to predict response likelihood with sufficient statistical accuracy, whereas among the control group, 4 DV-s were significantly influenced by the overall predictive models: [REA1], [MON], [REA2], and [CHA]. Note, that analyses revealed accuracy issues in the results of the stratification method. These issues are addressed in detail under Limitations 4.1.

3.2.5 Analysing Control Variables

The analyses of the control variables showed that the influence of demographic variables in the overall models was significant only for [CHA]. In this case, occupational status [OCCUP] had a significant negative impact on the likelihood to respond (t_{199} = -2,589; p = 0,01), meaning individuals occupying better career positions were less likely to respond.

In the overall models, past victimisation was significant for 5 out of 8 DV-s, the exceptions being [ROF], [REA1] and [THR]. Among the phishing e-mails, [PHISHED] explained 5,7% – 22,9% (R^2 change) of variance in response likelihood. This means, that past victimisation is a significant confounding variable (i.e., confounder; Pourhoseingholi, Baghestani, & Vahedi, 2012) in analysing response likelihood. A confounder is an extraneous variable, whose presence affects the variables being studied so that the results do not reflect the actual relationship between the variables under study (Pourhoseingholi et al., 2012). Hence the need for adjustment described in Section 3.2.2.

3.2.6 Analysing Independent Variables

The third block IV1 comprised the 3 SD3 domain means as predictor variables. Overall, IV1 was highly to extremely significant on all cases, except for [REA1]. Among the DV-s significantly influenced, IV1 explained 7,3% - 15,4% of variance (R^2 change) in response likelihood.

Block 4 added IV2 into the regression model, meaning the 6 HEXACO domains. The addition of IV2 was significant for all DV-s, having an extremely significant effect on 6 DV-s and a significant effect on [ROF] and [REA1]. The IV2 block explained another 1,8% - 7,6% of variance (R^2 change) in response likelihood.

Lastly, block 5 added IV3, comprising the 10 STP2 domains. Even though the IV3 group comprised 11 variables, the last variable - STP2_OVERALL - was excluded from analyses on all cases, as the tolerance limit of 0,000 was reached. This is an indication, that the STP2 Overall Score did not increase the fit of the models. Hence, it was automatically excluded from the regression models. The addition of IV3 was also significant for all DV-s. Similarly to IV2, it had an extremely significant influence on 6 of the DV-s and a significant influence on the remaining [REA1] and [ROF]. IV3 further explained 4% - 9,8% of variance (R^2 change) in response likelihood.

Out of the individual independent variables, none of the domains stood out as excellent predictors of responding to the phishing e-mails across the overall models. However, 3 IV-s were tied as the most frequent positive predictors of response likelihood, all on 2 occasions. The STP2 Social Influence [STP2_SI], the HEXACO Honesty-Humility [HEX_HH] and the STP2 Sensation Seeking [STP2_SSI] domains. The most frequent negative predictor was the STP2 Need for Consistency [STP2_CON] domain, being a significant predictor on 2 occasions. Notably, the SD3 domain Psychopathy

[SDT_PSY] was a significant positive predictor of responding to both authentic-looking e-mails [REA1] and [REA2].

Regarding the SD3 domains, I was interested in whether individual SD3 traits had a significant effect on response likelihood among any of the DV-s. I found, that the Dark Triad traits were only significant for [REA2], Narcissism and Psychopathy both positively and significantly influencing response likelihood. Psychopathy did have a noticeable positive influence on [ROM] ($t_{104} = 1{,}750$; $p = 0{,}084$), yet the relationship was not statistically significant. None of the SD3 traits were significant predictors of responding to the phishing e-mails.

In addition to the phishing e-mails discussed this far, I also designed 2 authentic-looking e-mails labelled [REA1] and [REA2] and a phishing e-mail posing as a Red Cross charity fund-raising campaign for the victims of hurricane Dorian, labelled [CHA]. Regarding [CHA], none of the personality traits stood out as significant predictors of responding. Instead, past victimisation and occupational status were the only significant predictor variables in the overall model. The authentic-looking [REA1] and [REA2] showed varying results. Past victimisation was only significant for [REA2], whereas gender was significant for [REA1] (women being more willing to respond). Psychopathy stood out as a significant positive influencer on both cases, meaning individuals prone to impulsive behaviour were more likely to respond.

3.2.7 Summary of Models

After adding all the psychometric scales to the regressions, the overall models were all statistically significant according to ANOVA. Among the phishing e-mails, the overall models were able to explain 28,4% - 59,5% of variance in response likelihood and among [REA1] and [REA2] 23,7% and 35,8% respectively. Demographic variables were

only significant for [CHA]. The results show personality traits were significant predictors of response likelihood among all DV-s, accounting for 15,0% – 23,7% (R^2 change) of explained variance within the overall models. Past victimisation was highly significant for 4 out of 6 phishing emails, explaining 14,1% – 22,9% (R^2 change) of variance in response likelihood.

4 Discussion

Having gathered the data using the methods described in Chapter 2, I ran the quantitative statistical analyses described in the previous Chapter 3. The regression models checked out on all of the regression assumptions, meaning there were no significant problems with the data. This means, that the results of the analyses are correct and the method suitable for this research. Subsequently, the conclusions made in this chapter are correct to the extent that the quality of the data allows. This chapter discusses the results of these analyses, answering research questions, testing hypotheses and drawing conclusions where possible.

The demographic profile of the participants of the experiment was relatively homogenous, as desired. Analyses of the control variables revealed that demographic data had a significant influence on the model predicting past victimisation, but not the likelihood of responding to the e-mails assessed within this experiment. Time spent living in country of residence stood out as a significant demographic predictor of past victimisation. The longer an individual had lived in their country, the less likely they had been scam victims in the past. This finding suggests immigrants had been victims more often, either in their current or previous countries of residence, than long-term residents. Interestingly, living accommodations proved to be another significant control variable. The better the living accommodations, the more likely a participant had been a scam victim in the past. Similarly to occupational status, living accommodation is an indicator of wealth. Therefore, this finding could possibly mean that richer participants had been scammed more often.

Overall, the results of the analyses suggest personality traits are significant predictors of phishing susceptibility. First, I found personality traits have a strong and

significant relationship with past phishing victimisation. My regression model is able to accurately predict, whether or not a person has been phished in the past in 85,9% of the cases (see Classification Table in Appendix 2).

This finding had important implications for the following analyses, because I found that past scam victims were also more likely to respond to the phishing e-mails designed for this experiment. When comparing the decisions of the experimental and control group (see charts in Appendix 1), past scam victims would consistently respond more to the phishing e-mails, than the control group. This observation is evidence of an underlying security behaviour construct among the participants, most likely the *repeat-clicker* phenomenon, also noted and examined by several researchers (Correia, 2019; Whitty, 2019). *Repeat-clickers* represent a persistent minority of users who repeatedly fall victim to phishing e-mails (Klein, 2019). Given the high accuracy of my personality-based past scam victim prediction model, my results are consistent with the argument by Klein, (2019), who suggested individual traits account for the primary factor underlying the *repeat-clicking* behaviour.

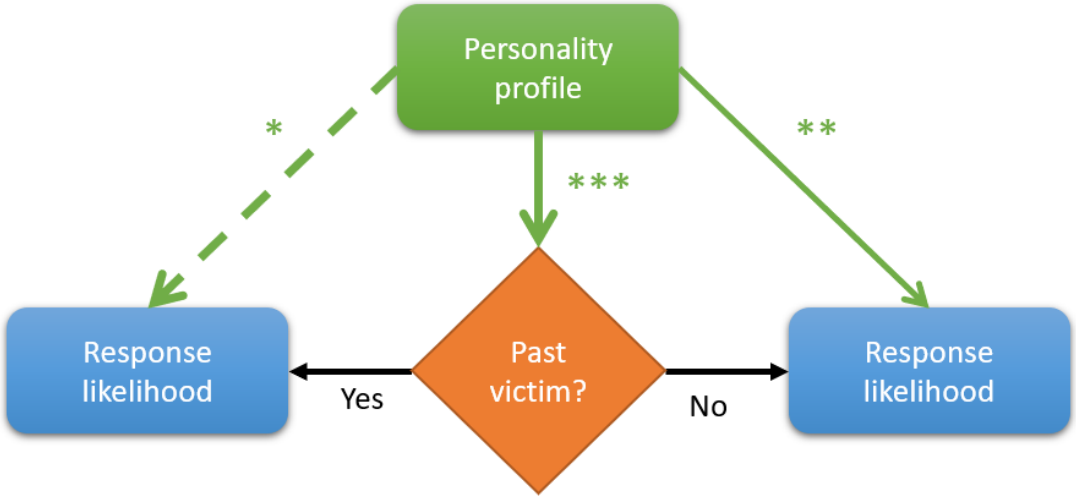


Figure 10. Relationship between personality, past victimisation and response likelihood.

To further examine the effect past victimisation had on my results, I used the stratification method described in Section 3.2.2 to compare the results of control and experimental groups. Figure 10 illustrates the conclusions of this comparison. The number of asterixis represents the strength and significance of the influence of personality traits. Stratification revealed that personality traits were better predictors of response likelihood among those participants, who have not been phished in the past. Among past victims, my model failed to predict likelihood of responding to any of the assessed e-mails with sufficient statistical accuracy, whereas among non-victims, responses to 4 e-mails were significantly influenced by personality traits.

This means, that if the individual has not fallen for a scam in the past (i.e., they are not a *repeat-clicker*), their personality profile is an important factor in predicting the likelihood to respond to a phishing e-mail. However, if one has fallen for a scam in the past, their *repeat-clicking* tendency is a better indicator of susceptibility to a spear-phishing e-mail (i.e., susceptibility to phishing in CRP). This statement should not be misinterpreted, meaning one should not be led to an underestimation of the importance

of personality traits among past victims. Mind, that the findings of Klein, (2019) and my own suggest *repeat-clicking* is highly predictable based on personality.

Analysing the influence of personality traits on the likelihood to respond revealed the Dark Triad and HEXACO personality traits to be extremely significant predictors of past victimisation. In the overall model, two personality domains stood out as most significant predictors of past victimisation. First, the HEXACO domain Conscientiousness had a significant negative influence on past victimisation. Conscientious people are highly competent and tend to detect information correctly (Cho et al., 2016). This finding is consistent with the conventional wisdom in phishing research (e.g. Halevi et al., 2015; Van De Weijer & Leukfeldt, 2017).

Second, Avoidance of Similarity [SIM] had a significant positive influence on past victimisation**.** Marketing **r**esearch has shown consumers to be likely to respond positively to marketing offers when they believed the offer to be unique or scarce (Kramer & Carroll, 2009; Modic, Anderson, & Palomäki, 2018). My results reveal people are more likely to be scammed in the past if they are attracted by uniquely perceived offers. This finding is consistent with past research, as this effect has also been noted in examining vulnerability to scams (Langenderfer & Shimp, 2001). Note that the effect sizes are small to moderate in most cases, however this is not unexpected in empirical studies (e.g. Moody et al., 2017; Ryan & Xenos, 2011), where diverse factors impact unexplained variance of a phenomena.

Moving on to the e-mails assessed within this experiment, personality traits proved to be significant predictors of response likelihood in CRP. Note, that I did not use stratification when analysing the effects of individual scales and domains. Instead, I adjusted the models for past victimisation. The reasoning behind this choice is explained

in detail in Section 3.2.2. My findings suggest that past victimisation and personality profile are equally successful in an overall model predicting likelihood to respond to phishing e-mail in CRP. This means, that including these two factors should be considered when building a model predicting phishing susceptibility in CRP. Using these two factors, my models were able to explain 28,4%-59,5% of variance among the decisions of the readers. This means, that personality traits provide ample insight into phishing susceptibility in central mode.

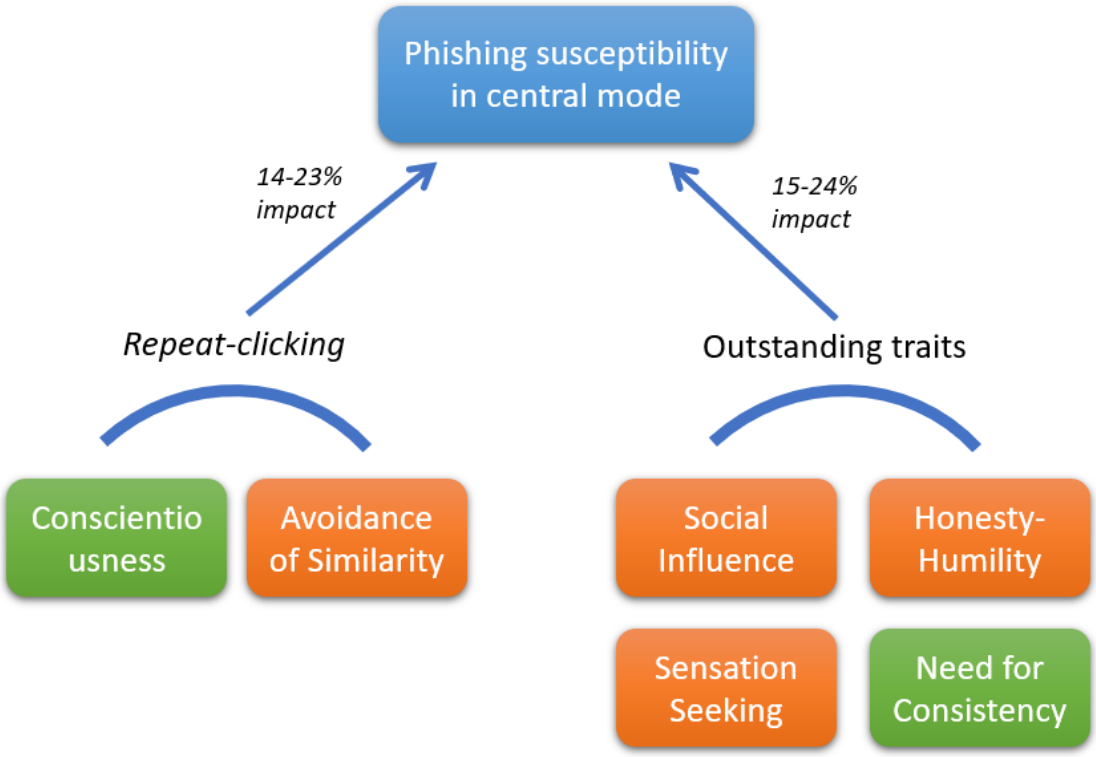


Figure 11. Influence of personality on phishing susceptibility in central route to persuasion.

Figure 11 summarizes and visualises my findings regarding the role of personality traits in influencing susceptibility in CRP. Important personality domains increasing susceptibility are shown in red and the domains decreasing susceptibility in green. Both the *repeat-clicking* phenomenon and the outstanding personality traits shown in Figure 11 were equally important (each contributing ~20% on average) in the overall model predicting susceptibility in central mode. Furthermore, I found that if a person is prone to *repeat-clicking*, this factor is a better indicator of susceptibility than the other outstanding personality traits. Whereas if an individual is not a *repeat-clicker*, Social Influence, Honesty-Humility, Sensation Seeking and Need for Consistency are the best predictors of susceptibility in CRP.

Each of these 4 domains was significant among 2 of the 6 phishing e-mails assessed. The Social Influence domain indicates, how likely an individual is to be

influenced by social pressure (Modic et al., 2018). My results revealed a positive relationship, meaning the more an individual succumbs to social pressure, the more likely they were to respond. This finding confirms the findings in related works in online scam context (Modic & Lea, 2014; Weeks, Ardèvol-Abreu, & De Zúñiga, 2017). Sensation Seeking and Honesty-Humility also had a positive influence on the likelihood to respond, meaning people who seek novel and intense experiences (Modic et al., 2018) or are honest, sincere, honest and modest (Ashton & Lee, 2009) were more likely to respond to the phishing e-mails. Need for Consistency was the only significant negative predictor, indicating individuals feeling strong need for consistency and structure are less likely to respond.

These findings have both theoretical and practical implications. In theory, my findings suggest that a model aiming to predict spear-phishing susceptibility should accommodate personality as an influencing factor. In order to assess an individual's susceptibility to spear-phishing, one should first distinguish if an individual is prone to the *repeat-clicking* tendency. If they are, they should be considered as susceptible to spear-phishing based on their personality profile. If they are not prone to *repeat-clicking*, further measurement should be used to assess their personality-related susceptibility. Additionally, my findings suggest, that measuring personality has the potential to reveal, which persuasion themes *non-repeat-clickers* are most susceptible to.

Moving on to the research questions and hypotheses stated in Sections 1.3 and 1.4, I was first interested, if there would be differences in personality between victims in peripheral and central modes (RQ1). (H1) proposed, that reported personality scores would reveal significant differences between past phishing victims and the phishing victims of this experiment.

In terms of the predictive power of personality traits, they were significant on both cases. Personality traits accounted for 40% of variance for past victimisation and 15-24% for likelihood of responding to the e-mails in this experiment. This finding suggests, that personality traits were better predictors of past victimisation, forming a 2/3 of the predictive power of the overall model, while personality traits merely accounted for 1/3 to 1/2 of total variance among the responses in this experiment.

This finding would indicate, that there are significant differences in the personality of the two persuasion modes, had past victimisation not significantly influenced the responses in my experiment. I found that past victimisation was a significant positive predictor of responding in 4 out of 6 phishing e-mails. This means, that past victimisation is the best overall predictor of responding to phishing e-mails in CRP. Furthermore, since past victimisation is highly predictable based on personality, I conclude that the same personality domains (Conscientiousness and Avoidance of Similarity) are the best overall predictors of responding to phishing e-mails in both central and peripheral modes. Therefore, the answer to RQ1 is that there are no major differences in personality between the personality profiles of victims in peripheral and central modes. This finding has an important theoretical implication, namely that the

Examining the importance of individual personality traits in each predictive model revealed some differences, however. First, although different personality traits were significant predictors of responding to specific phishing e-mails, there were no salient traits determining response likelihood across all of the phishing e-mails in my experiment. This was not surprising, as each of the e-mails in the experiment was designed with a different appeal. In contrast, Conscientiousness and Avoidance of Similarity stood out as salient predictors of past victimisation. Hence, the influence of personality traits varied significantly between the control and experimental group. Therefore, I confirm H1: my

findings suggest significant differences between the personality profiles of past phishing victims and those of this experiment.

This finding is irrelevant in light of the influence of past victimisation, however. I suspect Conscientiousness and Avoidance of Similarity were insignificant on their own, because past victimisation was significantly correlated with these domains. Therefore, I believe the correct conclusion to be drawn is that which I suggested in answering RQ1 – the *repeat-clicking* phenomenon, explained best by Conscientiousness and Avoidance of Similarity domains, is the best overall predictor of susceptibility in peripheral and central modes.

Reminding RQ2, I was interested, if any personality traits stand out as significant predictors of overall phishing e-mail response likelihood in CRP. Given the importance of *repeat-clicking* in overall susceptibility, I conclude Conscientiousness and Avoidance of Similarity are the best individual traits predicting susceptibility in central mode. If these two traits do not reveal the *repeat-clicking* tendency, Social Influence, Honesty-Humility, Sensation Seeking and Need for Consistency are next in line in predictive power.

Regarding the importance of the variables each scale assessed, SD3 and STP2 proved more significant predictors than the HEXACO scale. Entering the predictor variables block-wise, grouped by each scale, revealed that the SD3 items were significant predictors for each predictive model, except for the authentic-looking [REA1], while the addition of the HEXACO scale items was significant only for [REA1]. This finding suggests, that the SD3 items are more important predictors of phishing susceptibility, than the HEXACO items. The reason behind the insignificance of the HEXACO scale might be explained to an extent by the fact, that the variance explained by SD3 and HEXACO

scales somewhat overlap (i.e., there is collinearity between the predictor variables). Finally, the addition of the STP2 scale was significant for [EGO], [CHA] and [MON].

Finally, H2-4 exclusively addressed the Dark Triad personality traits. I was interested, if any Dark Triad personality trait would stand out in CRP as a significant predictor of responding to a message with a certain appeal (RQ3). H2 proposed, that people scoring high on Narcissism would be more susceptible to a message targeting the ego. My results reveal 4 variables were significant in predicting responding to [EGO]. In order of importance, these variables were Sensation Seeking, past victimisation [PHISHED], Need for Consistency and Honesty-Humility. Narcissism did not show a significant influence on the likelihood of responding to [EGO]. Therefore, I rejected H2.

H3 posited, that scoring high on Machiavellianism increases the response likelihood to a message proposing an opportunity to benefit at the expense of the sender. Within this experiment, [MON] was this opportunity in guise of an offer from a gullible and rich person. Machiavellianism did not show a significant influence on the likelihood of responding to [MON]. In fact, Machiavellianism showed a negative, though statistically insignificant influence. Therefore, I also rejected H3. Instead, Sensation Seeking, Honesty-Humility and past victimisation were significant positive variables, while Avoidance of Similarity and Need for Consistency were significant negative variables influencing the likelihood of responding to [MON].

Lastly, H4 proposed, that scoring high on Psychopathy increases the likelihood of responding to a message indicating a chance of romance. To measure this, I had men assessing [ROF] and women assessing [ROM]. Results revealed Social Influence to be the only significant personality trait across the responses of both e-mails, having a positive influence on response likelihood. Past victimisation was only significant for

[ROM], being the most influential predictor. While Psychopathy influenced positively the likelihood to respond, the relationships were statistically insignificant in both cases. Therefore, I rejected H4.

In order to answer RQ3, I had to examine if any of the Dark Triad traits at all significantly influenced the responding to any e-mails. Analyses revealed that none of the Dark Triad traits had significant influence within the overall models predicting responses to the phishing e-mails. Unexpectedly, Psychopathy was a positive influencer for both [REA1] and [REA2] and Narcissism was a positive influencer for [REA2]. This finding suggests that the Dark Triad traits are significant predictors of responding to authentic e-mails, rather than phishing e-mails. I suspect these results are caused by the multidimensionality of the Dark Triad traits (Miller, Vize, Crowe, & Lynam, 2019). For example, in addition to impulsiveness and lack of empathy, Psychopathy has been associated with boldness (Patrick, Fowles, & Krueger, 2009), which would indicate that braver individuals were more likely to respond to the authentic-looking e-mails.

Nevertheless, I was surprised to find that all of the Dark Triad traits were insignificant in predicting the likelihood of responding among all of the phishing e-mails. This means that I ended up rejecting all hypotheses regarding the relationship between the Dark Triad traits and likelihood of responding. This would indicate, that the Dark Triad traits have no significant effect in phishing susceptibility in central mode, yet I suspect there were several methodological and a scientific reason for the poor predictive performance of these traits. First, there were several methodological limitations discussed in the next Section 4.1. In addition to these limitations, it is possible that the e-mail material used within this experiment was not appealing enough to produce valid results. For example, I suspect the success rate of [ROF] could have been increased by use of a romantic message more appealing to women.

The scientific reason I pointed out is the recent criticism on use of the Dark Triad construct in multivariate statistical analyses, such as my own. In particular, Miller, Vize, Crowe, & Lynam, (2019) have pointed out that the Dark Triad facets could become substantially correlated in statistical analyses, especially Machiavellianism and Psychopathy. This would mean that the correlated traits would share a significant proportion of explained variance, each individual trait becoming less strongly related to the measured variable. Comparing zero-order correlations with partial and part correlations (see Coefficients tables in Appendixes 3-8) does reveal significant overlap in explained variance. While each trait would be strongly correlated with response likelihood regardless of other independent variables (i.e., zero-order correlations are high), each Dark Triad trait loses the majority of their strength when removing the variance overlapping with other variables (i.e., part and partial correlations are low). Whether or not this issue was caused by the Dark Triad traits being intercorrelated or from correlations with other traits in the model, the insignificance of individual Dark Triad traits within my analyses supports the criticism on the validity of the Dark Triad construct, rather than overrides it.

4.1 Limitations

This study has several limitations to consider. The most serious limitations come from the data-collection method, which relies on the assumptions of a simulated environment. First, my study suffers the same limitations Janczewski et al., (2013) did, who used a similar phishing e-mail assessment method in their research. Similarly to their experiment, participants of my experiment were not required to click on any links, open attachments or provide personal information. It is therefore possible that, in a real-world situation, participants may have behaved differently. This study was also a role play, and

the manner in which participants deal with e-mails in an experimental environment may not relate precisely to how participants would deal with actual emails received in their personal inboxes (Steven Furnell, 2007).

Furthermore, most experts in psychological research suggest that self-report data should not be used alone, as it tends to be biased (Althubaiti, 2016). My study relies almost entirely on self-reported data, meaning the validity of information may have been compromised by a number of factors, including careless responding, social desirability effects and deliberately exaggerated responses (Chan, 2009). Although I accounted for several self-report biases (e.g., social desirability, recall, confirmation, measurement error) in the experimental design as recommended by relevant research (Althubaiti, 2016), self-report data is often combined with other types of information in order to increase the accuracy of results on subject matter (Kuvaas, 2009). Another way to validate my research would be confirming these results by other methods, such as mimicking real phishing attacks or a study involving smaller population and direct observation strategies (Orkin et al., 2014) or checking to see if similar studies produce consistent results over time (Hopwood, Good, & Morey, 2018).

The final limitation I'd like to point out from methodological perspective concerns the use of stratification when comparing the results of control and experimental groups. Although research recommends stratification as one of the ways to address confounders in analyses (Pourhoseingholi et al., 2012), stratification has been shown to produce Type I errors (Kazempour, 1995). The presence of Type I errors is an indication that the differences revealed by the comparison may not be correct in magnitude, or exist at all (Kazempour, 1995). Upon examining correlations, this suspicion proved correct for [ROM] and [MON], where the Durbin-Watson statistic was out of normal bounds. This

is an indication of dependence between residuals, meaning that in these cases, regression suggested significance where perhaps there was none (Field, 2009).

Moving on to the measurements, the first limitation is a restriction of the simulated environment. This study used only the readers' likelihood of responding to measure message appeal and phishing susceptibility. While this is a reasonable indirect approach to measure potential phishing victimisation, responding is only one (and likely not the most common) reactions spear-phishing e-mail aim to induce. In order to increase ecological validity, alternative motives behind spear-phishing, such as clicking links and opening attachments could be employed to observe direct victimisation.

Next, this study relies on the concepts of central and peripheral routes to persuasion of ELM. However, there was no instrument I could use to measure, which path to persuasion a respondent chose in information processing. I had no practical way to confirm that the participant read the message and took CRP, rather than decided upon peripheral cues. Therefore, I relied on the theoretical premises of ELM for designing CRP inducing e-mails. Additionally, I mixed authentic-looking e-mails among phishing e-mails in order to avoid forming a confirmation bias among the participants. By using survey opening time as a surrogate measure, I was able to confirm only that the survey was open long enough to permit reading the e-mails.

After I had already gathered the data and conducted the experiment, I did come across scales for necessary measurements, employed in the analogous Heuristic-Systematic Model (HSM; Chen & Chaiken, 1999). These scales were used to similar ends to measure path to persuasion in the paper by Vishwanath, (2015), where a 6-item scale was used to assess heuristic processing and a 7-item scale to assess systematic processing.

These scales and other principles from HSM could be used in future research to provide more accurate measurements of paths to persuasion.

Regarding measuring message appeal, despite my efforts, I was unable to find a scale or statistical model usable for the purposes of this research. The closest available instrument was the Personal Involvement Inventory (PII; Zaichkowsky, 1985) scale, which comprises 20 items. Future research could use some items from this scale to measure involvement. For example, Vishwanath, Herath, Chen, Wang, & Rao, 2011 measured the involvement construct in their information processing model using 9 items from the PII. Due to the high number of items in PII and the number of assessments participants had to make, I chose to indirectly measure response likelihood using a Likert-type 5-item scale instead. Note, that this problem comes from selection of methods and could be avoided altogether by using the phishing attack simulation method. Mimicking phishing attacks would enable to gather observational data on direct victimisation, such as opening, clicking and responding instead, similarly to Vishwanath, (2015).

The final limitation I would like to point out is related to contextual variables in phishing susceptibility. Several researchers have highlighted the importance of the context of the reader in decision-making: media use and e-mail habits (Vishwanath, 2015), how many e-mails they usually work with (i.e., e-mail load; Vishwanath et al., 2011), how confident they are in assessing e-mails (Rao, Li, & Wang, 2018), knowledge of scams (Wang et al., 2012), etc. Regarding scam knowledge, the participants of the study were not informed, that their ability to manage phishing e-mails was being assessed. In such case, research has shown scam knowledge has no significant effect on participants' ability to recognize phishing e-mails. (S Furnell, Clarke, & of Plymouth. Centre for Security, 2011; Wang et al., 2012).

This finding was supported by Ms. Tiiu Mamers, an expert on human aspects of cyber security, who concluded on the 2020 Interdisciplinary Cyber Research conference (ICR; Tiiu Mamers, 2020): “It is more important what people do, than what they know”. She pointed out, that people often know they should be careful when working with e-mails, yet they seldom care enough about this matter to alter their behaviour. The self-reports in this experiment revealed that the ability of participants to identify phishing e-mails based on the sender domain deception indicator was low. Therefore, I conclude scam knowledge had no significant effect on the likelihood to respond in my study.

However, my research excluded most of such contextual variables. Given that my research focused on examining the relationship between personality and phishing susceptibility (rather than model-building), I do not consider this as an important limitation in my study. Nevertheless, contextual variables have been shown to influence phishing susceptibility, which is why measuring important contextual variables should be considered in future research.

5 Summary

This Thesis addressed a gap in phishing susceptibility research. In particular, how readers decide upon responding to phishing e-mails, when employing central (also referred to as systematic) information processing mode. This problem is important, because spear-phishing often relies on text-based messages employing central route to persuasion, rather than relying on visceral triggers more often employed by untargeted phishing, which encourage peripheral processing. While the information security community has found effective ways to address the threat of untargeted phishing in form of awareness trainings and technical measures, spear-phishing remains difficult to protect against. This is because there are no technical means to eliminate the threat of spear-phishing, and we still know little about the factors motivating people to participate in the scenarios proposed in spear-phishing messages. Consequently, current literature lacks the insight on how to negate the persuasive effect of these factors.

In Section 1.1, I challenged the conventional wisdom in phishing research (along with the cited conclusion from Wang et al., 2012), which suggests visceral triggers and deception indicators are the two main aspects influencing an individual's decision to respond to a phishing email. I argued that there is no exhaustive literature on central information processing mode in phishing susceptibility, where behavioural theory suggests different principles apply in decision-making. Hence, this conventional wisdom cannot (and evidently has failed to) effectively address the problem of spear-phishing. Therefore, because the research model in Wang et al., (2012) had not been tested in central mode, nor did the model accommodate personality as a factor influencing susceptibility, I argued that their conclusion could only be true for peripheral processing of phishing e-mails.

Given the high percentage of variance explained by my personality-based models, I have succeeded in challenging their conclusion along with the conventional wisdom it represents. In 2 out of 8 cases, my MLR model was able to explain over 50% of variance in the likelihood of responding to the e-mails assessed in this experiment. This means, that at least in these cases, personality was the more important influencer of responding than visceral triggers and deception indicators. An important theoretical implication of this finding is, that in central route to persuasion, visceral triggers are less important predictors of responding than personality. Furthermore, as the e-mails the participants had to assess touched on their sensitive topics and feelings, I suspect self-report bias may have led to an underestimation of actual response rate. Therefore, I strongly recommend future phishing experiments include observational data, because I suspect the actual relationship is more significant.

In any case, these results should be interpreted with care, because they do not suggest personality traits are more important overall predictors of phishing susceptibility. Nor can my models be directly applied in predicting phishing susceptibility. My experiment was designed to examine a narrow niche: the effect of personality traits in central route processing of phishing e-mails. Therefore, my models excluded several factors shown to contribute to phishing susceptibility, including attention to visceral triggers and deception indicators. My findings merely highlight the importance of personality traits in central mode and future research could further examine the differences between phishing susceptibility in peripheral and central routes to persuasion. For example, one could examine central mode processing of e-mails applying models, which have been developed and previously used applied only to examine viscerally enticing phishing e-mails (e.g. Wang et al., 2012 & Vishwanath et al., 2011) and compare findings.

In this Thesis, I examined the relationship between personality and how likely e-mail reader are to respond to e-mails with different emotional and motivational appeals. To achieve this, I designed a phishing experiment, where participants were shown images of e-mails in a fictional Gmail inbox. Having read each e-mail, they were asked to self-report their hypothetical reaction in a survey format. They had 5 options to choose from, each indicating their likelihood to respond to a given e-mail. This experimental design was selected from available options used and discussed in literature, most notably in Finn & Jakobsson, (2007). I designed the e-mails used in the experiment to induce central route information processing, following the theoretical principles of the ELM model. Furthermore, I gathered demographic data and personality data using psychometric scales in survey format, followed by analyses of the data in logistic and linear regression models.

Overall, the results of my analyses suggest personality is a key factor in both peripheral and central mode susceptibility, providing ample insight into the decision-making process of a phishing e-mail reader. First, Conscientiousness and Avoidance of Similarity stood out as significant predictors of past phishing victimisation (i.e., the *repeat-clicking* tendency). Past victimisation was also the best overall predictor of responding in my experiment, meaning past victims were more likely to respond to the e-mails assessed in my experiment. Therefore, my findings suggest *repeat-clicking* is the best overall predictor of phishing susceptibility in central information processing mode. Because literature and my findings suggest the *repeat-clicking* tendency is highly predictable based on personality, I conclude that the personality traits predicting overall phishing susceptibility are similar for both central and peripheral modes to persuasion. While *repeat-clicking* has been previously examined in phishing susceptibility, my findings are the first to highlight the importance of *repeat-clicking* in central information

processing mode. Nevertheless, the relationship between personality and the *repeat-clicking* tendency could be further examined in future research.

While the *repeat-clicking* tendency is highly associated with personality, I found past victimisation and measured personality to have similar predictive power in central route to persuasion. This indicates a difference between the two modes, meaning there is more variance in predictive power of specific traits in central, than in peripheral mode. This means, that the traits Conscientiousness and Avoidance of Similarity seem to be more important in peripheral, than in central route to persuasion. While no salient traits (except for *repeat-clicking* phenomenon) predicted overall susceptibility in central mode, stratification revealed that if a person does not fit the profile of a *repeat-clicker*, significant traits increasing their susceptibility are Social Influence, Sensation Seeking and Honesty-Humility, while Need for Consistency decreases susceptibility. This means, that while *repeat-clicking* comes first in importance when assessing susceptibility in central mode, these four salient traits are next in line influencing susceptibility.

Continuing on individual traits, this Thesis focused on the Dark Triad personality traits and their relationship with emotional and motivational appeals commonly presented in phishing e-mails. I was interested, if any Dark Triad trait was associated with responding to an e-mail carrying a specific appeal. Although I rejected all of the hypotheses raised on relationships between specific traits and appeals, I found different outstanding traits to predict responding to each e-mail in the experiment. Contrary to my expectations, I found that individual Dark Triad traits were only significant when predicting responding to authentic e-mails, instead of the phishing e-mails. These results were likely caused due to the multidimensionality of the Dark Triad traits (e.g., in addition to unethical intentions, relevant literature associates Psychopathy with boldness).

Nevertheless, my findings indicate a relationship between personality traits, the emotional and motivational appeals presented in phishing e-mails and the likelihood of a reader to respond to an e-mail with a specific appeal. In future research, phishing susceptibility could be further examined in association with specific appeals. For example, research concerning spear-phishing susceptibility could measure victimization in central information processing mode when employing the reasoning from cause, sign and analogy appeals described in Table 1. Another approach would be employing e-mails appealing to multiple factors (e.g., combine techniques that utilize financial and scarcity motives in one scenario), as suggested in Workman, (2008).

As discussed before, an important theoretical implication of my findings is, that the influence of specific personality traits varies (likely in accordance with specific appeals) more in central information processing mode than in peripheral. However, my experiment involved one appealing message sample per Dark Triad trait, which means I have not gathered the substantial data required for decisive insight into the specific relationships each trait and appeal have. Therefore, the problem concerning the lack of knowledge about how personality influences spear-phishing victimisation, remains unsolved. Future research could provide these data by analysing more e-mails in central mode using different measuring instruments and context-specific improvements (more details on potential improvements are found in Section 4.1). This means, that future research could solve the problem of central processing of phishing e-mails, which in turn could be applied in practice to decrease the threat of spear-phishing.

References

Alseadoon, I. (2014). The impact of users' characteristics on their ability to detect phishing emails. *Doctoral Thesis*.

Althubaiti, A. (2016). Information bias in health research: Definition, pitfalls, and adjustment methods. *Journal of Multidisciplinary Healthcare*, *9*, 211–217. https://doi.org/10.2147/JMDH.S104807

Ashton, M. C., & Lee, K. (2009). The HEXACO-60: A short measure of the major dimensions of personality. *Journal of Personality Assessment*, *91*(4), 340–345. https://doi.org/10.1080/00223890902935878

Bell, E., & Bryman, A. (2007). The ethics of management research: An exploratory content analysis. *British Journal of Management*, *18*(1), 63–77. https://doi.org/10.1111/j.1467-8551.2006.00487.x

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*, 51–61. https://doi.org/10.1016/j.chb.2015.01.039

Butavicius, M., Parsons, K., Pattinson, M., Mccormac, A., Calic, D., & Lillie, M. (2017). Understanding Susceptibility to Phishing Emails: Assessing the Impact of Individual Differences and Culture. *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)* , *2016*(Haisa), 12–22.

Cezar, A., Cavusoglu, H., & Raghunathan, S. (2017). Sourcing Information Security Operations: The Role of Risk Interdependency and Competitive Externality in Outsourcing Decisions. *Production and Operations Management*, *26*(5), 860–879. https://doi.org/10.1111/poms.12681

CHAN, D. (2009). So why ask me? Are self report data really that bad? *Statistical and Methodological Myths and Urban Legends: Doctrine, Verity and Fable in the Organizational and Social Sciences*, 309–335.

Chen, S., & Chaiken, S. (1999). The heuristic-systematic model in its broader context. In *Dual-process theories in social psychology*. (pp. 73–96). New York, NY, US: The Guilford Press.

Cho, J. H., Cam, H., & Oltramari, A. (2016). Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA 2016*, 7–13. https://doi.org/10.1109/COGSIMA.2016.7497779

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), 1–12. https://doi.org/10.1186/s40163-019-0099-7

Devaux, M., & Sassi, F. (2016). Social disparities in hazardous alcohol use: Self-report bias may lead to incorrect estimates. *European Journal of Public Health*, *26*(1), 129–134. https://doi.org/10.1093/eurpub/ckv190

Ferreira, A., & Teles, S. (2019). Persuasion: How phishing emails can influence users and bypass security measures. *International Journal of Human Computer Studies*, *125*(November 2017), 19–31. https://doi.org/10.1016/j.ijhcs.2018.12.004

Field, A. (2009). *Discovering Statistics Using SPSS ISM (London, England) Introducing Statistical Methods Series*.

Finn, P., & Jakobsson, M. (2007). GOST PAPER: Designing and conducting phishing experiments. *IEEE Technology and Society Magazine, Special Issue on Usability*

and Security, 1–21.
Furnell, S, Clarke, N., & of Plymouth. Centre for Security, C. N. R. (2011). *Proceedings of the Fifth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2011) , London, United Kingdom 7-8 July 2011*. Center for Security, Comunications & Network Research, University of Plymouth.
Furnell, Steven. (2007). Phishing: can we spot the signs? *Computer Fraud & Security*, *2007*(3), 10–15. https://doi.org/https://doi.org/10.1016/S1361-3723(07)70035-0
Furnell, Steven. (2013). Still on the hook: The persistent problem of phishing. *Computer Fraud and Security*, *2013*(10), 7–12. https://doi.org/10.1016/S1361-3723(13)70092-7
Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, *18*(1), 22–44. https://doi.org/10.17705/1jais.00447
Halevi, T., Memon, N., & Nov, O. (2015). Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2544742
Herley, C. (2010). The Plight of the Targeted Attacker in a World of Scale. *Workshop on the Economics of Information Security*, 12. Retrieved from http://weis2010.econinfosec.org/papers/session5/weis2010_herley.pdf
Herley, C., & Florêncio, D. (2009). A profitless endeavor: Phishing as tragedy of the commons. *Proceedings New Security Paradigms Workshop*, 59–70. https://doi.org/10.1145/1595676.1595686
Hopwood, C. J., Good, E. W., & Morey, L. C. (2018). Validity of the DSM–5 Levels of Personality Functioning Scale–Self Report. *Journal of Personality Assessment*, *100*(6), 650–659. https://doi.org/10.1080/00223891.2017.1420660
Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94–100. https://doi.org/10.1145/1290958.1290968
Janczewski, L., Wolfe, H. B., & Shenoi, S. (2013). Security and Privacy Protection in Information Processing Systems: 28th IFIP TC 11 International Conference, SEC 2013 Auckland, New Zealand, July 8-10, 2013 Proceedings. *IFIP Advances in Information and Communication Technology*, *405*(December 2017). https://doi.org/10.1007/978-3-642-39218-4
Kalimeri, K., Beiró, M. G., Bonanomi, A., Rosina, A., & Cattuto, C. (2020). Traditional versus facebook-based surveys: Evaluation of biases in self-reported demographic and psychometric information. *Demographic Research*, *42*, 133–148. https://doi.org/10.4054/DemRes.2020.42.5
Kazempour, K. (1995). Impact of Stratification Imbalance on Probability of Type I Error. *The American Statistician*, *49*(2), 170–174. https://doi.org/10.2307/2684632
Kim, D., & Hyun Kim, J. (2013). Understanding persuasive elements in phishing e-mails:A categorical content and semantic network analysis. *Online Information Review*, *37*(6), 835–850. https://doi.org/10.1108/OIR-03-2012-0037
Klein, C. (2019). The Enduring Mystery of the Repeat Clickers, (September). Retrieved from https://www.history.com/news/the-enduring-mystery-of-the-lewis-chessmen
Kleitman, S., Law, M. K. H., & Kay, J. (2018). It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. *PLoS ONE*, *13*(10), 1–30. https://doi.org/10.1371/journal.pone.0205089
Kramer, T., & Carroll, R. (2009). The effect of incidental out-of-stock options on preferences. *Marketing Letters*, *20*(2), 197–208. https://doi.org/10.1007/s11002-

008-9059-9
Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005
Kuvaas, B. (2009). A test of hypotheses derived from self-determination theory among public sector employees. *Employee Relations*, *31*, 39–56. https://doi.org/10.1108/01425450910916814
Langenderfer, J., & Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing*, *18*(7), 763–783. https://doi.org/https://doi.org/10.1002/mar.1029
McNamee, R. (2005). Regression modelling and other methods to control confounding. *Occupational and Environmental Medicine*, *62*(7), 472–500. https://doi.org/10.1136/oem.2002.001115
Miller, J., Vize, C., Crowe, M., & Lynam, D. (2019). *A critical appraisal of the Dark Triad literature and suggestions for moving forward*. https://doi.org/10.31234/osf.io/mbkr8
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), 1–21. https://doi.org/10.1371/journal.pone.0194119
Modic, D., & Lea, S. E. G. (2014). Scam Compliance and the Psychology of Persuasion. *SSRN Electronic Journal*, *304*. https://doi.org/10.2139/ssrn.2364464
Moody, G. D., Galletta, D. F., & Dunn, B. K. (2017). Which phish get caught An exploratory study of individuals′ susceptibility to phishing. *European Journal of Information Systems*, *26*(6), 564–584. https://doi.org/10.1057/s41303-017-0058-x
Orkin, S. H., Nathan, D. G., Ginsburg, D., Look, A. T., Fisher, D. E., & Lux, S. (2014). *Nathan and Oski's Hematology and Oncology of Infancy and Childhood E-Book*. Elsevier Health Sciences. Retrieved from https://books.google.ee/books?id=gjWaBQAAQBAJ
Patrick, C., Fowles, D., & Krueger, R. (2009). Patrick CJ, Fowles DC, Krueger RF. Triarchic conceptualization of psychopathy: Developmental origins of disinhibition, boldness, and meanness. Dev Psychopathol. 2009;21(Special Issue. *Development and Psychopathology*, *21*, 913–938. https://doi.org/10.1017/S0954579409000492
Paulhus, D. L., & Williams, K. M. (2002). The Dark Triad of personality: Narcissism, Machiavellianism and psychopathy. *Journal of Research in Personality*, *36*(6), 556–563. https://doi.org/10.1016/S0092-6566(02)00505-6
Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. *Advances in Experimental Social Psychology*, *19*(C), 123–205. https://doi.org/10.1016/S0065-2601(08)60214-2
Pourhoseingholi, M. A., Baghestani, A. R., & Vahedi, M. (2012). How to control confounding effects by statistical analysis. *Gastroenterology and Hepatology from Bed to Bench*, *5*(2), 79–83. https://doi.org/10.22037/ghfbb.v5i2.246
Rao, H. R., Li, Y., & Wang, J. (2018). Overconfidence in Phishing Email Detection. *Journal of the Association for Information Systems*, *17*(11), 759–783. https://doi.org/10.17705/1jais.00442
Rosenman, R., Tennekoon, V., & Hill, L. G. (2011). Measuring bias in self-reported data. *International Journal of Behavioural and Healthcare Research*, *2*(4), 320. https://doi.org/10.1504/ijbhr.2011.043414
Ryan, T., & Xenos, S. (2011). Who uses Facebook? An investigation into the relationship between the Big Five, shyness, narcissism, loneliness, and Facebook

usage. *Computers in Human Behavior*, *27*(5), 1658–1664. https://doi.org/10.1016/j.chb.2011.02.004

Scharkow, M. (2016). The Accuracy of Self-Reported Internet Use—A Validation Study Using Client Log Data. *Communication Methods and Measures*, *10*, 13–27. https://doi.org/10.1080/19312458.2015.1118446

Tabachnick, B., & Fidell, L. (2012). *Using Mulivariate Statistics*. *5th ed.* (Vol. 3).

Tiiu Mamers. (2020). 6th Interdisciplinary Cyber Research 2020. In *Human Aspects of Cyber Security*. Tallinn: ICR 2020.

Van De Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big Five Personality Traits of Cybercrime Victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407–412. https://doi.org/10.1089/cyber.2017.0028

Vishwanath, A. (2015). Examining the Distinct Antecedents of E-Mail Habits and its Influence on the Outcomes of a Phishing Attack. *Journal of Computer-Mediated Communication*, *20*(5), 570–584. https://doi.org/10.1111/jcc4.12126

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. https://doi.org/10.1016/j.dss.2011.03.002

Walster, E., Aronson, E., & Abrahams, D. (1966). On increasing the persuasiveness of a low prestige communicator. *Journal of Experimental Social Psychology*, *2*(4), 325–342. https://doi.org/10.1016/0022-1031(66)90026-6

Wang, J., & Chen, R. (2009). An Exploration of the Design Features of Phishing Attacks, *4*.

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, *55*(4), 345–362. https://doi.org/10.1109/TPC.2012.2208392

Warner, C. H., Appenzeller, G. N., Grieger, T., Belenkiy, S., Breitbach, J., Parker, J., … Hoge, C. (2011). Importance of Anonymity to Encourage Honest Reporting in Mental Health Screening After Combat Deployment. *Archives of General Psychiatry*, *68*(10), 1065–1071. https://doi.org/10.1001/archgenpsychiatry.2011.112

Weeks, B. E., Ardèvol-Abreu, A., & De Zúñiga, H. G. (2017). Online influence? Social media use, opinion leadership, and political persuasion. *International Journal of Public Opinion Research*, *29*(2), 214–239. https://doi.org/10.1093/ijpor/edv050

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277–292. https://doi.org/10.1108/JFC-10-2017-0095

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. https://doi.org/10.1016/j.chb.2017.03.002

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *JASIST*, *59*, 662–674. https://doi.org/10.1002/asi.20779

World Medical Association. (2013). Declaration of Helsinki, Ethical Principles for Scientific Requirements and Research Protocols. *Bulletin of the World Health Organization*, *79*(4), 373. Retrieved from https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/

Zaichkowsky, J. L. (1985). Measuring the Involvement Construct. *Journal of Consumer Research*, *12*(3), 341. https://doi.org/10.1086/208520

Zaichkowsky, J. L. (2014). Measuring the Involvement Construct, (October). https://doi.org/10.1086/208520

Appendix 1 – Stratification Statistics

Response Likelihood

DV	R^2	R^2 adj	F	p	Durbin-Watson Statistic: PHISHED = 0 (Selected)	Durbin-Watson Statistic: PHISHED ~= 0 (Unselected)
MON	42,4%	19,3%	$F_{28,70} = 1,837$	p < 0,05	1,810	1,272
ROM	53,4%	12,9%	$F_{27,31} = 1,317$	n.s.	2,147	1,535
ROF	66,9%	-14,5%	$F_{27,11} = 0,822$	n.s.	1,626	2,019
THR	36,2%	6,9%	$F_{28,61} = 1,234$	n.s.	1,757	1,914
CHA	54,3%	35,5%	$F_{28,68} = 2,885$	p < 0,001	2,193	2,000
EGO	39,5%	14,9%	$F_{28,69} = 1,607$	n.s.	1,642	1,894
REA1	42,8%	19,3%	$F_{28,68} = 1,819$	p < 0,05	2,320	2,024
REA2	43,5%	19,8%	$F_{28,67} = 1,839$	p < 0,05	2,344	1,649

Note. Model summaries among control group (PHISHED = 0).

Response Likelihood

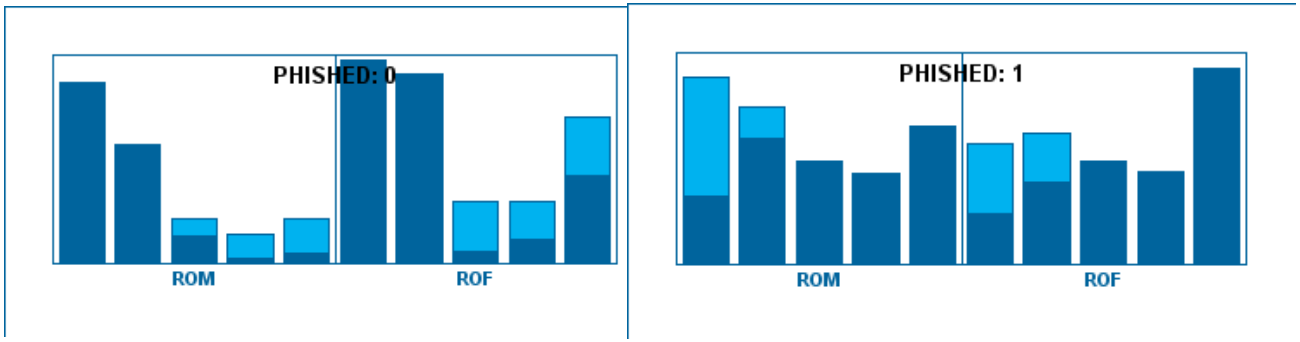
DV	R^2	R^2 adj	F	p	Durbin-Watson Statistic: PHISHED = 1 (Selected)	Durbin-Watson Statistic: PHISHED ~= 1 (Unselected)
MON	38,8%	13,3%	$F_{28,67} = 1,519$	n.s.	2,038	1,622
ROM	75,2%	37,9%	$F_{27,18} = 2,019$	n.s.	2,638	1,503
ROF	62,5%	18,5%	$F_{27,23} = 1,421$	n.s.	1,824	1,721
THR	34,9%	6,5%	$F_{28,64} = 1,227$	n.s.	2,216	1,789
CHA	35,7%	9,2%	$F_{28,68} = 1,347$	n.s.	1,782	1,719
EGO	32,0%	4,4%	$F_{28,69} = 1,160$	n.s.	2,151	1,552
REA1	36,6%	10,9%	$F_{28,69} = 1,425$	n.s.	2,376	1,609
REA2	36,7%	10,7%	$F_{28,68} = 1,409$	n.s.	2,065	1,335

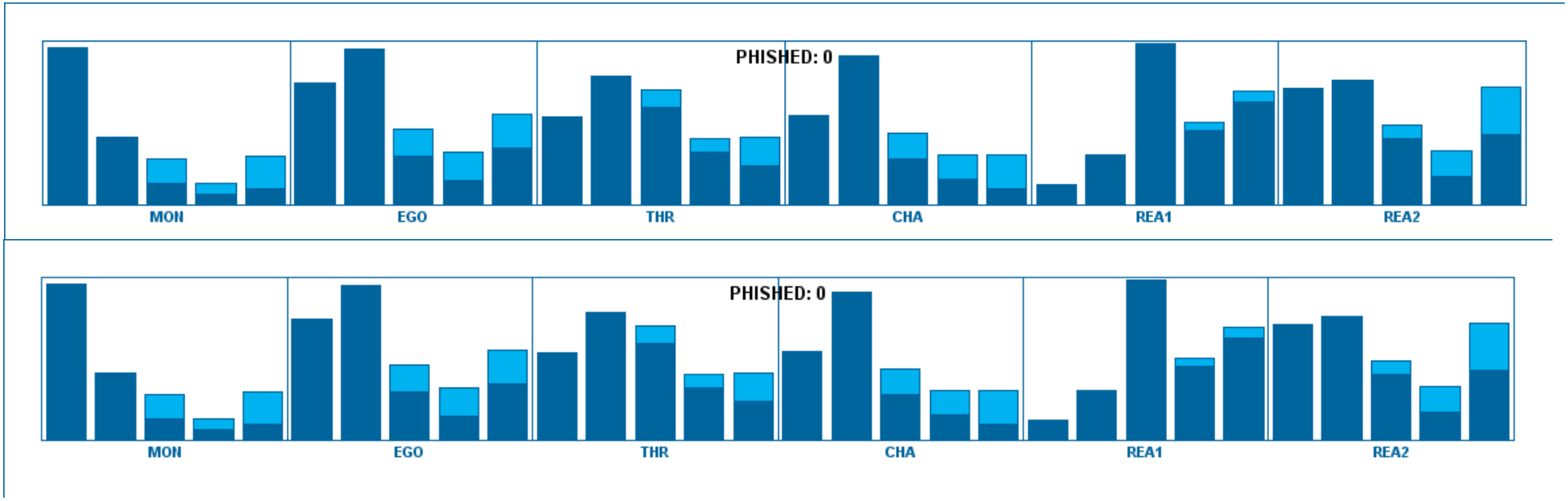
Note. Model summaries among experimental group (PHISHED = 1).

Chart Information

Settings	Value
Subgroups Defined by	PHISHED
Missing Value Treatment	variable by variable
Colour for Entire Sample	light-blue
Colour for Subgroups	dark blue
Pattern for Entire Sample	solid
Pattern for Subgroups	solid

Settings for the charts that follow





Note. For each chart, leftmost bar represents the answer ’Delete the e-mails and block the sender’ and rightmost bar represents the answer ‘Respond to this e-mail’

Appendix 2 – PHISHED Statistics

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
PHISHED	200	0	1	,49	,501
SEX	198	1	2	1,46	,500
AGE	200	1	7	3,95	1,393
INET	200	1	6	4,04	,850
LIV	200	1	8	4,10	2,126
MAR	200	1	6	3,40	,936
EDU	200	1	6	4,03	,891
CORES	200	1	17	15,13	2,884
CORLE	200	1	8	7,46	1,396
OCCUP	200	1	9	5,46	1,604
HEX_HH	200	1,24	4,70	3,2539	,64148
HEX_EM	200	1,40	4,80	3,1741	,62152
HEX_X	200	1,30	5,00	3,0918	,61645
HEX_A	200	1,90	4,60	3,2464	,48075
HEX_C	200	1,60	5,00	3,4005	,70737
HEX_O	200	1,30	4,90	3,3727	,62005
SDT_MACH	200	1,00	4,89	3,4548	,77233
SDT_NAR	200	1,11	4,78	2,9039	,72638
SDT_PSY	200	1,00	4,11	2,5783	,89138
STP2_PRE	200	1,00	7,00	4,0912	1,52526
STP2_CON	200	1,00	7,00	4,8824	1,18404
STP2_SSI	200	1,00	6,83	4,6916	1,24681
STP2_SCN	200	1,00	6,83	4,2136	1,41786
STP2_SI	200	1,00	7,00	4,3489	1,39295
STP2_SIM	200	1,00	7,00	3,9913	1,66489
STP2_RI	200	1,00	6,67	3,4130	1,89236
STP2_ATA	200	1,00	7,00	4,3534	1,44303
STP2_COG	200	1,00	7,00	4,2108	1,45108
STP2_UNI	200	1,00	7,00	4,3972	1,31848
STP2_OVERALL	200	2,10	6,23	4,2593	,92457
Valid N (listwise)	198				

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	15,156	10	,126
	Block	15,156	10	,126
	Model	134,450	28	,000

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	140,016[a]	,493	,657

a. Estimation terminated at iteration number 6 because parameter estimates changed by less than ,001.

Contingency Table for Hosmer and Lemeshow Test

		PHISHED = 0		PHISHED = 1		
		Observed	Expected	Observed	Expected	Total
Step 1	1	20	19,683	0	,317	20
	2	19	19,104	1	,896	20
	3	18	18,009	2	1,991	20
	4	14	15,834	6	4,166	20
	5	15	12,143	5	7,857	20
	6	6	7,570	14	12,430	20
	7	5	4,291	15	15,709	20
	8	3	2,270	17	17,730	20
	9	0	,936	20	19,064	20
	10	0	,161	18	17,839	18

Classification Table[a]

			Predicted		
			PHISHED		
	Observed		0	1	Percentage Correct
Step 1	PHISHED	0	86	14	86,0
		1	14	84	85,7
	Overall Percentage				85,9

a. The cut value is ,500

Hosmer and Lemeshow Test

Step	Chi-square	df	Sig.
1	5,147	8	,742

Variables in the Equation

								95% C.I.for EXP(B)	
		B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
Step 1	SEX	,641	,571	1,260	1	,262	1,899	,620	5,817
	AGE	-,145	,194	,558	1	,455	,865	,592	1,265
	INET	-,339	,302	1,256	1	,262	,713	,394	1,289
	LIV	,215	,124	3,032	1	,082	1,240	,973	1,580
	MAR	,304	,311	,954	1	,329	1,356	,736	2,496
	EDU	-,140	,320	,191	1	,662	,869	,464	1,629
	CORES	-,162	,120	1,840	1	,175	,850	,672	1,075
	CORLE	-,454	,296	2,352	1	,125	,635	,356	1,134
	OCCUP	-,092	,166	,310	1	,577	,912	,659	1,262
	SDT_MACH	-,130	,521	,062	1	,803	,878	,317	2,437
	SDT_NAR	-,161	,652	,061	1	,805	,851	,237	3,058
	SDT_PSY	,338	,547	,382	1	,537	1,402	,480	4,101
	HEX_HH	,478	,553	,747	1	,387	1,613	,545	4,771
	HEX_EM	-,123	,480	,066	1	,798	,884	,345	2,264
	HEX_X	,985	,668	2,178	1	,140	2,678	,724	9,910
	HEX_A	-,377	,587	,413	1	,521	,686	,217	2,168
	HEX_C	-1,438	,603	5,693	1	,017	,237	,073	,774
	HEX_O	-,017	,544	,001	1	,975	,983	,338	2,856
	STP2_PRE	-,044	,378	,014	1	,907	,957	,457	2,005
	STP2_CON	,203	,301	,455	1	,500	1,225	,679	2,212
	STP2_SSI	-,013	,310	,002	1	,967	,987	,537	1,814
	STP2_SCN	,062	,298	,043	1	,835	1,064	,593	1,910
	STP2_SI	,401	,353	1,291	1	,256	1,493	,748	2,981
	STP2_SIM	,647	,314	4,241	1	,039	1,911	1,032	3,539
	STP2_RI	,510	,330	2,387	1	,122	1,665	,872	3,181
	STP2_ATA	,277	,292	,902	1	,342	1,319	,745	2,337
	STP2_COG	,210	,379	,307	1	,580	1,234	,587	2,594
	STP2_UNI	,016	,337	,002	1	,963	1,016	,524	1,968
	Constant	-1,267	6,705	,036	1	,850	,282		

Casewise List[b]

		Observed		Predicted	Temporary Variable		
Case	Selected Status[a]	PHISHED	Predicted	Group	Resid	ZResid	SResid
4	S	0**	,883	1	-,883	-2,746	-2,141
14	S	0**	,913	1	-,913	-3,232	-2,234
49	S	0**	,888	1	-,888	-2,817	-2,196
83	S	0**	,837	1	-,837	-2,269	-2,185
110	S	1**	,165	0	,835	2,249	2,018
124	S	1**	,088	0	,912	3,222	2,442
147	S	1**	,140	0	,860	2,480	2,100
165	S	1**	,221	0	,779	1,876	2,060
168	S	1**	,128	0	,872	2,607	2,165
171	S	1**	,192	0	,808	2,053	2,183
176	S	1**	,199	0	,801	2,007	2,194
198	S	1**	,032	0	,968	5,534	2,689

a. S = Selected, U = Unselected cases, and ** = Misclassified cases.

b. Cases with studentized residuals greater than 2,000 are listed.

Appendix 3 – MON Statistics

Response likelihood for [MON] (5 blocks, enter procedure)

Block #	R^2	R^2 adj	F	p	δR^2	δF	ps
1	10,8%	6,5%	$F_{9,190} = 2,547$	$p < 0,01$	10,8%	$F_{9,190} = 2,547$	$ps < 0,01$
2	29,9%	26,2%	$F_{10,189} = 8,066$	$p < 0,001$	19,1%	$F_{1,189} = 51,629$	$ps < 0,001$
3	40,2%	36,1%	$F_{13,186} = 9,631$	$p < 0,001$	10,3%	$F_{3,186} = 10,707$	$ps < 0,001$
4	42,1%	36,0%	$F_{19,180} = 6,894$	$p < 0,001$	1,9%	$F_{6,180} = 0,978$	n.s.
5[a]	50,3%	41,8%	$F_{29,170} = 5,923$	$p < 0,001$	08,1%	$F_{10,170} = 2,781$	$ps < 0,01$

a. Durbin-Watson d = 1,946

Casewise Diagnostics[a,b]

Case Number	Std. Residual	MON	Predicted Value	Residual
21	2,621	5,000	2,049	2,9511
73	2,007	4,000	1,741	2,2594
102	2,749	5,000	1,905	3,0950
156	-2,223	1,000	3,503	-2,5032

a. Dependent Variable: MON

b. When values are missing, the substituted mean has been used in the statistical computation.

Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	,511	4,807	2,503	1,0460	200
Residual	-2,5032	3,0950	,0000	1,0407	200
Std. Predicted Value	-1,904	2,203	,000	1,000	200
Std. Residual	-2,223	2,749	,000	,924	200

a. Dependent Variable: MON

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95,0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part
5	(Constant)	-,381	1,979		-,192	,848	-4,286	3,525			
	SEX	,165	,199	,056	,831	,407	-,227	,558	,098	,064	,045
	AGE	,111	,069	,105	1,600	,111	-,026	,247	,132	,122	,087
	INET	-,113	,103	-,065	-1,100	,273	-,316	,090	-,052	-,084	-,060
	LIV	-,039	,046	-,056	-,841	,401	-,130	,052	,040	-,064	-,046
	MAR	,050	,104	,032	,478	,633	-,156	,255	,114	,037	,026
	EDU	,134	,105	,081	1,274	,204	-,074	,343	,166	,097	,069
	CORES	,026	,033	,051	,795	,428	-,039	,091	-,105	,061	,043
	CORLE	-,062	,068	-,059	-,911	,364	-,197	,073	-,241	-,070	-,049
	OCCUP	,042	,058	,046	,729	,467	-,072	,157	,138	,056	,039
	PHISHED	,533	,231	,181	2,313	,022	,078	,988	,508	,175	,125
	SDT_MACH	-,226	,190	-,118	-1,193	,235	-,600	,148	,350	-,091	-,065
	SDT_NAR	,185	,215	,091	,859	,391	-,240	,611	,452	,066	,046
	SDT_PSY	,110	,221	,066	,498	,619	-,326	,547	,545	,038	,027
	HEX_HH	,379	,190	,165	1,994	,048	,004	,755	-,299	,151	,108
	HEX_EM	,092	,159	,039	,582	,562	-,221	,405	-,018	,045	,031
	HEX_X	,168	,218	,070	,772	,441	-,262	,599	,188	,059	,042
	HEX_A	-,153	,209	-,050	-,733	,464	-,565	,259	-,088	-,056	-,040
	HEX_C	,025	,201	,012	,125	,901	-,371	,421	-,468	,010	,007
	HEX_O	-,115	,181	-,048	-,636	,525	-,472	,242	-,265	-,049	-,034
	STP2_PRE	,005	,135	,006	,041	,968	-,261	,272	,534	,003	,002
	STP2_CON	-,245	,101	-,197	-2,426	,016	-,445	-,046	,225	-,183	-,131
	STP2_SSI	,241	,105	,203	2,294	,023	,034	,448	,453	,173	,124
	STP2_SCN	-,011	,109	-,011	-,102	,919	-,226	,204	,422	-,008	-,006
	STP2_SI	,208	,116	,196	1,790	,075	-,021	,436	,524	,136	,097
	STP2_SIM	-,200	,094	-,225	-2,126	,035	-,385	-,014	-,532	-,161	-,115
	STP2_RI	,050	,119	,064	,419	,676	-,185	,285	,593	,032	,023
	STP2_COG	,138	,136	,136	1,012	,313	-,131	,407	,526	,077	,055
	STP2_UNI	-,109	,119	-,097	-,911	,363	-,344	,127	,447	-,070	-,049
	STP2_ATA	,026	,096	,025	,269	,788	-,163	,215	,478	,021	,015

a. Dependent Variable: MON

Appendix 4 – EGO Statistics

Response likelihood for [EGO] (5 blocks, enter procedure)

Block #	R^2	R^2 adj	F	p	δR^2	δF	ps
1	2,7%	-1,9%	$F_{9,190} = 0,596$	n.s.	2,7%	$F_{9,190} = 0,596$	n.s.
2	16,9%	12,5%	$F_{10,189} = 3,831$	$p < 0,001$	14,1%	$F_{1,189} = 32,071$	$ps < 0,001$
3	24,6%	19,3%	$F_{13,186} = 4,656$	$p < 0,001$	7,7%	$F_{3,186} = 6,326$	$ps < 0,001$
4	26,9%	19,1%	$F_{19,180} = 3,479$	$p < 0,001$	2,3%	$F_{6,180} = 0,946$	n.s.
5[a]	36,4%	25,6%	$F_{29,170} = 3,356$	$p < 0,001$	9,5%	$F_{10,170} = 2,553$	$ps < 0,01$

a. Durbin-Watson d = 1,824

Casewise Diagnostics[a,b]

Case Number	Std. Residual	EGO	Predicted Value	Residual
27	2,061	5,000	2,461	2,5394
40	2,192	5,000	2,299	2,7010
68	2,190	5,000	2,302	2,6980
115	-2,217	1,000	3,732	-2,7320
160	-2,204	1,000	3,715	-2,7153
193	-2,556	1,000	4,149	-3,1490

a. Dependent Variable: EGO

b. When values are missing, the substituted mean has been used in the statistical computation.

Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	,822	4,592	2,924	,8617	200
Residual	-3,1490	2,7010	,0000	1,1389	200
Std. Predicted Value	-2,439	1,935	,000	1,000	200
Std. Residual	-2,556	2,192	,000	,924	200

a. Dependent Variable: EGO

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95,0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part
5	(Constant)	-,366	2,165		-,169	,866	-4,640	3,909			
	SEX	-,217	,218	-,075	-,996	,321	-,646	,213	,061	-,076	-,061
	AGE	,023	,076	,022	,299	,765	-,127	,172	-,020	,023	,018
	INET	,055	,112	,033	,488	,626	-,167	,277	,036	,037	,030
	LIV	-,033	,050	-,049	-,651	,516	-,132	,067	-,013	-,050	-,040
	MAR	-,056	,114	-,037	-,490	,625	-,281	,169	-,003	-,038	-,030
	EDU	-,044	,115	-,027	-,382	,703	-,272	,184	,037	-,029	-,023
	CORES	,001	,036	,003	,035	,972	-,070	,072	-,082	,003	,002
	CORLE	-,002	,075	-,002	-,027	,979	-,150	,146	-,149	-,002	-,002
	OCCUP	,048	,063	,054	,751	,454	-,078	,173	,051	,058	,046
	PHISHED	,660	,252	,232	2,615	,010	,162	1,158	,396	,197	,160
	SDT_MACH	,060	,207	,032	,287	,775	-,350	,469	,309	,022	,018
	SDT_NAR	,086	,236	,044	,363	,717	-,380	,551	,353	,028	,022
	SDT_PSY	,356	,242	,223	1,473	,143	-,121	,834	,438	,112	,090
	HEX_HH	,448	,208	,201	2,152	,033	,037	,859	-,245	,163	,132
	HEX_EM	-,054	,174	-,023	-,309	,757	-,396	,289	-,063	-,024	-,019
	HEX_X	,240	,239	,104	1,008	,315	-,231	,712	,147	,077	,062
	HEX_A	,156	,228	,052	,682	,496	-,295	,606	-,028	,052	,042
	HEX_C	,041	,219	,021	,189	,850	-,392	,475	-,357	,014	,012
	HEX_O	-,202	,198	-,088	-1,022	,308	-,593	,188	-,182	-,078	-,063
	STP2_PRE	-,015	,148	-,016	-,100	,920	-,306	,277	,397	-,008	-,006
	STP2_CON	-,265	,111	-,220	-2,397	,018	-,484	-,047	,110	-,181	-,147
	STP2_SSI	,315	,115	,275	2,742	,007	,088	,541	,457	,206	,168
	STP2_SCN	,138	,119	,137	1,154	,250	-,098	,373	,395	,088	,071
	STP2_SI	,236	,127	,231	1,863	,064	-,014	,487	,399	,141	,114
	STP2_SIM	-,160	,103	-,187	-1,559	,121	-,363	,043	-,420	-,119	-,095
	STP2_RI	-,149	,130	-,198	-1,147	,253	-,407	,108	,426	-,088	-,070
	STP2_COG	-,069	,149	-,070	-,462	,645	-,363	,225	,355	-,035	-,028
	STP2_UNI	-,016	,130	-,015	-,123	,902	-,273	,241	,356	-,009	-,008
	STP2_ATA	-,086	,105	-,087	-,824	,411	-,294	,121	,334	-,063	-,050

a. Dependent Variable: EGO

Appendix 5 – ROM Statistics

Response likelihood for [ROM] (5 blocks, enter procedure)

Block #	R^2	R^2 adj	F	p	δR^2	δF	ps
1	12,8%	5,6%	$F_{8,96} = 1,768$	n.s.	12,8%	$F_{8,96} = 1,768$	n.s.
2	35,8%	29,7%	$F_{9,95} = 5,876$	$p < 0,001$	22,9%	$F_{1,95} = 33,888$	$ps < 0,001$
3	51,2%	44,8%	$F_{12,92} = 8,028$	$p < 0,001$	15,4%	$F_{3,92} = 9,662$	$ps < 0,001$
4	53,0%	43,1%	$F_{18,86} = 5,384$	$p < 0,001$	1,8%	$F_{6,86} = 0,558$	n.s.
5[a]	59,5%	44,5%	$F_{28,76} = 3,982$	$p < 0,001$	6,5%	$F_{10,76} = 1,216$	n.s.

a. Durbin-Watson d = 2,365

Casewise Diagnostics[a]

Case Number	Std. Residual	ROM	Predicted Value	Residual
21	2,523	5,0	2,405	2,5946
156	-2,443	1,0	3,512	-2,5122

a. Dependent Variable: ROM

Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	-,176	4,644	2,348	1,0725	107
Residual	-2,5122	2,5946	-,0119	,8910	107
Std. Predicted Value	-2,384	2,144	-,013	1,007	107
Std. Residual	-2,443	2,523	-,012	,867	107

a. Dependent Variable: ROM

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95,0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part
5	(Constant)	1,585	2,671		,593	,555	-3,736	6,905			
	AGE	,184	,094	,175	1,946	,055	-,004	,371	,246	,218	,142
	INET	-,089	,134	-,053	-,662	,510	-,355	,178	-,026	-,076	-,048
	LIV	-,020	,066	-,029	-,307	,759	-,153	,112	,043	-,035	-,022
	MAR	,067	,137	,045	,488	,627	-,206	,339	,041	,056	,036
	EDU	-,050	,160	-,030	-,314	,754	-,370	,269	,176	-,036	-,023
	CORES	,028	,061	,041	,461	,646	-,093	,150	-,071	,053	,034
	CORLE	-,011	,123	-,008	-,086	,932	-,255	,234	-,201	-,010	-,006
	OCCUP	-,113	,080	-,126	-1,404	,164	-,273	,047	,062	-,159	-,103
	PHISHED	,717	,281	,259	2,551	,013	,157	1,277	,536	,281	,186
	SDT_MACH	,244	,273	,138	,896	,373	-,299	,788	,501	,102	,065
	SDT_NAR	-,178	,320	-,099	-,555	,581	-,815	,460	,436	-,064	-,041
	SDT_PSY	,508	,290	,338	1,750	,084	-,070	1,086	,617	,197	,128
	HEX_HH	,228	,280	,107	,815	,418	-,330	,786	-,329	,093	,060
	HEX_EM	-,384	,223	-,162	-1,724	,089	-,828	,060	-,165	-,194	-,126
	HEX_X	,018	,330	,008	,054	,957	-,639	,675	,085	,006	,004
	HEX_A	,002	,279	,001	,007	,994	-,553	,557	-,153	,001	,001
	HEX_C	-,134	,280	-,070	-,480	,633	-,692	,423	-,505	-,055	-,035
	HEX_O	-,154	,260	-,072	-,594	,554	-,672	,363	-,426	-,068	-,043
	STP2_PRE	,059	,213	,068	,278	,782	-,365	,484	,586	,032	,020
	STP2_CON	-,204	,138	-,166	-1,479	,143	-,480	,071	,271	-,167	-,108
	STP2_SSI	-,210	,139	-,204	-1,504	,137	-,487	,068	,276	-,170	-,110
	STP2_SCN	,149	,145	,150	1,029	,307	-,139	,437	,487	,117	,075
	STP2_SI	,342	,164	,341	2,081	,041	,015	,669	,568	,232	,152
	STP2_SIM	-,019	,118	-,024	-,163	,871	-,255	,216	-,431	-,019	-,012
	STP2_RI	-,164	,174	-,228	-,938	,351	-,511	,184	,555	-,107	-,069
	STP2_COG	-,110	,202	-,117	-,546	,587	-,511	,291	,576	-,062	-,040
	STP2_UNI	,161	,161	,158	,997	,322	-,161	,483	,442	,114	,073
	STP2_ATA	,071	,149	,074	,476	,635	-,226	,367	,554	,055	,035

a. Dependent Variable: ROM

Appendix 6 – ROF Statistics

Response likelihood for [ROF] (5 blocks, enter procedure)

Block #	R^2	R^2 adj	F	p	δR^2	δF	ps
1	17,5%	9,4%	$F_{8,81} = 1,768$	$p < 0,05$	17,5%	$F_{8,81} = 2,151$	$ps < 0,05$
2	23,6%	15,0%	$F_{9,80} = 5,876$	$p < 0,01$	6,1%	$F_{1,80} = 6,334$	$ps < 0,05$
3	30,9%	20,1%	$F_{12,77} = 8,028$	$p < 0,01$	7,3%	$F_{3,77} = 2,707$	n.s
4	33,8%	17,0%	$F_{18,71} = 5,384$	$p < 0,05$	3,0%	$F_{6,71} = 0,529$	n.s.
5[a]	43,6%	17,7%	$F_{28,61} = 3,982$	$p < 0,05$	9,8%	$F_{10,61} = 1,055$	n.s.

a. Durbin-Watson d = 2,075

Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	,824	5,228	3,011	1,0210	92
Residual	-2,3431	2,5176	-,0330	1,1784	92
Std. Predicted Value	-2,147	2,155	-,011	,998	92
Std. Residual	-1,666	1,790	-,023	,838	92

a. Dependent Variable: ROF

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95,0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part
5	(Constant)	2,987	4,201		,711	,480	-5,414	11,388			
	AGE	-,132	,143	-,122	-,918	,362	-,419	,155	-,104	-,117	-,088
	INET	-,244	,219	-,133	-1,114	,270	-,683	,194	-,055	-,141	-,107
	LIV	,068	,091	,098	,751	,456	-,114	,250	,100	,096	,072
	MAR	,161	,246	,097	,657	,514	-,330	,652	,182	,084	,063
	EDU	-,297	,223	-,176	-1,334	,187	-,743	,148	-,120	-,168	-,128
	CORES	,040	,050	,094	,799	,428	-,060	,141	-,070	,102	,077
	CORLE	-,184	,111	-,202	-1,654	,103	-,407	,038	-,283	-,207	-,159
	OCCUP	,100	,122	,095	,817	,417	-,145	,344	,028	,104	,079
	PHISHED	,060	,518	,019	,116	,908	-,976	1,096	,405	,015	,011
	SDT_MACH	,246	,371	,120	,664	,509	-,495	,988	,259	,085	,064
	SDT_NAR	,221	,403	,097	,548	,586	-,586	1,027	,317	,070	,053
	SDT_PSY	,502	,480	,268	1,046	,300	-,458	1,463	,402	,133	,101
	HEX_HH	,267	,390	,104	,687	,495	-,512	1,046	-,231	,088	,066
	HEX_EM	,081	,419	,031	,194	,847	-,756	,919	,010	,025	,019
	HEX_X	-,374	,434	-,158	-,863	,392	-1,242	,493	,132	-,110	-,083
	HEX_A	,434	,490	,133	,886	,379	-,546	1,414	-,020	,113	,085
	HEX_C	,143	,456	,063	,313	,755	-,770	1,056	-,335	,040	,030
	HEX_O	-,402	,336	-,152	-1,197	,236	-1,075	,270	-,303	-,151	-,115
	STP2_PRE	-,097	,253	-,091	-,385	,702	-,602	,408	,432	-,049	-,037
	STP2_CON	-,222	,220	-,180	-1,011	,316	-,662	,217	,211	-,128	-,097
	STP2_SSI	,206	,229	,149	,900	,372	-,252	,665	,318	,115	,087
	STP2_SCN	-,323	,296	-,295	-1,089	,280	-,915	,270	,255	-,138	-,105
	STP2_SI	,513	,253	,454	2,025	,047	,007	1,020	,470	,251	,195
	STP2_SIM	-,233	,233	-,234	-1,000	,321	-,700	,233	-,447	-,127	-,096
	STP2_RI	-,007	,254	-,008	-,026	,979	-,515	,502	,462	-,003	-,003
	STP2_COG	-,090	,281	-,083	-,319	,751	-,652	,472	,415	-,041	-,031
	STP2_UNI	-,081	,249	-,065	-,327	,745	-,579	,416	,239	-,042	-,031
	STP2_ATA	-,001	,182	-,001	-,007	,995	-,364	,362	,313	-,001	-,001

a. Dependent Variable: ROF

Appendix 7 – THR Statistics

Response likelihood for [THR] (5 blocks, enter procedure)

Block #	R^2	R^2 adj	F	p	δR^2	δF	ps
1	6,2%	1,7%	$F_{9,190} = 2,547$	n.s.	6,2%	$F_{9,190} = 1,388$	n.s.
2	11,8%	7,2%	$F_{10,189} = 8,066$	$p < 0,01$	5,7%	$F_{1,189} = 12,172$	ps = 0,001
3	22,3%	16,8%	$F_{13,186} = 9,631$	$p < 0,001$	10,4%	$F_{3,186} = 8,311$	ps < 0,001
4	24,2%	16,2%	$F_{19,180} = 6,894$	$p < 0,001$	2,0%	$F_{6,180} = 0,775$	n.s.
5[a]	28,4%	16,2%	$F_{29,170} = 5,923$	$p < 0,001$	4,2%	$F_{10,170} = ,988$	n.s.

a. Durbin-Watson d = 2,037

Casewise Diagnostics[a,b]

Case Number	Std. Residual	THR	Predicted Value	Residual
42	2,004	5,000	2,722	2,2779
44	2,589	5,000	2,057	2,9428
73	2,015	5,000	2,710	2,2901
160	-2,162	1,000	3,458	-2,4576

a. Dependent Variable: THR

b. When values are missing, the substituted mean has been used in the statistical computation.

Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1,164	4,339	2,962	,6615	200
Residual	-2,4576	2,9428	,0000	1,0506	200
Std. Predicted Value	-2,718	2,082	,000	1,000	200
Std. Residual	-2,162	2,589	,000	,924	200

a. Dependent Variable: THR

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95,0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part
5	(Constant)	,234	1,998		,117	,907	-3,709	4,178			
	SEX	-,027	,201	-,011	-,136	,892	-,424	,369	-,028	-,010	-,009
	AGE	-,061	,070	-,069	-,875	,383	-,199	,077	,010	-,067	-,057
	INET	-,075	,104	-,051	-,724	,470	-,280	,130	-,050	-,055	-,047
	LIC	,063	,047	,108	1,351	,179	-,029	,155	,138	,103	,088
	MAR	,046	,105	,035	,440	,661	-,161	,254	,121	,034	,029
	EDU	,215	,106	,154	2,018	,045	,005	,425	,160	,153	,131
	CORES	-,028	,033	-,066	-,857	,393	-,094	,037	-,077	-,066	-,056
	CORLE	,069	,069	,077	,992	,323	-,068	,205	-,093	,076	,064
	OCCUP	-,059	,059	-,077	-1,014	,312	-,175	,056	-,011	-,078	-,066
	PHISHED	-,144	,233	-,058	-,620	,536	-,604	,315	,287	-,048	-,040
	SDT_MACH	-,169	,191	-,105	-,882	,379	-,547	,209	,280	-,068	-,057
	SDT_NAR	,019	,218	,011	,089	,929	-,410	,449	,267	,007	,006
	SDT_PSY	,289	,223	,207	1,293	,198	-,152	,729	,410	,099	,084
	HEX_HH	,196	,192	,101	1,022	,308	-,183	,575	-,191	,078	,066
	HEX_EM	,021	,160	,011	,134	,894	-,295	,338	,053	,010	,009
	HEX_X	,197	,220	,098	,895	,372	-,238	,632	,058	,068	,058
	HEX_A	-,159	,211	-,061	-,754	,452	-,574	,257	-,122	-,058	-,049
	HEX_C	,106	,202	,060	,521	,603	-,294	,505	-,338	,040	,034
	HEX_O	-,144	,182	-,072	-,791	,430	-,504	,216	-,255	-,061	-,051
	STP2_PRE	,152	,136	,187	1,119	,265	-,117	,421	,397	,085	,073
	STP2_CON	,016	,102	,015	,153	,879	-,186	,217	,188	,012	,010
	STP2_SSI	,085	,106	,085	,801	,424	-,124	,294	,273	,061	,052
	STP2_SCN	,097	,110	,111	,882	,379	-,120	,314	,345	,067	,057
	STP2_SI	,022	,117	,025	,188	,851	-,209	,253	,331	,014	,012
	STP2_SIM	,024	,095	,032	,250	,803	-,164	,211	-,299	,019	,016
	STP2_RI	,147	,120	,223	1,219	,225	-,091	,384	,422	,093	,079
	STP2_COG	,051	,138	,059	,368	,713	-,221	,322	,394	,028	,024
	STP2_UNI	-,237	,120	-,252	-1,970	,050	-,474	,000	,226	-,149	-,128
	STP2_ATA	,020	,097	,023	,206	,837	-,171	,211	,299	,016	,013

a. Dependent Variable: THR

Appendix 8 – CHA Statistics

Response likelihood for [CHA] (5 blocks, enter procedure)

Block #	R^2	R^2 adj	F	p	δR^2	δF	ps
1	7,6%	3,2%	$F_{9,190} = 1,731$	$p < 0,01$	7,6%	$F_{9,190} = 1,731$	n.s.
2	28,1%	24,3%	$F_{10,189} = 7,393$	$p < 0,001$	20,5%	$F_{1,189} = 54,005$	$ps < 0,001$
3	37,0%	32,6%	$F_{13,186} = 8,391$	$p < 0,001$	8,8%	$F_{3,186} = 8,703$	$ps < 0,001$
4	40,8%	34,5%	$F_{19,180} = 6,520$	$p < 0,001$	3,8%	$F_{6,180} = 1,925$	$ps < 0,001$
5[a]	48,0%	39,2%	$F_{29,170} = 5,417$	$p < 0,001$	7,3%	$F_{10,170} = 2,375$	$ps < 0,001$

a. Durbin-Watson d = 1,941

Casewise Diagnostics[a,b]

Case Number	Std. Residual	CHA	Predicted Value	Residual
21	2,493	5,000	2,496	2,5042
109	2,703	5,000	2,284	2,7156
115	-2,723	1,000	3,736	-2,7360
119	-2,000	2,000	4,009	-2,0093
183	-2,010	1,000	3,019	-2,0189
191	-2,253	1,000	3,263	-2,2630

a. Dependent Variable: CHA

b. When values are missing, the substituted mean has been used in the statistical computation.

Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	,007	4,987	2,827	,8926	200
Residual	-2,7360	2,7156	,0000	,9285	200
Std. Predicted Value	-3,158	2,420	,000	1,000	200
Std. Residual	-2,723	2,703	,000	,924	200

a. Dependent Variable: CHA

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95,0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part
5	(Constant)	,479	1,765		,272	,786	-3,006	3,964			
	SEX	,002	,177	,001	,013	,990	-,348	,352	,016	,001	,001
	AGE	,042	,062	,045	,674	,501	-,080	,163	,047	,052	,037
	INET	-,083	,092	-,055	-,903	,368	-,264	,098	-,061	-,069	-,050
	LIV	-,021	,041	-,035	-,514	,608	-,102	,060	,043	-,039	-,028
	MAR	,026	,093	,019	,280	,780	-,157	,209	,063	,021	,015
	EDU	,111	,094	,077	1,177	,241	-,075	,296	,087	,090	,065
	CORES	,044	,029	,099	1,510	,133	-,014	,102	-,028	,115	,084
	CORLE	-,060	,061	-,065	-,989	,324	-,181	,060	-,226	-,076	-,055
	OCCUP	-,134	,052	-,167	-2,589	,010	-,236	-,032	-,051	-,195	-,143
	PHISHED	,429	,206	,167	2,086	,038	,023	,835	,497	,158	,115
	SDT_MACH	-,224	,169	-,134	-1,325	,187	-,558	,110	,340	-,101	-,073
	SDT_NAR	,155	,192	,087	,805	,422	-,225	,534	,439	,062	,044
	SDT_PSY	,018	,197	,012	,091	,928	-,372	,407	,491	,007	,005
	HEX_HH	-,038	,170	-,019	-,223	,824	-,373	,297	-,334	-,017	-,012
	HEX_EM	,093	,142	,045	,657	,512	-,186	,372	,049	,050	,036
	HEX_X	,004	,195	,002	,018	,985	-,381	,388	,191	,001	,001
	HEX_A	,264	,186	,099	1,420	,157	-,103	,632	,009	,108	,079
	HEX_C	-,067	,179	-,037	-,374	,709	-,420	,286	-,446	-,029	-,021
	HEX_O	-,063	,161	-,030	-,391	,697	-,381	,255	-,249	-,030	-,022
	STP2_PRE	,047	,120	,056	,393	,695	-,190	,285	,564	,030	,022
	STP2_CON	-,097	,090	-,089	-1,079	,282	-,275	,081	,304	-,082	-,060
	STP2_SSI	,105	,094	,102	1,127	,262	-,079	,290	,414	,086	,062
	STP2_SCN	-,076	,097	-,083	-,778	,437	-,268	,116	,419	-,060	-,043
	STP2_SI	,124	,103	,134	1,197	,233	-,080	,328	,552	,091	,066
	STP2_SIM	-,012	,084	-,016	-,146	,884	-,178	,153	-,465	-,011	-,008
	STP2_RI	,010	,106	,015	,093	,926	-,200	,220	,563	,007	,005
	STP2_COG	,219	,122	,247	1,804	,073	-,021	,459	,563	,137	,100
	STP2_UNI	,035	,106	,036	,330	,742	-,175	,245	,458	,025	,018
	STP2_ATA	,126	,086	,141	1,474	,142	-,043	,295	,536	,112	,082

a. Dependent Variable: CHA

Appendix 9 – REA1 Statistics

Response likelihood for [REA1] (5 blocks, enter procedure)

Block #	R^2	R^2 adj	F	p	δR^2	δF	ps
1	4,7%	0,2%	$F_{9,190} = 1,046$	n.s.	4,7%	$F_{9,190} = 1,046$	n.s.
2	4,9%	-0,1%	$F_{10,189} = 0,970$	n.s.	0,2%	$F_{1,189} = 0,320$	n.s.
3	8,5%	2,1%	$F_{13,186} = 1,330$	n.s.	3,6%	$F_{3,186} = 2,454$	n.s.
4	16,1%	7,3%	$F_{19,180} = 1,824$	$p < 0,05$	7,6%	$F_{6,180} = 2,735$	$ps < 0,05$
5[a]	23,7%	10,6%	$F_{29,170} = 1,816$	$p = 0,01$	7,5%	$F_{10,170} = 1,672$	n.s.

a. Durbin-Watson d = 2,246

Casewise Diagnostics[a,b]

Case Number	Std. Residual	REA1	Predicted Value	Residual
43	-2,693	1,000	3,844	-2,8436
121	-2,537	1,000	3,679	-2,6790
129	-2,202	1,000	3,326	-2,3258
183	-2,119	2,000	4,238	-2,2378

a. Dependent Variable: REA1

b. When values are missing, the substituted mean has been used in the statistical computation.

Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	2,176	4,972	3,569	,5433	200
Residual	-2,8436	2,0867	,0000	,9760	200
Std. Predicted Value	-2,563	2,584	,000	1,000	200
Std. Residual	-2,693	1,976	,000	,924	200

a. Dependent Variable: REA1

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95,0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part
5	(Constant)	-2,097	1,856		-1,130	,260	-5,761	1,566			
	SEX	,395	,186	,176	2,119	,036	,027	,763	,146	,160	,142
	AGE	-,040	,065	-,050	-,621	,535	-,168	,088	-,036	-,048	-,042
	INET	,102	,096	,077	1,055	,293	-,089	,292	,092	,081	,071
	LIV	,038	,043	,072	,879	,381	-,047	,123	,034	,067	,059
	MAR	-,015	,098	-,013	-,156	,876	-,208	,177	,031	-,012	-,010
	EDU	,029	,099	,023	,292	,770	-,166	,224	,021	,022	,020
	CORES	,021	,031	,053	,669	,504	-,040	,082	,011	,051	,045
	CORLE	-,072	,064	-,090	-1,118	,265	-,199	,055	-,124	-,085	-,075
	OCCUP	-,035	,054	-,051	-,652	,515	-,143	,072	,006	-,050	-,044
	PHISHED	-,279	,216	-,125	-1,289	,199	-,706	,148	,092	-,098	-,086
	SDT_MACH	,060	,178	,041	,337	,736	-,291	,411	,141	,026	,023
	SDT_NAR	,064	,202	,042	,317	,752	-,335	,463	,204	,024	,021
	SDT_PSY	,503	,207	,401	2,424	,016	,093	,912	,207	,183	,162
	HEX_HH	,372	,178	,214	2,088	,038	,020	,725	-,057	,158	,140
	HEX_EM	-,110	,149	-,061	-,736	,462	-,403	,184	-,140	-,056	-,049
	HEX_X	,309	,205	,171	1,512	,132	-,095	,713	,188	,115	,101
	HEX_A	,240	,196	,103	1,226	,222	-,146	,626	,107	,094	,082
	HEX_C	,207	,188	,131	1,101	,272	-,164	,578	-,086	,084	,074
	HEX_O	-,059	,169	-,033	-,346	,730	-,393	,276	-,100	-,026	-,023
	STP2_PRE	,072	,127	,098	,570	,570	-,178	,322	,193	,044	,038
	STP2_CON	-,037	,095	-,039	-,392	,696	-,224	,150	,117	-,030	-,026
	STP2_SSI	,117	,098	,130	1,186	,237	-,078	,311	,158	,091	,079
	STP2_SCN	-,182	,102	-,231	-1,784	,076	-,384	,019	,035	-,136	-,120
	STP2_SI	,266	,109	,332	2,447	,015	,051	,481	,229	,184	,164
	STP2_SIM	,031	,088	,046	,347	,729	-,143	,205	-,179	,027	,023
	STP2_RI	-,054	,112	-,091	-,480	,632	-,274	,167	,185	-,037	-,032
	STP2_COG	,147	,128	,191	1,149	,252	-,105	,399	,176	,088	,077
	STP2_UNI	-,197	,112	-,233	-1,768	,079	-,418	,023	,097	-,134	-,118
	STP2_ATA	-,084	,090	-,108	-,931	,353	-,261	,094	,167	-,071	-,062

a. Dependent Variable: REA1

Appendix 10 – REA2 Statistics

Response likelihood for [REA2] (5 blocks, enter procedure)

Block #	R^2	R^2 adj	F	p	δR^2	δF	ps
1	8,0%	3,6%	$F_{9,190} = 1,826$	n.s.	8,0%	$F_{9,190} = 1,826$	n.s.
2	20,8%	16,7%	$F_{10,189} = 4,976$	$p < 0,001$	12,9%	$F_{1,189} = 30,750$	$ps < 0,001$
3	28,1%	23,1%	$F_{13,186} = 5,594$	$p < 0,001$	7,3%	$F_{3,186} = 6,269$	$ps < 0,001$
4	31,7%	24,5%	$F_{19,180} = 4,405$	$p < 0,001$	3,6%	$F_{6,180} = 1,596$	n.s.
5[a]	35,8%	24,8%	$F_{29,170} = 3,267$	$p < 0,001$	4,0%	$F_{10,170} = 1,072$	n.s.

a. Durbin-Watson d = 2,006

Casewise Diagnostics[a,b]

Case Number	Std. Residual	REA2	Predicted Value	Residual
58	2,236	5,000	2,175	2,8253
129	-2,368	1,000	3,993	-2,9926
152	-2,465	1,000	4,115	-3,1146

a. Dependent Variable: REA2

b. When values are missing, the substituted mean has been used in the statistical computation.

Residuals Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	,982	4,827	3,149	,8719	200
Residual	-3,1146	2,8253	,0000	1,1678	200
Std. Predicted Value	-2,485	1,924	,000	1,000	200
Std. Residual	-2,465	2,236	,000	,924	200

a. Dependent Variable: REA2

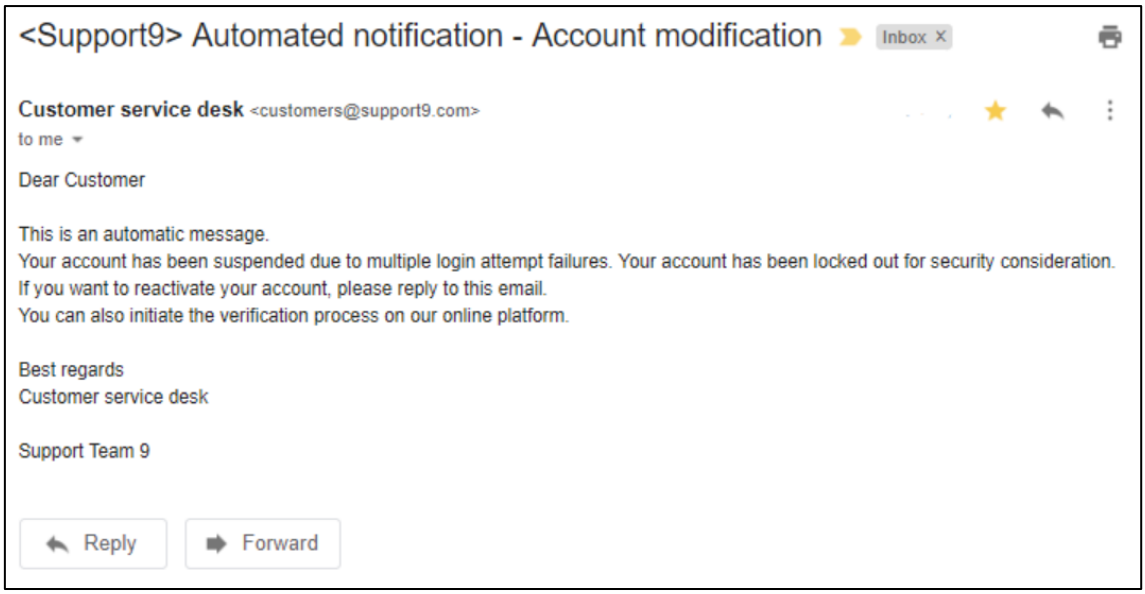
Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95,0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part
5	(Constant)	,209	2,220		,094	,925	-4,174	4,592			
	SEX	,154	,223	,053	,690	,491	-,286	,594	,159	,053	,042
	AGE	-,095	,078	-,091	-1,224	,222	-,248	,058	-,114	-,093	-,075
	INET	-,065	,115	-,038	-,567	,572	-,293	,162	,011	-,043	-,035
	LIV	,020	,052	,029	,389	,698	-,082	,122	-,020	,030	,024
	MAR	-,044	,117	-,028	-,380	,705	-,275	,186	-,036	-,029	-,023
	EDU	,017	,118	,011	,148	,883	-,216	,251	,057	,011	,009
	CORES	,045	,037	,088	1,208	,229	-,028	,117	-,064	,092	,074
	CORLE	-,092	,077	-,088	-1,194	,234	-,243	,060	-,227	-,091	-,073
	OCCUP	-,033	,065	-,036	-,509	,612	-,162	,095	-,045	-,039	-,031
	PHISHED	,883	,259	,303	3,410	,001	,372	1,393	,410	,253	,210
	SDT_MACH	,058	,213	,031	,273	,785	-,362	,478	,355	,021	,017
	SDT_NAR	,502	,242	,250	2,077	,039	,025	,980	,343	,157	,128
	SDT_PSY	,655	,248	,401	2,641	,009	,166	1,145	,443	,199	,162
	HEX_HH	,089	,213	,039	,417	,677	-,332	,510	-,302	,032	,026
	HEX_EM	,084	,178	,036	,474	,636	-,267	,436	-,004	,036	,029
	HEX_X	-,500	,245	-,211	-2,043	,043	-,983	-,017	,001	-,155	-,126
	HEX_A	,223	,234	,073	,951	,343	-,239	,685	-,098	,073	,058
	HEX_C	,334	,225	,162	1,483	,140	-,111	,778	-,264	,113	,091
	HEX_O	-,126	,203	-,053	-,620	,536	-,526	,275	-,198	-,047	-,038
	STP2_PRE	-,089	,151	-,093	-,585	,560	-,388	,210	,359	-,045	-,036
	STP2_CON	-,067	,113	-,054	-,588	,558	-,291	,157	,159	-,045	-,036
	STP2_SSI	,148	,118	,126	1,254	,212	-,085	,380	,362	,096	,077
	STP2_SCN	,019	,122	,018	,155	,877	-,222	,260	,384	,012	,010
	STP2_SI	,252	,130	,241	1,937	,054	-,005	,509	,392	,147	,119
	STP2_SIM	-,097	,105	-,111	-,918	,360	-,305	,111	-,326	-,070	-,056
	STP2_RI	-,268	,134	-,348	-2,006	,046	-,532	-,004	,374	-,152	-,123
	STP2_COG	-,066	,153	-,065	-,429	,669	-,367	,236	,328	-,033	-,026
	STP2_UNI	-,107	,134	-,097	-,799	,425	-,371	,157	,300	-,061	-,049
	STP2_ATA	,042	,108	,041	,386	,700	-,171	,254	,347	,030	,024

a. Dependent Variable: REA2

Appendix 11 – E-mail Images and Headers

Image of [THR]



[THR] Message Source

```
Delivered-To: ivo.malve@gmail.com
Received: by 2002:a25:a81:0:0:0:0:0 with SMTP id 123csp3851893ybk;
        Tue, 1 Oct 2019 06:43:55 -0700 (PDT)
X-Google-Smtp-Source:
APXvYqxfREgwIs2HjOiWeFs3p9LDjGAb4HBlbF+wGXSSrruwxEFP2LPNyrSaok3ddVVVuGBqArNF
X-Received: by 2002:a2e:8941:: with SMTP id b1mr16477895ljk.40.1569937435814;
        Tue, 01 Oct 2019 06:43:55 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1569937435; cv=none;
        d=google.com; s=arc-20160816;
        b=e2Z+gLa5i20OM20emsIWWgXciaFoe+cNctsY0S0n928U5emsA5TDE5A18eArt2oWms
         zglLHRnvh7oY84Hv8o6AOYDPk57cyT6Ui3zqXGk9eAliwpEgkjOHZFqB0okjqZRKY4I5
         CGOvzUgi9Zd8umfVdzL4XIV9Cvn1hDnMsrNRY3Mo4mDun7ElLF3wvBdYqmAfd3Q1/Me+
         EXbvGqtFsF0xmH/ONx8ZX/s3Nh1w8+Mq7V4mr+WbPiqjZuJYyUifnhf///9B2sJcNEZ7
         IVIVp+VKSy9tMCvrdYo9BpFjeXWxRudIMF1nZlkdTySkJeBKWrpjNSUnpIC65+bgb1nw
         ucbQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-
20160816;
        h=message-id:content-transfer-encoding:subject:date:reply-to:to:from
         :mime-version;
        bh=WK+4mHxHaW1LBT/n9QBltj1zZC/Jrt80A541Thokwk8=;
        b=wWK4WPAvR8zJOh/9MXJkIzLDKymp9pi7SyzQ+Xg1yXdL95gk81bAp0UxdPRZpslPUS
         rpwTHPznwDZlfMY5yhcyJpBS0bqwWFTkklYxaUL4JKakOSYNZ4UPOqREqUbTZhQb3m6N
         8CXFp3TEepPz5OggpsKa/QJyZPgx2ZKloSxBEWm5zjX2oUYhsJu5m4W+Lb2dy8ymnDss
         gN38pEve3iphKp+FvEGf4eV8YwkYGwYpptOIiNoPYZFO3nZevaOl/lOJ3UrY2SdAEJit
         0TlorKvYLPpv2d9Vh9Q15fTYkmMVxVWDWgRvAmS1C9m+Emi8Tifj3kkfWvXZEvhij/2a
         RJUw==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=neutral (google.com: 213.184.53.9 is neither permitted nor denied by best
guess record for domain of customers@support9.com) smtp.mailfrom=customers@support9.com
Return-Path: <customers@support9.com>
Received: from mail1.just.ee (mail1.just.ee. [213.184.53.9])
        by mx.google.com with ESMTPS id j14si15163848ljc.19.2019.10.01.06.43.55
        for <ivo.malve@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 01 Oct 2019 06:43:55 -0700 (PDT)
Received-SPF: neutral (google.com: 213.184.53.9 is neither permitted nor denied by best
guess record for domain of customers@support9.com) client-ip=213.184.53.9;
Authentication-Results: mx.google.com;
       spf=neutral (google.com: 213.184.53.9 is neither permitted nor denied by best
guess record for domain of customers@support9.com) smtp.mailfrom=customers@support9.com
X-AuditID: d5b83509-c51ff70000002a42-3b-5d93581acd37
MIME-Version: 1.0
```

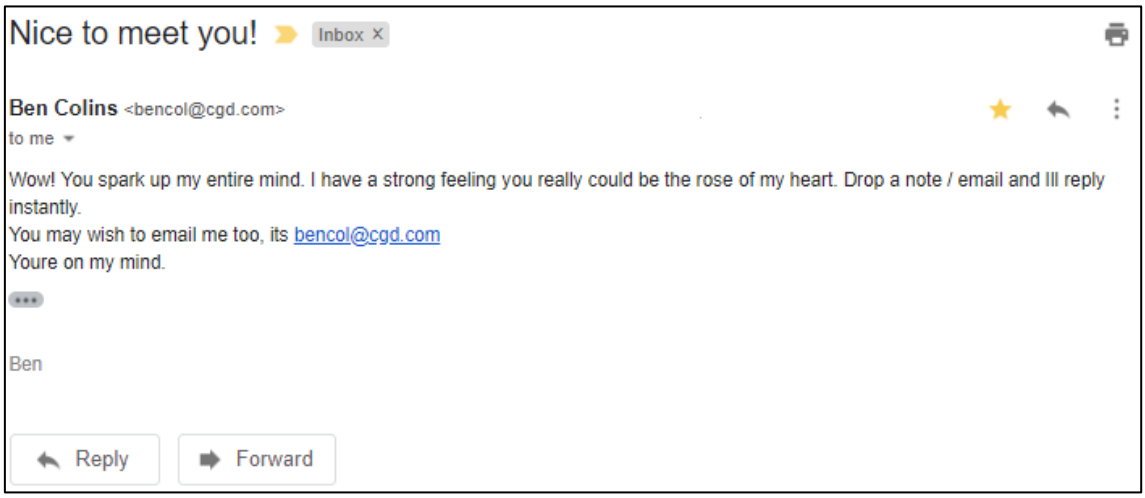
```
From: Customer service desk <customers@support9.com>
To: <ivo.malve@gmail.com>
Reply-To: <customers@support9.com>
Date: Tue, 1 Oct 2019 16:43:02 +0300
Subject: <Support9> Automated notification - Account modification
Content-Type: text/html; charset="us-ascii"
Content-Transfer-Encoding: quoted-printable
Message-ID: <080ac4a4-5c43-4c5e-8706-ac6f17e7284e@exch3.just.sise>
Return-Path: customers@support9.com
X-EXCLAIMER-MD-CONFIG: 0ffde1e1-0574-4cb5-b117-7534ebede067
X-Brightmail-Tracker:
H4sIAAAAAAAAA+NgFvrAJMWRmVeSWpSXmKPExsXCxWh2WFcqYnKswa97Fha33+c4MHrsnHWX
PYAxissmJTUnsyy1SN8ugSvj2LZLzAXvmCsebWtibWBcztzFyMkhIWAi0dx1jwnE5hUQlDg5
8wkLiM0GFJ987jhYjYiApMSuQyfBaoQElCSenz7ECGKzCKhIdOy8C1YvLOAosXL2C7B6ZgFt
iTMHHjPB2MsWvmaGmO8kcXfXCjaIOcoSbVu6GCFusJY4e/4l6wRGnllIzpiFZNQsJKMWMDKv
YuTNTczMMdTLKi0u0UtN3cQIDIerO0w5dzB+/WV4iFGAg1GJh/diyORYIdbEsuLK3EOMEhzM
SiK8Nn8mxQrxpiRWVqUW5ccXleakFh9ilOZgURLnff4JKCWQnliSmp2aWpBaBJNl4uCUamDU
uD1pgpvnTXcPPYMu9SOvV2+Y/+DjtsWxt2QuJwdUZB5JatV+fLEuYb3ZpnN/aoQiRQ4u2WBc
1eJ27tXZlUkXZit1VJtxT39hecvT6Fe2ZtTa6b79ynEPxfr5tkxn/MGxqPx8wDTxiTLSRzfM
uXlR73LuKZHGCKd1nPtcnBm9XEyvLNlsYZ2oxFKckWioxVxUnAgATVm00gMCAAA=



Dear Customer<br><br>

This is an automatic message.<br>
Your account has been suspended due to multiple login attempt failures. You=
r account has been locked out for security consideration. If you want to re=
activate your account, please reply to this email.<br>
You can also initiate the verification process on our online platform.<br>
<br>
Best regards<br>
Customer service desk<br>
<br>
Support Team 9
```

Image of [ROM]



[ROM] Message Source

```
Delivered-To: ivo.malve@gmail.com
Received: by 2002:a25:a81:0:0:0:0:0 with SMTP id 123csp3823746ybk;
        Tue, 1 Oct 2019 06:20:34 -0700 (PDT)
X-Google-Smtp-Source:
APXvYqwWsOK/RnJPViBB/qKYIbWN6c49zZB/EZyytx2kkIjgVRLFCPtUIuvCgrpAy9l4oykp8SkN
X-Received: by 2002:a19:dc10:: with SMTP id t16mr14725690lfg.85.1569936034852;
        Tue, 01 Oct 2019 06:20:34 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1569936034; cv=none;
        d=google.com; s=arc-20160816;
        b=OoVzxar3n5CTETq1wfkf7iWADDMZdyDboMap+scG4IB5ntgJUkOy1HuE2hpNW4P2p6
         LrEgpbXqoOzM9PbPHBQel5yYDPeHtJMgVO4HAYXXT0h1kkLJN9kVfkcYVCAcVAmiLgUz
         2gurh8IqNaUlhzTxJitv4Cn23d+sG6dsFNao3HkB9GnrgFkq41HhFFlajuPD6NBqBHO1
         OZsJyaciQQpTUwywiDQ6QXdKE6M7FJOMel79y7IYSQDVGHngVPlrxKdYoIRMmOTWxc2y
         GFNBtSYQ8ZPHRpuvnx491sicTJv5r/jTc2mmhQ5MbB2rXyzhiqd5YtjxErCxaWibYpQr
         KNOQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-
20160816;
        h=message-id:content-transfer-encoding:subject:date:reply-to:to:from
         :mime-version;
        bh=9aLdenVgv1toJgXG16sRp8dM5NW7FyN0zz/KWAwHw5s=;
        b=qmPQA1CVVqeF3pKoIwl7CURsMepUgJBpHHVxgzOqn0s5vif/4lw1myBpmixK/9i99R
         pnZKeF1M4oUh6Nc4rQEwyTbJjO3MtZN2doa+tpbLqpRTqekKR4819YQ/4G8RM2ClEKfk
         VIs85h+xfWtO8nxc1juqN2uoUZbBFpI8HPRDUmLrXqdyXKfYVjcdzsCtl5BbgHac/YQ6
         akSFgj5LLS430CnN8FVV+Dg/P0N3oHwp3BuFmmjdoxWcwhdfcFNAkFwAxEHIc4MOyHLw
         MJiV2fcM5OgPAJ1rOiz2tm0KK4gmtdJMN7vPDWWc91EgNw0ScVNBFj3kAcAVtAKZ8Thr
         3Y4g==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=neutral (google.com: 213.184.53.9 is neither permitted nor denied by best
guess record for domain of bencol@cgd.com) smtp.mailfrom=bencol@cgd.com
Return-Path: <bencol@cgd.com>
Received: from mail1.just.ee (mail1.just.ee. [213.184.53.9])
        by mx.google.com with ESMTPS id v72si14671162lje.221.2019.10.01.06.20.34
        for <ivo.malve@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 01 Oct 2019 06:20:34 -0700 (PDT)
Received-SPF: neutral (google.com: 213.184.53.9 is neither permitted nor denied by best
guess record for domain of bencol@cgd.com) client-ip=213.184.53.9;
Authentication-Results: mx.google.com;
       spf=neutral (google.com: 213.184.53.9 is neither permitted nor denied by best
guess record for domain of bencol@cgd.com) smtp.mailfrom=bencol@cgd.com
X-AuditID: d5b83509-c51ff70000002a42-b3-5d9352a2648a
MIME-Version: 1.0
From: Ben Colins <bencol@cgd.com>
To: <ivo.malve@gmail.com>
Reply-To: <bencol@cgd.com>
Date: Tue, 1 Oct 2019 16:19:20 +0300
Subject: Nice to meet you!
Content-Type: text/html; charset="us-ascii"
Content-Transfer-Encoding: quoted-printable
Message-ID: <08094077-9877-4aec-ba94-4437433983ec@exch3.just.sise>
Return-Path: bencol@cgd.com
```

X-EXCLAIMER-MD-CONFIG: 0ffde1e1-0574-4cb5-b117-7534ebede067
X-Brightmail-Tracker:
H4sIAAAAAAAAA+NgFnrHJMWRmVeSWpSXmKPExsXCxWh2SHdR0ORYg42rRSxuv89xYPTYOesu
ewBjFJdNSmpOZllqkb5dAlfGyjWt7AXrmComnjnE2MD4g7GLkYNDQsBEYvOhhC5GTg5eAUGJ
kzOfsIDYbAKKEv82b2UHsUUEJCV2HTrJBGILCUhJTF93lA3EZhFQkTi+biZYXBgofrNxPSuI
zSygLXHmwGMmGHvZwtfMEPOdJFqf9rGArBUSkJZYuUYDJCwhYC1x9vxL1gmMPLOQXDELyaRZ
SCYtYGRexcibm5iZY6iXVVpcopeauokRGApXd5hy7mD8+svwEKMAB6MSD6+FxuRYIdbEsuLK
3EOMEhzMSiK8Nn8mxQrxpiRWVqUW5ccXleakFh9ilOZgURLnff4JKCWQnliSmp2aWpBaBJNl
4uCUamCcW36n40Kn+k6XzN8ykcftjC63+IRN+dF7Irs0KGfzyWexRsYijboCaw3L3Nma3A4o
zFT4yHKkXsrqhe7j1sciG7Xj7P2jT+1btExo9tXExrx+nrJsaa6uy5OmxObdeGPUuyD3SimP
ZYLhlHnpBwVDmYPDlpWGLGmw82D/2BGn0t0i/NfATImlOCPRUIu5qDgRANa+xL4BAgAA

Wow! You spark up my entire mind. I have a strong feeling you really could =
be the rose of my heart. Drop a note / email and Ill reply instantly.

You may wish to email me too, its bencol@cgd.com
Youre on my mind.
Ben

Image of [ROF]

[ROF] Message Source

```
Delivered-To: ivo.malve@gmail.com
Received: by 2002:a25:c1c1:0:0:0:0:0 with SMTP id r184csp3412011ybf;
        Fri, 27 Sep 2019 05:45:53 -0700 (PDT)
X-Google-Smtp-Source:
APXvYqxPNftLDqpWMGaotkjK7qQMVvA+/1jzg0y2AS97Bbevnbe+ZjHQkKS/S7UjAi4wmI/DmP5Y
X-Received: by 2002:ac2:5dd0:: with SMTP id x16mr27587531fq.38.1569588353588;
        Fri, 27 Sep 2019 05:45:53 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1569588353; cv=none;
        d=google.com; s=arc-20160816;
        b=iCICALWUYzFup3BTLK3AVynQhJErJt5oK+orE+siGcq640e1W1anD0OkUpP2ptdO3J
         qk53dSqa6HR4t7BloHizMThALSP/m0nPadMgqlh5CJ3GTMKpYvAF9Um6w8PvNA44tOuy
         4d8lE1CYEBQbvT5LWscA+vQZ4l3ElDE8s+lNtUSjEpYrosHemhnd8v1EEByPqkN0M4P0
         1dMxvgDgN9DKID2lAW1n7BDsnj4PnBSFPnZeYuOFSHknCGoXvPyHx8tOlXNT4mzSBekU
         E+G5PzUC5+jb8G+bSBnwO98BzW66reO3F2dZKIDSrpsdBzvVK6BuaGw4v6MK5GZm/eAM
         4emw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-
20160816;
        h=message-id:content-transfer-encoding:subject:date:reply-to:to:from
         :mime-version;
        bh=esH0x0ondSTRsAZXInJea/zHn8KkcsoV4l7hiWVlHmM=;
        b=ghMBrDFlrsaAs/yRjKLb/r1DDKasofFo3mjifOfSl4vsEKKScWia1otHFpjAc4Ylcn
         lAfdcgwk/jd4koHhRWSVhjEqvgOwnsHquwoJXSAaAEPtNpGlQAQpfgjpHFafXo/DC5Ex
         wcaCWmM/X4Vb+dEYkBDbdR7q8gqAE+IVNY+3UxuP1MFGZ6kBfGNR9PvM2ZKXQsmJMQ+I
         M8geuYbO6GjFs4hDLEgzsZTGjaYEiDUGHfAUkyWYHUBiGVkCcqLewAT+BQqfPCJSs8bl
         /TmhXJF2FYUJXBLH31/W3su/dEeBnGaCdQ1GzslbNhJ7g0YWxXSg28nSm9ayaopY+lMg
         LgKg==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=neutral (google.com: 213.184.53.9 is neither permitted nor denied by domain
of upmailer338@webmails.com) smtp.mailfrom=upmailer338@webmails.com
Return-Path: <upmailer338@webmails.com>
Received: from mail1.just.ee (mail1.just.ee. [213.184.53.9])
        by mx.google.com with ESMTPS id v15si2660568ljg.16.2019.09.27.05.45.52
        for <ivo.malve@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Fri, 27 Sep 2019 05:45:53 -0700 (PDT)
Received-SPF: neutral (google.com: 213.184.53.9 is neither permitted nor denied by
domain of upmailer338@webmails.com) client-ip=213.184.53.9;
Authentication-Results: mx.google.com;
       spf=neutral (google.com: 213.184.53.9 is neither permitted nor denied by domain
of upmailer338@webmails.com) smtp.mailfrom=upmailer338@webmails.com
X-AuditID: d5b83509-c51ff70000002a42-8f-5d8e0480aeb0
MIME-Version: 1.0
From: Julia Bronn <upmailer338@webmails.com>
To: <ivo.malve@gmail.com>
Reply-To: <ivo.malve@gmail.com>
Date: Fri, 27 Sep 2019 15:44:22 +0300
Subject: Hi! This is Julia
Content-Type: text/html; charset="us-ascii"
Content-Transfer-Encoding: quoted-printable
```

```
Message-ID: <3e81ff28-4102-421d-b0cc-777e187e22a3@exch3.just.sise>
Return-Path: upmailer338@webmails.com
X-EXCLAIMER-MD-CONFIG: 0ffde1e1-0574-4cb5-b117-7534ebede067
X-Brightmail-Tracker:
H4sIAAAAAAAAA+NgFnrPJMWRmVeSWpSXmKPExsXCxWh2SLeBpS/WYPt5HYvb73McGD12zrrL
HsAYxWWTkpqTWZZapG+XwJUx8e5r5oKpzBU7Vl5lamA8y9TFyMEhIWAiMfuXQRcjJwevgKDE
yZlPWEBsNgEdie3XVrKC2CICkhK7Dp1kArGFBOQlnvfMYwSxWQRUJZoXz2ADsYUFpCReTXwK
ZjMLaEucOfCYCcZetvA1M8R8J4n2byfZIeaoSmxcMgUsLiFgLXH2/EvWCYw8s5CcMQvJqFlI
Ri1gZF7FyJubmJljqJdVWlyil5q6iREYDFd3mHLuYPz6y/AQowAHoxIPb9eb3lgh1sSy4src
Q4wSHMxKIry+kT2xQrwpiZVVqUX58UWlOanFhxilOViUxHk11wClBNITS1KzU1MLUotgskwc
nFINjP7X5+03s2/fyRymx7JT7dESh5JzJZLpihohbmJ1k3jvFjjtf2XSk9LdI/PTbftldWv9
98daOUSP+e76c/WdyvY1jRULLascRJcbXbsa7CU0+5XPbMOGR9I7/s2IXCn8+3Jb9v7NzAx7
GRZfP9Ai7RLdz7L5schy8RaJ3B1L1R+5sm/If/DYVomlOCPRUIu5qDgRAOAjM3gCAgAA
```

```
 Hi there!
 <br>
<br>
First of all, I would like to introduce myself.
My name is Julia and Im 24 years old. We dont know each other yet, but Im a=
 kind-hearted, truthful and joyful girl.
I saw your profile on social media and I thought it would be nice to talk t=
o you.

<br>
<br>
 Cheers, Julia <br>
  <br>
 <br>
```

Image of [EGO]

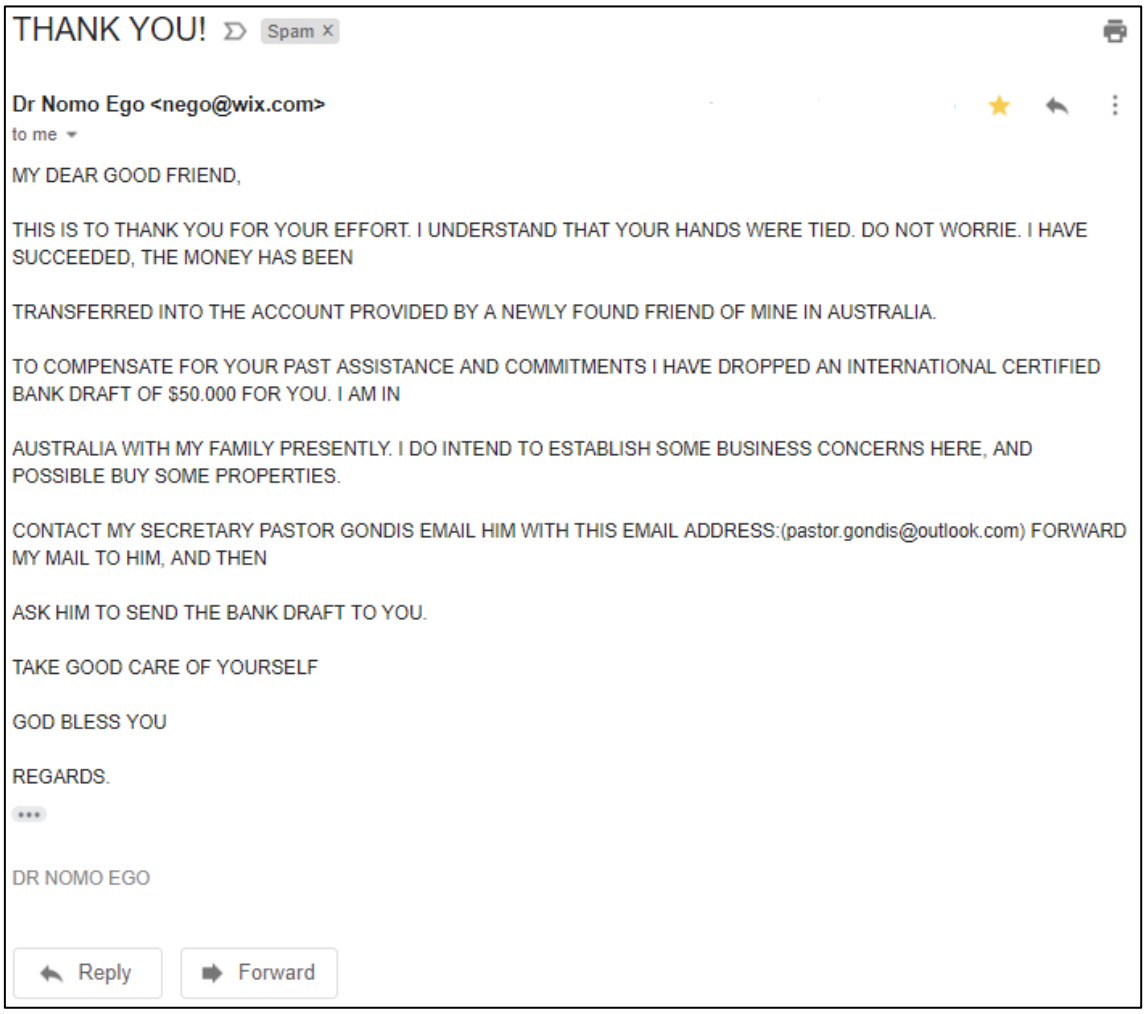
[EGO] Message Source

```
Delivered-To: ivo.malve@gmail.com
Received: by 2002:a25:a81:0:0:0:0:0 with SMTP id 123csp3886912ybk;
        Tue, 1 Oct 2019 07:13:05 -0700 (PDT)
X-Google-Smtp-Source:
APXvYqyFwd3s/aRRDiG2yEb5ZXAjHSakA64iORBsBq6vcgT25xcGWr38aoaqIu1YXVhjYRTEdKDr
X-Received: by 2002:a2e:814a:: with SMTP id t10mr2037041ljg.212.1569939185738;
        Tue, 01 Oct 2019 07:13:05 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1569939185; cv=none;
        d=google.com; s=arc-20160816;
        b=m3u05xXJb5gSy8hn/AYGmsPLdnKz4G7BM3ARXnHH0V1tFitVaPhXBTiEMrSUzviPpz
         ffh/2/ZtKVDIr6JA8L1muyzhXdZNeP/3WjarTNiMpluLwDMFK8AN1KGt18YI1jXcMCE6
         6ETADhx4enn4L13cyfcJZPzpXLZlrmkL7IrJOHdUg2xTNbBJmXRF4eDLvaq+e1Lkcg9z
         YcWr1xwtZN98lMZUmbuNE875V/tz1AJ/FQs+ikwKSIEUHQTph9JDIbZ6mc6zrb3f+nI4
         rzc+AvFcK0+nsPLWKzMC4o9EgOJsnrgDnroL0ZjdH/cA0HpT3vagFltmQkI4s88mvpQo
         vx4g==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-
20160816;
        h=message-id:content-transfer-encoding:subject:date:reply-to:to:from
         :mime-version;
        bh=kUXG0vbCEjn6fffikHp3AO0gDGDlJNNu34RhcWpndS0=;
        b=Zgk0kufftpnYkA5jcV6tlEvEoQM4f5l8lHxJGXnQ4pPn47RHW1KxKlQtr9GsEF0AYf
         D97shgAn79wGxJglIvsrB53Q8SKnraxXSjjgnwPhGwFPan4lC0A4XSZwFlKoXXXkYNMK
         FQdXZnzdWXyykF4atQVo+Z6qd7KkpJ5k4RXD09QbEyqW6eldn8L+CCWvBGvwnSCoesSV
         U70tnuBhtawyNd2gIAhc1Zy7cLtLoCrVCTfdaWuTyBvQ4V9kZkXxfdzANA4mwxZJld7c
         AE5iuEE7u7wlpv8YkZfbQe92K0fv5DZpChIJ7U2ZNKMu9p3roy1Bit4EMwhZOFSQTI9l
         EOzQ==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=fail (google.com: domain of csf@wikia.com does not designate 213.184.53.9 as
permitted sender) smtp.mailfrom=csf@wikia.com
Return-Path: <csf@wikia.com>
Received: from mail1.just.ee (mail1.just.ee. [213.184.53.9])
        by mx.google.com with ESMTPS id u127si14778767lja.176.2019.10.01.07.13.05
        for <ivo.malve@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 01 Oct 2019 07:13:05 -0700 (PDT)
Received-SPF: fail (google.com: domain of csf@wikia.com does not designate 213.184.53.9
as permitted sender) client-ip=213.184.53.9;
Authentication-Results: mx.google.com;
       spf=fail (google.com: domain of csf@wikia.com does not designate 213.184.53.9 as
permitted sender) smtp.mailfrom=csf@wikia.com
X-AuditID: d5b83509-c69ff70000002a42-29-5d935ef19c75
MIME-Version: 1.0
From: Collin F <csf@wikia.com>
To: <ivo.malve@gmail.com>
Reply-To: <csFf@wikia.com>
Date: Tue, 1 Oct 2019 17:12:00 +0300
Subject: Here's what I think of your post
```

```
Content-Type: text/html; charset="utf-8"
Content-Transfer-Encoding: base64
Message-ID: <6de451a9-bcd4-4967-b5b9-2e766345f847@exch4.just.sise>
Return-Path: csf@wikia.com
X-EXCLAIMER-MD-CONFIG: 0ffde1e1-0574-4cb5-b117-7534ebede067
X-Brightmail-Tracker:
H4sIAAAAAAAAA+NgFnrPJMWRmVeSWpSXmKPExsXCxWh2SPdj3ORYg3kHhC1uv89xYPTYOesu
ewBjFJdNSmpOZllqkb5dAlfG7bXtTAUdLBX7+4MaGL8wdzFyckgImEhsOjiRCcTmFRCUODnz
CQuIzSYgJ9G3+RcjiC0iICmx69BJsBohASmJjknP2UBsFgEViX2tu8FqhAU0JXbcmM4OYjML
aEi0zpkLZStKTOl+yA4x30ni54MuuDknZq5hgrjBWuLs+ZesExh5ZiE5YxaSUbOQjFrAyLyK
kTc3MTPHUC+rtLhELzV1EyMwGK7uMOXcwfj1l+EhRgEORiUe3oshk2OFWBPLiitzDzFKcDAr
ifDa/JkUK8SbklhZlVqUH19UmpNafIhRmoNFSZz3+SeglEB6YklqdmpqQWoRTJaJg1OqgdFg
Qe01j+ROE7kJ6ftv8F759qqX9bF0LMfdJLZZunK+RnuK7jhz7prFxZZvnR3zjoXxtkO058RX
FxRyg/c8Dcnh3fqpqthLa9XkGXuulq/UK5vqZbzfvnHxjjl1GX9euip0H/ioeCbGxaB/0xuZ
hWuOx6SGGyR2MH90Xu66sdNv6WFTv6IXB5VYijMSDbWYi4oTAd4ODCsCAgAA

DQoNCkhpPGJyPg0KSSByZWFkIHlvdXIgcG9zdCB5b3UgcG9zdGVkIG9uIHNvY2lhbCBtZWRpYSBy
ZWNlbnRseeKApiBhbmQgSSBkaXNhZ3JlZSB3aXRoIGV2ZXJ5IG9uZSBvZiB5b3VyIGlkZWFzLiBG
cmFua2x5LCBJdCBjb3VsZCBiZSB5b3UgYXJlIGp1c3QgYmFkIGF0IHdyaXRpbmcgYW5kIGV4cHJl
c3NpbmcgdGhlbSwgYnV0IHRoZXkgc2VlbWVkIHBsYWluIGlkaW90aWMuIEFueXdheXMsIEl2ZSB3
cml0dGVuIEgcmV2aWV3IG9uIHlvdXIgcG9zdCwgdGhhdCBJIHBsYW4gdG8gcHVibGlzaCBvbiBt
eSBibG9nLiBJZiB5b3VyZSBpbnRlcmVzdGVkIGluIHJlYWRpbmcgaXQsIGxldCBtZSBrbm93Lg0K
PGJyPjxicj4NCkJSPGJyPg0KQ29sbGluPGJyPg0KDQo=
```

Image of [MON]



[MON] Message Source

```
Delivered-To: ivo.malve@gmail.com
Received: by 2002:aed:2c24:0:0:0:0:0 with SMTP id f33csp705776qtd;
        Wed, 11 Nov 2020 09:55:51 -0800 (PST)
X-Google-Smtp-Source:
ABdhPJwu4j5nrpwDluECBwcd9FcRNIy9T1vCzxozGOG8JL5zVeVPm8GcAoR/ROF6sQIXkwfByD4t
X-Received: by 2002:a19:434a:: with SMTP id m10mr7425881lfj.153.1605117350934;
        Wed, 11 Nov 2020 09:55:50 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1605117350; cv=none;
        d=google.com; s=arc-20160816;
        b=jpJ77bnCUL/g4yJFDaZTkgLin5trHIoeUktv85e2WoAZ1mtWquV/j0YyZ2cznxRo+q
         dTA+YhUwBpvJ1RzjjekQ23eFqmSuuIgJ4vJowjn0FFXhjTlK10uOFdS5KU0vN14vyUgt
         ydF8RCnGcJn6z8LBM/kWoYgRNj2v+moBVyLaUwlPdDZ13YpRWQUv2NCsS/TOAhv6I18v
         d/3m5uQNlB4IbRUQeNJ+E/QzIBRbeiMxSM/+9DGDL7d6bR7LmoYcjW4SkTt0P1KAJnvE
         t4sBlNuPESk/6vF2H5wZLWo7AkOZfIUo74Wd++M5z6A8ISpJACxBiGKd61zgBXm/qTrC
         ce4Q==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-
20160816;
        h=message-id:content-transfer-encoding:subject:date:reply-to:to:from
         :mime-version;
        bh=PZxC5L6KvzVSoZUnCfS40PmN4n7uzd5omGfYJ0Pw6dg=;
        b=WGxhMrUSx1EzBr+SEw/4vu6Ym9f0uJQv5KvGyNqtLXYviqbNBs764WO+fv/yigC7p5
         /H4GOVU6oai0p58ikcC++EUmAGZMLUSC3lDlWf1Hm7ZnMOZn/ncrhHAOHBCXnt2GfjPY
         QqBh5e+8ndDyUImpPG/cKH7cvehVLe2fT90pK+NfE8hlFHQfQWkfm6dwkpjDDGZgPTt+
         pnI4ihbpZb6JzwsVgAI1bnn4HhLhVtbLXhk/XJrmxR9Wt4fj9LAKAiuI08+WHuE8spKe
         ON51rmx7MCVVAJZTDNVSDhoh8VSXX5BZ5LMLnfgHHmSo4kDOi+1RcdS/peJcwt/AcGjZ
         aerw==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=softfail (google.com: domain of transitioning nego@wix.com does not designate
213.184.59.131 as permitted sender) smtp.mailfrom=nego@wix.com;
```

```
       dmarc=fail (p=QUARANTINE sp=QUARANTINE dis=QUARANTINE) header.from=wix.com
Return-Path: <nego@wix.com>
Received: from mail2.rik.ee (mail2.rik.ee. [213.184.59.131])
        by mx.google.com with ESMTPS id t27si1192366ljo.331.2020.11.11.09.55.50
        for <ivo.malve@gmail.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
        Wed, 11 Nov 2020 09:55:50 -0800 (PST)
Received-SPF: softfail (google.com: domain of transitioning nego@wix.com does not
designate 213.184.59.131 as permitted sender) client-ip=213.184.59.131;
Authentication-Results: mx.google.com;
       spf=softfail (google.com: domain of transitioning nego@wix.com does not designate
213.184.59.131 as permitted sender) smtp.mailfrom=nego@wix.com;
       dmarc=fail (p=QUARANTINE sp=QUARANTINE dis=QUARANTINE) header.from=wix.com
X-AuditID: d5b83b83-05bff70000002338-38-5fac25a5193a
MIME-Version: 1.0
From: Dr Nomo Ego <nego@wix.com>
To: <ivo.malve@gmail.com>
Reply-To: <nego@wix.com>
Date: Wed, 11 Nov 2020 19:55:49 +0200
Subject: THANK YOU!
Content-Type: text/html; charset="us-ascii"
Content-Transfer-Encoding: quoted-printable
Message-ID: <5edc0d22-0f5b-44cb-bacf-79a049212830@exch2.just.sise>
Return-Path: nego@wix.com
X-EXCLAIMER-MD-CONFIG: 0ffde1e1-0574-4cb5-b117-7534ebede067
X-Brightmail-Tracker:
H4sIAAAAAAAAA+NgFvrOJMWRmVeSWpSXmKPExsVyOKCgX3ep6pp4g8n/jC1uv89xYPTYOesu
ewBjFJdNSmpOZllqkb5dAlfG+WViBcvYK1ZPesnUwDidrYuRk0NCwETizeZGdhj78LSFjCA2
r4CgxMmZT1i6GDk42AQUJNZ0M4GERQQkJXYdOglmCwlISKz+fhKsnEVAVeL16o1gY4QFhCVa
eiczg9jMAtoSZw48ZoKxly18zQwx3kni1OYXTCDjhYBmPrphDXGBtcTZ8y9Zuxi5gOz7bBKf
p95mm8DINwvJRbOQjJ2FZOwCRuZVjDy5iZk5RnpFmdl6qambGIGBc3WHdfMOxiUfUw4xMnEw
HmKU4GBWEuH9xLImXog3JbGyKrUoP76oNCe1+BCjNAeLkjivwsxV8UIC6YklqdmpqQWpRTBZ
Jg5OqQbGyfv82qJnbwoWfVblsd6uLuOhTFuz9OG70ZtXnREM/6XCO71M4+bhfUc0Vrbc2Zdk
c3b52y6VeVZKuyRnc8wUCfpz5X6nOMtHmSsu1p03//95LBVylvN2Yrndjcda+6Yp8asnT/EP
U7xgaFphc29f/ck/U/w+bJsdvuaEkLzBiQsdsp3VPvzeSizFGYmGWsxFxYkAZS4ZHAoCAAA=
X-Brightmail-Tracker:
H4sIAAAAAAAAA+NgFnrAJMWRmVeSWpSXmKPExsXCZcTJq7tUdU28wf0HOha33+c4MHrsnHWX
PYAxissmJTUnsyy1SN8ugSvj/DKxgmXsFasnvWRqYJzO1sXIySEhYCJxeNpCRhCbV0BQ4uTM
JyxdjBwcbAIKEmu6mUDCIgKSErsOnQSzhQQkJFZ/PwlWziKgKvF69UZ2EFtYQFiipXcyM4jN
LKAtcebAYyYYe9nC18wQ450kTm1+wQQyXgho5qMb1hAXWEucPf+SdQIjzywkR8xCMmkWkkkL
GJlXMfLmJmbmGOlllRaX6KWmbmIEBsLhgIL+HYytE9/qHWJk4mA8xCjBwawkwvuJZU28EG9K
YmVValF+fFFpTmrxIUZpDhYlcV6FmavihQTSE0tSs1NTC1KLYLJMHJxSDUwBTheNLnu/eKm0
Zr+3ntusK0oH5We71GoapDxrynVeH/YkOCJRbNrPRLtrFsInlH+1LF1dauhwfmPl9pvLNG9u
eLU1uqSwKISf4ePuSWbXLtrNmX7z8Mdtv26fnBG95ohNMmfzlbVN/zer7X7cfci8Z3Wb0OHl
jAV+t2rN3hy23hKdYyTf+0xLwf/nAQHTY2qbnJYJRz/Xq+RV5Jn67Vp4cYDjDrmf28Uj7DYv
WR2mq3jlSP7JhRJF3nw/9lwrtrCedOXy8yLhGM6v3D2cnjOUMlrFZHJbtoqrWsr9+bxz5qmG
4qsVgsodJ2bfcTgU8WS9p9PijyfTIwSy61f5Rzs9mVP0TFF/3ln7aXutRS2VWIozEg21mIuK
EwHbW43TcwIAAA==
```


MY DEAR GOOD FRIEND,

THIS IS TO THANK YOUR FOR YOUR EFFORT. I UNDERSTAND THAT YOUR HANDS WERE TI=
ED. DO NOT WORRIE. I HAVE SUCCEEDED, THE MONEY HAS BEEN

TRANSFERRED INTO THE ACCOUNT PROVIDED BY A NEWLY FOUND FRIEND OF MINE IN AU=
STRALIA.

TO COMPENSATE FOR YOUR PAST ASSISTANCE AND COMMITMENTS I HAVE DROPPED AN IN=
TERNATIONAL CERTIFIED BANK DRAFT OF $50.000 FOR YOU. I AM IN

AUSTRALIA WITH MY FAMILY PRESENTLY. I DO INTEND TO ESTABLISH SOME BUSINESS =
CONCERNS HERE, AND POSSIBLE BUY SOME PROPERTIES.

CONTACT MY SECRETARY PARTOR GONDIS EMAIL HIM WITH THIS EMAIL ADDRESS:(pasto=
r.gondis@outlook.com) FORWARD MY MAIL TO HIM, AND THEN

ASK HIM TO SEND THE BANK DRAFT TO YOU.

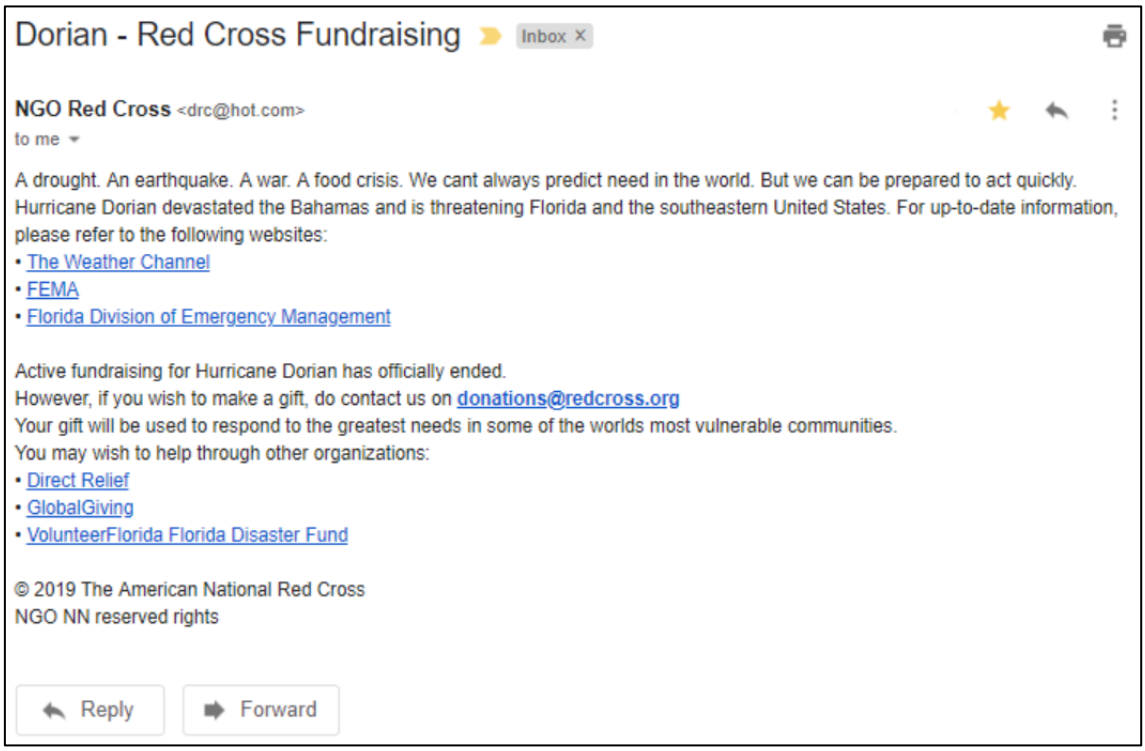
TAKE GOOD CARE OF YOUSELF

GOD BLESS YOU

REGARDS.

DR NOMO EGO

Image of [CHA]



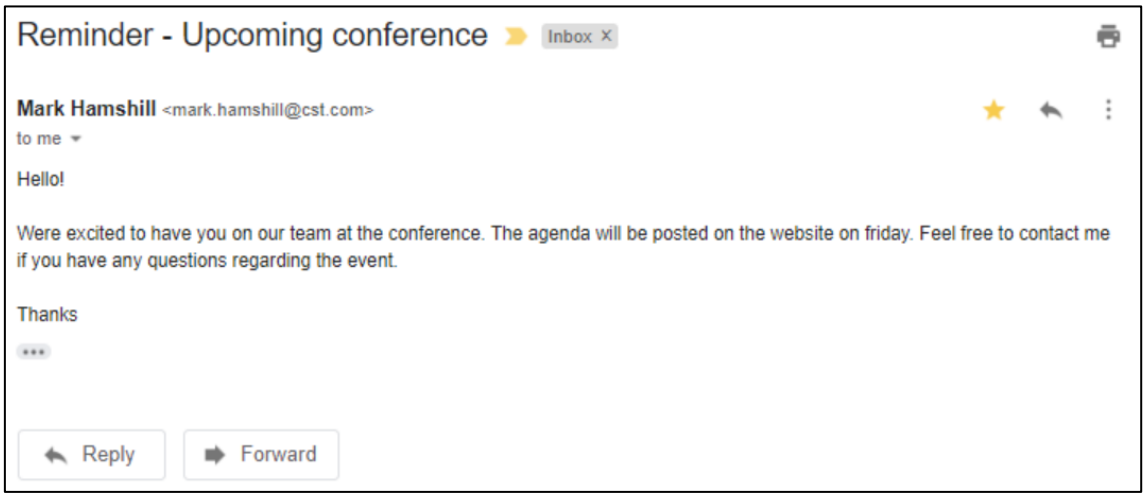
[CHA] Message source

```
Delivered-To: ivo.malve@gmail.com
Received: by 2002:a25:a81:0:0:0:0:0 with SMTP id 123csp3915584ybk;
        Tue, 1 Oct 2019 07:35:36 -0700 (PDT)
X-Google-Smtp-Source:
APXvYqzuVdYEfHO6oGi2kWlh7uGS1OaaHWa/EWnINHeogptTiipd186dhac2AA01jMTb8yrSSaTV
X-Received: by 2002:a05:651c:c4:: with SMTP id 4mr16326762ljr.111.1569940536498;
        Tue, 01 Oct 2019 07:35:36 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1569940536; cv=none;
        d=google.com; s=arc-20160816;
        b=eTJf4/IE/ic6j3VxBEFJJZ0+4WLv9EdiXbtY1vXzX4fKFUkHC5eHth2yxbNefHVhMU
         LFsj/UNaO+r1hiOboIdPB5s55k82jWQZwS38MPnAUSOG3DPUtHRMzf6rL3xTnxuor/+m
         +utRMOrp3enbHkMhs+z2HlviARxesp8D6R8EKuhq1tojThWecImArBB5dve647ZSblqC
         WQs9+4CTpr7ZEZEGPFYdADNFQ8oD1qdHufSrfY2uZHl0MaDMBMHAVNb+/rzsbscKydA7
         ssT18vq6NC7nsJmIjLPwnBCDSgRJU5b7XZxYiiWvHnk/FahopIdZbKR7lmPIxKQ1yXVS
         13gQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-
20160816;
        h=message-id:content-transfer-encoding:subject:date:reply-to:to:from
         :mime-version;
        bh=CsQ+16qBb5NPty7xF/2wccyn91vEDI6u+dtSBuv/UgU=;
        b=E73LrJQ8CdQHz2zEhsSa09ldmzAhAhFvFBs4dkMMPbdBdPrk1BbKClY1fpHccolxM0
         +KcMolTILW7u+GEZWkib/iPJ4wCXtPANm8G1d2V8SvW9lQS+19gFZWW8RaN03ZSJJwwn
         kIRvpsZFt+yEIJbQi1vKARE+E18GHcrAi/YUAMpJrbNEAjnGwwRhenXkHeQj+WqwK0C+
         g5FutmksdFsQJgww/WDEsClcxWEdJ1enpVIuLc9G2ozQ0RufZMv+WVa4ITWXsA1Wc/sH
         +I63xOzg+t9vRzimoVX7g2n1e4U01kJRpBSraXeS2oclXVF/5iVvtCh4EE0xh1Z0YFie
         5Ttw==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=softfail (google.com: domain of transitioning drcc@hot.com does not designate
213.184.53.9 as permitted sender) smtp.mailfrom=drcc@hot.com
Return-Path: <drcc@hot.com>
Received: from mail1.just.ee (mail1.just.ee. [213.184.53.9])
        by mx.google.com with ESMTPS id q18si15150003ljg.131.2019.10.01.07.35.35
        for <ivo.malve@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 01 Oct 2019 07:35:36 -0700 (PDT)
Received-SPF: softfail (google.com: domain of transitioning drcc@hot.com does not
designate 213.184.53.9 as permitted sender) client-ip=213.184.53.9;
Authentication-Results: mx.google.com;
       spf=softfail (google.com: domain of transitioning drcc@hot.com does not designate
213.184.53.9 as permitted sender) smtp.mailfrom=drcc@hot.com
```

```
X-AuditID: d5b83509-c69ff70000002a42-ef-5d936437b222
MIME-Version: 1.0
From: NGO Red Cross <drcc@hot.com>
To: <ivo.malve@gmail.com>
Reply-To: <nego@wix.com>
Date: Tue, 1 Oct 2019 17:34:01 +0300
Subject: Dorian - Red Cross Fundraising
Content-Type: text/html; charset="utf-8"
Content-Transfer-Encoding: base64
Message-ID: <eee8c9f6-e708-4849-8ff5-5c273076102a@exch3.just.sise>
Return-Path: drcc@hot.com
X-EXCLAIMER-MD-CONFIG: 0ffde1e1-0574-4cb5-b117-7534ebede067
X-Brightmail-Tracker:
H4sIAAAAAAAAA+NgFnrPJMWRmVeSWpSXmKPExsXCxWh2WNc8ZXKswc0Feha33+c4MHrsnHWX
PYAxissmJTUnsyy1SN8ugSvj2dblzAXruCtm75NsYGzg7mLk5JAQMJG4sWoWO4jNKyAocXLm
ExYQm01ASaL3ZR8TiC0iICmx69BJMFtIQEJi9feTjCA2i4CKRPf65WC2sIC6xOlTPllBbGYB
DYnWOXPZIWxFiSndD6HmO0n8XtPMAjFHUuLF0SvsEDdYS5w9/5J1AiPPLCRnzEIyahaSUQsY
mVcx8uYmZuYY6mWVFpfopaZuYgQGw9Udppw7GL/+MjzEKMDBqMTDezFkcqwQa2JZcWXuIUYJ
DmYlEV6bP5NihXhTEiurUovy44tKc1KLDzFKc7AoifM+/wSUEkhPLEnNTk0tSC2CyTJxcEo1
MAbbZxq+Xb22wbp4WfSJrotdk67fuGZi9d1YvWj+2izVkxtzdHkzPpcVPmtec0ZAKJrdXXeC
mZncO4n8UlctY6mE9wc/mxxnUMm6Fm1f1Xan/l7b1lSx+fzzX195nrRx96qOqR9OzZ5lkJl7
UbNi4znrP7Uhio84WF7Vbc98xPHw3IYNlyyv7FViKc5INNRiLipOBAAULx5MAgIAAA==

DQoNCkEgZHJvdWdodC4gQW4gZWFydGhxdWFrZS4gQSB3YXIuIEEgZm9vZCBjcmlzaXMuIFdlIGNh
bnQgYWx3YXlzIHByZWRpY3QgbmVlZCBpbiB0aGUgd29ybGQuIEJ1dCB3ZSBjYW4gYmUgcHJlcGFy
ZWQgdG8gYWN0IHF1aWNrbHkuIA0KSHVycmljYW5lIERvcmlhbiBkZXZhc3RhdGVkIHRoZSBCYWhh
bWFzIGFuZCBpcyB0aHJlYXRlbmluZyBGbG9yaWRhIGFuZCB0aGUgc291dGhlYXN0ZXJuIFVuaXRl
ZCBTdGF0ZXMuIEZvciB1cC10by1kYXRlIGluZm9ybWF0aW9uLCBwbGVhc2UgcmVmZXIgdG8gdGhl
IGZvbGxvd2luZyB3ZWJzaXRlczoNCuKAogk8YSBocmVmPSJnb29nbGUuY29tIj5UaGUgV2VhdGhl
ciBDaGFubmVsPC9hPiA8YnI+DQrigKIJPGEgaHJlZj0iZ29vZ2xlLmNvbSI+RkVNQTwvYT4gPGJy
Pg0K4oCiCTxhIGhyZWY9Imdvb2dsZS5jb20iPkZsb3JpZGEgRGl2aXNpb24gb2YgRW1lcmdlbmN5
IE1hbmFnZW1lbnQ8L2E+IDxicj48YnI+DQoNCkFjdGl2ZSBmdW5kcmFpc2luZyBmb3IgSHVycmlj
YW5lIERvcmlhbiBoYXMgb2ZmaWNpYWxseSBlbmRlZC4gPGJyPg0KSG93ZXZlciwgaW YgeW91IHdp
c2ggdG8gbWFrZSBhIGdpZnQsIGRvIGNvbnRhY3QgdXMgb24gPGI+ZG9uYXRpb25zQHJlZGNyb3Nz
Lm9yZzwvYj48YnI+DQpZb3VyIGdpZnQgd2lsbCBiZSB1c2VkIHRvIHJlc3BvbmQgdG8gdGhlIGdy
ZWF0ZXN0IG5lZWRzIGluIHNvbWUgb2YgdGhlIHdvcmxkcyBtb3N0IHZ1bG5lcmFibGUgY29tbXVu
aXRpZXMuDQo8YnI+WW91IG1heSB3aXNoIHRvIGhlbHAgdGhyb3VnaCBvdGhlciBvcmdhbml6YXRp
b25zOg0K4oCiCTxhIGhyZWY9Imdvb2dsZS5jb20iPkRpcmVjdCBSZWxpZWY8L2E+IDxicj48YnI+
ogk8YSBocmVmPSJnb29nbGUuY29tIj5Wb2x1bnRlZXJGbG9yaWRhIEZsb3JpZGEgRGlzYXN0ZXIgRnVuZDwvYT4g
PGJyPjxicj4NCsKpIDIwMTkgVGhlIEFtZXJpY2FuIE5hdGlvbmFsIFJlZCBDcm9zczxi
cj4NCk5HTyBOTiByZXNlcnZlZCByaWdodHMNCg0K
```

Image of [REA1]



[REA1] Message Source

```
Delivered-To: ivo.malve@gmail.com
Received: by 2002:a25:a81:0:0:0:0:0 with SMTP id 123csp3928980ybk;
        Tue, 1 Oct 2019 07:46:26 -0700 (PDT)
X-Google-Smtp-Source:
APXvYqzJzwwvdgWP3Tq8BhsoFzcUYFbN0gsO+d8aK3ZVbeWG5ocZsVkzPJRvWvWaseaN6XJGKOy4
X-Received: by 2002:ac2:4114:: with SMTP id b20mr15384765lfi.19.1569941186422;
        Tue, 01 Oct 2019 07:46:26 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1569941186; cv=none;
        d=google.com; s=arc-20160816;
        b=Iw+jAbrwS+KOoK0Vr1aW7DV2uZCWLy7r0mahBIlamIHnVPNdvocKOXr9Dqz1ZZV4lJ
         axlpSZOZy0ijEajv8TAgtLToZH0V/HWDbOx1nCYO7M+aNoQezuwzCti8mucaVgID2cCn
         jSYYepNbt4x61UQBOtxJVVc3lEt6yiY/9RA3txRv7cgedvFauXCrRprFitWI4cwRVG1a
         bctk7m0hWQEAJC6RnFXS7DgkDjweUWmNeAmlpf7AfpgeErtT9GVt4rceMlsl9OAKPqeX
         UWrmMwA63yZm3GuN/YdnjqGGM3kTcNCZv8tcF+r3xVXyUSAyeFyvRerLr7KwUdHkoTCF
         3XEg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-
20160816;
        h=message-id:content-transfer-encoding:subject:date:reply-to:to:from
         :mime-version;
        bh=TYzt18bRlWZVO7kdjKFdRZiOO//82GJPpzvKRlDwdMA=;
        b=zY1Y0DkqXmNMvZTcrFcW+OlsuJSwyUZaIpNbc8qDpRUE6R2KBJqFPwALPns0LbSleK
         PW9yeNhTp3HVh83DsOhs/p7+GGGs2akG7yrAB9DARZ7hnqFS1NsL2IHj0+Pky1uFK+YI
         YtjrMNqggj6oTv79LlJRbsTvTgwTjzZTFr/41LtIG2X+WISzyv7tYymx7t04+tzxy0z6
         +eUNoZ/OlI2MjLpv83W3JwZgO7IqkffwT9SXMc0wz/vEAjaeDpEuU1Hm3sq6J2OP4Tav
         5VtZUQfDU/1xjZ3mF/1O83e1vIRC/6q+vuC4L1Elek7i5wPX9SDEP/APl3PGnJGzuuF2
         TDSA==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=neutral (google.com: 213.184.53.9 is neither permitted nor denied by best
guess record for domain of mark.hamshill@cst.com) smtp.mailfrom=mark.hamshill@cst.com
Return-Path: <mark.hamshill@cst.com>
Received: from mail1.just.ee (mail1.just.ee. [213.184.53.9])
        by mx.google.com with ESMTPS id u17si16281760lje.228.2019.10.01.07.46.26
        for <ivo.malve@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 01 Oct 2019 07:46:26 -0700 (PDT)
Received-SPF: neutral (google.com: 213.184.53.9 is neither permitted nor denied by best
guess record for domain of mark.hamshill@cst.com) client-ip=213.184.53.9;
Authentication-Results: mx.google.com;
       spf=neutral (google.com: 213.184.53.9 is neither permitted nor denied by best
guess record for domain of mark.hamshill@cst.com) smtp.mailfrom=mark.hamshill@cst.com
X-AuditID: d5b83509-c51ff70000002a42-2e-5d9366c14d8d
MIME-Version: 1.0
From: Mark Hamshill <mark.hamshill@cst.com>
To: <ivo.malve@gmail.com>
Reply-To: <ne@wix.com>
Date: Tue, 1 Oct 2019 17:45:21 +0300
Subject: Reminder - Upcoming conference
Content-Type: text/html; charset="us-ascii"
Content-Transfer-Encoding: quoted-printable
Message-ID: <ec24eefe-efc3-4dae-be58-e2f6d0382241@exch4.just.sise>
Return-Path: mark.hamshill@cst.com
```

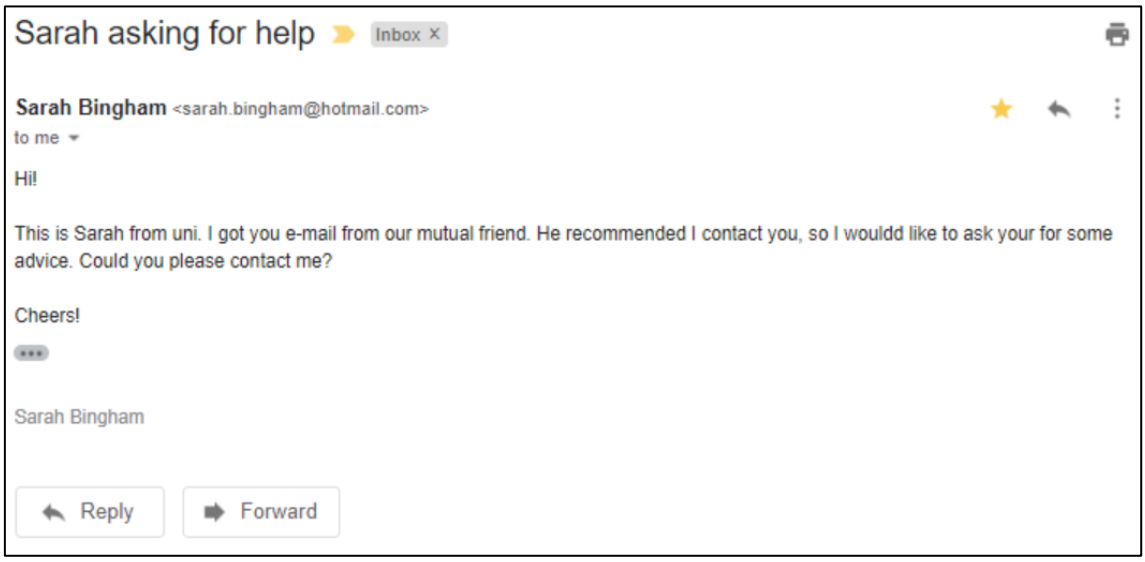
X-EXCLAIMER-MD-CONFIG: 0ffde1e1-0574-4cb5-b117-7534ebede067
X-Brightmail-Tracker:
H4sIAAAAAAAAA+NgFnrHJMWRmVeSWpSXmKPExsXCxWh2WPdg2uRYg+evzS1uv89xYPTYOesu
ewBjFJdNSmpOZllqkb5dAlfGwxdiBZuYKrYs2MPewNjI1MXIwSEhYCIx9Sd3FyMnB6+AoMTJ
mU9YQGw2AW2J21272EBsEQFJiV2HTjKB2EICYhL/V0wAi7MIqEgc2D6PFcQWFlCXWPH1N5jN
DNR75sBjJhh72cLXzBDznSTmX9rLBjFHSWLW405GEFtCwFri7PmXrBMYeWYhOWMWklGzkIxa
wMi8ipE3NzEzx1Avq7S4RC81dRMjMBSu7jDl3MH49ZfhIUYBDkYlHt6LIZNjhVgTy4orcw8x
SnAwK4nw2vyZFCvEm5JYWZValB9fVJqTWnyIUZqDRUmc9/knoJRAemJJanZqakFqEUyWiYNT
qoFxof6PNe8XHKtaFsrDcT6/4UzMUoasRSmLVxzj/+x0d365ftKzB+aPftS28UoEPPn38LbD
jveNnv8/s8T1lSUvvy56/ebEn1XZEUvnxNWIHvo9tzFAlXUVY5FfxA+rI79vG05/qGfRk3Lq
T+7kCjmV+TrVxzzYjadr5sb3n0l99vJ1mOa0QI8sJZbijERDLeai4kQACvk/3AECAAA=

Hello!

Were excited to have you on our team at the conference. The agenda will be =
posted on the website on friday. Feel free to contact me if you have any qu=
estions regarding the event.

Thanks
Mark Hamshill

Image of [REA2]



[REA2] Message Source

```
Delivered-To: ivo.malve@gmail.com
Received: by 2002:a25:a81:0:0:0:0:0 with SMTP id 123csp3934094ybk;
        Tue, 1 Oct 2019 07:50:36 -0700 (PDT)
X-Google-Smtp-Source:
APXvYqzh/iRRriDSCkQ9jtE5+2it7QxJHmYSQYTo/A9u/2v3aDa4Rb+g5+fzMyDpnYYlmUhHUrKE
X-Received: by 2002:a2e:9118:: with SMTP id m24mr16311960ljg.95.1569941436422;
        Tue, 01 Oct 2019 07:50:36 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1569941436; cv=none;
        d=google.com; s=arc-20160816;
        b=SqlbH/VFiiO3hiAItVtnrZkhaZvN4yPlBawL2L/YQKCR+XB2J80cgVpTqMeZLy+FHZ
         jkdsKewLSkPhjrQQ+pF/Ms94Jl/s7XkdShkb2xBTQSz6gBKr+PjZTsj8oMXlxmNBxytr
         GvLXtKia58h/4g3S5kIMKtj2rQgmD/YF002neYNbZbcMW9jaQNxWhZpPuk8X3Zu/fk10
         j7LWMU6NvcPXBADWQxro03v922PskVM8unLxki4cTMIeuFFW01CGLsT8CyM8XnvuXWAb
         PsT/gvEvLFDrApiwh80vwVKvhnJUqwulOxUaAy0aj45ZDT87UcXjOpFnHvCLkskyDzb5
         sCeQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-
20160816;
        h=message-id:content-transfer-encoding:subject:date:reply-to:to:from
         :mime-version;
        bh=QZGg7oVPcUKMOmnUyMtJNQv9oVnMNJw09pvB4k9UYoA=;
        b=NsK5l064bI441bz2oNsCL7VgnC3EnmqXbLf9em+oCSwzs/DZVsJ00mfAA9Sl4firuZ
         sWDrd2k93yLKbNf2Qsd4Q2uv1CatKsW62gPL9tZkTdYOcITT/fGGWmip6Hp9YBd2/YIR
         dHQuY1olMmCv7C7lOCGPUFsLkcElvgeSFND8cDRSoRUQZ+X9i8OgjC8nlgk/GzMeNnMU
         EIC90uLD4BQYbM4qepzNmrTwIgDUv3BgCZ8K/ZACAgSrbKjCYP1+JfZu4eAEcQ5gqUaA
         VuCDc0iqKjff/UykTk8ATQNNq6Q/0SiZLnbYVJcH0YLH4gRzEuLDvq8FhogtddMvTtjZ
         jDNg==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=softfail (google.com: domain of transitioning sarah.bingham@hotmail.com does
not designate 213.184.53.9 as permitted sender) smtp.mailfrom=sarah.bingham@hotmail.com;
       dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=hotmail.com
Return-Path: <sarah.bingham@hotmail.com>
Received: from mail1.just.ee (mail1.just.ee. [213.184.53.9])
        by mx.google.com with ESMTPS id t5si13861888lfl.50.2019.10.01.07.50.36
        for <ivo.malve@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 01 Oct 2019 07:50:36 -0700 (PDT)
Received-SPF: softfail (google.com: domain of transitioning sarah.bingham@hotmail.com
does not designate 213.184.53.9 as permitted sender) client-ip=213.184.53.9;
Authentication-Results: mx.google.com;
       spf=softfail (google.com: domain of transitioning sarah.bingham@hotmail.com does
not designate 213.184.53.9 as permitted sender) smtp.mailfrom=sarah.bingham@hotmail.com;
       dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=hotmail.com
X-AuditID: d5b83509-c51ff70000002a42-8d-5d9367bb20b2
MIME-Version: 1.0
From: Sarah Bingham <sarah.bingham@hotmail.com>
To: <ivo.malve@gmail.com>
Reply-To: <ne@wix.com>
Date: Tue, 1 Oct 2019 17:49:01 +0300
```

```
Subject: Sarah asking for help
Content-Type: text/html; charset="us-ascii"
Content-Transfer-Encoding: quoted-printable
Message-ID: <490381fe-20cb-4aed-b54e-5c9cf881bf5c@exch4.just.sise>
Return-Path: sarah.bingham@hotmail.com
X-EXCLAIMER-MD-CONFIG: 0ffde1e1-0574-4cb5-b117-7534ebede067
X-Brightmail-Tracker:
H4sIAAAAAAAAAA+NgFnrHJMWRmVeSWpSXmKPExsXCxWh2SHdP+uRYg/O6Frff5zgweuycdZc9
gDGKyyYlNSezLLVI3y6BK6Pv8GO2gmVMFc3zb7I0MH5n7GLk5JAQMJH42f6AFcTmFRCUODnz
CQuIzSagL3Fk22I2EFtEQFJi16GTTCC2kICYxP8VE8DiLAIqEhcmzmQGsYUF5CTWnmgCm8ks
oC1x5sBjJhh72cLXzBDznSSWXF4PtIsDaI6axLdPkhAnWEucPf+SdQIjzywkV8xCMmkWkkkL
GJlXMfLmJmbmGOpllRaX6KWmbmIEhsLVHaacOxi//jI8xCjAwajEw3sxZHKsEGtiWXFl7iFG
CQ5mJRFemz+TYoV4UxIrq1KL8uOLSnNSiw8xSnOwKInzPv8ElBJITyxJzU5NLUgtgskycXBK
NTBm5wss5LTRnvJs6eNbLaqNM3Y+Lf0SpBTeKmAo3/Ppy09hKz2z/zdOXvku3yj2vXF7oUA4
94GTbBn1aZ+vmD1YUJnns+nTgXN7Z6nPfh7/6En+jdZIC+O1MYu0/nL5anxQefJq4mvNJxyv
HEu1hJMqzz05PZlViX/tXr6Ca00ffzZcVTmmaOynxFKckWioxVxUnAgA18GFVAECAAA=



Hi!<br><br>
This is Sarah from uni. I got you e-mail from our mutual friend. He recomme=
nded I contact you, so I wouldd like to ask your for some advice. Could you=
 please contact me?
<br><br>
Cheers!<br>
Sarah Bingham<br>
```