University of Twente
Faculty of Behavioural, Management and Social sciences
Bachelor of Science in Communication Science

Information safety at the workplace:

A research into safe email behaviour among employees of the municipality of Enschede

Bachelor Thesis

Lilian Boerkamp
s1679821

Supervisor: Dr. A.D. Beldad

Municipality of Enschede
Client IT department: B.M.M. Tel
Client Communication department: E.C.M. Hoekstra

Date: 24-6-2018

Abstract

Objectives Information safety forms a hot topic in today's technology-oriented society. With personal data on the line, the relevance of protecting corporate information systems is increasing in importance. Especially in governmental organizations that have the responsibility of protecting and storing much privacy-sensitive data, a solid protection should be a high priority among all employees involved. However, when it comes to safeguarding data in organizations, research indicates that the end-users of information systems might form the weakest link. Hereby, email behaviour seems to be of the greatest importance. Research has namely shown that most security breaches in municipalities happened because of sending files to the wrong addressees. Thus, in order to investigate which variables influence safe email behaviour, a research has been conducted. Also, other information security-related behaviours were further investigated. The outcomes of this research can assist the municipality of Enschede in optimizing their internal awareness campaign regarding information safety.

Method In this research, a survey study was implemented. With this survey, information security behaviour has been further investigated. By means of a combined model of the Protection Motivation Theory and the Theory of Planned Behaviour, an online questionnaire was send out to the employees of the municipality of Enschede (N = 582). The data were analysed by means of a hierarchical regression analysis in SPSS, combined with Independent Sample T-tests and ANOVA-analyses.

Results The results showed that knowledge and skills, attitude and descriptive norm have a significant positive effect on safe email behaviour. Also, the hypothesis regarding the negative effect of response costs on behaviour could be supported. Also, age showed to have a significant effect on safe email behaviour. However, the hypotheses regarding perceived severity, response efficacy, injunctive norm and perceived vulnerability could not be supported based on the gathered data. Regarding information security-related behaviours, it could be seen that the employees scored well on some of the behaviours, while others still needed improvement. Also, significant differences were found in information security behaviours regarding the different departments within the municipality.

Conclusions Addressing response costs, knowledge and skills, attitude and descriptive norm seems important in improving safe email behaviour. In addition, regarding the campaign, attention should be paid to the different needs regarding the several departments within the municipality, in order to fully optimize the campaign. Also, the insights into the scores on different information security-related behaviours can be helpful in designing the contents of the campaign.

Implications The outcomes of this study can be of great value for information security managers or campaign creators in improving communication about information safety. Also, the theoretical implications are relevant for research in the field of safe email behaviour.

Keywords: Safe email behaviour, Information safety, Protection Motivation Theory, Theory of Planned Behaviour

Table of contents

1. Introduction

In order to safeguard private data, organizations often rely on and invest in information security systems (Hwang & Cha, 2018; Ifinedo, 2012; Ifinedo, 2014; Workman, Bommer, & Straub, 2008). In overcoming threats and reducing the risk of organizational harm, companies tend to take countermeasures as anti-virus systems, firewalls and password systems (Lee, Lee, & Yoo, 2004; Workman et al., 2008). Also, security policies are put in place in order to aim at a better information security level (Lee et al., 2004).

However, just having technical measures and security policies in place seems to be insufficient. Research has shown that human security incidents often account for damage to organizational information (Cox, 2012; Ifinedo, 2012; Siponen, Mahmood, & Pahnila, 2014). According to Son (2011), employees can be seen as the 'weakest link' when it comes to information security (p. 296). Employees' misuse of information systems might not always be intentional, but with having access to organizational network systems, employees often are the target for hackers and thieves that make use of this access to information systems (Son, 2011).

The misuse of information systems by employees can cause a company great harm, on both a financial and a reputational level (Myrry et al., 2009; Ng, Kankhalli, & Xu, 2008). Therefore, research indicates that the success of information security measures heavily relies on the behaviour of employees as the end-users (Rhee, Kim, & Ryu, 2009). For this reason, many organizations start awareness and training programs in order to educate their employees about the possible consequences of engaging in risky behaviour (Cox, 2012; Ng et al., 2008; Vance, Siponen, & Pahnila, 2012). These programs or campaigns primarily aim at training employees on how to act in a technological and information-intensive environment, in order to strive for better organizational information safety. However, in practice, many information security training programmes are made with few considerations for the human aspect (Son, 2011). Though, as research has shown that employees might form an insider threat in information security, this underlines the relevance of considering human behaviour when designing security interventions. Therefore, the municipality of Enschede has asked to conduct a research regarding information security behaviour, in order to improve their internal awareness campaign.

As one of the largest municipalities in the Netherlands, the municipality of Enschede has the responsibility to store and safeguard much data, such as personal data, data of employees and data of clients and partners. This responsibility, which should be borne by all employees, also leads to numerous risks regarding the protection of these data. In the past years, this has actually led to security breaches in several municipalities, mainly due to human errors (Cordioli, 2017). According to research, 41% of the errors relate to sending personal data to the wrong addressees, or sending the wrong files as a result of being incautious in, for example, email usage (Cordioli, 2017). Hereby, this

percentage accounts for the most information security breaches within municipalities. As security breaches can cause great harm for both municipalities as for other individuals involved, the relevance of further investigating the email behaviour of employees can be underlined.

The need for risk-aware employees who act responsibly when sending emails is, thus, of great relevance. Elaborating on the existing gap in the literature, this research aims at investigating the different factors that influence safe email behaviour. This security-related behaviour will be central in the first part of the research because of its prominence in daily business practice and because of the amount of data leakages that have been caused by these behaviours. The research question that will be answered in the first part of this research is, therefore, formulated as follows:

RQ1: 'Which factors influence safe email behaviour among employees?'

In order to answer this research question, an empirical research will be conducted. First, the literature on safe email behaviour will be consulted. Based on these findings, a research model will be presented accompanied by hypotheses that will be tested within the research. The overall aim of this research is, therefore, to find out which factors influence safe email behaviour. The theoretical implications of this study can be of great value for research into the field of information security behaviour. Until today, research can namely be found investigating predictors of information security, compliance with security policies and computer security behaviour (Cox, 2012; Ifinedo, 2014; Ng et al., 2014; Woon, Tan, & Low, 2005). However, research into the factors that influence safe email behaviour within organizations is not prominent in literature. In addition, research on this topic within the context of a municipality has not been further investigated yet, which underlines the relevance and novelty of this research.

Second, in the light of the information security awareness campaign, the current security-related behaviours of employees of the municipality of Enschede will be further investigated. The municipality of Enschede namely has several policies regarding safe information usage and data handling, in which they are interested to know how employees score. Thereby, it will also be investigated whether differences exist between the several departments within the municipality of Enschede. The practical and theoretical implications of this part of the study can be of great value for the municipality of Enschede, as well as for information security managers or campaign creators in improving communication about information safety. Insights into information security-related behaviours can namely give assistance in designing effective interventions, specifically in the context of information-intensive governmental organizations. Therefore, a second research question will be added to this study.

RQ2: How do employees of the municipality of Enschede score on information security-related behaviours?

Within this research, a theoretical background will be provided first. Within this theoretical framework, a description will be given of the present literature within the field of information safety, applied to the research context of safe email behaviour. Thereafter, a description of the method used within this study will be provided. In addition, the results of the research will be presented. Next, a discussion on the research will be given. Within this discussion, directions for future research will be provided as well. Last, the conclusions of this research will be presented.

2. Theoretical framework

Within this theoretical framework, an elaboration on the theory on safe email behaviour will be provided first. In addition, in the second part of this framework, attention will be paid to information security-related behaviours within the context of the municipality of Enschede.

Part I - Safe email behaviour

2.1. The importance of safe email usage

In today's' society, many organizations deal with great amounts of information in their daily practice. For this reason, organizations use different methods and techniques in order to protect their information systems from threats to its security (Posey, Roberts, & Lowry, 2015). In order to do this, organizations often try to reduce the risk of organizational harm with technical solutions as firewalls, password security systems and virus scanners (Lee et al., 2004; Workman et al., 2008). Thereby, most companies seem to be dependent on their internal information systems (Haeussinger & Kranz, 2013). However, many information security managers seem to overestimate the benefits these technologies bring, without considering the relevance of human behaviour in safeguarding information assets (Posey et al., 2015).

This lack of understanding could lead to major problems for organizations. Research namely shows that end-users of information systems might form a great threat to an organization's information security (Cox, 2012; Ifinedo, 2012; Siponen et al., 2014). Several studies indicate that even more than half of the security lapses are caused by employees (Haeussinger & Kranz, 2013; Siponen & Vance, 2010; Vance, Siponen, & Pahnila, 2012). Although technological measures are of great importance, just implementing technological measures is, therefore, not enough (Aytes & Conolly, 2003; Klein & Luciano, 2016; Posey et al., 2015; Safa et al., 2015).

Recognizing the need for information safety, many organizations start training and awareness programs to educate their employees on how to behave in an information-intensive context (Cox, 2012; Ng et al., 2008; Posey et al., 2015; Vance et al., 2012). In information security studies, research also underlines the relevance of these awareness and training programs in influencing information security behaviour (Bulgurcu, Cavusoglu, & Benbasat, 2010). However, before deciding on how to best design and communicate these programs, it is important to look into the research on human behaviour in relation to information security. However, in practice, many organizations tend to start security programmes without considering human behaviour in information safety (Son, 2011). In order to understand how to best achieve an information secure organization, it is important to further investigate what might influence individuals when it comes to safeguarding information.

Regarding safeguarding information, research has shown that most of the security breaches within municipalities, namely 41%, can be found within sending files and addressing these (Cordioli, 2017). In the past years, this has led to security breaches in several municipalities, mainly due to human errors (Cordioli, 2017). Thus, because of its relevance in daily business practice, safe email behaviour will form the basis of this study. Safe email behaviour can be defined as being cautious in addressing emails and sending files by means of using email. Thus, this relates both to adding the right attachments to emails, as making sure to send them to the correct addressees. These behaviours are of great importance, as these are all dependent on the behaviours of individual employees: Only technical measures regarding safe email usage are, thereby, not enough (Rhee et al., 2009).

Thus, as human behaviour plays a vital role in safe email behaviour, it is important to further investigate which variables might influence individual email behaviour. Important to note is that, in behavioural research, many studies in the information security context focused on the effect of different constructs on behavioural intent instead of actual behaviour (Vance et al., 2012; Ifinedo, 2012; Ifinedo, 2014). However, in this research self-reported safe email behaviour will be used as the dependent variable. While this variable might be subject to self-reporting bias, it is perceived to be more objective and more convenient to be self-assessed than behavioural intentions (Ng et al., 2008).

In order to better understand the human factor in email behaviour, studies will be discussed that have tested multiple variables and its influence on behaviour. These previous studies have aimed at online security behaviours (Anderson & Agarwal, 2010; Chenoweth, Minch and Gattiker, 2009; Crossler, 2010; Lee, Larose, & Rifon, 2008; Ng et al., 2014) as well as information safety in general and compliance behaviour regarding information security policies (Ifinedo, 2012; Ifinedo, 2014; Son, 2011; Vance et al., 2012). Interesting insights can be drawn from these studies that could be applied to the context of safe email behaviour. Many studies have also applied interesting communication or psychological theories to the context of information safety. In order to find out which of these theories might also be relevant in the context of safe email behaviour, a detailed overview of the existing literature will be provided.

2.1.1. Protection Motivation Theory

An example of a theory that is applied in the information safety context is Rogers' (1983) Protection Motivation Theory. This theory explains why individuals might protect themselves or not. The theory thereby tries to give guidance in how risky behaviours can be encountered (Sommestad, Karlzén, & Hallberg, 2015). The theory claims that an individual will form a believe about the perceived vulnerability and severity of a threat, weighted against the efficacy and response beliefs on the other hand (Anderson & Agarwal, 2010). The Protection Motivation Theory, therefore, describes how the intention to protect oneself from possible dangers relies on two appraisals: Threat appraisal and coping appraisal (Ifinedo, 2012; Rogers, 1983).

The threat appraisal concept can be split into several underlying variables. First, the perceived severity variable, which describes an individual's assessment of the harshness of the consequences of a possible risk (Ifinedo, 2012). It, thus, describes the level of perceived impact (Vance et al., 2012). It is expected that the more severe a threat is perceived, the higher the chance is that one will protect oneself (Rogers, 1983). Several studies have indicated the effect of the perceived severity construct. For example, Vance et al. (2012) empirically tested this variable and found a significant effect on the intention to comply with security policies. Moreover, Chenoweth et al. (2009) conducted an empirical research into the effects of perceived severity on behavioural intentions in the context of anti-spyware usage. Thereby, they found a significant positive influence of perceived severity on the dependent variable in the study. In addition, research of Siponen et al. (2014) found a significant positive effect of perceived severity on compliance with information security policies. Therefore, it is expected that this variable might also influence safe email behaviour. Thus, it will be included in this research. The first hypothesis that will be tested in this research is, therefore, as follows:

H1 = Perceived severity positively influences safe email behaviour

The second variable belonging to the threat appraisal construct is perceived vulnerability. This variable describes one's evaluation of the probability a threat will occur if no action is taken (Ifinedo, 2012; Vance et al., 2012). In other words, it is the evaluation of whether a threat is likely to happen or not (Posey et al., 2015). It is expected that the higher the vulnerability is perceived, the higher the chances are that one will be motivated to protect oneself (Rogers, 1983). While research of Vance et al. (2012) could not find a significant effect of this variable in the context of information security, several studies indicate otherwise. For example, research of Ifinedo (2012) empirically found a significant positive relationship between perceived vulnerability and compliance intentions in the information security context. In addition, Siponen et al. (2014) found a similar positive effect. Moreover, in the context of taking information security measures, Workman et al. (2008) found a significant effect of perceived vulnerability on both self-assessed as well as observed security behaviour.

Also, in the context of online security behaviour, specifically of making data back-ups and using anti-spyware software, empirical studies indicated an effect of perceived vulnerability on the intention to conduct information security behaviour (Chenoweth et al., 2009; Crossler, 2010). In addition, research of Lee et al. (2008) indicated a significant effect of perceived vulnerability of Internet viruses on the intention to adopt protective behaviours. Therefore, this variable will be included in this research, as it is expected to have a relationship in the context of safe email behaviour as well. Thus, the next hypothesis that will be tested in this research is as follows:

H2 = Perceived vulnerability positively influences safe email behaviour

According to the Protection Motivation Theory, the third and last threat appraisal variable is rewards. This variable describes both the intrinsic as well as extrinsic rewards one perceives when not conducting the behaviour that could reduce threats (Vance et al., 2012). This variable is less used when applying the Protection Motivation Theory to the context of information safety behaviour. Woon et al. (2005), for example, did not see any possible rewards in not enabling security measures. Vance et al. (2012) on the other hand did use this construct in their research, but operationalized this as the reward of saving time. However, as the time aspect of coping with a threat is already present in the response costs construct, that will be elaborated on soon, it is chosen not to include this variable in this study, thereby following earlier examples of the application of the Protection Motivation Theory (Ifinedo, 2012; Workman et al., 2008). Also, it is not expected that, within the context of this research, one would feel externally rewarded when not being cautious in sending emails.

In addition, the coping appraisal construct has three underlying variables. The first is response efficacy. The construct of response efficacy describes if an individual perceives the recommended response as effective (Rogers, 1983). It describes the evaluation of the effectiveness of the recommended behaviour in avoiding negative consequences (Boer & Seydel, 1996). It is expected that the more positive this belief is, the more likely it is that an individual will take safety measures. In the context of safe email behaviour in organizations, this could relate to whether an employee believes that an action will actually reduce harm.

Prior studies already underlined the significant effect of response efficacy in the information security context. For example, research of Chenoweth et al. (2009) indicated a significant positive effect of response efficacy on the intention to adopt anti-spyware technologies. In addition, research also indicated an effect of response efficacy on password changing, in the context of protecting files (Crossler, 2010). Moreover, Ifinedo (2012) found a significant positive effect between the response efficacy construct and the intention to comply with an organization's security policies. Also, within the context of virus protection behaviour, Lee et al. (2008) found a significant positive effect of response efficacy. Further research on response efficacy within the context of email behaviour is scarce, but it is expected that this variable might be of influence in this study as well. Based on the above-mentioned empirical results, this variable will, therefore, be added to this study accompanied by the following hypothesis:

H3 = Response efficacy positively influences safe email behaviour

The second variable of the coping appraisal construct is response costs, that describes the perceived costs in terms of, for example, money, time and effort in relation to the recommended behaviour (Ifinedo, 2012; Posey et al., 2015; Woon et al., 2005). In the case of email behaviour, this might imply that an individual believes that being cautious takes too much time and as a result refuses to conduct safe behaviour. Several studies already indicated this effect. For example, research of

Vance et al. (2012) indicated a negative effect of response costs on information security behaviour. In addition, Chenoweth et al. (2009) found a significant negative effect of response costs on the intention to use anti-spyware technologies. Also, in the context of protection motivation, Posey et al. (2015) indicated a significant negative influence of response costs. Still, not all studies found a significant effect of response costs on information security behaviour. However, this was then attributed to scale composition or external variables, such as response (Ifinedo, 2012). As it is expected that this variable might have an effect in this research context, it is added to the study. The hypothesis is, thereby, formulated as follows:

H4 = Response costs negatively influence safe email behaviour

The third and last variable of the coping appraisal construct is self-efficacy, that describes an individual's belief about if the recommended behaviour can be performed (Ifinedo, 2012; Rhee et al., 2009; Rogers, 1983). Research indicates that this perceived personal efficacy will determine whether a threat will be coped with or not (Bandura, 1977). For example, research from Ifinedo (2014) indicated a significant relationship between self-efficacy and information security compliance intentions. This effect has also been found by several other studies. Research of Crossler (2012), for example, indicated that self-efficacy regarding backing-up data, password changing and access controls has a significant effect on protection behaviour regarding file losses. In addition, Herath and Rao (2009) found a significant positive relationship between self-efficacy and the intention to comply with security policies. This effect had also been empirically found by other studies (Ifinedo, 2012; Siponen et al., 2014; Vance et al., 2012).

In addition, research of Rhee et al. (2009), who investigated the concept of self-efficacy in the context of information security behaviour in particular, indicated an effect of the self-efficacy construct on all dependent variables tested, which related to, for example, installing virus scanners, making back-ups and using strong passwords. The influence of self-efficacy in the context of computer viruses has also been found by research of Lee et al. (2008). Thus, the relevance of this construct within the context of information security can be underlined. As it is expected that this variable might also be of influence in the context of safe email behaviour, a hypothesis regarding this construct will be added to the research:

H5 = Self-efficacy positively influences safe email behaviour

2.1.2. Theory of Planned Behaviour

In his research into information security compliance, Ifinedo (2012) extended the Protection Motivation Theory with another model that can help in explaining individual behaviour: The Theory of Planned Behaviour (Ajzen, 1991). The Theory of Planned Behaviour consists of three constructs

that are expected to influence (the intention to perform) certain behaviours. These constructs are attitude, perceived behavioural control and subjective norm. The first construct, attitude, describes an individual's evaluation of the behaviour. This evaluation can be both positive or negative (Ajzen, 1991). The second construct, perceived behavioural control, refers to the ease or difficulty of conducting a certain behaviour, perceived by an individual. The third and last construct, subjective norm, describes the social pressure from one's surroundings one perceives related to the behaviour. In general, it holds true that the more positive an individual's attitude, perceived behavioural control and subjective norm are in relation to the behaviour, the higher the chance is one will actually perform the behaviour (Ajzen, 1991).

Ifinedo (2012) has empirically tested this theory with regard to the intention to comply with information systems security policies. In this study, a significant effect of attitude on information security behaviour was found. In addition, Bulgurcu et al. (2010) investigated the antecedents of an employee's compliance with information security policies. They found that one's attitude towards this compliance significantly contributes to behavioural intentions. Moreover, Siponen et al. (2014) tested the effect of attitude on compliance intentions and found a significant positive relationship between these two variables. In addition, research has indicated a significant effect of attitude towards security behaviour and intentions regarding taking security measures (Anderson & Agarwal, 2010). It is expected that this variable can also be of influence in the context of safe email behaviour. Therefore, the following hypothesis will be included in this research:

H6 = Attitude positively influences safe email behaviour

In several studies, the perceived behavioural control construct is tested as the self-efficacy construct because of the overlapping interpretation. Research of Ifinedo (2012), that merged the Protection Motivation Theory and the Theory of Planned Behaviour, also tested the perceived behavioural control by means of self-efficacy, not by means of a separate construct. Thus, no new hypothesis will be added regarding the perceived behavioural control construct.

The third and last variable in the Theory of Planned Behaviour, the subjective norm, also has been tested in earlier studies. Research from Cox (2012) indicated a significant effect of this variable on behavioural intentions in the context of information security. In addition, Bulgurcu et al. (2010) found a significant relationship between subjective norms and compliance with information security policies. However, in some studies, the concept of subjective norm is criticized for having just modest influence on behavioural intentions (Sheeran & Orbell, 1999). Several decades ago, Deutsch and Gerard (1955), therefore, made a distinction between two different kinds of social influences. Elaborating on this, Sheeran and Orbell (1999) make a distinction between the so called injunctive norm, which is the perceived social pressure, and the descriptive norm, which is the perceived behaviour of significant others. Cialdini and Goldstein (2004) also make a distinction between these

two types of norms, describing the injunctive norm as "what is typically approved/disapproved" and the descriptive norm as "what is typically done" (p. 597). In the context of information systems and protection motivation, a similar differentiation in this construct has also been used by Herath and Rao (2009), who found empirical evidence supporting both social influence variables. In the information security context, this distinction has also been made by Anderson and Agarwal (2010), who found positive significant relationships of these variables on security behavioural intentions. As it is expected that both the injunctive and the descriptive norm might be of relevance in the context of safe email behaviour as well, these two variables will be included within this study. Thus, the next two hypotheses that will be included in this research, are as follows:

H7 = Injunctive norm positively influences safe email behaviour

H8 = Descriptive norm positively influences safe email behaviour

2.2. Organizational context

While both the Protection Motivation Theory and the Theory of Planned Behaviour primarily focus on individual characteristics in relation to behaviour, literature also indicates that the organizational context might play an important role when it comes to predicting behaviour. For example, knowledge of the rules an organization has regarding information security might influence an employee's behaviour. Research suggests that the knowledge about what something is and what to do might influence if someone intends to act or actually acts (Sheeran, 2002).

Also, research of D'Arcy, Hovav and Galletta (2009) suggests that one should have knowledge of security policies in order act accordingly. Therefore, it is expected that if someone knows what to do when it comes to information security, he or she will be more likely to actually perform the expected safe email behaviour. Thus, this knowledge construct will be added to the research model. Thereby, the following hypothesis will be tested within this research:

H9 = Knowledge of expected behaviour positively influences safe email behaviour

2.3. Demographic variables

Besides the variables that have been introduced above, some other variables will be added to this study. These variables are age, managerial status, IT experience and working years at the municipality. First, age is added as a variable, as research indicates effects of this variable on information security-

related behaviours (Anderson & Agarwal, 2010; McCormac et al., 2010). An example of such research within the context of emails, is a research of Sheng, Holbrook, Kumaraguru, Cranor and Downs (2010). They found that younger people are more likely to be susceptible towards phishing emails than people with an older age. Furthermore, research of Pattinson, Butavicius, Parsons, McCormac and Calic (in McCormac et al., 2010) indicated a positive effect of age on information security behaviour. Furthermore, research of McCormac et al. (2010) indicates a significant positive effect of age on information security awareness. Thus, as age differences in safe email behaviour might exist as well, this variable will be included in the research. Therefore, the following hypothesis will be added to this study:

H10 = Age positively influences safe email behaviour

Furthermore, when it comes to one's managerial status, this variable might be of influence as well in the context of safe email behaviour. To illustrate this, Posey et al. (2015) found a significant effect of an employee's position on protection motivation and protective behaviours. Within this research, it could also hold true that employees with a managerial position are more likely to conduct safe email behaviour, as they might feel that they have an example position with regard to other employees. Thus, managers might feel more responsible regarding acting safely in sending emails. Therefore, this variable is added as an independent variable in this study, accompanied by the following hypothesis:

H11 = Managerial status positively influences safe email behaviour

Regarding IT experience, this variable could have a positive effect as well on safe email behaviour. For example, Albrechtsen and Hovden (2009) proposed that differences in security behaviour might exist between individuals with different levels of IT experience. In the context of emails, research of Sheng et al. (2010) also provides interesting insights. They namely found a significant negative effect of self-assessed technology knowledge on being susceptible to phishing emails. Thus, within the context of this research, it could hold true that employees with a better experience in IT are also more likely to perform safe email behaviour, as they know how to operate a computer. For that reason, the variable of IT experience will be added to the research model, accompanied by the following hypothesis:

H12 = IT experience positively influences safe email behaviour

Looking at the variable of working years at the municipality of Enschede, this could play a role in safe email behaviour as well. Hereby, the Social Bond Theory can be helpful. This theory

"describes the binding ties or social bonding that individuals have with their group" (Ifinedo, 2014, p. 70). Hereby, individuals who have a tighter bonding, are less likely to conduct wrong behaviours. Therefore, it could hold true that employees who work at the municipality longer, might feel more committed towards the organization than new colleagues. Research of Safa et al. (2015) also shows that committed individuals are less likely to perform risky behaviours within the context of information security policy compliance. Therefore, it is expected that the variable of working years at the municipality of Enschede might be relevant as well within the context of this research. For this reason, the variable is added to the research model, accompanied by the following hypothesis:

H13 = Working years positively influence safe email behaviour

The full research model regarding email behaviour can be found in figure 2.1. As can be seen within this figure, both the Protection Motivation Theory and the Theory of Planned Behaviour form the basis of the research model. Besides, the other aforementioned variables that are important in this study have been added. In merging these theories, the perceived behavioural control variable is fused into the self-efficacy variable, as research also suggested (Ifinedo, 2012).

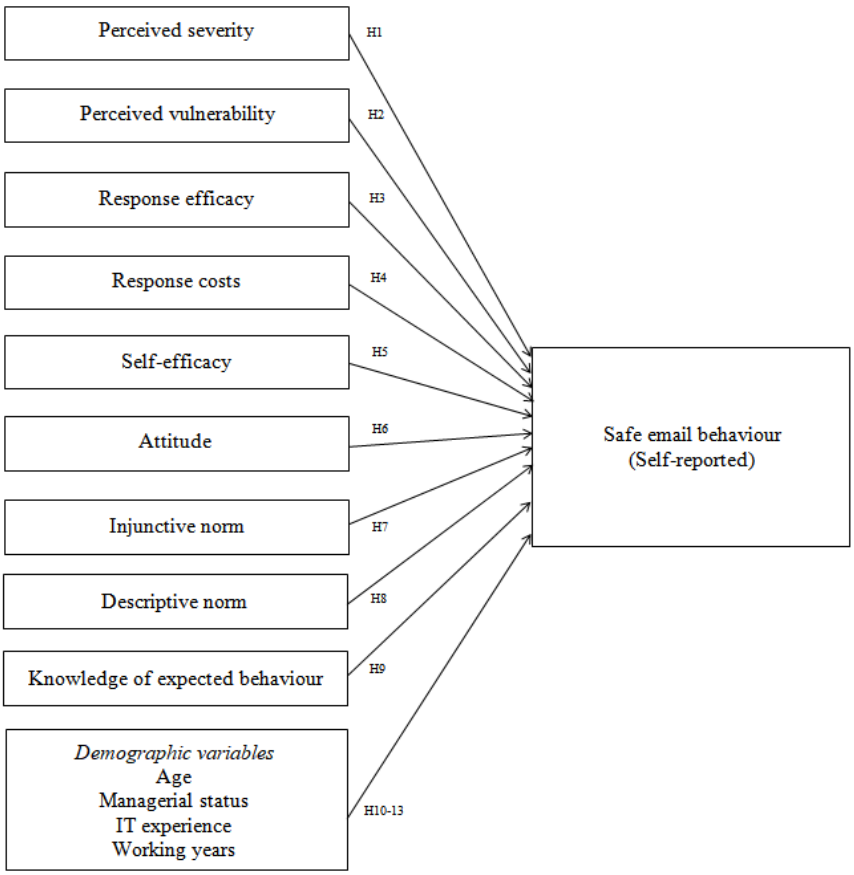


Figure 2.1. Research model safe email behaviour

Part II - Information security-related behaviours

2.4. Information security at the municipality of Enschede

Besides being cautious in sending emails, several other possible risks exists regarding information safety within a municipality. In order to prevent information-related risks to happen, it is important that information security behaviour is performed by employees, as the end-users of information systems. In literature, the concept of information security behaviour is defined as "the behaviors of individuals which relate to protecting information and information systems assets" (Crossler, Bélanger, & Ormond, 2017, p. 2). This is a rather broad definition, as these behaviours will be different in each organizational context. Still, to make employees perform the right behaviours, organizations often translate risky behaviours into information security policies, containing both the inappropriate as well as appropriate behaviours, tailored to the needs of an organization (Moody, Siponen, & Pahnila, 2018). Thus, in measuring how employees within the municipality of Enschede score on information security-related behaviours, the information security policies of the municipality of Enschede will serve as a guideline in this part of the research.

First, possible risks exists if employees fail to lock their computer when leaving their workspace. This might form a risk as this can enable outsiders to access information without permission, something employees should be cautious of. Another risky behaviour is, then, writing down passwords. However this might help employees in remembering their often difficult passwords, it might form a danger for the information security of the municipality. As unauthorized individuals could namely see the passwords, the chance of data leakages increases.

Regarding computer usage, some other behaviours are of great importance. For example, using up-to-date virus scanners in order to protect information systems. Also, when working elsewhere, employees should be aware of the dangers of using public WiFi connections. When using these for work-related tasks, problems in information safety could namely occur. Regarding this internet usage and preventing unwanted access to information, employees should also be cautious when accessing websites. Checking the safety of a website could then be of great importance. Furthermore, it is important not to send information from work email to private email addresses, as this could come with security dangers. In addition, when receiving emails, employees should be cautious. If an email does not feel reliable, then clicking on links and attachments within this email should be avoided.

Last, regarding phone usage, employees should be cautious as well. First, when an employee receives an unreliable phone call, it is important not to give away any private information and, thus, to end the connection. Also, in order to safeguard personal data, it is important that employees secure their phones with passwords. If not, unauthorized individuals could namely access these phones easily.

However, the extent to which employees of the municipality of Enschede are aware of the above-mentioned behaviours, is yet unknown. Still, in the light of the upcoming campaign, it is

important to gain insight into this. Insights into this can namely assist in deciding on the contents of the campaign, and will show which behaviours are the most critical to address. Therefore, a second dimension will be added to this research, in which the following research question will be answered:

RQ1: How do employees of the municipality of Enschede score on information security-related behaviours?

In addition, the municipality of Enschede would like to know how employees score on certain independent variables, as described before. Just as with the information security-related behaviours, this could namely give guidance in designing the contents of the campaign. For example, if it turns out that the response costs are considered as high, the campaign should focus on the fact that it does not have to cost much time to take action. Also, if employees, for example, do not perceive the municipality as vulnerable to information security threats, it might be important to communicate the possible risks regarding information safety. As these variables are namely expected to influence behaviour, it is important to gain insight into this. Thus, a third research question will be added to the second part of the research:

RQ2: How do the employees of the municipality of Enschede score regarding the antecedents of information security behaviour?

Third, the municipality would like to gain insight into differences in behaviour between departments. Insight into this could namely guide in optimizing the campaign towards the different groups of employees. It namely is possible to design the campaign based on the needs within the different departments. Therefore, the third research question that will be added to this study, is as follows:

RQ3: Which differences exists in behaviour between the different departments within the municipality of Enschede?

Fourth and last, it is helpful to gain further insight into differences in behaviour with regard to IT experience. As IT experience is a skill that might be improved by means of training, or by means of providing tips in a campaign, investigating this is relevant. If it namely holds true that employees with a better experience in IT also act safer regarding different information security-related behaviours, it could be important to aim at increasing this experience by means of the campaign. Therefore, the fourth and last research question that will be added, is as follows:

RQ4: Which differences exists in behaviour among employees with different IT experiences within the municipality of Enschede?

These four research questions will give guidance in establishing the current security-related behaviours of employees of the municipality of Enschede. Insights into this might help in deciding on how to best optimize the information security campaign. Furthermore, the results of this second part of the research could guide the decision for choosing the most pressing topics in communicating about information security behaviour.

3. Method

3.1. Design

For this research, a survey study was conducted. This method was chosen in order to be able to collect data on a large scale. Hereby, the study was conducted among employees of the municipality of Enschede as they form the research population within this study. By means of an online questionnaire, insights were gathered into the predictors of safe email behaviour in the context of the municipality of Enschede. The results of the study served as input for investigating the antecedents of safe email behaviour, as well as determining the current level of security-related behaviours of the employees of the municipality of Enschede. As for this study a large dataset was expected, it was chosen to gather the data by means of an online survey, that was built by means of the survey software programme Qualtrics. This method was chosen, as this enables to accurately and automatically collect great amounts of data over a longer period of time (Bolger, Davis, & Rafaeli, 2003; Van den Berg & Van der Kolk, 2014). Also, this method might make respondents more inclined to participate, as it enables individuals to anonymously fill out data.

3.2. Selection of respondents

In total, 602 respondents participated in the survey within this research. This indicates a response rate of approximately 35% ($N \approx 1700$). These responses all had been gathered within the time period of April 16 2018 to April 29 2018. The whole target group of this research was reached by means of a personal email, sent out by the researcher. Within this email, the employees of the municipality were invited to take part in the research. This email can be found in appendix 2. Also, on April 18, a similar message was posted by the researcher on the internal communication means of the municipality, named IntEns, as a means of a reminder. Also, the media department of the municipality shared this message on April 18 2018 within its own news feed. Thus, the invitation to take part in the research was visible during the whole period of data gathering.

Of the responses, one was deleted because this respondent did not work in any department of the municipality of Enschede. In addition, one respondent was deleted because this respondent was younger than 18, and eighteen respondents were excluded from the analysis as they did not fill in the survey completely. The choice was made not to exclude responses because of time reasons, as the questionnaire enabled the respondents to start the survey at one time, and to finish it at another time. As every respondent filled out the questionnaire on the same day as it was started (median = 7.57 minutes), this should pose no problems to the data.

3.3. Research participants

In total, 582 responses remained and were included in the data analysis (N = 582). Of these respondents, 62 have a managerial position within the municipality, whereas 520 have not. In addition, the mean IT experience is 8.51, measured on a 10-point scale (no experience/much experience), ranging from self-assessed scores of 3 to 10 ($\mu = 8.51$). As can be seen, gender is not part of the demographics. This question namely could not be asked based on the sensitivity of this subject within the municipality. Also, regarding age, scales have been used based on an example of literature (Ifinedo, 2012). In addition, the decision was made to use age ranges instead of an open question for this variable, in order to prevent possible restraints for respondents regarding identification. Other demographics of the respondents that took part in the survey can be found in table 3.1.

Table 3.1.
Demographics of research participants

	n (N = 582)	Percentage (100%)
Age		
18-30	60	10,31%
31-40	105	18.04%
41-50	152	26,12%
51-60	181	31,10%
Older than 60 years	84	14,43%
Working years		
5 years or shorter	151	25,95%
6-10 years	100	17,18%
11-20 years	169	29,04%
Longer than 20 years	162	27,84%
Managerial position		
Yes	62	10,65%
No	520	89,35%
Department[*]		
Board Enschede (BST)	1	0,17%
Management (DIR)	1	0,17%
Group staff (CS)	40	6,87%
Business and Management Support (BMO)	178	30,58%
Program Service (DV)	31	5,33%
Registry (RG)	2	0,34%
Program Social Support (MO)	81	13,92%
Program Economy, Work and Education (EWO)	133	22,85%
Domain Physical (DF)	125	21,48%
Maintenance Enschede (OE)	1	0,17%
IT experience		
3	1	0,17%
4	2	0,34%
5	5	0,86%
6	18	3,09%
7	72	12,37%
8	193	33,16%
9	149	25,60%
10	142	24,40%

[*] Because it is possible that an employee works in more than one department, the total adds up higher than N = 582.

3.4. Procedure

The survey started with a short description of the context of the study, as well as an informed consent. Within this informed consent, it was clearly stated that the responses were gathered anonymously, and that respondents could end their participation in the survey at any time, without having to provide a reason. Also, contact information of the researcher was given, so that the respondents were able to reach out to the researcher in case of any questions. In addition, the estimated survey completion time of seven to eight minutes was provided to the respondent. After the respondent read this information, he or she could continue with the survey. Then, some demographical questions were asked, such as age, department and working years. Thereafter, the main part of the survey started. First, twelve questions were asked about information security-related behaviours, to which the respondents had to provide answers. In addition, the respondents had to answer several questions that relate to the independent variables within the research model.

At the end of the survey, the respondents were thanked for their participation. Also, information was given on how the respondents could be kept posted about the campaign and other news on information security within the municipality. In order to prevent bias, this specific information about the campaign was provided at the end of the survey, instead of at the beginning. The data were analyzed by means of the programme SPSS. Before the survey was distributed among the employees of the municipality of Enschede, the survey procedure had been approved by the Ethics Committee of the Faculty of Behavioural, Management and Social sciences of the University of Twente.

3.5. Pre-test

Before the survey was spread, it was screened by experts who were also members of the research population. For this pre-test, five employees of the municipality of Enschede, some who were also involved in the design of the campaign, checked the questionnaire from beginning to end. The employees who took part in the pre-test (N = 5) work in different teams within the municipality, namely in IT (n = 1), communications (n = 1), social support (n = 1), legal affairs (n = 1), and work and income (n = 1). Based on the feedback from these employees, the questionnaire had been adjusted. Adjustments that were made related to, for example, individual questions and the order of the question blocks. Also, the writing style in the introduction had been made less formal based on the feedback from the pre-test, as an informal writing style was considered more common within the municipality of Enschede. After the feedback of the first pre-test had been implemented, the questionnaire was checked again by the same group of respondents in order to review the questionnaire for one last time.

3.6. Measures

Within this study, the online survey method was used. In the survey, questions were asked aimed at measuring the variables present in the research model. A full overview of the items used, including the source the items were adapted from, can be found in appendix 1. First, perceived severity was measured within the survey. The items used were derived from earlier research of Workman et al. (2008) and Vance et al. (2012). An example of an item measuring perceived severity is *'It is very severe when someone accesses information of the municipality without permission'*. Regarding perceived vulnerability, these items were also based on literature (Herath & Rao, 2009; Ifinedo, 2012; Workman et al., 2008). One of the items used is *'I think there is a high chance that the information safety of the municipality will be in danger'*.

In addition, the items measuring the response efficacy variable were based on literature (Herath & Rao, 2009). An example of an item is *'I cannot do much on my own to protect information of the municipality'*. Regarding the response costs construct, research from Woon et al. (2005) and Workman et al. (2008) formed the basis. An item present in the survey, is as follows: *'Taking measures to protect information costs a lot of time'*. With regard to the self-efficacy items, based on research of Ifinedo (2012) and Workman et al. (2008), an example of an item is *'Taking measures to protect information is easy for me'*.

Moreover, the knowledge of expected behaviour construct was operationalized by means of a set of items. As a scale to measure this was not yet present in literature, this scale was created. An example of an item is *'I know what the municipality expects of me regarding protecting information'*. Regarding the attitude construct, an item scale is used that was based on research of Anderson and Agarwal (2010) and Ifinedo (2012). One of the items used within this scale is as follows: *'Taking measures to protect information is necessary'*. With regard to the injunctive norm item scale, based on literature (Herath & Rao, 2009; Ifinedo, 2014), an example of an item used is *'My colleagues think I should take measures to protect information'*. Regarding the descriptive norm construct, based on research of Herath and Rao (2009), one of the items used is as follows: *'I think that the majority of the employees takes measures to protect information'*. For all of the above-mentioned variables, a 7-point Likert scale was used, ranging from 'Totally disagree' to 'Totally agree'. This 7-point format was chosen as research has shown that, compared to a 3- and 5-point Likert scale, the uncertain or neutral responses are chosen less (Matell & Jacoby, 1971). Therefore, this could make the responses more accurate.

Furthermore, in the survey, safe email behaviour was operationalized by means of two items. These items were self-created, and related to being cautious in addressing emails and in adding attachments. An example of an item is *'Before I send an email, I check if I have directed it towards the right addressees'*. In addition, ten other statements were proposed aimed at measuring information security-related behaviours. The items used for this variable were self-created and based on the

information security policies of the municipality of Enschede, called *'Regels voor Veilig Werken'*. An example of such an item is *'When I leave my working space, I lock my computer'*. All items used within this scale relate to daily information security behaviour, so that all respondents could answer these questions. These items, relating to safe email behaviour and other information security-related behaviours, were measured by means of a 5-point Likert scale measuring the frequency of conducting the behaviours, ranging from 'Never' to 'Always'. The decision was made not to measure these questions on a 7-point Likert scale, as the independent variables, because of the understandability of answer options. Answer options like 'Almost never' would namely not make much sense.

3.7. Factor analysis

In order to see whether the items load on each other as expected, a factor analysis has been conducted. With a factor analysis, one can check if one variable can be separated into more variables based on factor loadings. To test this, the programme SPSS was used, following the method of principal component analysis, accompanied by a varimax rotation. Also, the decision was made to suppress coefficients lower than .4. As a result, the analysis distinguished between nine different factors, as could be seen by the eigenvalues higher than one. The results of the factor analysis can be found in table 3.2.

As can be seen, one of the items loads on two constructs. Therefore, this item needs to be excluded from further analyses. Also, both the self-efficacy construct and the knowledge of expected behaviour construct load heavily on each other. This might be explained by the fact that, combining these two constructs, can make sense. Making a knowledge and skills construct will namely encompass all needed prior experience that is necessary to conduct the right behaviours. Therefore, these two constructs will be merged into one construct, named 'knowledge and skills'.

As the self-efficacy and knowledge construct are now merged together, a new research model will be composed. Within this model, the earlier proposed hypotheses 5 and 9 will be fused into one new hypothesis. Based on the literature on self-efficacy and knowledge, it is expected that the higher the level of these knowledge and skills is, the more likely someone is to conduct safe email behaviour. Therefore, the hypothesis will be as follows:

H5 = Knowledge and skills positively influence safe email behaviour

Based on the newly formed hypothesis, the research model has been adjusted. The new version of the research model can be found in figure 3.1.

Table 3.2.
Factor analysis

	Factor								
	1	2	3	4	5	6	7	8	9
Safe email behaviour 1									.88
Safe email behaviour 2									.89
PS1			.81						
PS2			.88						
PS3			.86						
PV1							.71		
PV2							.88		
PV3							.88		
RC1					-.65				
RC2					-.76				
RC3					-.82				
A1		.79							
A2		.84							
A3		.86							
IN1				.87					
IN2				.87					
IN3				.73					
DN1						.83			
DN2						.78			
DN3						.64			
RE1								.59	
RE2								.74	
RE3								.66	
SE1*	.48				.54				
SE2	.69								
SE3	.67								
KEB1	.73								
KEB2	.77								
KEB3	.81								

Note. Perceived severity (PS), Perceived vulnerability (PV), Response costs (RC), Attitude, (A), Injunctive norm (IN), Descriptive norm (DN), Response efficacy (RE), Self-efficacy (SE), Knowledge of expected behaviour (KEB)
Note: Extraction method: Principal Components, Rotation Method: Varimax. Small coefficients under .40 were suppressed.
* This item is deleted because of overlapping factor loadings

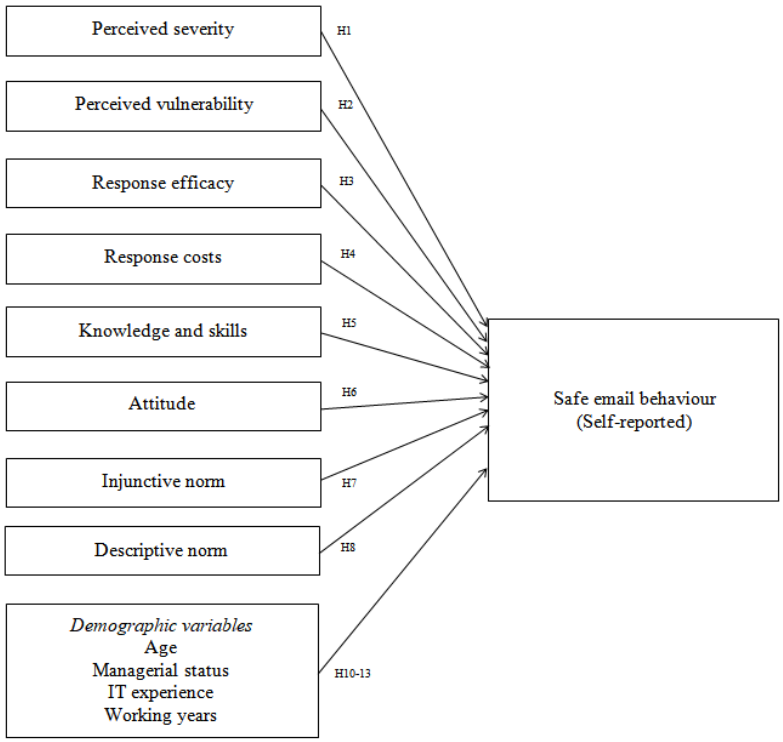


Figure 3.1. Research model safe email behaviour

3.8. Reliability analysis

Before any further analyses were made, the reliability per item scale was measured. In order to do this, the Cronbach's Alpha's of the separate constructs were calculated. An overview of these can be found in table 3.3. The Cronbach's Alpha represents the lower limit of the actual reliability (Van den Berg & Van der Kolk, 2014). Generally, a bottom line of .7 is used in literature (Nunally in Eltayeb, Zailani, & Ramayah, 2011).

Table 3.3.
Scale descriptives (N = 582)

	α	N-items	Mean	SD
Perceived severity	.87	3	6.53	.69
Perceived vulnerability	.77	3	4.45	1.23
Response efficacy	.56	3	5.55	.95
Response costs	.71	3	3.02	1.18
Knowledge and skills	.84	5	4.35	1.20
Attitude	.90	3	6.33	.72
Injunctive norm	.86	3	4.65	1.31
Descriptive norm	.79	3	4.93	1.00
Safe email behaviour	.79	2	4.49	.62

Note. The Cronbach's Alpha was calculated

As all of the Cronbach's Alpha's range between .71 and .90, this implies a sufficient reliability of the item scales. However, the Cronbach's Alpha of one of the constructs, response efficacy, seems insufficient (α = .56). Also, deleting variables within this construct did not raise the reliability of the scale. However, considering the relevance of this construct within the research, and considering the fact that the scale has been based on a validated scale from literature, the decision was made to include the construct in the upcoming analyses. Supporting this, literature also suggests that constructs with an alpha of at least .5 can be considered as reliable (Sproles & Kendall in Fan & Xiao, 1998). For a complete overview of the items present within the scales, appendix 1 can be consulted.

4. Results

Within this results section, an elaboration on the results regarding safe email behaviour will be provided first. In addition, in the second part of this section, attention will be paid to information security-related behaviours within the context of the municipality of Enschede.

Part I - Safe email behaviour

4.1. Descriptive statistics

First, an analysis was made in order to gain insight into the different items representing the eight independent variables within the research model. The results of this can be found in table 4.1. Within this table, it can be seen that the perceived severity regarding information security breaches is relatively high ($\mu = 6.53$). This means that, in general, employees seem to perceive the consequences of possible data leakages as quite harmful. However, the vulnerability of the municipality regarding these leakages is perceived much lower ($\mu = 4.45$). This implies that, however employees indicate that the consequences of security breaches are severe, they do not feel that the municipality is very vulnerable towards security threats.

Also, it can be seen that the response efficacy is rated moderately high ($\mu = 5.55$). This means that employees seem to believe that acting upon information security can make a difference. However, when looking at the knowledge and skills construct, this is more than one point lower ($\mu = 4.35$). So, however employees feel that taking action is effective, they do not always feel to have sufficient knowledge and skills themselves.

Table 4.1.
Antecedents of safe email behaviour (N=582)

	Mean	SD
Perceived severity	6.53	.68
Perceived vulnerability	4.45	1.23
Response efficacy	5.55	.95
Response costs	3.02	1.18
Knowledge and skills	4.35	1.20
Attitude	6.33	.72
Injunctive norm	4.65	1.31
Descriptive norm	4.93	1.00

Note. The items were measured by means of a 7-point Likert scale (Totally disagree/Totally agree)

Moreover, table 4.1. shows that the attitude of employees regarding information security behaviour is rather positive ($\mu = 6.33$). However, the norms regarding information security behaviour are not that high. The injunctive norm namely has a mean score of 4.65, and the descriptive norm a

mean score of 4.93. This seems to imply that employees feel the norm of taking action upon information security is not that strongly rooted in the organization. This could be partly explained by the fact that the knowledge of the expected behaviour as stated in the municipalities' policies, combined with the skills, is not optimal ($\mu = 4.35$). This knowledge might be improved by means of the campaign. Therefore, the above-mentioned results will be of great interest in the coming sections of this research as well.

Second, the dependent variable of email behaviour was further investigated. The results of this can be found in table 4.2. Within this table, it can be seen that employees seem to be relatively cautious when sending emails. The mean score is 4.49 out of five.

Table 4.2.
Safe email behaviour (N = 582)

	Mean	SD
Safe email behaviour	4.49	.62

Note. The items were measured by means of a 5-point Likert scale (Never/Always)

4.2. Test for multicollinearity

In order to test for multicollinearity, a Pearson correlation was conducted. This resulted in the correlations as presented in table 4.3. As can be seen, no highly correlated variables are present within the Pearson correlation analysis (Abrams, n.d.).

Table 4.3.
Correlation analysis

	BEH	PS	PV	RE	RC	A	IN	DN	KS
BEH									
PS	.16**								
PV	-.11**	.07							
RE	.14**	.27**	.01						
RC	-.22**	-.27**	.05	-.22**					
A	.21**	.48**	.10*	.33**	-.39**				
IN	.08	.17**	-.01	.28**	-.17**	.29**			
DN	.17**	.13*	-.17**	.22**	-.16**	.21**	.46**		
KS	.18**	.15**	-.11**	.31**	-.23**	.20**	.40**	.46**	

Note. A Pearson correlation analysis was conducted
Note. Safe email behaviour (BEH), Perceived severity (PS), Perceived vulnerability (PV), Response efficacy (RE), Response costs (RC), Attitude, (A), Injunctive norm (IN), Descriptive norm (DN), Knowledge and skills (KS)
** Correlation significant at the .01 level
* Correlation significant at the .05 level

Hereby, when regarding the Variance Inflation Factors of the variables within the regression model, all are under the value of 10, which is often used as a rule of thumb regarding checking for multicollinearity (O'brien, 2007). Also, the analysis shows a Durbin Watson value of 2.057 of the complete model, which indicates few to no autocorrelation within the regression model.

4.3. Regression analysis

4.3.1. Hierarchical regression

After the test for multicollinearity had been performed, a hierarchical regression analysis was conducted. This method of analyzing was chosen, as this enables to test several models and see whether adding variables significantly contributes to the model (Tabachnick & Fidell, 2001). Within this study, a three stage hierarchical regression was conducted with safe email behaviour as the dependent variable. The three steps were based on theoretical considerations (Tabachnick & Fidell, 2001). First, just the variables of the Protection Motivation Theory were added. Second the additional variables from the Theory of Planned Behaviour were added, and last the demographic variables. A summary of the outcomes of the hierarchical regression analysis can be found in table 4.4.

Table 4.4.
Summary of hierarchical regression analysis for variables predicting safe email behaviour

Variable	B	Std. error	Beta	t	R	R^2	ΔR^2
Step 1					.29	.08	.08
Perceived severity	.09	.04	.10	2.29**			
Perceived vulnerability	-.05	.02	-.10	-2.40**			
Response efficacy	.03	.03	.05	1.08			
Response costs	-.08	.02	-.15	-3.59***			
Knowledge and skills	.05	.02	.10	2.42**			
Step 2					.31	.10	.01
Perceived severity	.05	.04	.06	1.27			
Perceived vulnerability	-.05	.02	-.09	-2.30**			
Response efficacy	.02	.03	.03	.72			
Response costs	-.07	.02	-.12	-2.81***			
Knowledge and skills	.04	.02	.09	1.82*			
Attitude	.10	.04	.11	2.28**			
Injunctive norm	-.03	.02	-.07	-1.44			
Descriptive norm	.05	.03	.09	1.76*			
Step 3					.35	.12	.02
Perceived severity	.05	.04	.05	1.14			
Perceived vulnerability	-.05	.02	-.10	-2.39**			
Response efficacy	.02	.03	.03	.56			
Response costs	-.06	.02	-.11	-2.53**			
Knowledge and skills	.04	.02	.08	1.67*			
Attitude	.08	.04	.10	1.94*			
Injunctive norm	-.03	.02	-.07	-1.42			
Descriptive norm	.05	.03	.08	1.69*			
Age	.08	.03	.16	3.16***			
Working years	-.01	.03	-.02	-.36			
Managerial status	-.05	.08	-.02	-.57			
IT experience	.02	.02	.05	1.11			

Note. A hierarchical multiple regression analysis was conducted. Dependent variable: safe email behaviour
* Significant at the .1 level
** Significant at the .05 level
*** Significant at the .01 level

Based on the results of the hierarchical regression analysis, it can be seen that step 1, the variables of the Protection Motivation Theory, contribute significantly to the model ($F(5,576) = 10.62$, $p = .00$), with a variance value of 8%. When including the variables of the Theory of Planned Behaviour in step 2, these explain a significant additional variance of 1% ($F(8,573) = 7.81$, $p = .00$). Last, regarding step 3 in which the demographical variables were added, an additional variance of 2% was found. Also, this change in R^2 prove to be significant ($F(12,569) = 6.62$, $p = .00$).

When all the variables are included in the model, as could be seen within step 3, not all of these variables were significant. However, six of the variables were significant influencers of safe email behaviour. First, perceived vulnerability regarding information safety ($t = -2.39$, $p = .02$). However, the found relationship is negative, thus not as hypothesized. Second is response costs, which also holds a negative influence on email behaviour ($t = -2.53$, $p = .01$). Unlike perceived vulnerability, this relationship is as hypothesized. Third, knowledge and skills turned out to be of significant positive influence on safe email behaviour ($t = 1.67$, $p < .1$). This means that the more knowledge and skills one possesses regarding information security behaviour, the more likely one is to perform safe email behaviour.

Next, the analysis shows that attitude has a significant positive influence on email behaviour ($t = 1.94$, $p = .05$). This implies that the more positive one's attitude is towards information safety, the more likely this person is to conduct safe email behaviour. In addition, the descriptive norm variable has proven to be of significant positive influence on email behaviour ($t = 1.69$, $p = .09$). This means that the more positive the descriptive norm towards information security is, the more likely one is to perform safe email behaviour. Last, one of the demographic variables shows to have a significant positive relationship with safe email behaviour, namely age ($t = 3.16$, $p = .00$). This result implies that the older an employee is, the more likely he or she is to perform safe email behaviour. To conclude, the variables within the model together account for 12% of the variance in email behaviour.

4.3.2. Demographic variables

In order to have a closer look at differences in email behaviour between groups of employees, additional analyses were conducted. First, it is tested whether significant differences exist in the following variable: Age (see table 4.5.). By means of a One-way ANOVA-analysis, it is investigated whether differences in safe email behaviour exists with regard to age. The results showed that the group of 18 to 30 years old ($\mu = 4.32$) scores significantly lower on behaviour than the group of employees over 60 years old ($\mu = 4.70$, $p = .00$). Also, the group of employees between 31 and 40 ($\mu = 4.33$) scores significantly lower on safe email behaviour than the group of employees between 41 and 50 ($\mu = 4.53$, $p = .08$), and lower than employees over 60 years old ($\mu = 4.70$, $p = .00$). In addition, employees between 31 and 40 score significantly lower on safe email behaviour than employees between 51 and 60 ($\mu = 4.52$, $p = .08$).

Table 4.5.
ANOVA age

	Mean	SD	n
18-30[a]	4.32	.60	60
31-40[a]	4.33	.72	105
41-50[a]	4.53	.59	152
51-60[a]	4.52	.60	181
60 years or older[a]	4.70	.48	84

Note. A One-way ANOVA-analysis was conducted, Bonferroni.
[a] Significant results at the .1 level

Moreover, an ANOVA-analysis was performed in order to see whether differences exist in working years (see table 4.6.). The results indicate that one significant difference exists in behaviour regarding working years at the municipality of Enschede. It can namely be seen that people who work 5 years or shorter at the municipality ($\mu = 4.38$) score significantly lower on behaviour than employees who work at the municipality longer than 20 years ($\mu = 4.55$, $p = .09$). Other differences in working years were not found.

Table 4.6.
ANOVA working years

	Mean	SD	n
5 years or shorter[a]	4.38	.64	151
6-10	4.56	.58	100
11-20	4.51	.59	169
longer than 20 years[a]	4.55	.63	162

Note. A One-way ANOVA-analysis was conducted, Bonferroni.
[a] Significant results at the .1 level

Also, the influence of managerial status on information security was measured by means of an Independent Sample T-test. However, this T-test showed no significant differences. On the other hand, regarding the variable of IT experience, significant differences were found (see table 4.7.). Based on the analysis, it could be seen that the minimum score on IT experience was a 3, whereas the maximum score was a 10 (median = 8.50). Using the median-split method, it was tested whether people who scored themselves a 7 or lower (n = 98), score significantly different compared to people scoring an 8 or higher (n = 484). This analysis indicated a significant difference, in which employees with a higher score on IT experience ($\mu = 4.09$) score significantly better on safe email behaviour than their colleagues with a lower score on IT experience ($\mu = 3.79$, $p = .02$). Thus, it can be concluded that the scores on safe email behaviour differ regarding age, working years and IT experience.

Table 4.7.
T-test IT experience

	Mean	SD	n
7 or lower	3.79	.55	98
8 or higher	4.09	.45	484

Note. An Independent Sample T-test was conducted. Test variable safe email behaviour

4.4. Hypotheses

Regarding the hypotheses, some can be supported, whereas some cannot. Table 4.8. gives an overview of the hypotheses. As can be seen, hypothesis 4, 5, 6, 8 and 10 could be accepted. A significant negative relationship namely was found between response cost and email behaviour, and significant positive relationships could be found between knowledge and skills, attitude, descriptive norm, age and the dependent variable of safe email behaviour. On the other hand, no support could be found for hypothesis 1, 2, 3, 7, 11, 12 and 13. Still, regarding hypothesis 2, a significant effect was found. However, this effect was opposite than expected, namely negative instead of positive. An overview of the research model, including the values of β and R^2, can be found in figure 4.1.

Table 4.8.
Hypotheses

Hypothesis	Relationship	Supported or not
H1	Perceived severity --> Safe email behaviour	Not supported
H2*	Perceived vulnerability --> Safe email behaviour	Not supported
H3	Response efficacy --> Safe email behaviour	Not supported
H4	Response cost --> Safe email behaviour	Supported
H5	Knowledge and skills --> Safe email behaviour	Supported
H6	Attitude --> Safe email behaviour	Supported
H7	Injunctive norm --> Safe email behaviour	Not supported
H8	Descriptive norm --> Safe email behaviour	Supported
H10	Age --> Safe email behaviour	Supported
H11	Working years --> Safe email behaviour	Not supported
H12	Managerial status --> Safe email behaviour	Not supported
H13	IT experience --> Safe email behaviour	Not supported

* A significant negative relationship was found

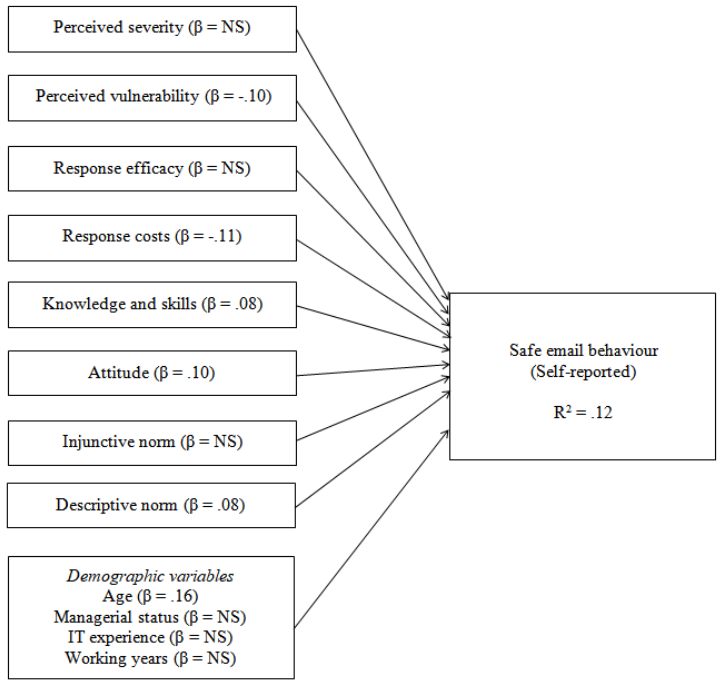


Figure 4.1. Research model safe email behaviour

Part II - Information security-related behaviours

4.5. Information security behaviour

In the light of the campaign, it is also interesting to look at the separate items that relate to information security behaviour. Insight into this can namely be helpful in advising on the focus of the campaign. In table 4.9., it can be seen that some of the behaviours are done more frequently than others.

Table 4.9.
Information security related behaviours (N = 582)

	Mean	SD
When I leave my working space, I lock my computer	3.57	1.45
Before I send an email, I check if I have added the right attachments	4.47	.71
Before I send an email, I check if I have directed it towards the right addressees	4.52	.65
In order to remember by passwords, I write them down (offline)	2.32	1.58
When I want to work from home, I send the files I need to my private email account	1.28	.67
When I am being called and I do not trust the caller, I will break the phone connection	3.42	1.53
I am cautious of whether unauthorized people walk around in my department	3.24	1.24
I use public WiFi connections (for example in the train or in shops/restaurants) when I am busy with my work	1.57	.90
I make sure my mobile phone is secured with a password/code	4.94	.36
Before I use an internet site, I check if it is a reliable connection (for example by looking at the green lock/at https)	3.01	1.36
If I receive an email from an unknown sender, I click on links and attachments to see what it is about	1.44	.88
I make sure that the system I am working on has an up-to-date virus scanner	3.96	1.28

Note. The items were asked in Dutch on a 5-point Likert scale (Never/Always)
Note. The reverse asked items are shown as the original items

For example, on securing phones with codes or passwords, the mean score is 4.94 out of 5. Within this item, 560 employees said to always conduct this behaviour. However, on the question if employees pay attention to unauthorized persons on their department, the mean score is only 3.24 out of 5. Thereby, only 112 employees said to always do this, which means that 470 employees do not always pay attention to unauthorized persons within the municipality. Also, the descriptive statistics show that 369 of the respondents do not always lock their computer screen when leaving their workspace. Still, 357 of the respondents say to do this often or always. Another striking result is that 108 respondents say to write down their passwords in order to remember them, which is a possible risk to information safety. In addition, only 88 of the respondents say to always check if a website is reliable before using it. With regard to working at home, 465 of the respondents never send files to their private email address, thus the majority of the employees seems to work safely in this manner. This also holds true for opening files and clicking on links from unknown emails. Of the respondents, 416 employees say to never do this. However, this still implies that 166 of the respondents sometimes

do open files or click on links in emails from unknown senders. A more detailed overview of the provided answers, including graphic pie-chart representations, can be found in appendix 3.

The results regarding the other items within the research, namely the items representing the independent variables, can be found in table 4.1. at the beginning of this chapter. Also, an explanation regarding these results can be found there.

4.6. Differences between departments

As the information security awareness campaign will be implemented per department, it is interesting to investigate differences in behaviour between departments. Hereby, the relative position of the six largest departments regarding sample size will be researched by means of dummy variables, namely Group staff (CS), Business and Management Support (BMO), Program Service (DV), Program Social Support (MO), Program Economy, Work and Education (EWO), and Domain Physical (DF). Within these analyses, Independent Sample T-tests were conducted. The results will be provided per department. An overview of the full results regarding the T-tests can be found in appendix 4. Furthermore, the mean scores per department on the different information security-related behaviours can be found in table 4.10.

Table 4.10.
Mean scores per department on information security-related behaviours

	CS	BMO	DV	MO	EWO	DF
When I leave my working space, I lock my computer	3.90	3.93	3.77	3.28	3.62	3.06
Before I send an email, I check if I have added the right attachments	4.58	4.49	4.58	4.46	4.40	4.46
Before I send an email, I check if I have directed it towards the right addressees	4.63	4.60	4.65	4.54	4.41	4.49
In order to remember by passwords, I write them down (offline)	2.45	1.89	2.65	2.64	2.68	2.20
When I want to work from home, I send the files I need to my private email account	1.25	1.31	1.35	1.19	1.32	1.22
When I am being called and I do not trust the caller, I will break the phone connection	3.45	3.67	3.42	3.11	3.50	3.19
I am cautious of whether unauthorized people walk around in my department	3.78	3.46	3.48	3.06	3.18	2.96
I use public WiFi connections (for example in the train or in shops/restaurants) when I am busy with my work	2.00	1.50	1.26	1.44	1.42	1.82
I make sure my mobile phone is secured with a password/code	5.00	4.90	4.97	4.99	4.99	4.87
Before I use an internet site, I check if it is a reliable connection (for example by looking at the green lock/at https)	3.03	3.35	3.03	2.83	2.79	2.86
If I receive an email from an unknown sender, I click on links and attachments to see what it is about	1.43	1.30	1.61	1.44	1.59	1.45
I make sure that the system I am working on has an up-to-date virus scanner	4.28	4.20	3.84	3.59	3.92	3.84

Note. The items were asked in Dutch on a 5-point Likert scale (Never/Always)
Note. CS = Group staff, BMO = Business and Management Support, DV = Program Service, MO = Program Social Support, EWO = Program Economy, Work and Education, DF = Domain Physical

4.6.1. Group staff

First, within the department Group staff (n = 40), significant differences could be found in two types of behaviours. First, the analysis showed that employees from the department Group staff are significantly more alert on unauthorized persons on their floor (μ = 3.78) than employees from other departments (μ = 3.20, p = .01). However, the analysis also showed that employees from the department Group staff make significantly higher use of public WiFi networks when being busy with work (μ = 2.00) than their colleagues from other departments (μ = 1.54, p = .00).

4.6.2. Business and Management Support

Second, within the department Business and Management Support, (n = 178) significant differences could be found regarding eight different behaviours. These results indicate that this department works relatively safe as compared to the other departments, First, the analysis showed that employees of the department Business and Management Support are significantly more likely to lock their system when leaving their workspace (μ = 3.93) than employees from other departments (μ = 3.40, p = .00). Second, employees from this department are more likely to check whether they addressed their emails correctly (μ = 4.60) than the other departments (μ = 4.49, p = .08). In addition, the analysis showed that employees of the department Business and Management Support act more safely regarding passwords, as these employees are less likely to write down their passwords (μ = 1.89) than their colleagues from other departments (μ = 2.52, p = .00). Moreover, regarding safe phone usage, employees from this department are more likely to end the connection if they do not trust the caller (μ = 3.67) as compared to employees from other departments within the municipality of Enschede (μ = 3.31, p = .01).

In addition, the analysis showed that employees from the department Business and Management Support are more alert on unauthorized persons on their floor (μ = 3.46) than employees from other departments (μ = 3.15, p = .01). Also, regarding internet usage, employees from this department are more likely to check the reliability of a website before using it (μ = 3.35), as compared to other departments (μ = 2.85, p = .00). Next, when receiving emails, employees of the department Business and Management Support tend to act safer. The analysis namely indicated that these employees are less likely to click on links or attachments in emails from unknown senders (μ = 1.30) than other employees within the municipality (μ = 1.50, p = .00). Last, regarding virus scanners, employees from this department tend to be more aware of having an up-to-date virus scanner on their system (μ = 4.20) than their colleagues from other departments (μ = 3.85, p = .00) .

4.6.3. Program Service

Third, the department Program Service (n = 31) was further investigated. Hereby, one significant difference in behaviour was found. This significant difference related to the usage of public WiFi connections when being busy with work-related tasks. The analysis namely showed that employees

from the department Program Service are significantly less likely to use these public connections (μ = 1.26) than their colleagues from other departments within the municipality of Enschede (μ = 1.59, p = .05).

4.6.4. Program Social Support

Fourth, the information security-related behaviours were further investigated within the department Program Social Support (*n* = 81). Hereby, significant differences could be found in four of the behaviours. First, it could be seen that employees of the department Program Social Support are significantly less likely to lock their system when leaving their workspace (μ = 3.28), as compared to employees from the other departments within the municipality (μ = 3.61, p = .06). In addition, employees of this department are more likely to write down their passwords (μ = 2.64) than other departments (μ = 2.27, p = .05), thus act less safe regarding this behaviour. Also, regarding phone usage, employees of the department Program Social Support are less likely to end the connection in the case of an unreliable caller (μ = 3.11) than employees of other departments (μ = 3.47, p = .05). Last, with regard to virus scanners, employees from this department are significantly less aware of using an up-to-date virus scanner on their system (μ = 3.59), as compared to their colleagues from other departments within the municipality of Enschede (μ = 4.01, p = .01).

4.6.5. Program Economy, Work and Education

Fifth, the department Program Economy, Work and Education (*n* = 133) was further investigated. Hereby, it could be seen that employees from this department are significantly less likely to check the addressees of an email before sending it (μ = 4.41), as compared to employees from other departments within the municipality (μ = 4.56, p = .02). Furthermore, regarding writing down passwords, employees of the department Program Economy, Work and Education are significantly more likely to do this (μ = 2.68) than colleagues from other departments (μ = 2.22, p = .00).

In addition, regarding the usage of public WiFi connections, the analysis showed that employees from this department are less likely to use these public connections (μ = 1.42) than their colleagues from other departments within the municipality (μ = 1.61, p = .03). Moreover, employees of this department are significantly more likely to secure their phone with a password (μ = 4.99) than other employees (μ = 4.92, p = .05). Next, regarding internet usage, employees of the department Program Economy, Work and Education are less likely to check the reliability of the connection before using a website (μ = 2.79), as compared to employees from other departments (μ = 3.07, p = .04). Last, regarding receiving emails, employees of this department are significantly more likely to click on links and attachments in emails from unknown senders (μ = 1.59) than their colleagues from other departments within the municipality of Enschede (μ = 1.40, p = .03).

4.6.6. Domain Physical

Last, behaviours within the department Domain Physical (n = 125) have been further investigated. Hereby, significant differences could be found in five types of behaviours. First, regarding locking the system when leaving the workspace, employees of this department are significantly less likely to perform this safe behaviour (μ = 3.06), as compared to other employees (μ = 3.70, p = .00). In addition, regarding safe phone usage, employees within the department Domain Physical tend to be less likely to end the connection in the case of an unreliable caller (μ = 3.19), compared to employees from other departments (μ = 3.48, p = .06). Furthermore, the analysis showed that employees from this department are less alert on unauthorized persons walking around on their floor (μ = 2.96) than other employees (μ = 3.32, p = .00). Moreover, regarding the use of public WiFi connections, employees from the department Domain Physical are significantly more likely to use these connections (μ = 1.82) than employees from other departments within the municipality of Enschede (μ = 1.50, p = .04). Last, regarding securing phones with a password, employees of this department are less likely to do so (μ = 4.87), as compared to their colleagues from other departments (μ = 4.96, p = .03).

4.7. Differences in IT experience

Last, based on the gathered data, it was investigated whether further helpful insights could be found. Hereby, the independent variable of IT experience was investigated, as prior research indicated that this variable might influence behaviour in the information security context. As IT experience is a skill that could be increased by means of training, or by means of providing tips within a campaign, it is helpful to investigate this. Therefore, with an Independent Sample T-test, it was examined whether employees with a lower IT experience (7 or lower, n = 98) score significantly different on the behaviours than employees with a higher IT experience (8 or higher, n = 484). The mean scores per behaviour, per level of IT experience, can be found in table 4.11.

The analysis indicated significant results on nine of the twelve behaviours tested. First, employees with a higher score on IT experience (μ = 3.71), score significantly higher than employees with a lower score (μ = 2.84, p = .00), regarding locking a system when leaving the workspace. Second, with regard to email behaviour, employees with a higher score on IT experience significantly check if they added the right attachments (μ = 4.49) and the right addressees (μ = 4.55) more often than employees with a lower score on IT experience (μ = 4.34, p = .05 and μ = 4.40, p = .03). Also, a significant difference can be found in password safety. The analysis namely showed that employees with higher score on IT experience are significantly less likely to write down their passwords (μ = 2.17) than employees with a lower score on IT experience (μ = 3.09, p = .00).

Table 4.11.
Mean scores per level of IT experience on information security-related behaviours

	7 or lower	8 or higher
When I leave my working space, I lock my computer	2.84	3.71
Before I send an email, I check if I have added the right attachments	4.34	4.49
Before I send an email, I check if I have directed it towards the right addressees	4.40	4.55
In order to remember by passwords, I write them down (offline)	3.09	2.17
When I want to work from home, I send the files I need to my private email account	1.48	1.24
When I am being called and I do not trust the caller, I will break the phone connection	3.18	3.47
I am cautious of whether unauthorized people walk around in my department	3.07	3.28
I use public WiFi connections (for example in the train or in shops/restaurants) when I am busy with my work	1.49	1.59
I make sure my mobile phone is secured with a password/code	4.88	4.95
Before I use an internet site, I check if it is a reliable connection (for example by looking at the green lock/at https)	2.77	3.05
If I receive an email from an unknown sender, I click on links and attachments to see what it is about	1.67	1.39
I make sure that the system I am working on has an up-to-date virus scanner	3.78	3.99

Note. The items were asked in Dutch on a 5-point Likert scale (Never/Always)

Furthermore, regarding working from home, employees with a higher score on IT experience significantly less often send files to their private email address ($\mu = 1.24$) than employees with a lower score on IT experience ($\mu = 1.48$, $p = .00$). Next, with regard to phone usage, employees with a higher score on IT experience tend to end the connection with an unreliable caller significantly more often ($\mu = 3.47$) than their colleagues with a lower score on IT experience ($\mu = 3.18$, $p = .09$). In addition, employees with a greater experience in IT are more likely to secure their phones with a password ($\mu = 4.95$) than less experienced employees in the field of IT ($\mu = 4.88$, $p = .07$). Moreover, employees with a higher score on IT experience significantly more often check the reliability of a website before using it ($\mu = 3.05$), as compared to employees with a lower score on IT experience ($\mu = 2.77$, $p = .06$). Last, with regard to receiving emails from unknown senders, the analysis showed that employees with a higher score on IT experience significantly less often click on attachments and links ($\mu = 1.39$) than their colleagues at the municipality with a lower score on IT experience ($\mu = 1.67$, $p = .00$). An overview of the full results of the T-test regarding IT experience can be found in appendix 5.

5. Discussion

5.1. Discussion of the results

Within this research, a combined model of the Theory of Planned Behaviour and the Protection Motivation Theory was used in order to gain insight into safe email behaviour within the context of the municipality of Enschede. The results showed that the variables of response costs, knowledge and skills, attitude, descriptive norm and age are of significant influence on the dependent variable of safe email behaviour. Thus, five of the hypothesized relationships could be supported based on the analysis of the data (see Table 4.9). However, the results could not confirm the other seven hypothesized relationships. First, no support could be found for the effects of perceived severity on safe email behaviour (see 4.3). This is striking, as the descriptive statistics do show that the perceived severity regarding information security breaches is rather high (Table 4.1.). Still, within earlier research in the context of information security compliance, the effect of this variable could also not be supported by Ifinedo (2012). Within this research, it was stated that the missing significance could have been caused by a missing relationship of this variable with the subject matter. It could hold true that perceived severity has no influence in the context of safe email behaviour as well. However, as this cannot be stated with certainty, additional research is needed in order to further investigate the variable of perceived severity.

Also, the positive relationship between response efficacy and safe email behaviour could not be supported (see 4.3). The analyses, however, did indicate that employees in general feel that acting upon information safety is effective (Table 4.1.). Still, an effect could not be found. This might be explained by a missing relationship as well. However, this is inconsistent with earlier findings regarding the Protection Motivation Theory. Still, as this variable was not tested before in the context of safe email behaviour in particular, it could hold true that no relationship exists within this particular field of study within information security. Also, the lack of a significant relationship might be explained by the translation of the items, as the reliability analysis also indicated a low Cronbach's Alpha of this construct (see page 25).

Furthermore, a significant influence of injunctive norm on email behaviour could not be supported (see 4.3). This is a result that is unexpected, based on the accompanying hypothesis. It could hold true that, within the context of email behaviour, employees might find it more important what their colleagues actually do, measured by the descriptive norm, rather than what they think that should be done, measured by means of the injunctive norm. Most employees might namely know that they are the ones who should be cautious with regard to information safety. The feeling that their colleagues, however, are not cautious themselves, might keep them from acting upon it. However, this should be

investigated further within the context of safe email behaviour in order to be able to make a statement about this.

In addition, one of the variables tested showed a relationship opposite than expected, namely the variable of perceived vulnerability (see 4.3). According to the results, it holds true that the higher the perceived vulnerability is, the less likely employees are to conduct safe email behaviour. However this relationship has not been found in literature, an explanation could be provided for this result. First, it could be caused by the translation of the items. Second, if employees believe that the vulnerability of the municipality is already too high, than they might also believe that acting safely will not contribute much anymore to the information safety of the municipality. On the other hand, earlier research also did not always find an effect of perceived vulnerability within the information security context. Research of Woon et al. (2005), for example, did not find an effect of this variable on the installation of virus scanners, and stated a lack of relationship with the subject matter could be accountable for this. Also, Vance et al. (2010) could not find an effect of this variable on the intention to comply with information security policies. Therefore, this variable needs to be further investigated within the context of safe email behaviour as well.

Regarding the demographic variables, it could be seen that age significantly influences safe email behaviour (see 4.3). Hereby, it holds true that the older an employee is, the more safely he or she behaves (see 4.3.2). No significant effects were found regarding the other demographic variables. This is somewhat unexpected, as the ANOVA-analyses and Independent Sample T-tests that were conducted did, besides age, indicate significant differences in safe email behaviour among employees with different working years (Table 4.6.) and IT experiences (Table 4.7). A possible explanation for the lack of a significant relationship between working years at the municipality and safe email behaviour could be found in the fact that being cautious in sending emails is important in every organization. Therefore, employees who do not work at the municipality that long, but who do have experience in other professional settings, might already know that conducting this behaviour is important. This could also be a support for why the regression analysis did indicate a significant effect of the variable of age, but not for working years. In addition, regarding IT experience, it could hold true that this experience is not especially needed within this research context, as anyone should be able to check if the right addressees or attachments are added to an email. However, as not much research has been done into this, additional research will be helpful in further investigating the influence of demographic variables in the context of safe email behaviour.

Furthermore, while this research explored the application of both the Theory of Planned Behaviour and the Protection Motivation Theory, the analyses show that the variance value of the independent variables is only 12% (Table 4.4.). This means that over 80% of the dependent variable of safe email behaviour could not be predicted based on the variables proposed in the model. Therefore, additional research is needed in order to investigate other variables that might influence safe email behaviour.

Last, within the second part of this research, information security behaviour was further investigated (see 4.5). Hereby, some interesting results arose regarding information security within the municipality. In the light of the upcoming campaign, these results might serve as guidelines in order to optimize the contents of the campaign. Also, as differences between departments are investigated as well, the campaign could be adapted to the needs within the several departments (see 4.6). In addition, differences in IT experience regarding information security-related behaviours were examined (see 4.7). As the analysis showed that employees with a better score on IT experience tend to behave safer in many situations, this underlines the relevance of having a good experience in handling computers. Therefore, the input of the second part of this research will be of great relevance in optimizing the information safety campaign of the municipality of Enschede.

5.2. Implications for theory

This research can offer relevant implications for research into safe email behaviour and information security behaviour. First, based on the factor analysis, a validated model could be constitued, including both the Protection Motivation Theory as well as the Theory of Planned Behaviour. The hierarchical regression analysis thereby showed that merging both theories together significantly contributes to the variance value of the model. However, as stated before, the variance value of the model was only 12%. Thus, additional research is needed in order to test other variables that might be relevant within the context of safe email behaviour. For example, the effects of organizational context variables, such as the influence of perceived organizational support or security culture (Eisenberger, Huntington, Hutchison, & Sowa, 1986; Greene & D'Arcy, 2010; Rhoades & Eisenberger, 2002) or personality factors could be applied within this research context.

Another contribution of this research relates to adding the organizational context variable of knowledge of expected behaviour. By means of including this variable into the research model, it has been shown how this variable, combined with self-efficacy, can be of great help as well in explaining behaviour. This implies that the organizational context could be a significant contributor in the context of safe email behaviour, thus underlining the relevance of having investigated this within this study.

In addition, as the Theory of Planned Behaviour has been extended by splitting the subjective norm variable into two separate constructs, as was done before within research of Anderson and Agarwal (2010) and Herath and Rao (2009) in the context of information safety, a further dimension was added to the research. Having found a significant relationship of descriptive norm, but not of the injunctive norm, within the context of safe email behaviour, this underlines the relevance of having made this decision. Last, as several demographic variables have been tested within this research as well, this broadens the scope of the study.

Overall, this research provides a great starting point for further research within the context of safe email behaviour, as not much research has been done so far into this topic. Also, in applying the Protection Motivation Theory and the Theory of Planned Behaviour to the specific context of safe email behaviour, an application that was not prominent in literature yet, valuable results could be gathered. In addition, as this research is the first to address safe email behaviour within the context of a municipality, the novelty of this research can be underlined.

5.3. Implications for practice

Besides theoretical implications, this research provides helpful insights for practice as well. First, the insights coming from the first part of the research, regarding safe email behaviour, can be of great help for campaign practitioners or information security experts in understanding individual email behaviour at the workplace. Also, the second part of this research can specifically be of great help to the municipality of Enschede in designing and optimizing their internal awareness campaign regarding information safety. As interesting insights namely were provided regarding information security-related behaviours, the contents of the campaign can be tailored to the specific needs of the organization.

First, the analyses showed how employees of the municipality score on the different information-security related behaviours. Here, it could be seen that some of the variables still need much attention. For example, the results showed that many employees tend to write down passwords, despite the security risks of this behaviour. In addition, many employees do not always lock their system when leaving their workspace. Insights into these behaviours can assist the municipality in designing the contents of the campaign, and in deciding on the most important topics to focus on.

Also, regarding the independent variables, some interesting implications can be pointed out. First, while employees perceive the consequences of possible data leakages as severe, the vulnerability of the municipality towards information security threats is perceived much lower. As this might keep employees from acting safely, this is important to address within the campaign. Also, the results show that employees do not always have sufficient knowledge and skills regarding taking information security measures. Thus, the campaign should aim at communicating the existing rules on information safety, as well as educating employees. Last, while the attitude towards information safety is considered as positive, both the injunctive norm and descriptive norm scores are not that high. This means that the organizational norms regarding information safety might not be strongly rooted within the municipality yet. Hereby, the campaign could play a critical role if it is communicated that everyone within the organization should contribute to securing the information safety of the municipality of Enschede.

Moreover, as the results of this research gave insights into differences between departments of the municipality of Enschede as well, this can guide the project team responsible for the campaign in designing the kick-off meetings for the different departments. Based on the results, it can namely be seen that some behaviours need more attention than others in some of the departments. For example, the analysis showed that the department of Business and Management Support seems to score relatively well on the information security-related behaviours, whereas in several other departments more room for improvement exists. When considering this, the effectiveness of the campaign might be enhanced, thus resulting in a more information security aware organization.

Furthermore, as the analysis indicated different scores on the information security-related behaviours among employees with different IT experiences, this underlines the relevance of training and educating employees in how to operate a computer. As employees with a lower score on IT experience namely scored worse on most of the behaviours, training them, or providing them with tips by means of the campaign, seems extremely relevant.

Last, the insights coming from this research might be of help for other municipalities or public organizations as well, as the municipality of Enschede formed the context of research. The results of this research can then be of use in designing and implementing campaigns regarding safe email behaviour or, more general, information security behaviour.

5.4. Limitations and suggestions for future research

Although this study provides helpful insights into the context of information security behaviour, some limitations can be addressed. First, although an attempt was made to prevent this, it could be possible that respondents were inclined to answer the questions in a socially desired manner (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). This implicates that some of the respondents might not have answered the questions based on reality, but rather based on a want to presenting oneself favourably. This might have implications for the gathered data. In addition, although explained within the survey, it could hold true that the respondents interpreted the contents of 'information' differently, which might have impacted the results.

Furthermore, within this study, a large amount of responses (N = 582) was gathered (see Table 3.1.). This is beneficial for the quality of the results. However, as the research was conducted in the context of one organization, this could have implications for the generalizability of the results. Therefore, future research in the context of other organizations is needed in order to support the results that have been found. Also, as the research has been designed to measure the respondents opinions on information security in general, the first part of this research might have been improved if the items measuring the independent variables related specifically to safe email behaviour. Therefore, it could hold true that the items did not represent precisely what needed to be measured, thus, the content

validity of this research might be improved if the items are slightly changed to the context of safe email behaviour (Van den Berg & Van der Kolk, 2014; Yang, 2011). However, as using these items was not possible within this research context, future research should aim at further investigating this.

In addition, as the variable of perceived vulnerability gave unexpected results within this study (see 4.3), this could form the subject of future research. Future research could aim at investigating the reasons for a possible negative relationship between perceived vulnerability and safe email behaviour. Insights into this might provide more clarity to the application of the Protection Motivation Theory in the context of safe email behaviour, thus, making it a valuable subject for future research. Also, future research might aim at investigating the other variables from the Protection Motivation Theory and the Theory of Planned Behaviour, of which the relationships with safe email behaviour could not be supported based on this research, namely perceived severity, response efficacy and the injunctive norm. Furthermore, as the variance value of the model was only 12%, future research should investigate which other variables might be of interest, such as personality variables or organizational context variables.

Last, an aim of this research was to give insight into information security behaviour in order to optimize the awareness campaign of the municipality of Enschede. Research of Mamonov and Benbunan-Fich (2018) indicated an effect of awareness on behaviour in the information security context. However, further research should examine whether the awareness campaign actually has an effect on the behaviour of the employees.

6. Conclusions and recommendations

With this research, a study was designed to provide further insights into safe email behaviour by means of combining the Protection Motivation Theory and the Theory of Planned Behaviour. Regarding safe email behaviour, important insights can be derived from the results. Because the constructs of response costs, knowledge and skills, attitude and descriptive norm proved to influence safe email behaviour among employees, it could be important to address these constructs in communication or campaigns on safe email behaviour.

In improving information security in organizations, many researchers investigated or acknowledged the need of training and awareness programs (Bulgurcu, et al., 2010; Cox, 2012; Ng et al., 2008; Posey et al., 2015; Vance et al., 2012). Also, empirical research has shown that awareness could have a positive effect on protective behaviour in the information security context (Mamonov & Benbunan-Fich, 2018). Regarding the construct of response costs within the Protection Motivation Theory, awareness might be created if one could make clear that acting safely will not cost much time, money or effort (Sommestad et al., 2015). The campaign of the municipality of Enschede should also cover this aspect. For example, it can be noted that it does not have to take too much effort to safeguard personal data. Just being cautious when sending emails, for example, can already be helpful. Regarding the combined knowledge and skills construct, the campaign should also explain employees what to do, so that these employees will feel secure in performing information security behaviours, such as safe email behaviour. Supporting this, research of Bulgurcu et al. (2010) showed that self-efficacy can be improved by means of informing employees on what to do. Besides, it is expected that creating awareness towards how to act in a given situation can positively influence employees' knowledge on what to do. Also, in the campaign, the expected behaviour needs to be communicated prominently, as clear guidelines regarding information safety might improve knowledge as well.

Taking into account the Theory of Planned Behaviour, Bulgurcu et al. (2010) also stated that creating information safety awareness directly influences an individual's attitude towards the behaviour. Within the campaign, it could also be tried to keep this attitude positive, by means of stating the importance of information safety. In addition, the awareness campaign of the municipality of Enschede should aim at setting the norm of behaving safely with information. Therefore, the campaign can, as a result, also influence the perceived social influence variables. The relevance of this can be supported by research of Nolan, Schultz, Cialdini, Goldstein and Griskevicius (2008) who state that communicating how individuals should act in a given situation, i.e. the descriptive norm, could positively influence behaviour. Still, besides these variables, the variables that did not indicate a significant relationship with safe email behaviour, within the first part of this research, should be further investigated in order to examine their role within the context of safe email usage.

Second, it has been investigated how employees of the municipality score on different information security-related behaviours. Hereby, it can be seen that room for improvement exists on several fields. For example, much employees still do not always lock their computer or remember their passwords without writing them down. As these behaviours could pose problems in the light of the information safety at the municipality of Enschede, it is important to address the right behaviours within the campaign. Also, the analyses indicated significant differences between the departments of the municipality. Insights into this can be helpful in optimizing the campaign per department. Also, IT experience showed to be of great relevance regarding the information security-related behaviours, thereby underlining the need for training employees in order to improve their computer skills. Still, future research is needed in order to investigate whether the actions within the campaign actually contribute to an increase in awareness and safer behaviours.

7. References

Abrams, D. R. (n.d.). *Introduction to Regression.* Retrieved from https://dss.princeton.edu/online_help/analysis/regression_intro.htm

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. doi:10.1016/0749-5978(91)90020-T

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security, 28*(6), 476-490. doi:10.1016/j.cose.2009.01.003

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643. doi:10.2307/25750694

Aytes, K., & Conolly, T. (2003). A research model for investigating human behavior related to computer security. *AMCIS 2003 Proceedings*, 260.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191. doi:10.1037/0033-295X.84.2.191

Boer, H., & Seydel, E. R. (1996). Protection Motivation Theory. In M. Conner, & P. Norman (Eds.), *Predicting Health Behaviour: Research and Practice with Social Cognition Models. Eds. Mark Conner, Paul Norman* (pp. 95-120). Buckingham: Open University Press.

Bolger, N., Davis, A., & Rafaeli, E. (2003). Diary methods: Capturing life as it is lived. *Annual Review of Psychology, 54*(1), 579-616. doi:10.1146/annurev.psych.54.101601.145030

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548. doi:10.2307/25750690

Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on System Sciences* (pp. 1-10). doi:10.1109/HICSS.2009.74

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annual Review of Psychology, 55*, 591-621. doi:10.1146/annurev.psych.55.090902.142015

Cordioli, B. (2017, May 10). Meer meldingen van datalekken door gemeenten. *NOS*. Retrieved from https://nos.nl/nieuwsuur/artikel/2172451-meer-meldingen-van-datalekken-door-gemeenten.html

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior*, *28*(5), 1849-1858. doi:10.1016/j.chb.2012.05.003

Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. *System Sciences (HICSS), 2010 43rd Hawaii International Conference on System Sciences* (pp. 1-10). doi:10.1109/HICSS.2010.311

Crossler, R. E., Bélanger, F., & Ormond, D. (2017). The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. *Information Systems Frontiers*, 1-15. doi:10.1007/s10796-017-9755-1

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98. doi:10.1287/isre.1070.0160

Deutsch, M., & Gerard, H. B. (1955). A study of normative and informational social influences upon individual judgment. *The Journal of Abnormal and Social Psychology*, *51*(3), 629. doi:10.1037/h0046408

Eisenberger, R., Huntington, R., Hutchison, S., & Sowa, D. (1986). Perceived organizational support. *Journal of Applied Psychology*, *71*(3), 500. doi:10.1080/1359432X.2017.1319817

Eltayeb, T. K., Zailani, S., & Ramayah, T. (2011). Green supply chain initiatives among certified companies in Malaysia and environmental sustainability: Investigating the outcomes. *Resources, Conservation and Recycling*, *55*(5), 495-506. doi:10.1016/j.resconrec.2010.09.003

Fan, J. X., & Xiao, J. J. (1998). Consumer decision-making styles of young-adult Chinese. *Journal of Consumer Affairs*, *32*(2), 275-294. doi:10.1111/j.1745-6606.1998.tb00410.x

Greene, G., & D'Arcy, J. (2010). Assessing the impact of security culture and the employee-organization relationship on IS security compliance. In *5th Annual Symposium on Information Assurance (ASIA'10)* (pp. 1). doi:10.1.1.295.8181

Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior. *International Conference on Information Systems (ICIS), 34*.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125. doi:10.1057/ejis.2009.6

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, *81*, 282-293. doi:10.1016/j.chb.2017.12.022

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95. doi:10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69-79. doi:10.1016/j.im.2013.10.001

Klein, R. H., & Luciano, E. M. (2016). What influences information security behavior? A study with Brazilian users. *JISTEM-Journal of Information Systems and Technology Management*, *13*(3), 479-496. doi:10.4301/S1807-1775201600030000

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology*, *27*(5), 445-454. doi:10.1080/01449290600879344

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, *41*(6), 707-718. doi:10.1016/j.im.2003.08.008

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32-44. doi:10.1016/j.chb.2018.01.028

Matell, M. S., & Jacoby, J. (1971). Is there an optimal number of alternatives for Likert scale items? Study I: Reliability and validity. *Educational and Psychological Measurement*, *31*(3), 657-674. doi:10.1177/001316447103100307

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151-156. doi:10.1016/j.chb.2016.11.065

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1). doi:10.25300/MISQ/2018/13853

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126-139. doi:10.1057/ejis.2009.10

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825. doi:10.1016/j.dss.2008.11.010

Nolan, J. M., Schultz, P. W., Cialdini, R. B., Goldstein, N. J., & Griskevicius, V. (2008). Normative social influence is underdetected. *Personality and Social Psychology Bulletin*, *34*(7), 913-923. doi:10.1177/0146167208316691

O'brien, R. M. (2007). A caution regarding rules of thumb for Variance Inflation Factors. *Quality & Quantity*, *41*(5), 673-690. doi:10.1007/s11135-006-9018-6

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879. doi:10.1037/0021-9010.88.5.879

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214. doi:10.1080/07421222.2015.1138374

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816-826. doi:10.1016/j.cose.2009.05.008

Rhoades, L., & Eisenberger, R. (2002). Perceived organizational support: A review of the literature. *Journal of Applied Psychology*, *87*(4), 698. doi:10.1037/0021-9010.87.4.698

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social Psychophysiology: A Sourcebook*, 153-176.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78. doi:10.1016/j.cose.2015.05.012

Sheeran, P. (2002). Intention—behavior relations: A conceptual and empirical review. *European Review of Social Psychology*, *12*(1), 1-36. doi:10.1080/14792772143000003

Sheeran, P., & Orbell, S. (1999). Augmenting the theory of planned behavior: Roles for anticipated regret and descriptive norms. *Journal of Applied Social Psychology*, *29*(10), 2107-2142. doi:10.1111/j.1559-1816.1999.tb02298.x

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010, April). Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373-382). ACM. doi:10.1145/1753326.1753383

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217-224. doi:10.1016/j.im.2013.08.006

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*, 487-502. doi:10.2307/25750688

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy (IJISP)*, *9*(1), 26-46. doi:10.4018/IJISP.2015010102

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, *48*(7), 296-302. doi:10.1016/j.im.2011.07.002

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics*. New York, NY: Pearson.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198. doi:10.1016/j.im.2012.04.002

Van den Berg, S. M., & van der Kolk, H. (2014). *Data collection and scale development*. London, UK: SAGE.

Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. *ICIS 2005 Proceedings*, *31*.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799-2816. doi:10.1016/j.chb.2008.04.005

Yang, W. C. (2011). Applying content validity coefficient and homogeneity reliability coefficient to investigate the experiential marketing scale for leisure farms. *Journal of Global Business Management*, *7*(1), 1.

8. Acknowledgements

Hereby I would like to thank anyone involved in the process of writing my bachelor thesis. First of all, my supervisor Dr. Ardion Beldad for his helpful insights and feedback on my research. The meetings about my research helped me a lot within this study, as they enabled me to conduct the research as best as possible. Also, I would like to thank Berend Tel and Ilse Hoekstra from the municipality of Enschede for their involvement during the writing of this thesis. I am glad that I could work on this interesting assignment and that I could bring the theory on information safety into practice. Also, I would like to say thank you to all employees of the municipality of Enschede who have taken the time to fill out the questionnaire. All in all, I much enjoyed working on this assignment, and I hope that the research gave interesting insights regarding safe email behaviour and information security-related behaviours at the municipality of Enschede!

9. Appendices

9.1. Appendix 1 - Item scales

Table 9.1.
Item scales

Construct	Items (Dutch)	Adapted and translated from	α
Perceived severity (PS)	- Een inbreuk op de informatiebeveiliging van de gemeente beschouw ik als een serieus probleem - Het is zeer schadelijk als iemand zonder toestemming toegang krijgt tot informatie van de gemeente - Bedreigingen ten aanzien van de informatieveiligheid van de gemeente zijn zeer schadelijk	Workman et al. (2008) and Vance et al. (2012)	.87
Perceived vulnerability (PV)	- Ik denk dat iemand toegang tot vertrouwelijke informatie kan krijgen zonder dat daar toestemming voor gegeven is - Ik heb het gevoel dat de gemeente kwetsbaar is voor dreigingen ten aanzien van de informatiebeveiliging - Ik denk dat de kans groot is dat de informatieveiligheid van de gemeente gevaar oploopt	Workman et al. (2008), Ifinedo (2012) and Herath and Rao (2009)	.77
Response efficacy (RE)	- Iedere medewerker kan een verschil maken bij het beschermen van informatie van de gemeente - Ik kan in mijn eentje weinig doen om informatie van de gemeente te beveiligen - Als ik maatregelen neem, kan ik een verschil maken bij het helpen beschermen van informatie	Herath and Rao (2009)	.56
Response costs (RC)	- De ongemakken van het nemen van maatregelen om informatie te beveiligen zijn groter dan de voordelen - Als ik mijn informatie beveilig, lijden mijn andere werkzaamheden hieronder - Het nemen van maatregelen om informatie te beveiligen kost mij veel tijd	Workman et al. (2008) and Woon, Tan and Low (2005)	.71
Knowledge and skills (KS)	- Het nemen van maatregelen om informatie te beveiligen is gemakkelijk voor mij* - Ik bezit de benodigde vaardigheden om de informatie van de gemeente te beveiligen - Ik bezit de vaardigheden om anderen ervan te weerhouden toegang te krijgen tot informatie van de gemeente - Ik weet wat de gemeente van mij verwacht op het gebied van het beveiligen van informatie - Ik ken het beleid van de gemeente op het gebied van informatiebeveiliging - Ik weet wat ik zou moeten doen om de informatie van de gemeente te beschermen	Workman et al. (2008) and Ifinedo (2012), also some items were created for this study	.84
Attitude (A)	- Het nemen van maatregelen om informatie te beschermen is een goed idee - Het nemen van maatregelen om informatie te beschermen is noodzakelijk - Het nemen van maatregelen om informatie te beschermen is belangrijk	Ifinedo (2012) and Anderson and Agarwal (2010)	.90
Injunctive norm (IN)	- Mijn leidinggevende vindt dat ik maatregelen moet nemen om informatie te beschermen - Mijn collega's vinden dat ik maatregelen moet nemen om informatie te beschermen - De IT-afdeling vindt dat ik maatregelen moet nemen om informatie te beschermen	Herath and Rao (2009) and Ifinedo (2014)	.86
Descriptive norm (DN)	- Ik denk dat de meerderheid van de medewerkers van de gemeente maatregelen neemt om informatie te beschermen - Ik geloof dat mijn collega's maatregelen nemen om informatie te beschermen - Ik denk dat er binnen het programma waarin ik werkzaam ben maatregelen worden genomen om informatie te beschermen	Herath and Rao (2009)	.79
Safe email behaviour	- Voordat ik een e-mail verstuur, controleer ik of ik de juiste bijlagen heb toegevoegd - Voordat ik een e-mail verstuur, controleer ik of ik deze aan de juiste personen heb gericht	Created	.79

Note. This item was removed due to overlapping factor loadings

9.2. Appendix 2 - Invitation message research

Beste medewerker van de Gemeente Enschede,

Ik wil je hierbij graag uitnodigen om deel te nemen aan de enquête rondom informatieveiligheid. Deze enquête maakt onderdeel uit van mijn afstudeeronderzoek in opdracht van de Gemeente Enschede. Het doel van dit onderzoek is om meer te weten te komen over de meningen en het bewustzijn ten aanzien van informatieveiligheid. Binnenkort zal namelijk de organisatiebrede campagne 'Veilig werken. Zo doe je dat!' worden gestart. Je deelname aan deze vragenlijst draagt bij aan het optimaliseren van deze campagne en wordt daarom erg gewaardeerd.

Het voltooien van de vragenlijst zal ongeveer 7-8 minuten in beslag nemen. Voor de beste gebruikerservaring is het aan te raden de vragenlijst in te vullen op een pc of laptop. Klik op onderstaande link om de vragenlijst te starten:

link

Mocht je vragen hebben over het onderzoek, kan je contact met mij opnemen.
Alvast hartelijk dank voor je deelname.

Met vriendelijke groet,

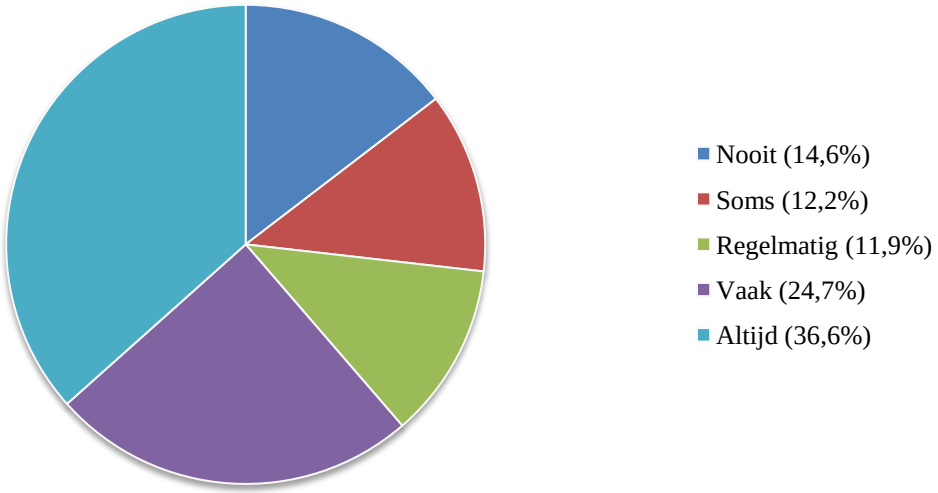
Lilian Boerkamp
Student Communicatiewetenschap, Universiteit Twente

9.3. Appendix 3 - Items and graphic representations behaviour

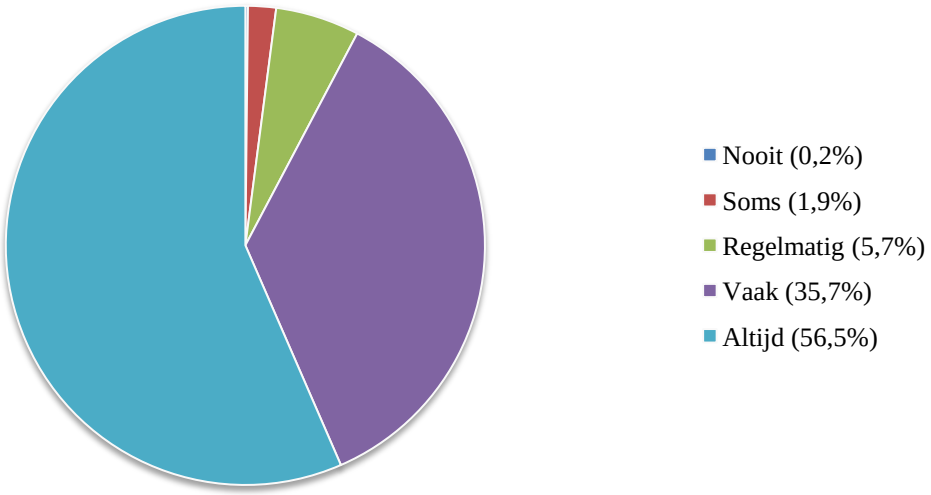
Table 9.2.
Answers provided to behaviour items

	Nooit	Soms	Regelmatig	Vaak	Altijd
	n	n	n	n	n
Als ik mijn werkruimte verlaat, vergrendel ik mijn laptop	85	71	69	144	213
Voordat ik een e-mail verstuur, controleer ik of ik de juiste bijlagen heb toegevoegd	1	11	33	208	329
Voordat ik een e-mail verstuur, controleer ik of ik deze aan de juiste personen heb gericht	0	6	31	197	348
Om mijn wachtwoorden en/of toegangscodes te onthouden, schrijf ik deze op (offline)	281	101	38	54	108
Als ik thuis wil werken, stuur ik de bestanden die ik nodig heb door naar mijn privé e-mailadres	465	93	11	6	7
Als ik word gebeld en ik vertrouw de afzender niet, verbreek ik de verbinding	78	145	43	87	229
Ik ben er alert op of er onbekenden/onbevoegden op mijn afdeling rondlopen	45	147	123	155	112
Ik maak gebruik van openbare WiFi-verbindingen (bijvoorbeeld in de trein of winkels/restaurants) als ik met werkgerelateerde zaken bezig ben	360	154	36	22	10
Ik zorg ervoor dat mijn mobiele telefoon beveiligd is met een vergrendelingscode of wachtwoord	2	1	6	13	560
Voordat ik een internetsite gebruik, controleer ik in de adresbalk of het een veilige verbinding is (bijvoorbeeld door naar het groene slotje/naar 'https' te kijken)	107	123	100	164	88
Als ik een e-mail krijg waarvan ik de afzender niet ken, klik ik op eventuele links en bijlagen om te kijken waar het over gaat	416	121	16	13	16
Ik zorg ervoor dat een systeem waarop ik werk beschikt over een up-to-date virusscanner	46	49	68	141	278

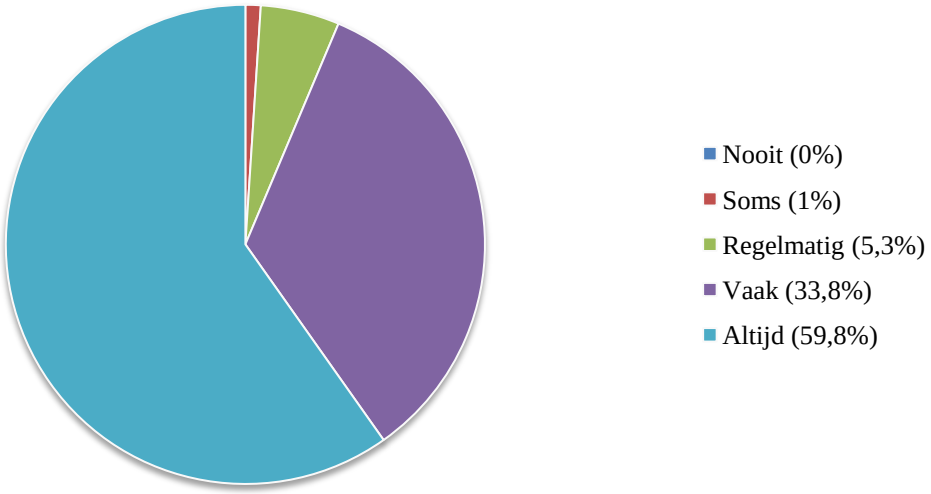
Vergrendelen systeem bij verlaten werkplek



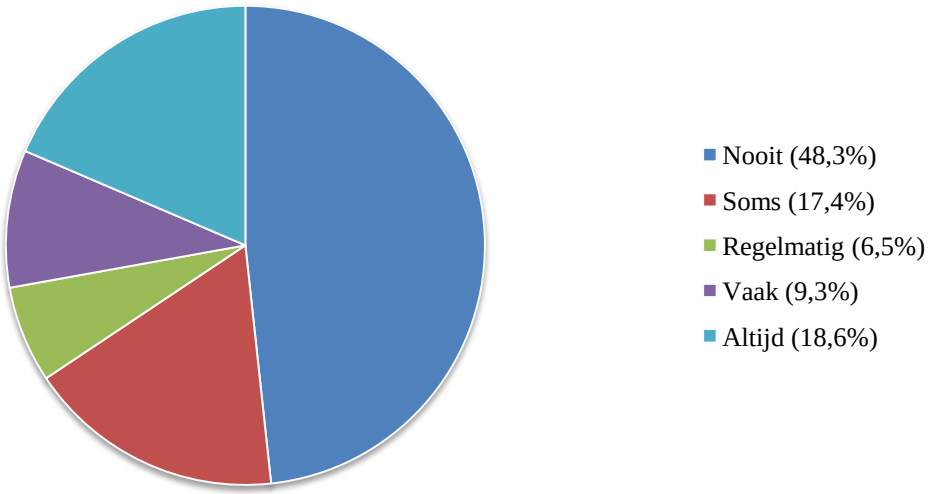
Bijlagen controleren voor verzenden e-mail



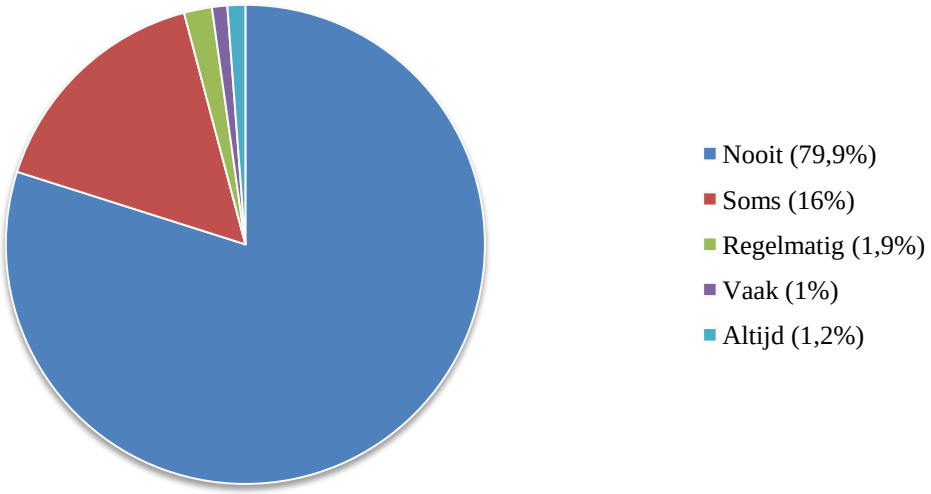
Geadresseerden controleren voor verzenden e-mail



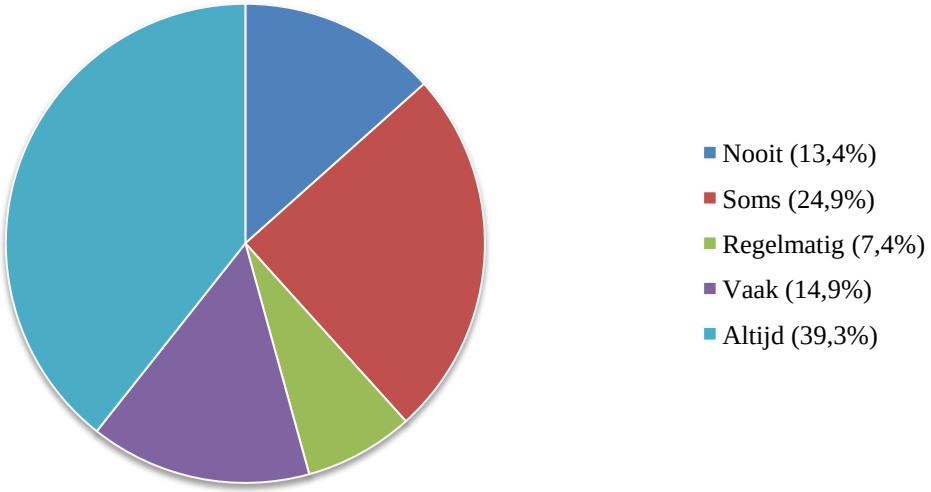
Wachtwoorden opschrijven



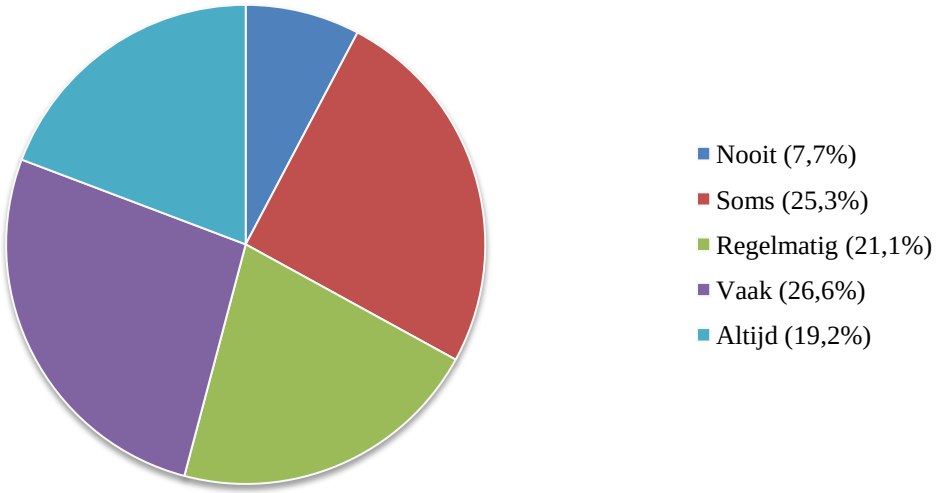
Bestanden doorsturen naar privé e-mail



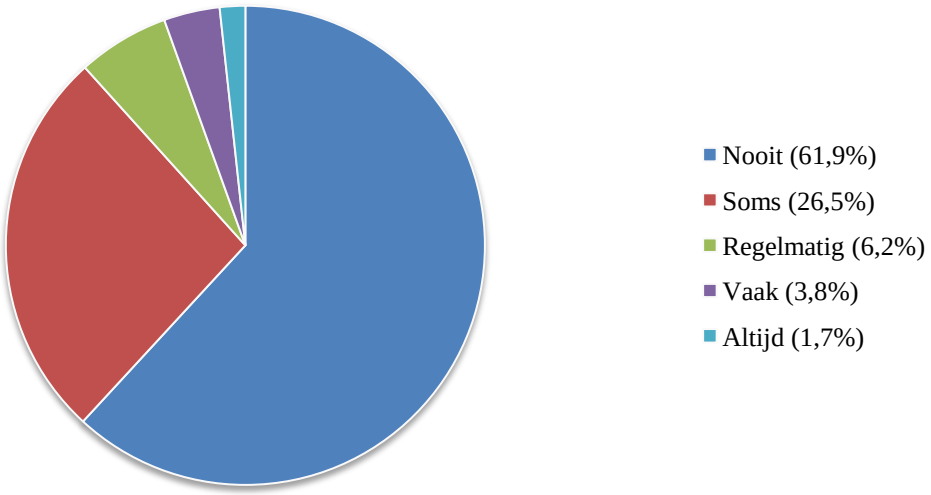
Verbinding verbreken indien onbetrouwbare beller



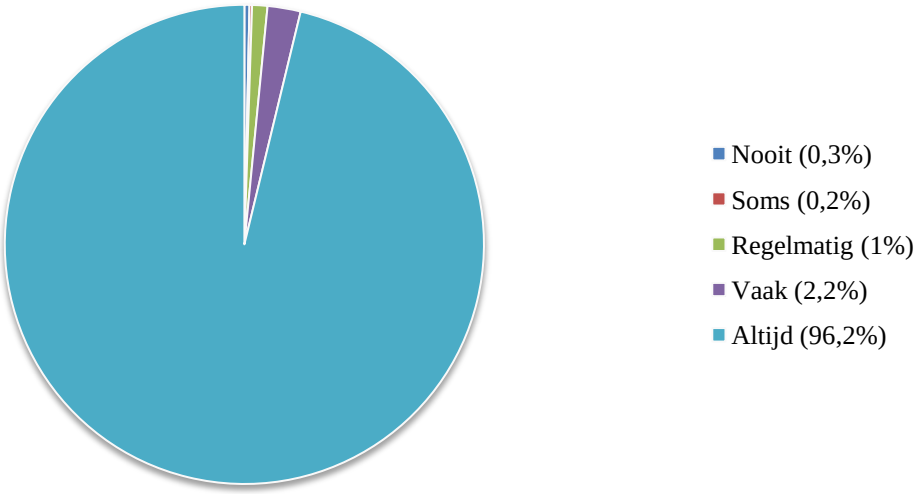
Alert op onbekenden/onbevoegden op afdeling



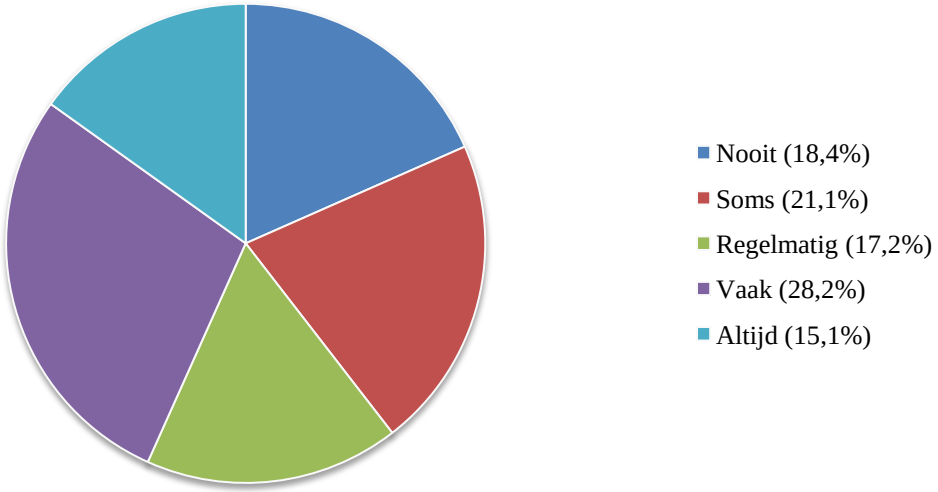
Openbare WiFi gebruiken voor werk



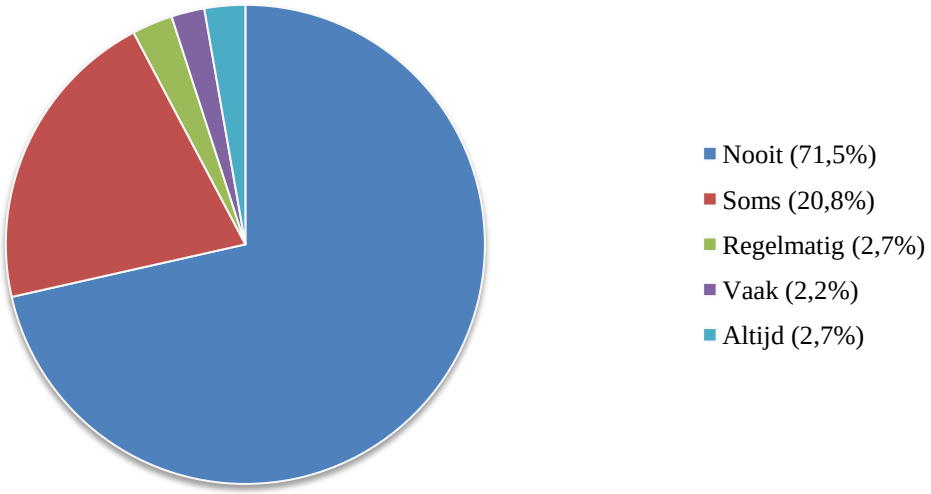
Code of wachtwoord op telefoon



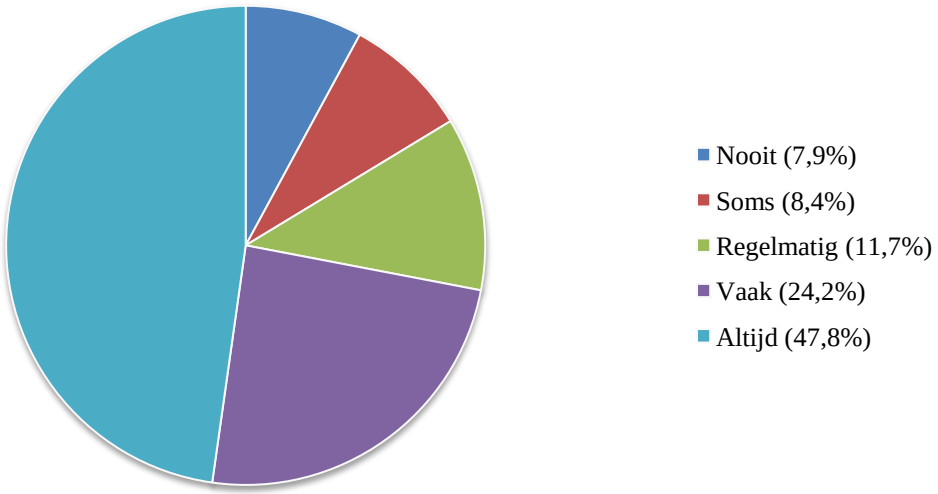
Betrouwbaarheid verbinding website controleren



Op links/bijlagen klikken in onbekende e-mail



Werken op systeem met up-to-date virusscanner



9.4. Appendix 4 - T-test results departments

Table 9.3.
T-test Group staff (CS)

Item	CS or not	N	Mean	SD	Std. Error Mean
BEH 1	No	542	3.54	1.46	.06
	Yes	40	3.90	1.30	.21
BEH 2	No	542	4.46	.71	.03
	Yes	40	4.58	.59	.09
BEH 3	No	542	4.52	.65	.03
	Yes	40	4.63	.59	.09
BEH 4	No	542	2.32	1.58	.07
	Yes	40	2.45	1.52	.24
BEH 5	No	542	1.28	.67	.03
	Yes	40	1.25	.71	.11
BEH 6	No	542	3.42	1.54	.07
	Yes	40	3.45	1.45	.23
BEH 7	No	542	3.20	1.24	.05
	Yes	40	3.78	1.12	.18
BEH 8	No	542	1.54	.86	.04
	Yes	40	2.00	1.22	.19
BEH 9	No	542	4.93	.37	.02
	Yes	40	5.00	.00	.00
BEH 10	No	542	3.00	1.35	.06
	Yes	40	3.03	1.39	.22
BEH 11	No	542	1.44	.89	.04
	Yes	40	1.43	.75	.12
BEH 12	No	542	3.93	1.29	.06
	Yes	40	4.28	1.09	.17

Note. An Independent Sample T-test was conducted

Table 9.4.
T-test Business and Management Support (BMO)

Item	BMO or not	N	Mean	SD	Std. Error Mean
BEH 1	No	404	3.40	1.48	.07
	Yes	178	3.93	1.31	.10
BEH 2	No	404	4.46	.71	.04
	Yes	178	4.49	.70	.05
BEH 3	No	404	4.49	.66	.03
	Yes	178	4.60	.62	.05
BEH 4	No	404	2.52	1.63	.08
	Yes	178	1.89	1.35	.10
BEH 5	No	404	1.26	.66	.03
	Yes	178	1.31	.68	.05
BEH 6	No	404	3.31	1.56	.08
	Yes	178	3.67	1.44	.11
BEH 7	No	404	3.15	1.24	.06
	Yes	178	3.46	1.22	.09
BEH 8	No	404	1.60	.92	.05
	Yes	178	1.50	.83	.06
BEH 9	No	404	4.95	.26	.01
	Yes	178	4.90	.52	.04
BEH 10	No	404	2.85	1.37	.07
	Yes	178	3.35	1.26	.09
BEH 11	No	404	1.50	.91	.05
	Yes	178	1.30	.76	.06
BEH 12	No	404	3.85	1.32	.07
	Yes	178	4.20	1.15	.09

Note. An Independent Sample T-test was conducted

Table 9.5.
T-test Program Service (DV)

Item	DV or not	N	Mean	SD	Std. Error Mean
BEH 1	No	551	3.55	1.45	.06
	Yes	31	3.77	1.52	.27
BEH 2	No	551	4.46	.71	.03
	Yes	31	4.58	.56	.10
BEH 3	No	551	4.52	.65	.03
	Yes	31	4.65	.55	.10
BEH 4	No	551	2.31	1.57	.07
	Yes	31	2.65	1.74	.31
BEH 5	No	551	1.27	.66	.03
	Yes	31	1.35	.80	.14
BEH 6	No	551	3.42	1.53	.07
	Yes	31	3.42	1.52	.27
BEH 7	No	551	3.23	1.25	.05
	Yes	31	3.48	1.15	.21
BEH 8	No	551	1.59	.91	.04
	Yes	31	1.26	.51	.09
BEH 9	No	551	4.94	.37	.02
	Yes	31	4.97	.18	.03
BEH 10	No	551	3.00	1.36	.06
	Yes	31	3.03	1.35	.24
BEH 11	No	551	1.43	.85	.04
	Yes	31	1.61	1.20	.22
BEH 12	No	551	3.96	1.27	.05
	Yes	31	3.84	1.53	.28

Note. An Independent Sample T-test was conducted

Table 9.6.
T-test Program Social Support (MO)

Item	MO or not	N	Mean	SD	Std. Error Mean
BEH 1	No	501	3.61	1.44	.06
	Yes	81	3.28	1.47	.16
BEH 2	No	501	4.47	.72	.03
	Yes	81	4.46	.63	.07
BEH 3	No	501	4.52	.65	.03
	Yes	81	4.54	.61	.07
BEH 4	No	501	2.27	1.56	.07
	Yes	81	2.64	1.63	.18
BEH 5	No	501	1.29	.69	.03
	Yes	81	1.19	.48	.05
BEH 6	No	501	3.47	1.52	.07
	Yes	81	3.11	1.57	.17
BEH 7	No	501	3.27	1.24	.06
	Yes	81	3.06	1.23	.14
BEH 8	No	501	1.59	.91	.04
	Yes	81	1.44	.82	.09
BEH 9	No	501	4.93	.39	.02
	Yes	81	4.99	.11	.01
BEH 10	No	501	3.03	1.34	.06
	Yes	81	2.83	1.46	.16
BEH 11	No	501	1.44	.89	.04
	Yes	81	1.44	.82	.09
BEH 12	No	501	4.01	1.24	.06
	Yes	81	3.59	1.46	.16

Note. An Independent Sample T-test was conducted

Table 9.7.
T-test Program Economy, Work and Education (EWO)

Item	EWO or not	N	Mean	SD	Std. Error Mean
BEH 1	No	449	3.55	1.46	.07
	Yes	133	3.62	1.41	.12
BEH 2	No	449	4.49	.67	.03
	Yes	133	4.40	.83	.07
BEH 3	No	449	4.56	.60	.03
	Yes	133	4.41	.78	.07
BEH 4	No	449	2.22	1.52	.07
	Yes	133	2.68	1.72	.15
BEH 5	No	449	1.27	.61	.03
	Yes	133	1.32	.84	.07
BEH 6	No	449	3.40	1.52	.07
	Yes	133	3.50	1.57	.14
BEH 7	No	449	3.26	1.24	.06
	Yes	133	3.18	1.25	.11
BEH 8	No	449	1.61	.92	.04
	Yes	133	1.42	.78	.07
BEH 9	No	449	4.92	.41	.02
	Yes	133	4.99	.09	.01
BEH 10	No	449	3.07	1.36	.06
	Yes	133	2.79	1.31	.11
BEH 11	No	449	1.40	.83	.04
	Yes	133	1.59	1.01	.09
BEH 12	No	449	3.96	1.29	.06
	Yes	133	3.92	1.28	.11

Note. An Independent Sample T-test was conducted

Table 9.8.
T-test Domain Physical (DF)

Item	DF or not	N	Mean	SD	Std. Error Mean
BEH 1	No	457	3.70	1.40	.07
	Yes	125	3.06	1.53	.14
BEH 2	No	457	4.47	.71	.03
	Yes	125	4.46	.69	.06
BEH 3	No	457	4.53	.66	.03
	Yes	125	4.49	.59	.05
BEH 4	No	457	2.36	1.60	.08
	Yes	125	2.20	1.50	.13
BEH 5	No	457	1.29	.71	.03
	Yes	125	1.22	.45	.04
BEH 6	No	457	3.48	1.51	.07
	Yes	125	3.19	1.57	.14
BEH 7	No	457	3.32	1.23	.06
	Yes	125	2.96	1.25	.11
BEH 8	No	457	1.50	.86	.04
	Yes	125	1.82	.98	.09
BEH 9	No	457	4.96	.34	.02
	Yes	125	4.87	.44	.04
BEH 10	No	457	3.05	1.34	.06
	Yes	125	2.86	1.39	.12
BEH 11	No	457	1.44	.89	.04
	Yes	125	1.45	.82	.07
BEH 12	No	457	3.99	1.28	.06
	Yes	125	3.84	1.28	.11

Note. An Independent Sample T-test was conducted

9.5. Appendix 5 - T-test results IT experience

Table 9.9
T-test IT experience

Item	IT	N	Mean	SD	Std. Error Mean
BEH 1	7 or lower	98	2.84	1.51	.15
	8 or higher	484	3.71	1.39	.06
BEH 2	7 or lower	98	4.34	.90	.09
	8 or higher	484	4.49	.66	.03
BEH 3	7 or lower	98	4.40	.73	.07
	8 or higher	484	4.55	.63	.03
BEH 4	7 or lower	98	3.09	1.64	.17
	8 or higher	484	2.17	1.52	.07
BEH 5	7 or lower	98	1.48	.91	.09
	8 or higher	484	1.24	.60	.03
BEH 6	7 or lower	98	3.18	1.61	.16
	8 or higher	484	3.47	1.51	.07
BEH 7	7 or lower	98	3.07	1.29	.13
	8 or higher	484	3.28	1.23	.06
BEH 8	7 or lower	98	1.49	.78	.08
	8 or higher	484	1.59	.92	.04
BEH 9	7 or lower	98	4.88	.48	.05
	8 or higher	484	4.95	.33	.02
BEH 10	7 or lower	98	2.77	1.36	.14
	8 or higher	484	3.05	1.35	.06
BEH 11	7 or lower	98	1.67	1.03	.10
	8 or higher	484	1.39	.83	.04
BEH 12	7 or lower	98	3.78	1.34	.14
	8 or higher	484	3.99	1.27	.06

Note. An Independent Sample T-test was conducted