Emerald Information Management and Computer Security

Comparing three models to explain precautionary online behavioural intentions

Journal:	*Information and Computer Security*
Manuscript ID	ICS-03-2017-0018
Manuscript Type:	Original Article
Keywords:	Information security behaviour, Protection motivation theory, Reasoned action approach, Online banking, Human aspects

Comparing three models to explain precautionary online behavioural intentions

1. Introduction

To date, society is becoming increasingly networked and connected (van Dijk, 2012). As more services to customers are offered online, such as banking, government and health, security becomes increasingly important. Harm can be done to individuals, the economy and society when security is compromised, for example, by means of data breaches and distributed denial-of-service attacks. As stated in the Netherlands' first National Cybersecurity Strategy, (secure) IT is fundamental for our prosperity and well-being and essential for economic growth. This means that besides increasing the adoption and use of IT, it is equally important to ensure its safety and security (Dutch Ministry of Security and Justice, 2011). It is evident that societal issues like cybersecurity need to be addressed by different parties, such as Internet service providers, telecom organizations and governmental agencies. However, it is equally important that end-users behave in a secure fashion, as they play an essential role in safeguarding the online domain. Moreover, they are essential for achieving online security (Furnell *et al.,* 2006; Liang and Xue, 2010; Ng *et al.,* 2009).

The present study deals with safety and security of online banking from an end-user perspective. Online banking is a means by which customers can access different kinds of banking services via the Internet. By 2015, 85% of Dutch citizens aged 16 and over had adopted this service (Eurostat, 2016). However, as the Internet also attracts criminals (Bossler and Holt, 2009; van Wilsem, 2011), online banking is not without risk. End-users are, for example, confronted with phishing and malware attacks (Jansen and Leukfeldt, 2015), techniques fraudsters use to obtain user-credentials in order to steal money from their bank accounts. Because banks cannot control their customers' behaviour or the devices their customers use, it is important that end-users are aware of threats aimed at online banking and are able to prevent threats from manifesting in harm (Furnell and Clarke, 2012; Jansen, 2015). A challenge here is that although end-users are ultimately responsible for their own online behaviour and the security of their devices, they often have insufficient knowledge or lack the tendency to protect themselves (Furnell *et al.,* 2008) and are also not adequately aware of the online threats they are faced with (Kritzinger and von Solms, 2010).

Furthermore, an international phenomenon regarding online banking is a shift in responsibility towards the end-user (Anderson, 2007; Davinson and Sillence, 2014). On the one hand, this is not surprising because the safety and security of online banking cannot only be addressed by banks. However, there is some debate on how far user-responsibility should

go, as online banking is a service that is pushed towards bank customers. It is not a voluntary choice in the sense that as traditional banking services are made more expensive and less accessible, for example by closing local bank offices. Ultimately, a combination of technical, human, but also legal aspects is required to ensure a safe online environment. To that extent, end-users thus also have responsibilities regarding the safety and security of online banking. In this paper, we study what motivates end-users to protect themselves against online threats by analysing three social cognitive models. A better understanding of precautionary online behaviour is required to enhance safety and security from an end-user perspective.

The current study evaluates three models in terms of their effectiveness in explaining precautionary online behaviour. We compare protection motivation theory (PMT) (Maddux and Rogers, 1983; Rogers, 1975), the reasoned action approach (RAA) (Fishbein and Ajzen, 2010) and an integrated model which comprises PMT and RAA variables. PMT and RAA seem equally valuable in the present context and are discussed in more detail in Section 2. By testing individual and integrated models we make two contributions: first, theoretical knowledge is advanced and, second, maximum effectiveness is pursued (Lippke and Ziegelmann, 2008; Sommestad *et al.,* 2015). In addition, based upon Ifinedo's (2012) work, we expect the integrated model to provide a more comprehensive account of the determinants of precautionary online behaviour. Our main interest is aimed at explained variance rather than assessing the quality of the models (see for example Prochaska *et al.,* [2008]).

Both PMT and RAA (including RAA's predecessors), have been tested extensively to predict numerous behavioural intentions and actual behaviours. However, to our knowledge they have not been widely compared in the information security domain, nor have they been extensively tested in an integrated fashion. Comparison is needed to help researchers make informed decisions about the usefulness of social cognitive models in this area. Therefore, the aim of our study is to evaluate the usefulness of PMT and RAA in explaining precautionary online behaviour. In addition, our study advances the understanding of precautionary online behaviour, which is still limited (Anderson and Agarwal, 2010; Liang and Xue, 2010; Ng *et al.,* 2009). The results are useful for scholars and practitioners who want to study and improve online safety and security practices by end-users in general, and safe and secure online banking in particular.

2. Background literature and development of hypotheses

In this section, first an overview is presented of PMT (Section 2.1) and RAA (Section 2.2), complemented with definitions of the predictor variables and a set of hypotheses that are tested in this study. This is followed by a discussion of precautionary online behavioural intention, the target behaviour of our study (Section 2.3).

2.1 Protection motivation theory

To date, several models exist that try to explain and predict behaviour (Floyd *et al.,* 2000). In the information systems domain, extensive research is done on the adoption of technology. Examples of adoption theories include the technology acceptance model (Davis, 1989) and the unified theory of acceptance and use of technology (Venkatesh *et al.,* 2003). However, most of these studies focus on *beneficial technologies*, of which online banking can be considered an example. *Protective technologies*, which focus on preventing negative outcomes, are an under-studied subject in this area (Chenoweth *et al.,* 2009). Moreover, studies on precautionary online behaviour and on how such behaviour can be changed are scarce (Ng *et al.,* 2009). Because research has shown that significant difference exists between beneficial and protective technologies (Dinev and Hu, 2005), it seems that other theories than adoption theories might be more appropriate.

We believe that PMT provides an appropriate theoretical background for the current study. First, the theory has been successfully applied to understand and predict the use of numerous protective measures (Milne *et al.,* 2000). Second, PMT has evolved over time towards a powerful explanatory theory for precautionary behaviour (Floyd *et al.,* 2000). Third, PMT includes the concept of risk, which is absent in adoption theories (Johnston and Warkentin, 2010). Another important argument in favour of PMT, or its variants (e.g. threat control model [Workman *et al.,* 2008], technology threat avoidance theory [Liang and Xue, 2009] and fear appeals model [Johnston and Warkentin, 2010]), is that they have recently been applied to the information security domain (Boss *et al.,* 2015; Vance *et al.,* 2012). These studies have shown that PMT provides a useful framework for predicting precautionary online behaviour. This has been demonstrated for both home computer users (Anderson and Agarwal, 2010; Chenoweth *et al.,* 2009; Crossler, 2010; Johnston and Warkentin, 2010; Lai *et al.,* 2012; Liang and Xue, 2010) and end-users who operate within an organizational context (Herath and Rao, 2009; Ifinedo, 2012; Lee, 2011; Lee and Larsen, 2009; Pahnila *et al.,* 2007; Vance *et al.,* 2012; Workman *et al.,* 2008, 2009). We also considered an alternative, yet similar theory: the health belief model (HBM) (Rosenstock *et al.,* 1988). This has previously

also been applied to information security issues (Davinson and Sillence, 2010; Ng *et al.,* 2009). A primary difference between HBM and PMT is that HBM consists of a set of variables that have an effect on behaviour, while PMT arranges its predictor variables in cognitive processes that individuals apply in order to evaluate threats and coping measures (Prentice-Dunn and Rogers, 1986; Weinstein, 1993). We therefore believe that the variables and processes included in PMT makes this theory more suitable for improving our understanding of precautionary online behaviour than HBM. Finally, PMT is useful for developing interventions (Floyd *et al.,* 2000), as it is viewed as a framework to develop and evaluate persuasive communications (Norman *et al.,* 2005).

According to PMT, end-users are motivated to protect themselves based on threat appraisal and coping appraisal processes, which implies that end-users first evaluate possible threats and then possible coping strategies. These evaluations determine users' protection motivation, in other words their intention to proceed, continue or avoid a given behaviour (Floyd *et al.,* 2000). "Protection motivation is an intervening variable that has the typical characteristics of a motive: it arouses, sustains, and directs activity" (Rogers 1975, p. 98). Depending on the level of protection motivation aroused, end-users will adopt an adaptive or maladaptive coping response. The former means that end-users actually follow the recommended response, in this case taking precautions. The latter holds that end-users do not follow the recommended response, thereby potentially exposing themselves increasingly to online threats.

In PMT, the threat appraisal process consists of perceived vulnerability and perceived severity. Crossler (2010) describes perceived vulnerability as the personal probability or likelihood of a security incident occurring and perceived severity as the impact of consequences resulting from a security incident. The rewards-construct is also part of PMT's threat appraisal process, but is often omitted (Milne *et al.,* 2000) – also in our study – because the theoretical difference between a reward associated with not following the coping response and a response cost (part of the coping appraisal process) is in doubt (Abraham *et al.,* 1994). Threat appraisal is a unique component in PMT, not present in RAA. Based on the notions above,

H1: perceived vulnerability positively influences precautionary online behavioural intention;
H2: perceived severity positively influences precautionary online behavioural intention.

The coping appraisal process includes an evaluation of the estimated coping strategies to avoid or minimize a threat. This process consists of response efficacy, self-efficacy and response costs. Milne *et al.* (2000) describe the first construct as the perceived effectiveness of a response in reducing a threat, the second as users' belief whether they are able to perform the recommended response and the third as how costly performing the response will be to the user. Notably, we use a domain-specific interpretation of self-efficacy as proposed by Rhee *et al.* (2009, p. 818) who term this 'self-efficacy in information security': "a belief in one's capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability". Hence,

H3: response efficacy positively influences precautionary online behavioural intention;
H4: self-efficacy positively influences precautionary online behavioural intention;
H5: response costs negatively influence precautionary online behavioural intention.

2.2 Reasoned action approach

Although specific theories are preferred when studying specific behaviour, more general theories for predicting human behaviour may contain variables that are important within the context that is being investigated. One such theory is RAA, which evolved from the popular theory of reasoned action (Fishbein and Ajzen, 1975) and the theory of planned behaviour (Ajzen, 1991). The essence of Fishbein and Ajzen's (2010) framework is that attitude towards behaviour, perceived norms and perceived behavioural control determine users' intention to perform a given behaviour. It is assumed that behavioural intention predicts actual behaviour. Moreover, they believe that their approach is unified, accounting for any behaviour. Therefore, their approach should also be appropriate for information security behaviour.

Attitude reflects a user's positive or negative feelings towards performing the target behaviour (Fishbein and Ajzen, 1975). A positive attitude towards certain behaviour is considered to positively influence that behaviour. An additional rationale for adopting this construct is that its relation with intentional behaviour is extensively tested and corroborated (Venkatesh *et al.,* 2003). Based on these notions,

H6: a positive attitude positively influences precautionary online behavioural intention.

Perceived norms, unique in RAA compared to PMT, refer to perceived social pressure and are made up of injunctive norms – perceptions what should or ought to be done – and descriptive

norms – perceptions that others are or are not performing the target behaviour (Fishbein and Ajzen, 2010). According to Anderson and Agarwal (2010) there has been a lack of attention to social variables in information systems research, while these variables are considered important for users' behaviour. Consequently,

H7: injunctive norms positively influence precautionary online behavioural intention;
H8: descriptive norms positively influence precautionary online behavioural intention.

Fishbein and Ajzen (2010) describe perceived behavioural control as perceptions about being capable of or having control over the target behaviour. Perceived behavioural control is viewed as a combination of self-efficacy (also found in PMT, H4) and locus of control (Workman *et al.,* 2008). Rather than selecting the single construct of perceived behavioural control, we have chosen to adopt these two constructs because they are distinct (Bandura, 1977). Locus of control is either internal or external (Rotter, 1966; Workman *et al.,* 2008). End-users who have a high level of internal locus of control believe that they are in control of the outcomes of a certain event. In this context, internal locus of control can translate into proactive behaviour by end-users, taking responsibility for their online safety. End-users who are characterized by external locus of control believe that the outcome is controlled powerful others or by fate. This could translate into reactive behaviour, leaving responsibility to others, expectedly their bank. Consequently,

H9: internal locus of control positively influences precautionary online behavioural intention.

2.3 Precautionary online behaviour

The recommended responses that banks want their customers to take are found in the so-called uniform safety rules for online banking. These rules are defined in the general terms and conditions of all banks in the Netherlands and are in effect as of January 1 2014. The items of the outcome variable of this study are based on these rules. The five rules for safe online banking comprise: (a) keep your security codes secret, (b) make sure that your debit card is not used by others, (c) secure the devices you use for online banking properly, (d) check your bank account regularly and (e) report incidents directly to your bank. In summary, precautionary online behaviour includes both technical and non-technical measures against security threats.

The dependent variable thus consists of items that refer to multiple actions. Although this approach is sometimes criticized (Blythe *et al.,* 2015), because predictor variables might influence protection motivation for one behaviour, but not for another, others (Crossler and Bélanger, 2014) defend this approach, stating that precautionary behaviour against online threats constitutes taking multiple actions. Based on this notion and practical considerations (lack of validated scales for precautionary online behaviour and length of questionnaire), we chose to ask participants questions about their intentions to adhere to the uniform safety rules, as intentions are acknowledged to be the most immediate predictor of actual behaviour (Fishbein and Ajzen, 2010). Moreover, we followed the work of others in constructing the dependent variable, who also measured intentions that signified various actions (Anderson and Agarwal, 2010; Herath and Rao, 2009; Ifinedo, 2012). In conclusion, we justify our approach with our aim to gain insight into the safety and security intentions of end-users, based on the totality of rules presented to them by Dutch banks.

3. Method

In this section, we describe the methods used to test the hypotheses and evaluate which model is most effective in predicting users' motivation for precautionary online behaviour. First, we discuss the survey questionnaire and procedure (Section 3.1). Second, we provide details on the survey participants (Section 3.2). We then discuss data analysis, validity and reliability of measures (Section 3.3).

3.1 Survey questionnaire and procedure

Based on literature study, using international databases ACM Digital Library, ScienceDirect and Web of Science, we developed a questionnaire. We based the questionnaire items on the work of Anderson and Agarwal (2010), Herath and Rao (2009), Ifinedo (2012), Ng *et al.* (2009), Witte (1996) and Workman *et al.* (2008). The items used a 5-point Likert-scale (ranging from totally disagree to totally agree), were translated in Dutch, were programmed in LimeSurvey (an open-source online survey tool) and were presented in random order. All predictor variables were measured by three items and precautionary online behaviour was measured by four items. Two examples of the items adopted: 'the uniform safety rules help in preventing online banking fraud' (RE1) and 'it is my intention to comply with the uniform safety rules' (PM4). The full questionnaire is available on request from the corresponding author. Before the participants were presented with these items, the uniform safety rules were

explicitly defined, to ensure that participants have a common understanding of these rules as much as possible.

A draft version and an interactive online version of the questionnaire were pretested qualitatively by 12 individuals, from the target population, major figures from the banking sector and academic peers. Based on the results of pre-testing, some minor revisions – such as clarifying instructions and specifying terms and concepts – were made to the questionnaire. The interactive online version was also pre-tested quantitatively by 34 students. Some adjustments needed to be made regarding the wording of the items, since three scales showed low reliability (self-efficacy, response costs and locus of control). For the main study, participants were recruited by an external recruitment service of online survey panels. The questionnaire was online in May-June 2015.

3.2 Survey participants

In total, 1200 Dutch users of online banking services completely filled out the online questionnaire. Participants' age ranged from 18 to 85 years (M = 49, SD = 14.5) and the gender distribution was 55% female and 45% male. Participants had completed at most lower secondary education (15%), upper secondary education (32%) or higher education (53%) and were employed (54%), self-employed (7%), retired (19%) or had a different work status (20%), such as student and unemployed.

They were experienced Internet users as more than halve of the participants indicated to make use of it over 15 years (53%) and about a third between 11-15 years (30%). One in 25 indicated to use the Internet 5 years or less (4%) and one in eight 6-10 years (13%). Besides online banking, they used the Internet for various purposes, most notably for e-mail (98%), searching for information (90%), buying products or services (80%), reading news (79%) and social networking (66%). The majority of participants were frequently on line, that is more than 20 hours a week (39%) and between 10-20 hours a week (29%). About one in ten was less than 3 hours on line per week (9%) and about a quarter between 3-10 hours (24%).

Participants were reasonably experienced users of online banking services. The largest group had 6-10 years of experience with online banking (44%). About a third was more experienced, that is 11-15 years (22%) and over 15 years (12%). Just below 1% had less than a year's experience with online banking and 22% 1-5 years. Online banking is frequently used to check the account balance. About a quarter of participants did this on a daily basis (24%) and over a third on a weekly basis (38%). The remaining participants did this once every two weeks (18%), once a month (12%) and less than once a month (8%). Making payments via

online banking was done less frequently. Most participants did this once every week (30%) or every two weeks (35%). The remainder of the participants reported doing this daily (4%), monthly (23%) or less than once a month (8%).

3.3 Data analysis, validity and reliability

Partial-least-squares path-modelling (PLS), using SmartPLS 2.0 (Ringle *et al.,* 2005), was used for data analysis. PLS can be described as a class of multivariate techniques to study relationships between measured variables and latent variables and relationships between latent variables (Hair *et al.,* 2014). PLS is compatible with multiple regression analysis, analysis of variance and unrelated *t*-tests, the results of which are special cases of the results of PLS, but which do not account for measurement error, while PLS does. As recommended by Henseler *et al.* (2009), we used a standard bootstrapping procedure (N = 5000) to test the significance of the model parameters.

Component loadings of the individual items, except one item of response costs (RC3) which was subsequently deleted, loaded highly (≥ .70) on the corresponding component, providing evidence for uni-dimensionality of the items. However, we had to remove two self-efficacy (SE1 and SE3) and attitude (AT2 and AT3) items, because these items loaded high on protection motivation as well (see Appendix, Table A1). Therefore, both constructs were represented by only one item in the structural models, posing a potential threat to reliability. We chose to retain these constructs since these are important components in PMT and RAA respectively. Construct reliability was assessed using the composite reliability co-efficient; for all items, the cut-off point of .70 was exceeded (see Appendix, Table A2).

Convergent validity was assessed using the average variance extracted (AVE) by a construct from its indicators, which all, except for locus of control (.65), exceeded the cut-off point of .70. However, we chose to retain this construct as more variability in the items of locus of control was accounted for by its component than was not. Discriminant validity was assessed by analysing the square root of AVE by each construct from its indicators, which should be greater than its correlation with the remaining constructs (Fornell-Larcker-criterion). All values met this condition (see Appendix, Table A3). Additional SPSS analyses showed a lack of multicollinearity.

4. Results

The structural models with test results are presented in Figures 1-3. We evaluate the significance of the model predictors of precautionary online behaviour.[1]

_____ Insert Figures 1 and 2 about here. _____

64% of variance in precautionary online behaviour was explained by PMT's predictors perceived vulnerability, perceived severity, response efficacy, self-efficacy and response costs (Figure 1). The strongest positive predictor was response efficacy, followed by self-efficacy and perceived severity and the negative predictor response costs. Perceived vulnerability had no significant effect on precautionary online behaviour.

63% of variance in precautionary online behaviour was explained by RAA's predictors attitude, injunctive norms, descriptive norms, self-efficacy and locus of control (Figure 2). The strongest positive predictor was attitude, followed by self-efficacy, locus of control (internal) and descriptive norms. Injunctive norms had no significant effect on precautionary online behaviour.

In addition to evaluating the explained variance of both structural model, we also calculated the effect size. According to Hair *et al.* (2014), this provides information on how substantive the impact is of both models. In terms of the effect size f^2, the additional variance explained by PMT over and above RAA ($f^2 = .16$) and the additional variance explained by RAA over and above PMT ($f^2 = .13$) both represent approximately a medium effect ($f^2 = .15$; Hair *et al.* [2014]).

_____ Insert Figure 3 about here. _____

In the integrated model, explained variance of 68% is highest (Figure 3). The PMT variables perceived severity, response efficacy and response costs, the RAA variables attitude, descriptive norms and locus of control, and self-efficacy from both models were significant predictors of precautionary online behaviour (see Figures 1-3). Therefore, all hypotheses are accepted, except for H1 and H7 – thus perceived vulnerability and injunctive norms were not significant predictors.

[1] The asterisks indicate a significance level of .001 and *ns* stands for not significant.

5. Limitations

Our study has some limitations. First, the attitude construct contained one item only for hypotheses-testing, which potentially threats reliability. Only three items were included in the questionnaire to measure this rather complex construct. Although the scale itself was reliable, two items loaded too heavily on protection motivation. Future research could make use of a more robust measure of attitude, since its explanatory power is often shown (Ifinedo, 2012, 2014; Venkatesh *et al.,* 2003). However, Herath and Rao (2009) found no significant relationship between attitude and security policy compliance. They attributed this result to factors such as context, sample and other extraneous factors. Furthermore, they argue that the predictive power of attitude might be reduced by the inclusion of other constructs, such as self-efficacy and norms. Hence, the precise effect of attitude in this regard is an interesting topic for future research.

A second limitation can be attributed towards the self-efficacy construct, which was represented by one item for hypotheses-testing as well, also possibly threatening reliability. Similar to the attitude scale, the self-efficacy scale itself was reliable, but again two items loaded too heavily on protection motivation. Future research needs to address this limitation using a more robust measure. Specifically, multiple-item measures lead towards higher predictive validity (Hair *et al.,* 2014), which could mean that self-efficacy is even a stronger predictor than it already is.

Third, we relied on self-reported behavioural intention, which could be considered a limitation. Therefore, we recommend observing actual behaviour in future studies, particularly to overcome the intention-behaviour gap (see also Boss *et al.*'s [2015] commentary on PMT studies and Crossler *et al.*'s [2013] agenda for future behavioural information security research).

6. Conclusions and discussion

The aim of our study was to evaluate the usefulness of PMT and RAA in explaining precautionary online behaviour. PMT and RAA both show good explanatory power, which indicates that both seem valuable in explaining this kind of behaviour. A main contribution of the combined model is that it shows that the individual predictors of the two constituent models (PMT and RAA) remain significant, thereby potentially providing practitioners more opportunities for prevention to increase people's precautionary behaviour. Significant predictors should, for example, be emphasized in prevention campaigns in an effort to achieve

behavioural change. Increased precautionary behaviour of end-users is beneficial for banks, as it might reduce the number of online banking fraud incidents.

Considering predictor variables of PMT, response efficacy and self-efficacy are most important. This means that the more effective a measure is perceived and the better the ability of carrying out a measure is perceived, the more likely precautionary behaviour is, which concurs with previous studies (Crossler, 2010; Ifinedo, 2012; Lee, 2011; Liang and Xue, 2010; Workman *et al.,* 2008). In contrast to Sommestad *et al.*'s (2015) findings, our results show that coping response (from PMT) is significant in explaining variance. Attitude, from RAA, can also be considered a primary predictor variable. The more positive the attitude towards precautionary online behaviour, the more likely such behaviour is, which is also demonstrated in earlier studies (Anderson and Agarwal, 2010; Fishbein and Ajzen, 2010; Venkatesh *et al.,* 2003). Scholars and practitioners should acknowledge these primary variables when developing prevention campaigns.

Secondary determinants of explaining precautionary online behaviour, which behave in accordance with literature, are perceived severity (Chenoweth *et al.,* 2009; Gurung *et al.,* 2009; Lee, 2011; Vance *et al.,* 2012; Workman *et al.,* 2008) and locus of control (Ifinedo, 2014; Workman *et al.,* 2008). If end-users evaluate the impact of a threat as high and believe that threat prevention is something they are in control of (internal locus of control), the more likely they will adopt a recommended coping measure. Therefore, these variables should also be considered when implementing prevention strategies. Moreover, underscoring personal responsibility is found to be an important aspect in stimulating protection motivation (Boehmer *et al.,* 2015; Shillair *et al.,* 2015).

The final two constructs that were significant predictors of protection motivation are the negative predictor response costs and the positive predictor descriptive norms. Both are in the proposed direction as was expected based on literature (Chenoweth *et al.,* 2009; Herath and Rao, 2009; Lee, 2011; Liang and Xue, 2010; Vance *et al.,* 2012). This means that when end-users consider the costs of a measure not outweighing its benefits and believe that others are taking precautions, they are likely to (also) perform precautionary online behaviour. The former is important for banks, meaning that they should find a favourable balance between the usability of their services and the tangible and intangible costs of precautionary measures. The latter could, for example, be achieved by showing in prevention campaigns how others are taking precautionary measures.

Perceived vulnerability had no significant effect on protection motivation. Earlier studies found mixed results for this construct. Gurung *et al.* (2009) and Vance *et al.* (2012)

also reported a non-significant relationship. However, Chenoweth *et al.* (2009), Lee (2011) and Workman *et al.* (2008) found a positive relationship between perceived vulnerability and protection motivation. Crossler's (2010) study on the other hand revealed a negative relationship. He explains that different outcomes can be attributed to the specific threats and behaviours studied and that future research is necessary to determine its true relationship.

Injunctive norms were non-significant as well, contradicting earlier studies (Herath and Rao, 2009; Ifinedo, 2012, 2014). However, contrary to our study, these studies took place in organizations, while security of online banking may be seen as an individual rather than a social issue. It is probably not a subject that is often addressed in social conversations.

Although there seems to be overlap between the models, it is important to stress that theory is advanced by testing the usefulness of these theories in the study of online behaviours. However, considering the advancement of theory, Ogden (2003) argues that this is problematic due to the unspecific nature of the constructs involved. Indeed, though the scales we used and the relationships we found were predetermined based on theory, the questionnaire items needed to be specified to the online domain in general and specifically to the online banking context. Another problem Ogden (2003) identifies is that social cognitive models often rely on analytic truths instead of synthetic truths. Qualitative exploratory research is recommended in order to identify predictor variables that are accountable for the variance we were not able to explain.

For now, it seems that the integrated model is most effective in explaining variance. This conclusion is consistent with the work of Herath and Rao (2009) and Ifinedo (2012). However, as explained by Lippke and Ziegelmann (2008), one theory can be more suitable for explaining a specific behaviour across populations and another for explaining diverse behaviours in a specific population. It is uncertain to what extent the results are generalizable to other countries, since different countries have different payment cultures. For example, the uptake of online banking is high in the Netherlands and Nordic countries as compared to other European countries (Eurostat, 2016). Additionally, other cultural differences, such as uncertainty avoidance and power distance – both within and between countries – could have an influence on precautionary online behaviour (Crossler *et al.,* 2013), as well as the political and economic situation of a country (Aldás-Manzano *et al.,* 2009), for example on risk perceptions. Future research is needed – across different domains, behaviours and populations – to advance our knowledge in behavioural information security and to understand which of these (or competing) models best explains precautionary online behaviour of end-users.

In conclusion, our recommendations for enhancing precautionary online behaviour should be tested in practice. A fruitful way forward might be using experimental manipulations of PMT and RAA variables, as recommended by Shillair *et al.* (2015), in order to find the most promising strategies for this. To our knowledge, studies that investigate the power of either model's predictors to create preventative measures are lacking. Additionally, future studies could benefit from including measuring fear and using fear appeal manipulations in order to enhance such strategies (Boss *et al.,* 2015). Furthermore, it is important to find out how and how often end-users should be presented with such information, in order to most effectively promote precautionary online behaviour.

Acknowledgements

This study is part of the Dutch Research Program on Safety and Security of Online Banking. This program is funded by the Dutch banking sector (represented by the Dutch Banking Association), the Police Academy and the Dutch National Police. The funders primarily took on a facilitating role in the entire research process and occasionally provided feedback on written materials, such as the questionnaire and the manuscript.

References

Abraham, C.S., Sheeran, P., Abrams, D. and Spears, R. (1994), "Exploring teenagers' adaptive and maladaptive thinking in relation to the threat of HIV infection", *Psychology & Health*, Vol. 9, No. 4, pp. 253–272.

Ajzen, I. (1991), "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50, No. 2, pp. 179–211.

Aldás-Manzano, J., Lassala-Navarré, C., Ruiz-Mafé, C. and Sanz-Blas, S. (2009), "Key drivers of internet banking services use", *Online Information Review*, Vol. 33, No. 4, pp. 672–695.

Anderson, C.L. and Agarwal, R. (2010), "Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions", *MIS Quarterly*, Vol. 34, No. 3, pp. 613–643.

Anderson, R. (2007), "Closing the phishing hole: Fraud, risk and nonbanks", in *Proceedings of the payments system research conferences*, available at: https://www.kansascityfed.org/publicat/pscp/2007/pdf/Anderson.pdf (accessed October 27 2016).

Bandura, A. (1977), "Self-efficacy: Toward a unifying theory of behavioral change", *Psychological Review*, Vol. 84, No. 2, pp. 191–215.

Blythe, J.M., Coventry, L. and Little, L. (2015), "Unpacking security policy compliance: The motivators and barriers of employees' security behaviors", in *Proceedings of the 11th symposium on usable privacy and security*, pp. 103–122.

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S. and Cotton, S. (2015), "Determinants of online safety behaviour: Towards an intervention strategy for college students", *Behaviour & Information Technology*, Vol. 10, No. 34, pp. 1022–1035.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D. and Polak, P. (2015), "What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors", *MIS Quarterly*, Vol. 39, No. 4, pp. 837–864.

Bossler, A.M. and Holt, T.J. (2009), "On-line activities, guardianship, and malware infection: An examination of routine activities theory", *International Journal of Cyber Criminology*, Vol. 3, No. 1, pp. 400–420.

Chenoweth, T., Minch, R. and Gattiker, T. (2009), "Application of protection motivation theory to adoption of protective technologies", in *Proceedings of the 42nd Hawaii international conference on system sciences*, pp. 1–10.

Crossler, R.E. (2010), "Protection motivation theory: Understanding determinants to backing up personal data", in *Proceedings of the 43rd Hawaii international conference on system sciences*, pp. 1–10.

Crossler, R.E. and Bélanger, F. (2014), "An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument", *ACM SIGMIS Database*, Vol. 45, No. 4, pp. 51–71.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers & Security*, Vol. 32, pp. 90–101.

Davinson, N. & Sillence, E. (2010), "It won't happen to me: Promoting secure behaviour among internet users", *Computers in Human Behavior*, Vol. 26, No. 6, pp. 1739–1747.

Davinson, N. and Sillence, E. (2014), "Using the health belief model to explore users' perceptions of 'being safe and secure' in the world of technology mediated financial transactions", *International Journal of Human-Computer Studies,* Vol. 72, No. 2, pp. 154–168.

Davis, F.D. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *MIS Quarterly*, Vol. 13, No. 3, pp. 319–340.

Dinev, T. and Hu, Q. (2005), "The centrality of awareness in the formation of user behavioral intention toward preventive technologies in the context of voluntary use", in *SIGHCI 2005 Proceedings, paper 10,* available at: http://elibrary.aisnet.org/Default.aspx?url=http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1004&context=sighci2005 (accessed October 27 2016).

Dutch Ministry of Security and Justice (2011), "*De nationale cyber security strategie: Slagkracht door samenwerking" [The national cybersecurity strategy: Strength through collaboration]*, The Hague: Ministry of Security and Justice.

Eurostat (2016), "Individuals using the internet for internet banking", available at: http://ec.europa.eu/eurostat/tgm/refreshTableAction.do;?pcode=tin00099&language=en (accessed October 27, 2016).

Fishbein, M. and Ajzen, I. (1975), *"Belief, attitude, intention and behavior: An introduction to theory and research",* Addison-Wesley, MA.

Fishbein, M. and Ajzen, I. (2010), *"Predicting and changing behavior: The reasoned action approach"*, Taylor & Francis, New York.

Floyd, D.L., Prentice-Dunn, S. and Rogers, R.W. (2000), "A meta-analysis of research on protection motivation theory", *Journal of Applied Social Psychology*, Vol. 30, No. 2, pp. 407–429.

Furnell, S. and Clarke, N. (2012), "Power to the people? The evolving recognition of human aspects of security", *Computers & Security*, Vol. 31, pp. 983–988.

Furnell, S., Jusoh, A. and Katsabas, D. (2006), "The challenges of understanding and using security: A survey of end-users", *Computers & Security*, Vol. 25, No. 1, pp. 27–35.

Furnell, S., Tsaganidi, V. and Phippen, A. (2008), "Security beliefs and barriers for novice Internet users", *Computers & Security*, Vol. 27, No. 7, pp. 235–240.

Gurung, A., Luo, X. and Liao, Q. (2009), "Consumer motivations in taking action against spyware: An empirical investigation", *Information Management & Computer Security*, Vol. 17, No. 3, pp. 276–289.

Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2014), *"A primer on partial least squares structural equation modeling (PLS-SEM)"*, SAGE Publications, Los Angeles.

Henseler, J., Ringle, C.M. and Sinkovics, R.R. (2009), "The use of partial least squares path modeling in international marketing, In: Sinkovics, R.R. (Ed.), *Advances in International Marketing (Vol. 20)*, Emerald, Bingley, pp. 277–320.

Herath, T. and Rao, H.R. (2009), "Protection motivation and deterrence: A framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18, No. 2, pp .106–125.

Ifinedo, P. (2012), "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory", *Computers & Security*, Vol. 31, No. 1, pp. 83–95.

Ifinedo, P. (2014), "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition", *Information & Management*, Vol. 51, No. 1, pp. 69–79.

Jansen, J. (2015), "Studying safe online banking behaviour: A protection motivation theory approach", in *Proceedings of the ninth international symposium on human aspects of information security & assurance*, pp. 120–130.

Jansen, J. and Leukfeldt, R. (2015), "How people help fraudsters steal their money: An analysis of 600 online banking fraud cases", in *Proceedings of the 2015 workshop on socio-technical aspects in security and trust*, pp. 24–31.

Jansen, J. and van Schaik, P. (2016), "Understanding precautionary online behavioural intentions: A comparison of three models", in *Proceedings of the tenth international symposium on human aspects of information security & assurance,* pp. 1–11.

Johnston, A.C. and Warkentin, M. (2010), "Fear appeals and information security behaviors: An empirical study", *MIS Quarterly*, Vol. 34, No. 3, pp. 549–566.

Kritzinger, E. and von Solms, S.H. (2010), "Cyber security for home users: A new way of protection through awareness enforcement", *Computers & Security*, Vol. 29, No. 8, pp. 840–847.

Lai, F., Li, D. and Hsieh, C.-T. (2012), "Fighting identity theft: The coping perspective", *Decision Support Systems*, Vol. 52, No. 2, pp. 353–363.

Lee, Y. (2011), "Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective", *Decision Support Systems*, Vol. 50, No. 2, pp. 361–369.

Lee, Y. and Larsen, K.R. (2009), "Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software", *European Journal of Information Systems*, Vol. 18, No. 2, pp. 177–187.

Liang, H. and Xue, Y. (2009), "Avoidance of information technology threats: A theoretical perspective", *MIS Quarterly*, Vol. 33, No. 1, pp. 71–90.

Liang, H. and Xue, Y. (2010), "Understanding security behaviors in personal computer usage: A threat avoidance perspective", *Journal of the Association for Information Systems*, Vol. 11, No. 7, pp. 394–413.

Lippke, S. and Ziegelmann, J.P. (2008), "Theory-based health behavior change: Developing, testing, and applying theories for evidence-based interventions", *Applied Psychology: An International Review*, Vol. 57, No. 4, pp. 698–716.

Maddux, J.E. and Rogers, R.W. (1983), "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change", *Journal of Experimental Social Psychology*, Vol. 19, No. 5, pp. 469–479.

Milne, S., Sheeran, P. and Orbell, S. (2000), "Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory", *Journal of Applied Social Psychology*, Vol. 30, No. 1, pp. 106–143.

Ng, B.-Y., Kankanhalli, A. and Xu, Y.C. (2009), "Studying users' computer security behavior: A health belief perspective", *Decision Support Systems*, Vol. 46, No. 4, pp. 815–825.

Norman, P., Boer, H. and Seydel, E.R. (2005), "Protection motivation theory", In: Conner, M. and Norman, P. (Eds.), *Predicting health behaviour (second edition)*, Open University Press, Maidenhead, pp. 81–126.

Ogden, J. (2003), "Some problems with social cognition models: A pragmatic and conceptual analysis", *Health Psychology*, Vol. 22, pp. 424–428.

Pahnila, S., Siponen, M. and Mahmood, A. (2007), "Employees' behavior towards IS security policy compliance", in *Proceedings of the 40th Hawaii international conference on system sciences*, pp. 156–165.

Prentice-Dunn, S. and Rogers, R.W. (1986), "Protection motivation theory and preventive health: Beyond the health belief model", *Health Education Research*, Vol. 1, No. 3, pp. 153–161.

Prochaska, J.O., Wright, J.A. and Velicer, W.F. (2008), "Evaluating theories of health behavior change: A hierarchy of criteria applied to the transtheoretical model", *Applied Pyschology: An International Review*, Vol. 57, No. 4, pp. 561-588.

Rhee, H.-S., Kim, C. and Ryu, Y.U. (2009), "Self-efficacy in information security: Its influence on end users' information security practice behavior", *Computers & Security*, Vol. 28, No. 8, pp. 816–826.

Ringle, C.M., Wende, S. and Will, A. (2005), "SmartPLS 2.0.M3", *Hamburg: SmartPLS,* available at: http://www.smartpls.com (accessed July 15 2015).

Rogers, R.W. (1975), "A protection motivation theory of fear appeals and attitude change", *The Journal of Psychology*, Vol. 91, No. 1, pp. 93–114.

Rosenstock, I.M., Strecher, V.J. and Becker, M.H. (1988), "Social learning theory and the health belief model", *Health Education Quarterly*, Vol. 15, No. 2, pp. 175–183.

Rotter, J.B. (1966), "Generalized expectancies for internal versus external control of reinforcement", *Psychological Monographs: General and Applied*, Vol. 80, No. 1, pp. 1–28.

Shillair, R., Cotten, S.R., Tsai, H.-Y.S., Alhabash, S., LaRose, R. and Rifon, N.J. (2015), "Online safety begins with you and me: Convincing Internet users to protect themselves", *Computers in Human Behavior*, Vol. 48, pp. 199–207.

Sommestad, T., Karlzén, H. and Hallberg, J. (2015), "The sufficiency of the theory of planned behavior for explaining information security policy compliance", *Information & Computer Security*, Vol. 23, No. 2, pp. 200–217.

Van Dijk, J. (2012), *The network society (third edition)*, SAGE Publications, London.

Van Wilsem, J. (2011), "Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization", *European Journal of Criminology*, Vol. 8, No. 2, pp. 115–127.

Vance, A., Siponen, M. and Pahnila, S. (2012), "Motivating IS security compliance: Insights from habit and protection motivation theory", *Information & Management*, Vol. 49, pp. 190–198.

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003), "User acceptance of information technology: Toward a unified view", *MIS Quarterly*, Vol. 27, No. 3, pp. 425–478.

Weinstein, N.D. (1993), "Testing four competing theories of health-protective behavior", *Health Psychology*, Vol. 12, No. 4, pp. 324–333.

Witte, K. (1996), "Predicting risk behaviors: Development and validation of a diagnostic scale", *Journal of Health Communication*, Vol. 1, pp. 317–341.

Workman, M., Bommer, W.H. and Straub, D. (2008), "Security lapses and the omission of information security measures: A threat control model and empirical test", *Computers in Human Behavior*, Vol. 24, No. 6, pp. 2799–2816.

Workman, M., Bommer, W.H. and Straub, D. (2009), "The amplification effects of procedural justice on a threat control model of information systems security behaviours", *Behaviour & Information Technology*, Vol. 28, No. 6, pp. 563–575.

Appendix

_____ Insert Tables A1, A2 and A3 about here. _____

Table A1: Component loadings – original measurement model (full)

	PV	PS	RE	SE	RC	IN	DN	AT	LoC	PM
PV1	**0.89**	0.17	-0.26	-0.24	0.24	0.17	-0.02	-0.15	-0.27	-0.17
PV2	**0.91**	0.22	-0.28	-0.28	0.28	0.22	0.02	-0.18	-0.29	-0.20
PV3	**0.72**	0.21	-0.17	-0.15	0.12	0.11	-0.01	-0.06	-0.20	-0.09
PS1	0.22	**0.86**	0.06	0.16	-0.04	0.04	0.12	0.24	0.07	0.22
PS2	0.13	**0.87**	0.11	0.25	-0.11	-0.05	0.09	0.31	0.09	0.28
PS3	0.26	**0.88**	0.05	0.14	0.01	0.07	0.11	0.25	0.03	0.21
RE1	-0.25	0.08	**0.89**	0.60	-0.32	0.00	0.33	0.65	0.59	0.64
RE2	-0.23	0.03	**0.77**	0.47	-0.17	0.08	0.28	0.54	0.56	0.48
RE3	-0.25	0.10	**0.88**	0.59	-0.33	-0.02	0.33	0.65	0.61	0.66
SE1	-0.24	0.19	0.58	**0.89**	-0.46	-0.13	0.21	0.64	0.54	0.71
SE2	-0.24	0.18	0.57	**0.87**	-0.42	-0.08	0.25	0.65	0.51	0.65
SE3	-0.24	0.20	0.61	**0.91**	-0.51	-0.10	0.30	0.67	0.58	0.75
RC1	0.23	-0.07	-0.29	-0.49	**0.90**	0.31	-0.02	-0.40	-0.31	-0.40
RC2	0.24	0.00	-0.25	-0.40	**0.85**	0.34	-0.02	-0.27	-0.23	-0.30
RC3	0.10	0.12	0.19	0.05	**0.14**	0.22	0.20	0.18	0.15	0.14
IN1	0.17	0.03	0.05	-0.05	0.25	**0.88**	0.20	-0.01	0.06	0.01
IN2	0.20	0.02	-0.02	-0.14	0.36	**0.87**	0.13	-0.06	-0.03	-0.09
IN3	0.17	0.02	0.03	-0.09	0.30	**0.90**	0.18	-0.05	0.03	-0.03
DN1	0.02	0.13	0.32	0.28	-0.06	0.12	**0.87**	0.29	0.27	0.31
DN2	0.00	0.09	0.30	0.20	0.00	0.19	**0.86**	0.27	0.29	0.29
DN3	-0.03	0.10	0.34	0.27	-0.04	0.19	**0.88**	0.30	0.30	0.33
AT1	-0.17	0.23	0.65	0.65	-0.37	-0.04	0.27	**0.87**	0.50	0.68
AT2	-0.11	0.30	0.64	0.63	-0.33	-0.02	0.34	**0.90**	0.51	0.75
AT3	-0.16	0.29	0.67	0.70	-0.38	-0.06	0.29	**0.92**	0.55	0.82
LoC1	-0.26	0.13	0.61	0.56	-0.30	-0.02	0.26	0.54	**0.83**	0.56
LoC2	-0.27	0.04	0.56	0.53	-0.25	0.03	0.28	0.46	**0.81**	0.49
LoC3	-0.17	0.02	0.52	0.39	-0.19	0.08	0.29	0.41	**0.77**	0.41
PM1	-0.14	0.22	0.58	0.66	-0.36	-0.03	0.32	0.71	0.49	**0.88**
PM2	-0.19	0.25	0.65	0.69	-0.36	-0.02	0.32	0.72	0.53	**0.90**
PM3	-0.18	0.26	0.64	0.76	-0.40	-0.04	0.34	0.73	0.56	**0.90**
PM4	-0.16	0.25	0.66	0.72	-0.39	-0.07	0.29	0.83	0.55	**0.90**

Note. PV: perceived vulnerability. PS: perceived severity. RE: response efficacy. SE: self-efficacy. RC: response costs. IN: injunctive norms. DN: descriptive norms. AT: attitude. LoC: locus of control. PM: protection motivation.

Table A2: Descriptives and coefficients of reliability and convergent validity

	Mean (M)	Standard deviation (SD)	Average variance extracted (AVE)	Composite Reliability (CR)
Perceived vulnerability	2.61	0.71	0.71	0.88
Perceived severity	3.96	0.76	0.76	0.90
Response efficacy	4.18	0.67	0.72	0.88
Self-efficacy	4.38	0.70	1.00	1.00
Response costs	2.12	0.86	0.77	0.87
Attitude	4.49	0.67	1.00	1.00
Injunctive norms	2.59	1.02	0.65	0.84
Descriptive norms	3.60	0.74	0.76	0.90
Locus of control	4.04	0.71	0.64	0.84
Protection motivation	4.38	0.64	0.80	0.94

Table A3: Coefficients of discriminant validity

	PV	PS	RE	SE	RC	AT	IN	DN	LoC	PM
PV	**0.84**									
PS	0.22	**0.87**								
RE	-0.29	0.09	**0.85**							
SE	-0.24	0.18	0.57	**1.00**						
RC	0.27	-0.05	-0.31	-0.40	**0.88**					
AT	-0.18	0.24	0.64	0.60	-0.36	**1.00**				
IN	0.21	0.02	-0.02	-0.10	0.38	-0.05	**0.81**			
DN	0.00	0.12	0.37	0.25	-0.03	0.27	0.14	**0.87**		
LoC	-0.30	0.09	0.70	0.52	-0.30	0.51	-0.01	0.34	**0.80**	
PM	-0.19	0.28	0.71	0.65	-0.40	0.68	-0.09	0.36	0.61	**0.89**

Note. Off-diagonal values are correlations. Diagonal values are square root of average extracted variances. PV: perceived vulnerability. PS: perceived severity. RE: response efficacy. SE: self-efficacy. RC: response costs. AT: attitude. IN: injunctive norms. DN: descriptive norms. LoC: locus of control. PM: protection motivation.

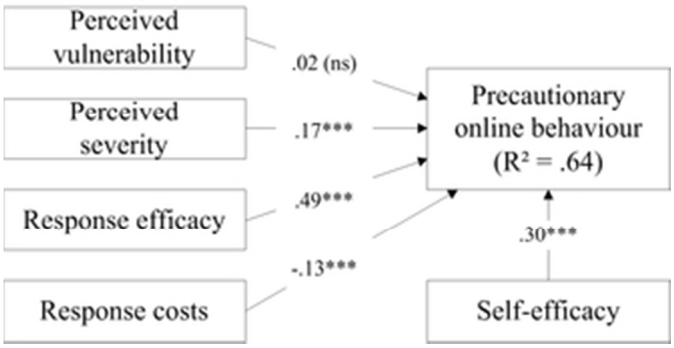

Figure 1: Structural model PMT variables

56x28mm (150 x 150 DPI)

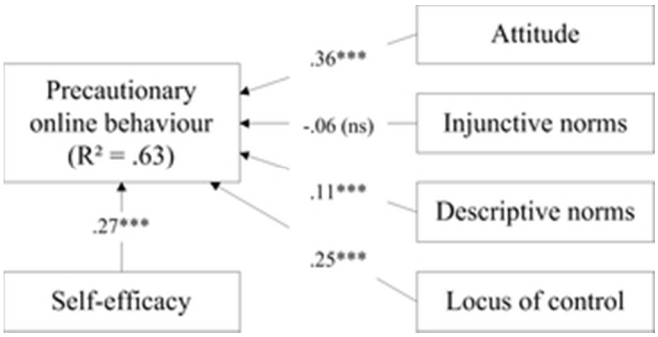

Figure 2: Structural model RAA variables

55x27mm (150 x 150 DPI)

Figure 3: Structural model PMT-RAA variables

56x17mm (150 x 150 DPI)