# An Empirical Mobile Security Study Based on the Big Five Model and the Theory of Planed Behaviour

## Masterarbeit

zur Erlangung des akademischen Grades „Master of Science (M.Sc.)“ im Masterstudiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Kaemmerer Vornome: Nico

[redacted]- [redacted]

Prüfer: Prof. Dr. Breitner

Hannover, den 1. Oktober 2012

**Table of contents** **Page**

# 1 Introduction

## 1.1 Motivation and relevance of the research field

Nowadays and inside the global community enabled by the internet and other similar digital technologies, users of modern communication devices are facing increasingly higher levels of security risks if they are not fully aware of the correspondent threats and protect their systems accordingly.[1] Therefore, technologies which protect computers and kindred systems from unauthorized access, viruses, disruptions, spyware or other threats have become progressively important in the highly networked society. Furthermore, with the increasing growth and rising importance of mobile-business, the production of smartphones in combination with a high range of fitting applications is spreading quickly. In 2010, smartphone sales were expected to make up almost 40% of the overall and global handset sales.[2] Due to a high supply of consumer oriented software connecting to almost every part of the everyday life and since the process of implementation and the direct use of these applications for the end-user have altered to be a matter of only a few minutes in most cases, the relevance of mobile-security becomes apparent.

Mobile devices today turn out to be portable electronic systems that store and potentially manipulate confidential information and therefore bring new risks to security due to the fact that they are yet fundamentally more vulnerable than stationary computer systems.[3] At the same time, a significantly increasing number of people who are actually using the option of active browsing and downloading from the internet can be registered with an upward tendency.[4] This tendency can on the one hand be noticed for the kind of people who are security savvy but on the other hand also for people who do not pay attention to a significant amount considering security issues. Adding relevance to the subject, an increasing amount of information is being stored on mobile devices.[5] Indeed, it has been recently suggested that new and critical data is stored in this context in coverage of more than 80% when referring to business scenarios. Completing the profile of high relevance for security endeavors, an alarming and most recent

[1] Cf. for this and the following Dinev et al. (2009), p. 391 f.

[2] Cf. Dörflinger (2010), p. 1.

[3] Cf. Tu/Yuan (2012), p. 1393.

[4] Cf. for this, the following and an exemplary investigation on these developments among students Androulidakis/Kandus (2011).

[5] Cf. for this and the following Botha/Furnell/Clarke (2009), p. 130.

development in the voluminous field of potential harassments can be recorded.[6] Referring to the mobile security report of 2012 on mylookout.com, tendencies in compositions of mobile threats are indicating a strong shift from classical hazards like spyware, toward professionally engineered and profit based malware in just a few years.[7]

While correctly functioning technology and software provides a foundational component in security matters, the individual person and corresponding handling of a critical situation often illustrate the source for success of failure.[8] Therefore, the affection for and utilization of protective software by smartphone users as well as the corresponding antecedents accordingly pose to be a field of high interest in this context.[9] It appears to be a reasonable assumption that organizations, which are engaged in the development of according protective software, are in need of empirical information about attitude- and awareness-shaping factors of the individual and potential customer.[10]

Consequently, the fight against negative technologies does not only require the development of effective protective information technologies but also an awareness of the potential behavior of the customer and further education of the user to deploy these technologies. When searching for such factors on the individual person's level, the personality of the affected user comes to mind since state of the art literature is widely considering it to be a comprehensive intention-shaping factor in a lot of different contexts.[11] Since the overall process which leads to the final result of action is to be observed, it is evidently necessary to connect the individual's personality to the actual intention-building cognitive process.

## 1.2 Study objective and research question

This study strives to develop a fitting approach toward the established topic of information security in the context of mobile devices by potentially comprising all

[6] Cf. for this, the following and a numerical breakdown of the developments the mobile security report 2012, on mylookout.com, p. 5 ff.

[7] While still widespread in concentrated geographical areas, the described approaches like premium sms services disguised as reliable software applications appear to be globally on the rise.

[8] Cf. for this and the following Gründer (2007), p. 20.

[9] Cf. Yeon et al. (2011), p. 311.

[10] Cf. for this and the following Dinev et al. (2009), p. 392.

[11] Cf. for the application and investigation of a personality-intention-relationship e.g. Zhao et al. (2010) and Gountas/Gountas (2007).

technologies considered as smartphones, independent from producer, brand or operation system. Narrowing the topic down to the perspective of behavioral research, a suitable and adjusted research framework is to be derived from state of the art literature with the eventual ambition of empirical testing. Therefore, the main objective of this study is to contribute to a further understanding of how individual personality traits of smartphone users shape their attitudes and actual intentions to make use of measures for mobile protection.

Based on the previously made statements, the main and general research question which is to be answered by the provided exposition, and expected to provide potential for relevant implications on a practical as well as on a theoretical level, will be:

*How are personality traits influencing the cognitive processes of mobile phone users to protect his/her mobile phone?*

As incorporated in the formulation of this research question, this study aims at merging and combining the 3 broad research fields of personality research, cognitive intention building research and IS/IT security research. Additional intricacy in this context is provided by the fact that one of the 3 research fields, namely the field of IS/IT security, has to be further modified to depict the not yet firmly established field of mobile security for final application.

Succeeding the foundation of the research at hand, a traditional scientific buildup will be chosen for examination.

## 1.3 Structural Approach

To achieve a comprehensive examination of the above stated problem and research question, the proceedings of the study will comprise 4 succeeding chapters. Chapter 2 starts with the illustration and demarcation of the rather new research field of mobile security by presenting research publications regarding the kindred topic of general information security to afterwards allow the deduction of a better understanding. Successively, a theoretical foundation on the big five personality traits is presented and existing applications in the context of IS research are given. To complete the theoretical section of the study, cognitive intention building approaches leading up to the theory of planned behavior as well as their connection to the field of IS research will be displayed. In chapter 3, hypotheses are then developed to outline the main expected coherences in the interaction of the presented theories and their adaption in the mobile security context. Building up on that, a distinct research framework with the objective to explain individual intention toward mobile security is developed on the basis of a comprehensive consultation of state of the art and interdisciplinary literature connecting the 3 mentioned theoretical fields. Hereupon, chapter 4 provides the major core of the study by motivating and using a quantitative research approach to answer and evaluate the assumed causalities inside the given model through practical testing. Tools and measures of empirical data processing are then illustrated for according application. Afterwards, the actual process of an executed survey which was conducted among end-users of smartphones and corresponding applications is described. This section includes preliminary ideas, the development of suitable items and an overview on the research sample regarding socio-demographical aspects and general findings. Furthermore, investigated results associated with the postulated hypotheses are presented, evaluated and comprehensively discussed, regarding potential limitations and drawbacks of the research constitution. Finally, chapter 5 summarizes the results of the study as well as future prospects and potentials for further complementing research possibilities and build-up investigations.

# 2 Theoretical foundations on IT security, personality traits and behavioral intention

## 2.1 Literature state of the art of IT security

### 2.1.1 General illustration of IT security

The security of information systems and technology, although in direct comparison still quite reluctantly addressed by the private user, has already become a part of core business processes in almost every organization.[12] In this context, IT security is nowadays regarded as an essential element of contribution for the overall success in business processes by being closely linked to a lot of other areas of operation.[13] As a consequence, the efficiency of conducted IT security measurements, personnel and integrated processes has already reached the magnitude of a competitive advantage.[14] The forms of threats and causes for the necessity of IT-security are manifold and independent from the private or business context while potentially generating far more

[12] Cf. Trcek (2003), p. 337.
[13] Cf. Schmidt (2006), p. 5.
[14] Cf. Gründer (2007), p. 12.

# 5 Conclusion

## 5.1 Summary of the results and research implications

Lately personality research emphasizes the relationship of personality variables to established and well-understood models.[251] Concurrently, scholars of general IS research have proposed that future research moves beyond the technology acceptance model. This study, concerning a closely related research field, can be viewed as respecting both of these stipulations by further integrating the construct of the TAM into a comprehensive framework with personality and intentional cognitive process research. Building up on the assumption that an individual's personality is significantly affecting the awareness of the need and the intention for the use of mobile security software and programs, this study focuses on the relationship between the big five personality traits and the theory of planned behavior to contribute to the understanding of the end-user's attitude- and intention-buildup. By incorporating the TAM as a part of the TPB, a reasonable interconnection has been created and exploited in the research process. As an initial position of the study, the research question:

*How are personality traits influencing the cognitive processes of mobile phone users to protect his/her mobile phone?*

was derived to specify the overall investigational focus. The present study also seeks to contribute and further expand the research field as other extant studies throughout security literature can be seen as having their major focus in the field of rather stationary technologies and devices. Considering the developed hypotheses which were implemented in the research framework on the basis of established state of the art literature, mostly throughout publications in the kindred field of IS- and IT-security, some major results can be summarized.

As the most important and significant finding, it can be stated that the traditional components of the TPB demonstrably cause the highest proportion of postulated direct influences on the behavioral intention by showing significant positive effects. For another crucial finding of the study it is to be mentioned that the derived modification of the attitude component contributed largely to understanding that participants are apparently not influenced by the objective difficulties to use security software but

[251] Cf. for this and the following Devaraj/Easley/Crant (2008), p 103.

largely rely on their own assumed abilities. Regarding the incorporated dimensions of personality, diverse findings can be denoted with a tendency toward those personality dimensions which are non-related to social intercourse but rather determining a person's character in a situational context. Furthermore, the specific context of mobile security is regarded to be accountable for divergence in resulting effects of personality traits when compared with other studies investigating the relationship of the FFM with the TPB approach.

There are some theoretical and practical implications which could be derived from the results of this study. As a theoretical aspect it can be emphasized that individual differences and characteristics of personality do play a role for the question of an affinity towards mobile security which is not to be neglected. Thus, the assessment that a combined personality-intention-approach can be regarded to be expedient in the mobile security context is perceived to be appropriate. On the practical side, an identification of possible profiles of people who are potential users of mobile security programs or devices might be possible when using the raised information and contribute to the corresponding development of these programs. Therefore, organizations which are concerned with that topic might actually benefit from kindred data, especially when the complete set of personality dimensions is used to determine a certain emphasis in traits. Considering general research fields, it might be expected that the implementation of a similar combination of the FFM and TPB might enhance the explanatory power of other frameworks in analogical studies or investigations.

As a closing thought, the presented findings of this study are to be viewed within the context of its limitations. When a rather new and complex concept like mobile security is chosen to be the core of a study, there has to be awareness that this term can only be investigated out of a certain perspective. The focus on the individual and the security possibilities of the device itself naturally constricts the complexity of the topic to enable the empirical approach. It has to be kept in mind that the change of the focus from e.g. the smartphone itself to external factors in connection, like the recently introduced and rapidly growing clouds throughout the internet, might shift the whole setup of investigation.[252]

[252] Cf. for these contemplations Shaikh/Haider (2011).

## 5.2 Future research prospects

As potentials for further research directions in this field are considered, successive studies about e.g. marketing schemes which build up on the present results and respond towards possible resentment for the customers' interest in mobile security might be further deliberated. Besides, the investigation of mobile security in an exclusively professional or business environment leaves capabilities for further studies and investigation since the study at hand focuses on the average individual use of smartphone protection to create a general overview. The specific context of business companies and organizations as institutions and the applications of mobile phones and their technological possibilities most probably require separate approaches of theoretical framework development and specifically selected groups for empirical data collection. Taking this idea to the next level, future research might contemplate the idea of preliminary profiling and categorizing smartphone users according to their expertise to generate even more and precise results for practical implications.

Furthermore, as this study focuses on the aspect of an individual's intention, amendatory investigations focusing on the actual development of use in different mobile security measures throughout different segments of the market remains a potential topic of interest.[253] Corresponding results might contribute the overall research in this field only up to a certain degree, as the intention toward a behavior cannot be completely equated with the actual behavioral outcome, although it remains a useful indicator.

When the investigational approach is shifted toward a more specific view on newly developed security measures, the aspect of continuance in intentional use might be a focus of successive studies. With the aspect of sustainability highly valued, kindred setups to the study at hand might be used to adapt existing research models from the general IS context for further examination.[254] Also, further demographical surveys in that context are not to be neglected. Since an effective identification of a profile for population groups who are suited for an in depth focus because of their affinity to be in touch with that field might turn out to be profit-yielding, constant studies regarding the change in demographical tendencies appear to be meaningful. A last aspect which is not

[253] The actual assumption of prospective developments in this field might be deducted from the socio-demographic information that more than 80% of the observed participants did not own their smartphone for more than 3 years. Therefore, additional habituation with these devices and a more comprehensive use and dealing with their varying functions can be seen as a highly presumable development.

[254] For an exemplary approach to examine the continuance of use in IS see Bhattacherjee (2001).

to be neglected is the potential for international investigation. Although the study at hand delivers an overview of respondents of a German background, studies among other national or cultural environments might be insightful and shed further light on the idea of those influences as exogenous variables inside the intention building process.

Concluding, it can be expected that the topic and research field of mobile security will remain a significant focus of future publications with a tendency to even rise in importance. Especially the fact that many forms of security and according measures are undergoing a process of further maturing to be able to cope with analogical stationary concepts consolidate these prognoses.[255] By not only being a field of theoretical contemplation but practical presence with a high potential of financial relevance for certain parties and organizations, the decline of awareness and attention towards comprehensive security threats and remedies is not soon to be presumable.

[255] Cf. Chaouchi/Maknavicius (2010), p. 4.