Why do People Adopt, or Reject, Smartphone Security Tools?

Norah Alkaldi and Karen Renaud

University of Glasgow, Glasgow, United Kingdom
e-mail: n.alkaldi.1@research.gla.ac.uk, karen.renaud@glasgow.ac.uk

Abstract

A large variety of security tools exist for Smartphones, to help their owners to secure the phones and prevent unauthorised others from accessing their data and services. These range from screen locks to antivirus software to password managers. Yet many Smartphone owners do not use these tools despite their being free and easy to use. We were interested in exploring this apparent anomaly. A number of researchers have applied existing models of behaviour from other disciplines to try to understand these kinds of behaviours in a security context, and a great deal of research has examined adoption of screen locking mechanisms. We review the proposed models and consider how they might fail to describe adoption behaviours. We then present the Integrated Model of Behaviour Prediction (IMBP), a richer model than the ones tested thus far. We consider the kinds of factors that could be incorporated into this model in order to understand Smartphone owner adoption, or rejection, of security tools. The model seems promising, based on existing literature, and we plan to test its efficacy in future studies.

Keywords

Smartphone security, Integrated Model of Behaviour Prediction, Security Tool Adoption

1. Introduction

People rely on their devices to store personal photos and make online purchases, and many have migrated such usage to their mobile devices. Digital interactions often require users to prove their identity and this generally requires provision of a password. People thus need to remember far more passwords than they reasonably can. To cope, many choose weak passwords, reuse the same password for all accesses or write them down (Adams & Sasse, 1999).

Password managers exist to ease the password memorial load and encourage the use of stronger passwords. However, surveys reveal that few users use password managers on their Smartphones. This reluctance applies to many security tools, not only password managers. For example, a survey of 1,656 smartphone users (Consumer Reports, 2012) revealed that although the Smartphone holds sensitive data, 64% of users did not lock their phones and 39% did not use any security measures.

The security measures that Smartphone owners ought to use include screen locks, patching of OS, anti-virus and anti-malware software, firewalls, anti-theft mechanisms, encryption and password managers (Parker *et al.*, 2011)(Jeon *et al*., 2011).

In order to test how widespread password manager usage was we ran a crowd-sourced poll of 100 people via CrowdFlower. We asked firstly whether people used a Password Manager Application. 29 people did, 46 did not, and the rest did not know what such an application was. For those in the latter group, we explained what a password manager was, and asked them whether they thought it might be useful. 13 of the 29 said yes. Among those who used a password manager, only 8 used it on their smartphones.

Poor usability has often been blamed for non-adoption of security measures (Furnell, 2005) (Adams & Sasse, 1999). However, even usable techniques, such as biometric authentication, have not enjoyed widespread adoption. A survey of iPhone users in Saudi Arabia (Aldaraiseh *et al.* ,2015) found that even though the majority of respondents agreed that TouchID was usable and secure, only 33% actually used it for securing their devices.

It would be helpful to model decision-making in a way that reflects factors that deter or encourage adoption in order to design interventions that are more likely to be adopted.

2. Theoretical Framework

Eisenhart (Eisenhart, 1991, p. 205) defines a theoretical framework as a "*structure that guides research by relying on a formal theory; that is, the framework is constructed by using an established, coherent explanation of certain phenomena and relationships*". The value of using a theoretical framework in a study lies in its ability to organize and focus the study and thus strengthen the research. Theory-based studies specify which key variables or factors influence a phenomenon of interest (Bloomberg & Volpe, 2015). Distinct theories address different units of practice so it is important to choose a suitable framework. The selection of the best-fit theoretical framework starts by identifying the problem, goal, and units of practice (Sussman & Sussman, 2001), not because a theory is in vogue, familiar or interesting.

Four behavioural theories have been used in the field of information system security in order to model security-related end-user behaviour (Lebek *et al*., 2014). They are *General Deterrence Theory* (Gibbs, 1975), *Theory of Planned Behaviour* (TPB) (Aizen, 1991), *Technology Acceptance Model* (TAM) (Davis, 1989) and *Protection Motivation Theory* (PMT) (Rogers, 1975). One that has not yet been used in this area is the *Integrated Model of Behaviour Prediction* (IMBP) (Fishbein , 2000) (Fishbein & Yzer, 2003), a relatively recent theory that is quite similar to TPB but with some improvements. Table 1 provides an overview of these models, depicting the factors they incorporate, and critiques each model.

Table 1 An overview of selected theoretical models

Model	Factors Influencing Behaviour	Critique	Security-related Studies
General Deterrence Theory (GDT)	Fear of consequences	Evidence that consequences, on their own, do not inform behaviour	Chen & Li, 2014
Theory of Planned Behaviour (TPB)	Attitude, subjective norms, and perceived behavioural control	Assumption that intention infallibly leads to behaviour. Does not model the impact of external factors	Ngoqo & Flowerday, 2015
Technology Acceptance Model (TAM)	Perceived usefulness and ease-of-use	Too Technology oriented. Does not consider the psychological motivations of end users Ignores influence of norms and self-efficacy and individual characteristics	Hsu *et al*., 2011
Protection Motivation Theory (PMT)	Threat appraisal: (perceived severity, perceived vulnerability) and coping appraisal: (perceived self-efficacy, perceived response efficacy)	Assumes rationality of behaviour and that their adoption of certain behaviour can be motivated by fear	Gundu & Flowerday, 2012
Integrated Model of Behaviour Prediction (IMBP)	Intention, skills, environmental factors, beliefs, attitudes, perceived normative pressure(subjective and descriptive norms) and self- efficacy	Acknowledges irrationality of human behaviour	

The first four models seem rather simplistic to describe human behaviour, and, except for TPB, rely on rationality of human behaviour, which is bound to make a model lack predictive power. The IMBP model might be the only model rich enough to come close to describing human decision-making in the security context and to be helpful in understanding adoption or rejection of security tools.

3. Applying IMBP in the Smartphone Security Domain

Smartphone security behaviour involves the adoption of security tools such as screen lock, the awareness of security threats, and other security-related practices such as granting excessive permissions to an application. Behaviours can be categorized as

either positive or negative behaviours. Positive security behaviours are behaviours of *commission* such as choosing strong passwords or the use of anti-virus applications. Negative behaviours imply *omission*: *not* 'jailbreaking' a phone or *not* granting excessive permissions to applications. All behaviours seek to prolong the device life span and to prevent any unwanted situations.

It is common practice by academic researchers to borrow theories from other domains. The healthcare domain provides many theories that seek to model human health behaviours, for example, Protection Motivation Theory and the Health Belief Model. These theories were developed to understand health behaviour such as exercising, following healthy diet and using protection and hygiene products in order to prevent diseases. There are similarities between health and security behaviours. Both are trying to avoid unwanted situations and the adoption of these behaviours resulted in avoidance of diseases or security incidents. Therefore, it seems promising to use one of these theories to understand smartphone security behaviour. IMBP was developed in 2000 based on the Health Beliefs Model, the Theory of Reasoned Action and Social Cognitive Theory. All of these three theories have been tested in the computer security domain; therefore, this model's foundations have thus been tested. This model suggests three determinants of someone's intention to engage in a behaviour. These three variables, also called 'proximal variables', are: *attitude*, *perceived norm* and *self-efficacy*. Also, this model considered other 'distal' or background variables, which play an indirect role in influencing the behaviour and they are mediated by the proximal variables (Fishbein & Yzer, 2003). Although the distal variables that can be considered are specified in the model (Fishbein, 2000), the number of variables is virtually unlimited (Fishbein & Ajzen, 2011).

Since IMBP is a relatively new model its validity has not been widely tested, and such testing as has been carried out has mostly been in the health or education domains (Robbins & Niederdeppe, 2015) (Kreijns *et al.*, 2013). Because this model has not been tested in the field of human-centred security, this section will consider the factors that should be incorporated in order to model smartphone security behaviours.

The distal variables in this model include demographic variables, such as age, gender and culture, personality trait, moods, media exposure and other individual differences (e.g. perceived risk) (Fishbein & Yzer, 2003). Except for media exposure, all these factors are individual characteristics. However, since these factors can be extended in the model (Fishbein & Ajzen, 2011), the existing human-centric literature suggests other variables that might play an important role in smartphone users reluctant to adopt security-related behaviours, for example. In order to isolate the factors that have been shown to have an effect on smartphone users security decisions, related work in human-centric studies in the smartphone security domain are briefly reviewed:

Gender. Skog (2002) has reported a big difference between males and females in their attitudes to their smartphones. While males emphasised the functional features, females paid more attention to the appearance thereof. Barn *et al*., (2014) found that male students were less cautious about their privacy than female students. They were

also more likely to share their personal data and contact details with other applications and to shop online using their phones.

Shared devices. Karlson *et al*, (2009) and Hang *et al*, (2012) shed light on the role of sharing on adopting security measures. As most of the current authentication systems, such as the screen lock mechanism, follow an "all-or-nothing" approach; they reported on the privacy concerns of smartphone users sharing their devices with others.

Privacy concerns. 208 Android users were asked about their privacy concerns (Felt *et al*., 2012). They claimed they had aborted the installation of an application at least once due to excessive permission requests. This highlights the impact of privacy concerns on smartphone users' security decisions.

Context. Researchers found a correlation between smartphone locking behaviour and context of use. Harbach *et al*., (2014) performed a real-life field study to investigate unlocking behaviours of smartphone users by using an application that automatically logged locking activities of 52 Android smartphone users for a month. They found that users spent up to 9% of the overall device usage time interacting with the unlock screen and, in about 1/4 of smartphone usage situations, owners considered the locking screen to be unnecessary. Moreover, this study found that even those who did lock their devices considered it unnecessary when in private locations. They suggested implementation of context-dependent locking.

Egelman *et al*., (2014) replicated the study done by (Harbach *et al*., 2014) but with some modifications to complement the findings. Their study investigated several threat models by comparing participants' perceptions of the sensitivity of the stored data on their devices. Based on an experimental investigation, they suggested design guidelines to help improve smartphone unlocking adoption. Although the Harbach *et al.* study reported the superfluity of unlocking in private, the latter study found that 1/4 of the participants enabled locking to protect their data specifically from family and friends. Thus, they suggested that personal preferences be considered when designing locking mechanisms.

These studies reveal that smartphone users have differing preferences with respect to their decisions to secure their Smartphones in different contexts. Since security measures are mostly designed with fixed features for all smartphone users, they do not fit in with individual users' preferences and this mismatch might well lead to non-adoption. For example, most unlocking functions protect all the data in the mobile devices except perhaps use of the camera. Some users might prefer to release other applications from the need for authentication too. The current atomicity of locking might discourage use of the locking mechanism altogether.

Personality. In their study into using message-based interventions to change the screen lock behaviour of smartphone users (Van Bruggen *et al*., 2013) researchers collected personality data based on the "Big Five" personality traits and could not find any significant correlation between personality traits and the success of

interventions except from a very small impact of "agreeableness" in terms of responding to the intervention.

Device Operating System. Some studies (Ophoff & Robinson, 2014) (Benenson *et al*., 2013) examined differences in user security behaviours on different mobile platforms; particularly between Android and iOS. It was found that Android users were more likely to install security applications such as virus scanners, as compared to IOS users. However, it was not clear that this was due to increased awareness levels or because of their confidence in Apple to protect their phones (Benenson *et al*., 2013) (Mylonas *et al*., 2013).

Morality. Van Bruggen *et al*., (2013) studied the adoption of Smartphone security behaviours, focusing on screen lock behaviour. They conducted an observation study on 149 Android users over period of five months to explore the baseline usage of security measures by smartphone users and to study the ability of message interventions to change security behaviour. They designed three types of intervention message: *morality*, *deterrence* and *incentives* and found that messages based on morality did have some impact on user behaviour.

Ethnicity. Barn *et al*., (2014) found a major difference in the levels of awareness of smartphone information security among users of different ethnic backgrounds. Users with a white ethnic background tended to be less concerned about data security than those from Black or Asian background.

Peer effect. Van Bruggen *et al*., (2013) reported a peer effect impact on screen locking behaviour, as a response to an intervention message. Those participants who changed their security behaviour as a consequence of the intervention were highly likely to have face-to-face contact with other participants who also changed their behaviours.

Technical skills. Users' technical skills affected their security-related adoption decisions on smartphones. Users who enabled encryption, remote data wipe, and remote device locator tended to be more technically savvy (Ophoff & Robinson, 2014).

Faulty or Incomplete Mental Models. Benenson *et al*., (2012) conducted the first study into the role of users in the security of smartphone devices. They used semi-structured interviews to investigate user attitudes to smartphone security. They concluded that faulty or incomplete mental models played a significant role in impacting users' security behaviours.

We have incorporated these factors into the IMBP model, depicted in Figure 1. The background variables in the model reflect factors that emerged from the literature. Most of these variables emerged from studies of the adoption of the Smartphone screen lock mechanism. Other studies considered mobile security practice in general. Some considered the omission of security behaviours, such as the adoption of other security measures, while yet others addressed the commission of insecure behaviours, such as people unthinkingly granting excessive permissions. Some

literature examined these variables for smartphone' users personal usage while others use them to study employee security behaviours. The majority of these studies were conducted on university students, even though the aims of these studies were to understand smartphone usage in general. Few studies focused on the security behaviours of a particular population such as older people.

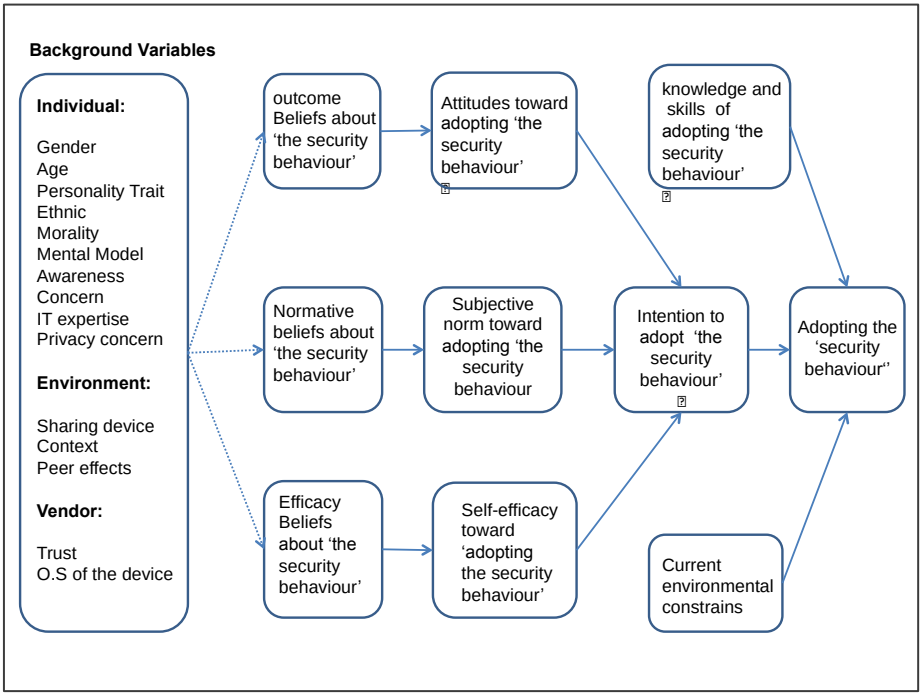

Figure 1 Applying IMBP to Smartphone Security

4. Discussion

This section discusses how well the model proposed in Figure 1 reflects smartphone security usage.

Background factors can be divided into three classes: *individual*, *environmental* and *vendor* variables. The first represents factors associated with the each individual user and they can be divided into two sections: *controlled* and *uncontrolled* variables. Uncontrolled variables are fixed features that users cannot change such as ethnicity, gender, age and personality. Studying these variables within the smartphone security domain can help in designing personalized security mechanisms or can help employers to design effective security policies. The controlled variables can be influenced by interventions such as morality, for example. The environmental category represents variables that can be impacted by the environment the user is interacting with. This includes peer influence or context of use. The final category is associated with the vendor of the device or the developer of a certain application such as the Operating System.

5. Conclusion

Freely available security tools and measures are not ubiquitously used by smartphone owners. We wanted to model security behaviours in order to understand adoption or rejection of these tools. The IMBP model appears to be the best model for reflecting a number of important factors informing smartphone security intentions. We tested the applicability this model by reviewing the research literature, and found it a promising match. Since this model has not yet been tested in human-centred security, future work will seek to validate the model with Smartphone owners.

6. References

Adams, A., & Sasse, M. A. (1999), "Users are not the enemy," *Communications of the ACM*, Vol. 42, No. 12, pp 40-46.

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

Aldaraiseh, A., Alomari, D., Alhamdi, H., Hamad, N., & Althemali, R. (2015), "Effectiveness of IPhone's TouchID: KSA Case Study," *International Journal of Advanced Computer Science and Applications (IJACSA)* , Vol. 6, No.1 ,pp 154-161.

Barn , B. S., Barn , R., & Tan, J.-P. (2014), "Young People and Smart Phones: An Empirical Study on Information Security," *2014 47th Hawaii International Conference on System Sciences (HICSS)*, pp 4504-4514.

Benenson, Z., Gassmann, F., & Reinfelder, L. (2013), "Android and iOS users' differences concerning security and privacy," *CHI '13 Extended Abstracts on Human Factors in Computing Systems*, pp 817-822.

Benenson, Z., Kroll-Peters, O., & Krupp, M. (2012), "Attitudes to IT security when using a smartphone," *Federated Conference on Computer Science and Information Systems (FedCSIS)*, pp 1179-1183, IEEE.

Bloomberg, L. D., & Volpe, M. (2015), *Completing Your Qualitative Dissertation: A Road Map From Beginning to End*, SAGE Publications, ISBN 9781-506307695.

Chen, H., & Li, W. (2014), "Understanding organization employee's information security omission behavior: An integrated model of social norm and deterrence," *Proceedings - Pacific Asia Conference on Information Systems, PACIS 2014*.

Consumer Reports. (2012), "Keep Your Phone Safe: How to Protect Yourself from Wireless Threats,"www.consumerreports.org/cro/magazine/2013/06/keep-your-phone-safe/index.htm, (Accessed 2nd October 2015).

Davis, F. D. (1989), "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, Vol. 13, No.3, pp 319-339.

Egelman, S., Jain, S., Portnoff, R. S., Liao, K., Consolvo, S., & Wagner, D. (2014), "Are

you ready to lock?," *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 750-761, ACM.

Eisenhart, M. (1991), "Conceptual frameworks for research circa 1991: Ideas from a cultural anthropologist; implications for mathematics education researchers," *Paper presented at the Proceedings of the Thirteenth Annual Meeting North American Paper of the International Group for the Psychology of Mathematics Education.* Virginia, USA.: Blacksburg.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012), "Android permissions: User attention, comprehension, and behaviour," *Proceedings of the Eighth Symposium on Usable Privacy and Security*, p. 3, ACM.

Fishbein, M. (2000), "The role of theory in HIV prevention," Vol. 12, pp 273–278.

Fishbein, M., & Ajzen, I. (2011), *Predicting and Changing Behavior: The Reasoned Action Approach*. New York: Taylor & Francis, ISBN: 9780-805859249.

Fishbein, M., & Yzer, M. C. (2003), "Using theory to design effective health behavior interventions," *Communication Theory* , Vol.13, No. 2, pp164–183.

Furnell, S. (2005), "Why users cannot use security?," *Computers & Security*, Vol.*24*, No. 4, pp 274–279.

Gibbs, J. P. (1975), *Crime, punishment, and deterrence.* New York: Elsevier, ISBN: 9780444990167.

Gundu, T., & Flowerday, S. (2012), "The enemy within: A behavioural intention model and an information security awareness process," *In Information Security for South Africa (ISSA)*.

Hang, A., Zezschwitz, E. v., De Luca, A., & Hussmann, H. (2012), "Too much information!: user attitudes towards smartphone sharing," *In Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design*, ACM.

Harbach, M., Zezschwitz, E. v., Fichtner, A., De Luca, A., & Smith, M. (2014), " It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception," *Symposium On Usable Privacy and Security (SOUPS 2014)*, pp 213-230.

Hsu, L., Wang, F., & Lin, C. (2011), "Investigating customer adoption behaviours in mobile financial services," *International Journal of Mobile Communications , Vol.9* , No. 5, pp 477-494.

Jeon, W., Kim, J., Lee, Y. and Won, D. (2011), "A *practical analysis of smartphone security," In Proceedings of the 2011 international conference on Human interface and the management of information - Volume Part I* (HI'11), Vol. Part I. Springer-Verlag, Berlin, Heidelberg, pp. 311-320.

Karlson, A. K., Brush, A., & Schechter, S. (2009), "Can I borrow your phone?: understanding concerns when sharing mobile phones," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp 1647-1650, ACM.

Kreijns, K., Van Acker, F., & Vermeulen, M. (2013), "What stimulates teachers to integrate

ICT in their pedagogical practices? The use of digital learning materials in education," *Computers in human behavior* , Vol.29, No.1, pp 217-225.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014), "Information security awareness and behavior: a theory-based literature review," *Management Research Review* , Vol.37 , No.12, pp 1049-1092.

Mylonas, A., Kastania, A., & Grit, D. (2013), "Delegate the smartphone user? Security awareness in smartphone platforms," *Computers & Security* , Vol.34, pp 47-66.

Ngoqo, B., & Flowerday, S. V. (2015), "Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users," *Computers & Security* , Vol.53, pp 132-142.

Ophoff, J., & Robinson, M. (2014), "Exploring end-user smartphone security awareness within a South African context," *Information Security for South Africa (ISSA)* , pp.1-7.

Parker, F., Ophoff, J., Van Belle, J. P. and Karia, R. (2015) "Security awareness and adoption of security controls by smartphone users," *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, Cape Town, pp. 99-104.

Robbins, R., & Niederdeppe, J. (2015), "Using the integrative model of behavioral prediction to identify promising message strategies to promote healthy sleep behavior among college students," *Health communication*, Vol.30, No.1, pp 26-38.

Rogers, R. W. (1975), "A protection motivation theory of fear appeals and attitude change," *Journal of Psychology* , Vol. 91, pp 93-114.

Skog, B. (2002), "Mobiles and the Norwegian teen: identity, gender and class," *Perpetual Contact* , pp. 255-273.

Sussman , S., & Sussman, A. N. (2001), "Chapter 4: Praxis in Health Behavior Program Development," In S. Sussman , *Handbook of Program Development for Health Behavior Research & Practice.* Thousand Oaks, California: SAGE Publications.

Van Bruggen, D., Liu, S., Kajzer, M., Striegel, A., Crowell, C. R., & D'Arcy, J. (2013), "Modifying smartphone user locking behaviour," *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13)*, p. 14, ACM.