

“If it’s urgent or it is stopping me from doing something, then I might just go straight at it”: a study into Home Data Security Decisions

Norbert Nthala and Ivan Flechais

Department of Computer Science,
University of Oxford,
Oxford, OX1 3QD, UK
{norbert.nthala, ivan.flechais}@cs.ox.ac.uk

Abstract. Data security incidents have led to a wave of security awareness campaigns by public institutions targeted towards the so-called home user. Despite this rise, studies have shown poor adoption rates of security measures by the target. In this paper, we conduct a qualitative investigation of 15 home users, analyse the data using Grounded Theory and present a model of factors of data security decisions made in the home. We further consolidate the literature on this topic and analyse our findings against it using meta-synthesis. From this we identify the critical issues that surround data security in the home environment. We finally present a consolidated theoretical model for investigating factors that influence security practices in the home, and suggest future work based on our findings.

Keywords: Home user · Data security · Decision making · Security-related behaviours · Grounded Theory · Meta-synthesis

1 Introduction

Incidents affecting personal information services and assets regularly hit the news headlines, and raising security awareness is the most commonly proffered solution to the widely perceived problem of inadequate security in the home [5]. Set against a backdrop of government-backed efforts to improve security, increases in spending on organisational IT security and a greater emphasis on compliance and data protection, securing the “home user” has received far too little attention. Despite a real, and growing, series of existing and foreseeable threats targeting the home user, research thus far has only scratched the surface of the breadth and depth of the problem domain – not least of which by tacitly proposing that home users are broadly defined as “not professionals in computing”. Furthermore, given that homes are also targeted to enable attacks on third parties (e.g. DDoS through compromised home devices, attacks on company data through compromised home computers tunneling into protected company networks, or attacks aiming to compromise key employees at home), the security

benefits of improving home data security are clear, and yet more needs to be done to understand how we can better achieve home data security.

The use of information technology in households is increasing, and the number of networked devices available to household users is also increasing and likely to continue to do so with the advent of smart cities, wearable computing, and other Internet of Things devices. Networked devices in the home include laptops/PCs, mobile phones, tablets, games consoles, routers, networked cars, smart meters, medical equipment and many more. Home networks can be wired, wireless, or both, and connect one or more household devices to the Internet through local Internet Service Providers (ISP) or through mobile data connections. In 2015, the International Telecommunications Union (ITU) reported that households with a computer in developed countries had increased from 55.5% in 2005 to 80.8% in 2015, while that of developing countries jumped from 14.6% in 2005 to 32.9% in 2015 [10]. ITU further reported that households with Internet access at home increased from 44.7% in 2005 to 81.3% in 2015 for developed countries, and from 8.1% in 2005 to 34.1% in 2015 for developing countries [10].

While organisations manage the security of their data and systems strategically through security policies, the protection of home users is left to the initiative of the users [11]. Home users utilise different online services, each requiring different security behaviour from users (e.g. passwords, tokens, privacy settings, and others). The complexity of these security requirements has led users to devise their own mechanisms and workarounds for managing the security for the online services. And while the number of services and devices that need security is growing, the time, knowledge, and budget that typical home users allocate to securing their data is small, and likely to remain so. Consequently, a large number of exploited vulnerabilities in computing systems involve users of the systems making bad choices [17]. Despite efforts by governments and commercial entities to improve the security of cyberspace by raising security awareness to home users, various studies [1, 2, 3, 9] show that home users still do not adequately apply security controls for their home systems and often ignore or do not act in ways that would keep them secure. Work has been undertaken on how to analyse and improve security awareness, including [4, 8], but a larger question remains as to whether awareness is the correct solution to the problem.

Many studies, including [13, 14, 16, 12, 15, 11], have referred to the concept of ‘the home (computer) user’ without satisfactorily defining this. Most do not define the concept [13, 12, 15, 11], and those that do tend to settle on broad generalities, e.g. “the distinguishing characteristic is that the users are not professionals in computing” [16], or “a citizen with varying age and technical knowledge who uses Information Communication Technologies (ICTs) for personal use anywhere outside their work environments” [14]. We argue that home user security is a growing concern that has not received sufficient attention, and that improving home data security needs to start from a more grounded understanding of home users, the context of use in which they operate, and how they make data security decisions.

This study focusses on understanding data security decisions made by home users: factors that influence outcomes of these decisions, common scenarios in which security decisions are made in the home, sources of information to enable decision-making, and sources of support and assistance for decision-making. This helps to provide clear evidence for future work to improve education, technology, and practices for home data security. This is all the more important in light of the October 2016 attack on Dyn which took down a number of major websites in the USA and is thought to have been enabled by insecure IoT devices in homes.

2 Literature Review

2.1 Understanding the Home

Home users consist of individuals from any demographic, ranging from children, teenagers, parents, working and non-working professionals, retired, elderly, infirm, and disabled individuals, each with different resources, education, skills, capabilities, and interests. To further clarify and define home users, and drawing from the work of Venkatesh [18] and Meshkova et al [19], we present a model of home computer users that spans three distinct spaces: social, activity, and technological.

Social Space The social space of home users is complex and has been explored according to Household (people living in one building) and Family (exploring different types of family unit) [20]. To this we add a third category of Neighbourhood and Friends (which encompasses geographical proximity such as housing estates, but also social proximity such as common interest groups, friendships, and other social groupings). This is supported by the study from Ng et. al. [?] that found that home users are influenced by different factors to practice security, among them family and peer influence. While the importance of individual stakeholders in home security decisions has not been explored, research exploring the role of individuals in the context of security design activities has clearly highlighted the importance of individual involvement, motivation, responsibility and communication in the decision-making process [21].

Activity Space The activity space aims to represent the type of computer centric pursuits that occur in a home. Different priorities exist in different homes, much determined by the home social space. The activities comprise, but are not limited to, family communications, correspondence, home shopping, remote (online) education, school work, word processing, and entertainment. The services and event of the ontology of the home environment presented in [19] belong to this space.

Technology Space According to Venkatesh [18], the technological structure of the home is complex and determines the operation of the system of its activities, and the patterns of home interactions relative to its goals. The level of

technology is distinct from one home to the next, however this is a crucial space to understand in exploring the issues of data security, as it intimately informs the threat and vulnerability space, and also strongly influences the type and complexity of technical controls.

2.2 Security Behavioural Theories

Several studies have utilised a number of predictive theories to study specific security behaviours of home users. These models are most often extensions of existing social cognitive theories of factors that produce risky behaviour in other decision situations [16]. Prominent among these models are the Theory of Planned Behaviour (TPB) [22], and the Protection Motivation Theory (PMT) [23]. Researchers have sought to explore antecedents from such theories as factors that influence a home user's security behaviour.

When applied to security behaviour, these two predictive theories operate on a general assumption that there are assets which are facing security threats, and that there are security controls available to counter the threats. We call this the security space. TBP considers the intention of a person to be an immediate determinant of an action or a behaviour. The behaviour in this case being applying appropriate security controls. TPB states that intentions are determined by three factors: attitude towards the behaviour, subjective norm (social influence), and perceived behavioural control. Ng and Rahim [11] used decomposed TPB (an extended version of TPB) to investigate the factors that influence a user's intention to practice home computer security. Their study found that both attitude and subjective norms had a significant positive relationship with the intention to practice computer security. However, the study could not clearly identify the relationship between perceived behavioural controls and the intention to practice home computer security due to a number of unexplained differences in the results. In a different study, Lee and Kozar [30] extended TPB with concepts from diffusion of innovations model, and IT ethics and morality to investigate factors affecting an individual's decision to adopt anti-spyware software. Their study found that attitude, subjective norms, perceived behavioural control, and denial of responsibility significantly affected an individual's intention to adopt.

PMT posits two closely related pathways whose balance determines the likelihood of a risky behaviour to occur. The *threat appraisal pathway* compares perceived rewards (intrinsic and extrinsic) with perceived threats (severity and vulnerability) that the behaviour poses. The *coping appraisal pathway* compares coping efficacy (self-efficacy and response efficacy) with perceived response costs of the behaviour. Milne et al [24] draw upon PMT and social cognitive theory to investigate the extent to which the level of perceived threat and likelihood of threat along with online self-efficacy affect online behaviours. Thus what factors lead consumers to make adaptive and maladaptive responses in the face of privacy and security threats. A national online survey was designed based on these theories and administered to 449 non-students. The researchers found out that self-efficacy plays a key role in a consumer's choice to perform risky online

behaviours, and perceived threat and likelihood of threat influence the decision to choose an adaptive or maladaptive behaviour.

Other researchers have however used other approaches, such as qualitative interviews to study security behaviours of home users. Redmiles et al [7] interviewed 25 participants in investigating where users learn security behaviours, and why users accept or reject different advice. The study reported that users get security advice from sources they trust which include workplace, service providers, IT professionals, family members and friends [7]. The study found that users reject advice due to too much marketing information, and threatening users' privacy. The researchers also indicated users disregard some security roles because they assume somebody is responsible for that. In a similar study, Herley [5] found three reasons that lead to users' rejection of security advice: they are overwhelmed; the benefit is moot in some cases or is perceived to be moot; and claimed benefits are not based on evidence.

3 Methodology

3.1 Grounded Theory

The aim of this study is to elicit data regarding data security decisions made by home users. For this purpose, we conducted semi-structured interviews to get the benefits of using a rigid script of well-defined, ordered questions to control the flow and consistency of the interview, while keeping the interview opened up for both depth and breadth topic exploration [25]. All respondents were asked identical questions in the same sequence, but the interviewer probed inductively on key responses. The questions took into consideration all the three home environment spaces discussed in **section 2.1** to ensure the home context was fully explored. We asked questions about participant demographics; devices and services they use; their concerns about data security, and if they have ever experienced a data security breach; what they did/do to secure their data, and who did it; what informs their choice of security measures; their attitude toward data security, largely elicited through specific scenarios; the kind of support they need(ed), and where they seek/sought it; and their expectations about the security of their data.

As the interview data was being collected, it was qualitatively analysed using Grounded Theory [26] to identify significant themes emerging from the data and to inform the next data collection. Due to its theory-building qualitative nature, grounded theory is well-suited to problems where little is already known. This makes it the ideal choice for studying factors and issues that affect the home user data security decision making.

Participants Fifteen participants from Oxford took part in the study: 9 Male (4 married, 5 single), and 6 Female (2 married, 4 single). Of these, 4 were Asian, 5 White, 4 African, and 2 Black American. Their ages ranged from 18 to 34.

The participants were recruited through snowball sampling, with the first set purposefully selected.

Our study was ethically reviewed and approved by the Social Sciences and Humanities Inter-divisional Research Ethics Committee at the University of Oxford.

3.2 Meta-synthesis

As explained in **section 2.2**, several studies on the security behaviour of home users have reported varying reasons and factors that influence such behaviour. In this view, we sought to consolidate the literature on this topic, and later compare it with results from our study to identify common elements and attempt to bridge the gaps that exist in the different findings. We used meta-synthesis [27] to achieve this. This is a non-statistical technique used to integrate, evaluate, and interpret the findings of multiple qualitative research studies. The studies may be combined to identify their common core elements and themes. Meta-synthesis involves analysing and synthesising key elements in each study, with the aim of transforming individual findings into new conceptualisations and interpretations.

A conventional literature search was done using different terms such as ‘home user’, ‘home computer user’, ‘security behaviour’, and many more. The databases searched included ACM Digital Library, IEEE Xplore, Compendex, Science Direct, ProQuest, and others. All papers published in English on the subject were included. Papers with a quantitative research focus, such as those using the behavioural theories to conduct surveys, were excluded. However, these excluded papers gave us a lead to the original qualitative papers of the theory employed, which we included in our study. Other relevant literature was identified through an iterative process based on the research papers.

4 Interview Results

Our analysis of security decision-making in the home highlighted four main themes that surround the process (see Figure 1): **Stimuli** (cues to action), **Support**, **Stakeholders**, and **Context**. We explore these in more detail below:

4.1 Stimuli

The participants outlined the following five different cues that drive their security decisions. All the cues however share one thing in common, security concern.

Security concern Home user data security concerns fall into three groups: *Uncertainty*, where the user is not sure about particular security aspects; *Loss*, where the user is concerned about losing either data or some material thing; and *Nuisance*, where the user is concerned about something causing inconvenience or annoyance.

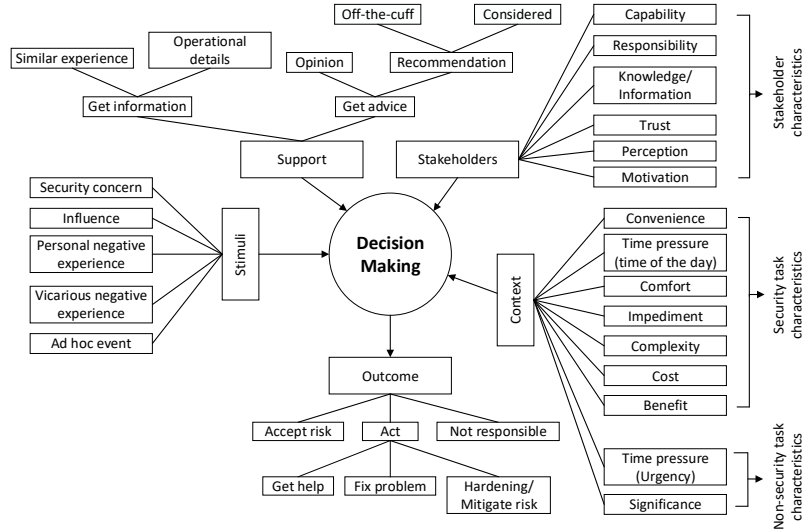


Fig. 1. Home data security decision-making factors model

Uncertainty includes issues like not being sure about how secure a user's credentials are with a service provider, who has access to them on the back-end? Should one accept access permission requests from applications? If accepted, what kind of data are the applications accessing in the background? One male participant said:

Like for my android, I am not sure about the permissions. Of course when you install an app, you give it permissions to read your mic, to use your camera, and use your storage. So I don't know to what extent those apps are doing the right thing. Is there a possibility that may be they are viewing my messages without me knowing, so I don't know. That's about all. For android, it's the permissions on the apps. I don't know what they are doing because I know that facebook, for example, has access to my photos. So I don't know how often it accesses my photos. Does it access the photos when am not using the app? And what does it do with my photos? [P3,M].

Loss was noted to be multifaceted with participants referring to both material and non-material loss. Loss of money (which is linked to loss of banking details) from a bank account through unknown transactions, for instance, was a common concern for all participants, with some having experienced this before (*personal negative experience*). One participant talking about his online banking experience said:

Something happened. That was the time I just stopped. I have been following up with the bank to find out who was removing the money, but because of my job

I don't have time. So they have been sending me letters. I just went there and told them I don't need it any more, so cancel it. Mostly I have cash in hand, so I don't bother much. [P2, M].

Some reported having heard about someone's (vicarious) negative experience from which they were motivated to act on their security behaviours:

...on the newspaper or whatever, from time to time you read those stories that some people lost their money in the bank and the bank denied the responsibility of controlling... So basically may be someone else withdrew money from the bank, from this person's account, but the bank say that all the process was authorised, 'there is no problem in our process'. [P7, M].

Other common concerns associated with loss include loss of confidentiality, loss of integrity, data loss, data theft, and loss of privacy. Different kinds of data linked to these concerns include health data, pictures, contact details, banking details, communication data, and location data. Some users reported that they perform a trade-off between the different kinds of data according to their specific needs, for instance:

...So I don't quite mind to share location, but I don't share my photos. [P14, F]

Concerns under nuisance include unwanted advertisements sent to personal address, nuisance calls, poor device performance, spam, and scam. One participant said:

I thought they were just gonna try and steal my data so they could call me all the time with nuisance calls, or they might just send a virus across, or you know use the data to find out about me and send me specific advertising things I don't like. [P10, F].

As can be seen here, security decisions, influenced by a concern, arise in a number of ways, including personal or vicarious negative experience, an ad hoc encounter such as a pop-up, or based on social influence, as can be seen below:

Normally, if I get a pop-up saying that isn't secure, I usually stop. [P15, M]

I'm only concerned because people think I should be concerned. I do understand the risks, but so far, like my bank account has never been hacked... Colleagues that I work with, the media say we should all be concerned about our privacy, and that's it really. [P4, F]

However, our analysis revealed that home users respond differently to different cues. Those who have had a negative experience put in much more effort to avoid similar or other breaches compared to those who are socially influenced. One respondent who had not experienced a security breach before said:

I mean it's like being concerned about not being chased by a dog that you have never seen. [P12, F]

4.2 Stakeholders

The analysis brought to light the importance of understanding the stakeholders who are crucial in ensuring data security in the home environment. These include all who play a role in home data security and/or in security decision-making. Security responsibility in the home lies with two distinct groups of stakeholders

(see Figure 2): **informal stakeholders**, composed of the social space in the home environment; and **business stakeholders**, composed of service providers, vendors, governments, and others.

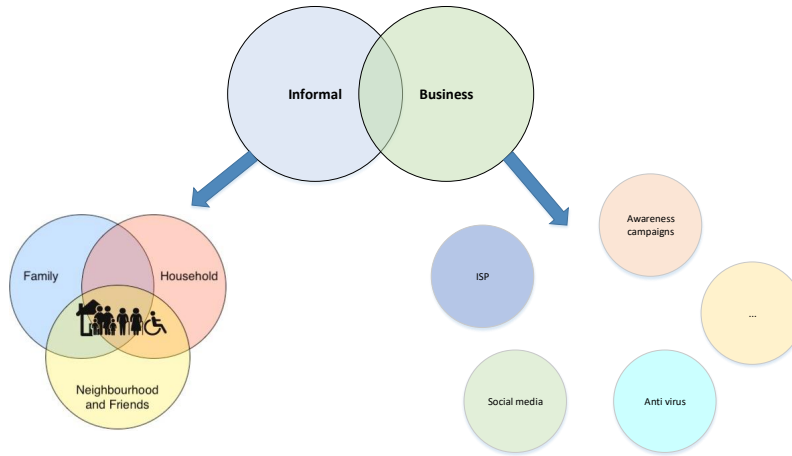


Fig. 2. Home data security stakeholders

As depicted in Figure 2, the social spaces in the informal sector can overlap (i.e. family can exist within one household or many, within one neighbourhood or multiple; households may contain families but do not have to, etc.). These differences influence the extent to which individuals become involved, motivated, and responsible for data security activities and decisions. For instance, just to quote some participants:

We always try to consult each other about security issues. As I'm an expert, I can differentiate between security and privacy, but my wife doesn't. So we look at those security issues in general... what I try to do is to try to explain the potential risks, and leave my partner to make a decision herself. [P5, M]

My mum will sometimes ring me and say I have got a text message that says I have won a mountain bike, and I will be like you should just delete that because it's just spam. Or she had once where it said she had entered a competition to win a car and she needed to follow the following link to verify her details. And she rang me up and say I haven't been to the airport, why am I getting these messages. I explained to her that people just got your data from somewhere, just delete it. [P4, F]

My supervisor is my security lecturer, is the one who recommended it. So I followed her advice... We had a short chat, and she explained how it works, and why it's important. Then I bought the idea. [P3, M]

The stakeholders in the business sector however frequently operate independently of each other. For instance, governments provide awareness campaigns; vendors provide antivirus software, password managers, and other services. In rare circumstances however, they do overlap. For instance, the National Cyber Security Alliance (NCSA) provides details and links to free security tools on its website. These stakeholders do also influence the security actions and decisions home users make in a number of ways explained below.

A number of interrelated characteristics of the stakeholder influence the overall decision-making process. The **capability**, that encompasses the skills, power, and ability of the respective responsible stakeholder play a crucial role in deciding what one is can and is supposed to do. This is also closely related to **knowledge/information** available to the stakeholder at the time a decision is made.

I take reasonable steps to be secure but maybe there is more I could do, but at the moment I don't know what else I could. [P11, F]

These two characteristics were also revealed to be influential among stakeholders when deciding whether to seek support and where to seek the service.

...usually I come and check with ... in IT. I tell him that I was trying to install this application, this popped up. I have tried Googling what it was or check if it is fine, but couldn't find anything. Do you think it will be ok? [P1, M]

I would probably have to read a bit more, or may be call someone who has a bit more experience than me, and see what they suggest. Because am not an expert so I would call someone who is much more familiar with IT related things. [P8, M]

I told you my friend, ..., because he is a Computer Engineer, mostly he has to put some security. [P2, M]

Another important characteristic in security decision-making is **responsibility**. The participants reported having considered whether they are responsible for doing a particular action or not. For some actions, stakeholders in the home believe someone, either among their social space or in the business sector, is responsible for keeping their data secure. Asked about who they think is responsible for implementing what they expect to be a good level of security, some participants said:

If it's a corporation [the service provider], a big company, then the government should be responsible. [P6, M]

would say it could be apple, it could be google I guess. When they allow those developers to upload their product to apple store or google store, I think they should be responsible for the security. [P7, M]

I guess [service providers should] limit the number of people that have access to the data. And for example on Facebook, I don't want any of my own personal information shared with advertisers. Yeah, just to not share personal information with advertisers or second hand parties or things like that. [P9, F]

So both parties. Both the providers of services and also the users of the services. The providers should ensure that the data of the users is secure enough that it is not likely to end in random people, but also important that the user inputs like good passwords, is able to make sure that whatever setting that they are in is also secure enough for them to use the service. [P12, F]

Another important influential characteristic about stakeholders is their perception. Users reported to make security decisions based on brand recognition. Well-known service providers or tools are considered to be more secure (**trust-worthy**), and therefore require little to no attention. One participant said:

But what I believe is that I only install apps from the big companies. I don't install apps from private developers. So that would mean that I somehow trust those big companies, and usually if anything goes wrong, it doesn't affect only me. It affects a lot of people. [P7, M]

Apart from trusting service provider and/or tools/services, **trust** also extends to a source of security information. This includes colleagues, IT professionals, family members, peers, and websites providing the information. This comprises a combination of both informal and business stakeholders. Some participants said on this:

I'm slightly more confident with those that haven't got hacked yet, so I'm more trusting of them. [P1, M]

The most trusted data for me is from the service provider, rather than others. [P5, M]

Usually I look at the developers in case of software. Well are they credible, or at least big developers or they are open source developers well regarded in the community, then I will trust. [P6, M]

The last characteristic of stakeholders that plays a role in security decision-making in the home is **motivation**. Our analysis revealed a number of ways that motivate users to make security decisions or to carry out security actions. Among these are influence from the peers and the media, perceived capability, perceived responsibility, and availability of security information through well known channels among others.

4.3 Support

The results showed that home users seek different kinds of support, from different sources based on the purpose. Three different types of support have been identified: **Provision of labour**, which involves provision of actual security work; **information provision**, which involves sharing experiences and/or operational details of some security tool for example; and **Advice**, which involves the provision of an opinion, an off-the-cuff recommendation, or a considered recommendation. Based on the context, users need either information or advice to help them make a decision or to act. The information can pertain to operational details, such as instructions to remove a virus from a device. A participant said:

Yeah, just to be able to use it and how it works, and what I should do and not just have this installed on my computer.. [P14, F]

At other times, users seek to learn from someone who has had a similar experience and how they tackled it. This normally applies to experiences of those one is close to and trusts. One participant said:

I have a few friends who do IT and know more, kind of comfortable with more complex things of computers. Sometimes I ask them, but most of the times it's about whether they have experienced the same or if they have done the same thing. So it's not always the specialists. Sometimes am even [more] competent [than the friends I ask] though. It's just if they have ever downloaded an app or something some other time, if they have seen any issues. [P1, M]

In addition to information, home users also seek advice from trusted stakeholders (colleagues, IT Professionals, relations and peers, and websites). Advice comes in two forms; first as an opinion, where the advice helps the user make their own decision. For instance:

It's more of an opinion. I want to ask someone because sometimes there is a tendency to overlook certain things. [P1, M]

Second as a recommendation, which can be further divided into two. An off-the-cuff recommendation does not involve much effort from the provider of the recommendation. The provider simply gives advice from s/he knows. For instance:

Usually which antivirus is good? Is it ok if someone installed this kind of software? [P15, M]

Asked what kind of support she sought online, one participant said:

I just wanted a recommendation of what would be the most effective thing to do. [P9, F]

A considered recommendation requires the provider to put in extra effort to have a clear understanding of the problem in question before giving the recommendation. Asked what they would do in a scenario where someone they gave advice to suffered a breach, one participant said:

I would just go back to what I said before and see what the problem is, and then investigate ways to try and solve the problem. I would probably have to read a bit more, or maybe call someone who has a bit more experience than me, and see what they suggest. [P8, M]

The third and final type of support commonly sought in the home is labour. Users who perceive themselves as not capable of acting on security issues turn to trusted and skilled stakeholders for technical help. This is usually sought from colleagues, IT professionals, relations, and peers. Some participants said:

There is a friend who usually comes here. Mostly he is the one. If the laptop has a virus, I give it to him. He just wipes it and upgrades it again. [P2, M]

Yes, for my grandmother... She is not very competent when it comes to technological applications, or computers or anything of that nature... So I just had to install something to scan her emails to make sure there are no malicious things in there. [P8, M]

I usually check my mum's computer every now and again. Check if it's looking alright, especially if she says she has had some pop-ups and things, to see if there

is anything I can do to help her out. And sometimes my partner will have a look at it as well to see if there is a bit more we are able to do. [P4, F]

4.4 Context

The context in which a security decision is made has two characterising categories; **security task characteristics**, which defines issues related to the required security task that stakeholders take into consideration when making security decisions, and **non-security task characteristics**, which relates to issues about the primary task that a user is required to do.

One influential theme on security task characteristics is **convenience**. Users weigh the convenience of available security countermeasures against the importance of their activities. If functionality is preferred to security, users are willing to bypass or ignore recommended secure behaviours. Talking about two-factor authentication, one participant said:

...the time that I'm working where there is no network, I can't login to gmail. So it's a big disadvantage. [P11, M]

Next, **time pressure (time of the day)** has been noted to influence the outcome of security decisions made in the home. This has been shown to influence what a user would do when faced with a security decision at a particular time. One such scenario is:

There was something that was preventing me from going on a website and I was pretty sure it was fine. It wanted me to install something. I wasn't convinced I actually needed to install it. It was actually crashing the site when I wasn't installing it, but this was in the evening and I really wanted to get this done. [P1, M]

Comfort is another issue taken into consideration on the subject at hand. Home users care about the security of their data, and take actions to keep it secure. However, they would like to do what they want comfortably and not let security overheads get in their way. As one way of ensuring this, they tend to differentiate between important services and those that are less secure. In doing so, much effort is put on securing the most important services. One of the participants echoed their experience:

It is much more comfortable if you can save your password in the browser. Well, I have been tempted to do that you know – just save it in the browser – I just don't need to retype it over and over again. I occasionally do that for something not so important: accounts like twitter; but for something much more important like bank account or email, I will never save it there. [P13, M]

Impediment: If a security-related task stands in the way of users in achieving their primary task, we found that users weigh the two and do a trade-off.

If it's urgent or it is stopping me from doing something, then I might just go straight at it. [P1, M]

The **complexity** of a security task in relation to the stakeholder's capability influences what s/he can do or decide. In most cases, there is an interplay of the different factors that influence the outcome of a security decision. For instance,

complexity would be weighed against capability, and availability of required support in cases where the stakeholder is not capable of undertaking a decision or action.

I read online that we should delete cookies to keep our data secure, but I don't know how to do it and there is no one to do it for me at home. So I just accept the risk, and maybe some hackers have already stolen my data. [P14, F]

Cost and Benefit: The cost of performing a security task includes time, effort, financial resources. These are usually weighed against the expected reward after performing the required action. Asked about seeking information to inform security decision in a particular scenario, one participant said:

I think it's only a 3 seconds decision, I don't spend any more time on this. So just to look at what they wrote and then make a decision. [P7, M]

All but four of the participants shared the idea that they installed a free antivirus to keep viruses in check. They did not care much about having a virus at some point because they could always have someone clean their devices, which they state is to different from losing money in the bank.

The non-security characteristics that come to users' attention in light of security include **time pressure (Urgency)**, which revolves around the time constraints for completing the primary task, for instance

...I urgently wanted an Internet connection to do some work. I connected to a network which had the same name as our usual library network and required the same login details, but a warning showed up saying it was not a secure connection. Since I wanted the Internet badly, I just ignored the warning and connected. When I finished working, I realised someone had been reading my unread emails. [P11, F]

Another consideration is the *significance* of the primary task. Users consider the importance of what they are doing or the importance of what they are looking for. They are ready to trade security for something else in order to achieve what they want if the situation calls for it.

It depends on how much I want to use the thing. If it's just a curiosity thing, and something flashes, I just close it down. If it's something am actively looking for, I might go back out and look on other stuff to find out if this is the only place I can find it. Then I go ahead and do it. [P1, M]

...it did this with one website, but I knew that it was OK. So I kept browsing. It was always like 'this website is not secure, are you sure you want to continue?'. I did so because I think it was something for the University. Usually if they say this, if it's not important then I leave it. [P10, F]

5 Analysis of Interview Results against Literature

As discussed in **section 2.2**, the two main theories that have been used in studying the security behaviour of home users are TPB and PMT.

One clear area that is not covered by either theory is the situation where users state that they do not feel responsible for performing a particular behaviour. This has been reported by two independent field studies: our study and

Redmiles et al [7]. To make sense of this phenomenon, we turn to the widely used Triangle Model of Responsibility (TMR) [28]. In security studies, though not explicitly stated, TMR comes into play in the study by Blyth [29]. In this study, the researcher developed a socio-technical model of trust that utilises the concepts of responsibilities and roles so as to link the technical and social aspects of trust into a single inductive logical framework.

TMR states that in order to make evaluative reckonings concerning responsibility, one must have information related to prescriptions (rules and norms that guide an agent’s conduct), an event (the action in question), and identity (the agent’s role and abilities). TMR also seeks to understand if there is connectedness between the agent and the event due to the agent’s role and perception of control. Interdisciplinary studies have also shown that perceived control is directly and significantly related to responsibility. Those who perceive the capability to perform an action are more likely to feel internally obligated, and hence motivated, to produce positive outcomes [31]. We argue that understanding the three antecedents from TMR, together with the factors from TPB and PMT, can give us a more complete understanding of the home data security context.

Security decisions and behaviours are executed in a world of risk and uncertainty. We noted during our analysis of the interviews and as can be seen in Figure 1, that participants frequently referred to the concept of understanding the risk, and in some cases going further to accept the risk. Studies and theories such as risk homeostasis claim that individuals adjust their behaviours in response to changing variables to keep what they perceive as a constant accepted level of risk. Pearman et. al. explored home-user computer security behaviour and concluded that risk compensation occurs. Adams [33, 34] explains the notion of risk compensation by presenting a risk thermostat. He claims that individuals execute a balancing behaviour between their propensity to take risks (risk appetite) and perceived danger (risk perception), where risk propensity is determined by perceived rewards, whereas accidents (negative experiences) influence perceived danger.

We consolidate all these concepts from the different theories and models from literature and our model in Figure 1, and present a breakdown of the different factors that affect home data security decisions. Three general categories of Motivation, Capability, and Context are complemented by perception factors (see Figure 3). In turn, capability and contextual factors influence a home user’s motivation to practice security behaviours.

It is important to note that there are two dimensions of responsibility: *perceived responsibility*, which is presented by TMR referring to individual responsibility; and *actual responsibility*, where users fully understand their role. For instance, our study identified stakeholders in the home environment who make decisions and/or carry out security tasks on behalf of others (who are not capable), which presents an understanding of the actual responsibility that one has towards the others. This included parents/guardians making data security decisions on behalf of their children, and competent children/nephews/nieces deciding on behalf of their parents or grand parents.

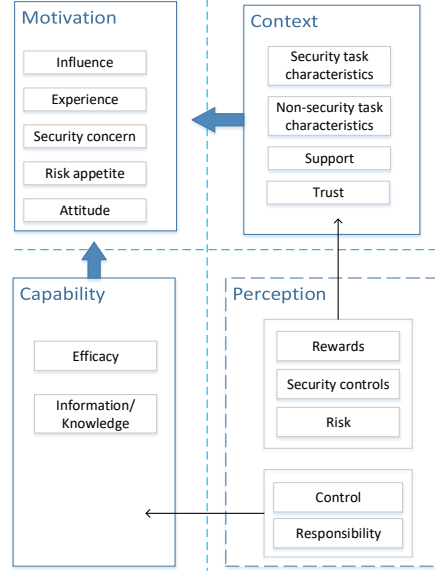


Fig. 3. Home data security environment

From this understanding of the home data security environment, we develop a consolidated theoretical model that can be used to investigate factors that influence home data security decisions and behaviours (see Figure 4).

6 Conclusion and Future Work

Home users are concerned about the security of their data, and do not deliberately ignore security advice or choose to behave insecurely. Our study reveals that home data security is a shared responsibility among different stakeholders, both business and informal. Contrary to the common approach of investigating home data security by targeting individuals, our findings suggest adopting a broad approach looking at all issues that play a role in security decisions and behaviours of home users, in particular focussing on the stakeholders and the context. A model of stakeholders that are involved in home data security has been presented, but further work needs to be carried out to explore this model in greater detail. Such work would look at the stakeholder’s role, level of involvement, and the impact they have on each other and the overall data security practice in the home.

Our findings have also revealed a number of issues related to support. Building on this, future work will seek to explore effective ways of delivering more tailored kinds of support to home users. This paper has also presented a consolidated theoretical model of home data security, bringing together existing

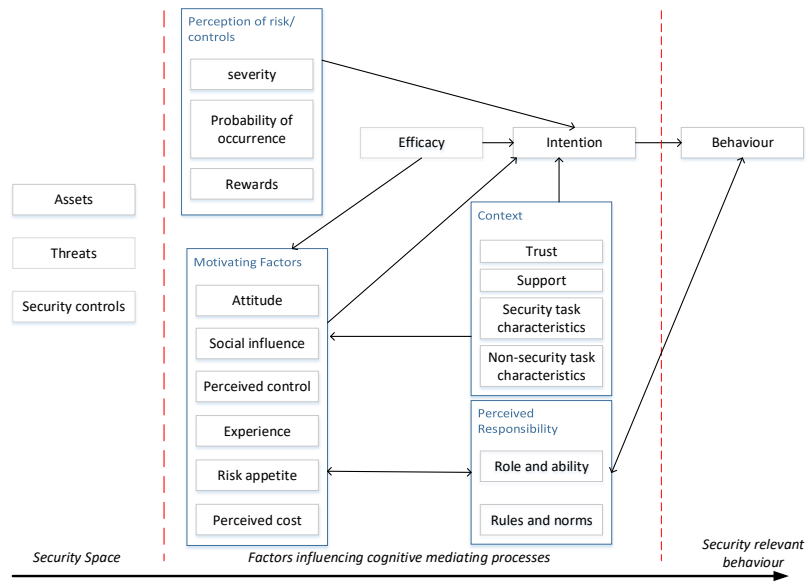


Fig. 4. Consolidated model of home data security behaviour

models informed by the insights gained from our data. This presents a good starting point for researchers seeking to explore factors that influence data security decisions in the home. Future work will seek to confirm and/or expand on this model, and explore how it may inform the design of technology and security approaches targeting the home user.

References

- [1] Kregg Aytes and Terry Connolly. Computer security and risky computing practices: A rational choice perspective. In: *Advanced topics in end user computing* 4 (2005), p. 257.
- [2] P Bryant, SM Furnell, and AD Phippen. Improving protection and security awareness amongst home users. In: *Advances in Networks, Computing and Communications* 4 (2008), p. 182.
- [3] SM Furnell, P Bryant, and Andrew D Phippen. Assessing the security perceptions of personal Internet users. In: *Computers & Security* 26.5 (2007), pp. 410417.
- [4] Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F. and Hong, J., 2010. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2), p.7.
- [5] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In: *Proceedings of the 2009 workshop on New security paradigms workshop*. ACM. 2009, pp. 133144.

- [6] Styles, M., 2013, July. Constructing Positive Influences for User Security Decisions to Counter Corporate or State Sponsored Computer Espionage Threats. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 197-206). Springer Berlin Heidelberg.
- [7] Redmiles, E.M., Malone, A. and Mazurek, M.L., 2015. I Think They're Trying To Tell Me Something: Advice Sources and Selection for Digital Security.
- [8] Nouh, M., Almaatouq, A., Alabdulkareem, A., Singh, V.K., Shmueli, E., Alsaleh, M., Alarifi, A. and Alfaris, A., 2014, June. Social information leakage: Effects of awareness and peer pressure on user behavior. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 352-360). Springer International Publishing.
- [9] Mendes, M.S., Furtado, E., Militao, G. and de Castro, M.F., 2015, August. Hey, I Have a Problem in the System: Who Can Help Me? An Investigation of Facebook Users Interaction When Facing Privacy Problems. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 391-403). Springer International Publishing.
- [10] ITU. Itu world telecommunication/ict indicators database. <http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>, 2016. Online; accessed on 16-April-2016.
- [11] B.-Y. Ng and M. Rahim. A socio-behavioral study of home computer users' intention to practice security. PACIS 2005 Proceedings, page 20, 2005.
- [12] U. H. Rao and B. P. Pati. Study of internet security threats among home users. In Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on, pages 217-221. IEEE, 2012.
- [13] C. L. Anderson and R. Agarwal. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *Mis Quarterly*, 34(3):613-643, 2010.
- [14] E. Kritzinger and S. H. von Solms. Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29(8):840-847, 2010.
- [15] B. P., F. S.M., and P. A.D. Improving protection and security awareness among home users. *Advances in Networks, Computing and Communications* 4, 2008.
- [16] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne. The psychology of security for the home computer user. In Security and Privacy (SP), 2012 IEEE Symposium on, pages 209-223. IEEE, 2012.
- [17] Rader, E. and Wash, R. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, 1(1), pp.121-144, 2015.
- [18] Venkatesh, A. A Conceptualization of the Household/Technology Interaction. NA - Advances in Consumer Research, UT : Association for Consumer Research, 1985, 12, 189-194
- [19] Meshkova, E., Riihijarvi, J., Mahonen, P. and Kavadias, C., 2008, June. Modeling the home environment using ontology with applications in software configuration management. In Telecommunications, 2008. ICT 2008. International Conference on (pp. 1-6). IEEE.
- [20] Hammel, E. A. & Laslett, P. Comparing household structure over time and between cultures Comparative studies in society and history, Cambridge Univ Press, 1974, 16, 73-109.
- [21] Flechais, I. & Sasse, M. A. Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-Science International Journal of Human-Computer Studies, Elsevier, 2009, 67, 281-29.

- [22] Ajzen, I., 1985. From intentions to actions: A theory of planned behavior. In *Action control* (pp. 11-39). Springer Berlin Heidelberg.
- [23] Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change. *The journal of psychology*, 91(1), pp.93-114.
- [24] Milne, G.R., Labrecque, L.I. and Cromer, C., 2009. Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, 43(3), pp.449-473.
- [25] Lazar, J., Feng, J.H. and Hochheiser, H., 2010. *Research methods in human-computer interaction*. John Wiley & Sons.
- [26] Glaser, B.G. and Strauss, A.L., 2009. *The discovery of grounded theory: Strategies for qualitative research*. Transaction publishers.
- [27] Walsh, D. and Downe, S., 2005. Metasynthesis method for qualitative research: a literature review. *Journal of advanced nursing*, 50(2), pp.204-211.
- [28] Schlenker, B.R., Britt, T.W., Pennington, J., Murphy, R. and Doherty, K., 1994. The triangle model of responsibility. *Psychological review*, 101(4), p.632.
- [29] Blyth, A., 2016, July. Responsibility Modelling and Its Application Trust Management. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 114-127). Springer International Publishing.
- [30] Lee, Y. and Kozar, K.A., 2008. An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management*, 45(2), pp.109-119.
- [31] Fishman, E.J., 2014. With great control comes great responsibility: The relationship between perceived academic control, student responsibility, and selfregulation. *British Journal of Educational Psychology*, 84(4), pp.685-702
- [32] Pearman, S. et al. (2016, June). Risk compensation in Home-User Computer Security Behavior: a Mixed-Methods Exploratory Study. Poster presented at SOUPS 2016, Colorado, USA.
- [33] Adams, J., 2013. Risk compensation in cities at risk. In *Cities at Risk* (pp. 25-44). Springer Netherlands.
- [34] Adams, J., *Risk*, London: University College Press, 1995, 228 pp, ISBN 1-85728-067-9 (HB), ISBN 1-85728-068-7 (PB)