# Home Data Security Decisions


Norbert Nthala

Linacre College

University of Oxford

A thesis submitted for the degree of

*Doctor of Philosophy*

Hilary Term 2019

# Acknowledgements

This doctoral research was funded by the Rhodes Scholarship and Oxford-Linacre African Scholarship. I would like to thank the Rhodes Trust, University of Oxford, and Linacre College for this opportunity. My sincere thanks should go to my supervisor, Prof Ivan Flechais, for the opportunity he gave me and for his unwavering belief and support. None of this would have happened without him.

I am grateful to Martin Kraemer and Neemah Yotamu who expeditiously read all the chapters. I would also like to thank colleagues from the departmental security reading group, human centred computing group, and the department at large for their feedback and comments on my work.

Special thanks should go to my parents and two siblings for their patience, love and support. To all friends, thank you for being you!

# Abstract

The most common solution to securing data in the home remains *increased awareness*. However, studies and increasing numbers of cyberattacks targeting the home point to very limited success of this intervention. Awareness campaigns can lead to information overload, do not impart security skills, implicitly assume that every home user is an administrator, and are largely ignorant of the specific context of the user. Unfortunately, little research has been done to understand the home user, the home context, and related security practices in order to inform the design of appropriate security interventions. A more grounded understanding of the home and security practices therein is required to address this gap.

The research presented in this dissertation focuses on understanding security practices in the home, and how they can inform the design of appropriate security technology to support such practices. The work was conducted in three steps: (a) empirical exploration of security support behaviours and factors that influence the outcome of security decisions in the home through 65 semi-structured interviews followed by a survey of 1128 UK participants; (b) development of a framework to guide the design of security technology for the home; and (c) a case study demonstrating applicability of the framework to the design of a network security toolkit for the home.

*Grounded Theory* was applied to analyse data from the interviews focussing on understanding security support behaviours. *Thematic Analysis* was also used to analyse the interview data to identify important concepts for understanding the security context in the home and factors that influence security decisions. Data from the survey was analysed using *descriptive and inferential statistics* to validate the previous qualitative results. Key findings include evidence of: (1) social networks serving as informal support networks in home security; (2) perceived competence being used to evaluate the quality of security support sources and work; and (3) visibility of harm influencing security decisions.

From this research, we propose the Home-Appropriate Network and Digital Security (HANDS) framework: a data-driven descriptive framework that enables designers of home technology to ground their design decisions in relevant contextual information. We demonstrate its application in a *Case Study* designing a network security toolkit for the home. The design was evaluated through 4 focus groups of

3 participants each, followed by a survey involving 616 UK participants. Thematic analysis was used to analyse data from the focus groups, while descriptive and inferential statistics were applied to analyse the quantitative data.

# Contents

# List of Figures

# 1 Introduction

In this chapter, we describe and motivate a research problem that this dissertation addresses. A research question is proposed based on our understanding of the problem and supported by a scoping study. We break down the question into sub-questions to make clear the main claim made by this proposal. The break down also helps to justify the research approach that was used. We conclude the chapter by presenting contributions arising from the research, and the structure of the dissertation.

## 1.1 Thesis Motivation

Information security is an enabler. By providing technologies, practices, procedures, and infrastructure that mitigate unacceptable risks, sufficiently secure systems allow stakeholders to profit from services and interactions that would otherwise be intolerably dangerous. The challenge is the need to ascertain what *sufficient security, unacceptable risks,* and *intolerable danger* mean for *relevant stakeholders.* This requires a clear understanding of delicate concepts such as privacy, confidentiality, integrity, availability, accountability, etc.; knowledge of threats, vulnerabilities, and controls; ability to understand, implement, use, and maintain security controls; and an ability to make tradeoffs to balance security and privacy concerns with business

imperatives: e.g. user privacy vs advert-supported services, availability protection vs costs of redundancy, or outsourcing to the cloud vs in-house control.

The nature and extent of these tradeoffs involves significant knowledge, experience, and skill to ensure that appropriate concerns are represented and balanced fairly. In recognition of this, information security and privacy budgets have grown and their profession has matured in recent years to provide the education, tools, and workforce that companies can draw from. While efforts are made to study and protect organisational settings, there remains a very significant gap in the skills, expertise, knowledge, and resources available to home users and families. Despite some initial work in exploring this domain [16, 103, 128, 204], more is needed.

Securing home devices, services, and data is increasingly difficult and necessary. While home users are not as attractive a target as many organisations, they are both commonplace and vulnerable to several attacks. Initial work in exploring the security and privacy of home computer users [16, 103, 128, 204] has highlighted the importance of this domain, and yet much more needs to be done to be able to address the scale and complexity of the security and privacy challenges.

According to a 2013 census, 74.4 percent of U.S. households use the Internet [207]. Similarly in 2015, 86 percent of households in the UK (22.5 million) had Internet access, up from 57 percent in 2006 [156]. Worldwide, Internet Live Stats reveals that over 46 percent of the world's population (3.4 billion) had Internet access in their homes by July 2016, up from 29 percent in 2010 [105]. As the number of connected homes increases worldwide, so too do the threats. Adding to the challenge of securing homes is the advent of smart and IoT devices.

In 2012, Rao and Pati [167] conducted a study in India revealing common threats and attacks facing home users: viruses, malware (spyware, key loggers, adware, etc), identity theft, privacy violation, and phishing. Large organisations generally mitigate these types of threat well. However, this is not the case for typical home computer users. Best practice in mitigating viruses in a home context seems to be limited to running antivirus software, patching, and displaying warnings (from web browsers and broad awareness campaigns) to avoid untrusted or malicious

websites. In contrast, in addition to antivirus software and patching solutions, larger organisations also have acceptable usage policies to manage risky behaviour from employees; segmented network architectures to avoid the spread of viruses; active firewalls; intrusion detection and prevention systems to identify and prevent problems before they cause significant damage; backup strategies to recover from incidents; and, perhaps most critically, an IT support function that can deal with problems should they arise. In comparison, home users have very few of the resources, capabilities, knowledge, skills, or tools to effectively protect themselves from the multitude of threats that seek to harm them directly.

Threats that directly harm the home are not the only concern. In today's highly interconnected world, the security of the cyberspace depends on the security of all the different devices connected to the Internet. Ng and Rahim state that home users play a crucial role in securing cyberspace. If not well-protected, home systems can be compromised by attackers and used to attack critical infrastructure and services (such as telecommunication and banking) that heavily depend on the secure functioning of the cyberspace [144]. While information security breaches affecting organisations receive much attention, breaches involving home users usually come to light only when home-connected devices or the home users themselves are involved in an attack affecting critical infrastructure. The October 2016 attack on Dyn, for instance, which is believed to have been enabled by insecure IoT devices in homes [27], triggered a number of reactions from different stakeholders, with some device manufacturers reported to have recalled their devices from the market. Computer users at home face many different kinds of attacks and threats of diverse complexity, affecting a variety of different stakeholders, and for which mitigation requires interventions both within and outside the home.

In recognition of the need for better security for home computer users, a key strategy for improving home security practices has focussed on increasing awareness [39, 97, 122, 169, 149]. Despite the effort put into such approaches, studies [21, 39, 79, 135] and recent events [27, 65, 132] show that home users remain vulnerable to several attacks facilitated by insecure practices and choices to ignore security advice.

In light of this, the research community has realised the need to explore other avenues for effective ways of securing the home user. Various approaches have since been proposed to help secure the home (e.g. [61, 87, 180] discussed in section 2.5.7).

The level of variance in the proposed approaches, from economics to public health, combined with the growing numbers of incidents and the clear lack of effectiveness in defending home users motivated this research into the nature of the problem of securing the home user. In order to devise more appropriate and effective security solutions, we believe that secure (and security) systems in the home must be designed from an empirical and grounded understanding of home users, the context of use in which they operate, and how they make data security decisions. This is a significant drive towards evidence-based practice.

## 1.2 Research Question

This thesis was motivated by the research question: **How can home data security practices be well understood and supported to help security entities design appropriate home user security approaches and home users to make appropriate data security decisions?**

However, providing scope to such a study from the onset proved to be quite elusive given the limited breadth of studies conducted on this topic so far. To rectify this problem, we started off with a scoping study of 15 semi-structured interviews. Demographics for our participants are presented in section 3.2.3.1. The aim of the scoping study was to make an initial exploration of security practices (which we consider to consist of (i) security behaviours and (ii) the decisions that lead to such behaviours) in the home, from which we would identify a research gap for further exploration. Our research questions would then be refined based on the initial results. Respondents for this study were chosen from a snowball sample of home users in the UK. Two research questions guided our interviews during the scoping study:

1. What influences security decision-making in the home?

2. What kinds of security behaviours exist in the home?

We analysed the data using Thematic Analysis [35] to identify important themes emerging from the data. Our analysis identified a number of factors that influence the outcome of security decisions in the home, all of which were consistent with previous studies discussed in chapter 2. Analysis of the data on security behaviours revealed two separate categories of behaviours which we categorised as: *security work* and *security support*.

*Security work* is highly contextual and specific to technology platforms, comprising behaviours such as installing and using firewalls, antivirus software, patching, data backup, and parental controls. As reviewed in sections 2.5.5 and 2.5.6, our findings were consistent but much less comprehensive than previous studies in this area.

*Security support*, on the other hand, comprises two subcategories: support seeking and support giving. The work of Dourish et al. [62] on delegation and Redmiles at al. [169] on advice seeking and giving fall under security support. We noted that little work has been done to explore security support that is required or available in the home in great detail. This led us to focus our research on understanding security support in the home, the reasoning behind it, and how this understanding can help support and improve security practices in the home. We thus refined our main research questions to:

- RQ1: Which concepts are important in understanding security practices in the home?
- RQ2: What kind of security support behaviours exist in the home?
  - What are the characteristics of security support in the home?
  - Where do home users get security support?
- RQ3: What influences security decision-making in the home?
- RQ4: How can appropriate and effective home data security practices be supported?

This research does not seek to argue against security interventions currently in use or proposed. The work presented in this dissertation was motivated by the recognition of a limited scope of studies conducted in this area and the rise in security incidents targeting the home. We believe that meaningful and comparable information on home security approaches can strengthen the scientific foundations of new and existing approaches geared towards securing home users, and is needed to inform the work of different security practitioners and security researchers.

## 1.3 Contributions

The research reported in this dissertation was conducted on a topic that has not been extensively studied. Most empirical research in security focusses on enterprise security. In the home, security research has largely been around understanding specific security behaviours, mostly use of security technology such as antivirus, data backup, parental controls, and patching. Our work took a different angle to explore security support behaviours and security decisions surrounding security work and security support. The empirical understanding was applied to the development of an intervention for supporting network security in the home. In summary, the contributions from this dissertation are as follows:

1. A model of the home context for understanding security practices (in chapter 4).

2. Theory of security support behaviours in the home (in chapter 5).

3. A model of factors that influence the outcome of security decisions in the home (in chapter 6).

4. Recommendations for supporting security in the home (in chapter 7).

5. A framework for designing and evaluating security technology for the home (in chapter 7).

6. A network security toolkit (SMART) for supporting security practices in the home (in chapter 8).

Figure 1.1 provides an overview of this dissertation showing how the research questions in section 1.2 and the contributions above are written up as chapters.

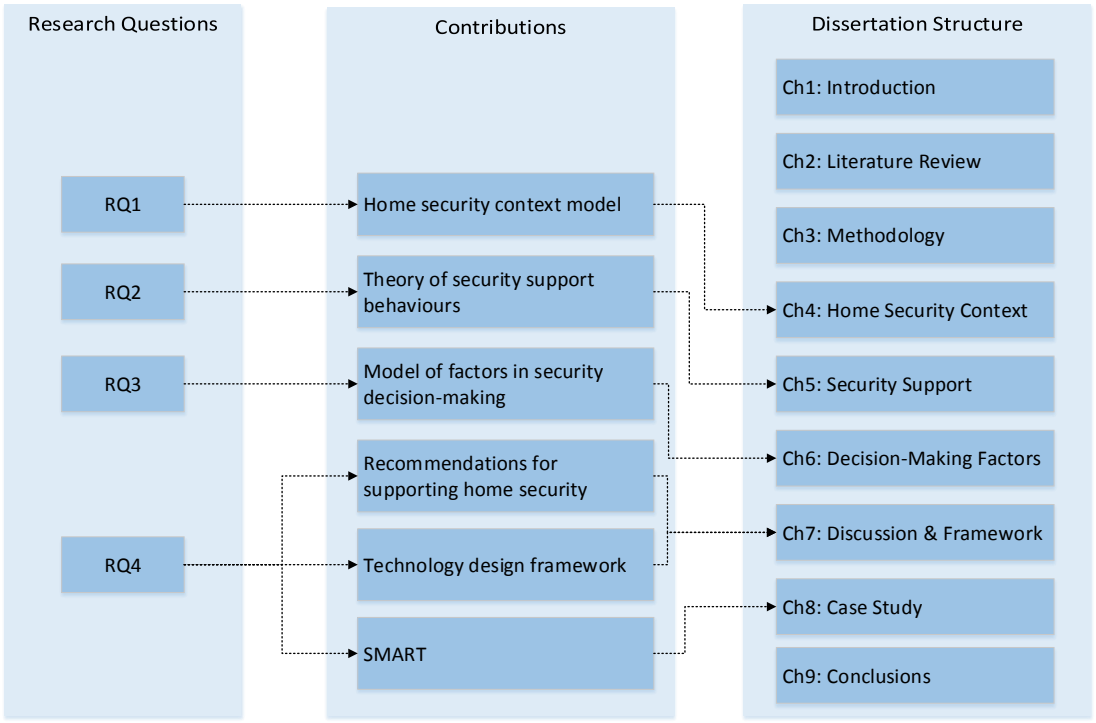


**Figure 1.1:** Dissertation roadmap

## 1.4 Dissertation Structure

Chapter 2 reviews the current state-of-the-art in security practice. We consider enterprise security practices that have matured over time and enjoy a range of supporting techniques. Given the focus of this dissertation, we take special interest in understanding how user behaviours and decisions are supported. Based on the brief discussion of enterprise security practices, we review security practices in the home, making clear the gap that this dissertation fits in.

Chapter 3 presents the methodology used for conducting this research. We justify our choice of approaches by reviewing related fields and how they have approached empirical studies. We consider approaches from Security, Information

Systems, and HCI; and we align and justify our selected methodology based on the understanding of where and how the different methods are used.

Chapter 4 presents a conceptual model of security context in the home, developed from our analysis of relevant literature and interview data. The model is aimed at setting the scene and guiding exploration of security practices in the home. We first present an overview of the model, and then describe each of three spaces that constitute the model: technology, activity, and social.

In chapter 5, we present our findings on security support in the home. The chapter starts with sources of security support in the home, followed by preferences of the sources, and ends with characteristics of security support in the home.

Chapter 6 presents factors that influence the outcomes of security decisions in the home. Results are reported from both Thematic Analysis and a survey. Particular attention is on factors that have not been reported in other studies: survival/outcome bias, confidence in a security measure, and factors for evaluating the quality and source of security support.

In Chapter 7, we interpret the findings from chapters 4, 5, and 6. We break down our discussion into three themes based on outstanding findings in the three chapters: evaluating security decisions and support, security responsibility and competence, and security technology. We then discuss the wider implications of our findings. We conclude the chapter by presenting a framework for designing and evaluating security technology for the home.

Chapter 8 reports on a case study to apply the framework developed in chapter 7. We begin the chapter by motivating the problem in securing networks in the home, demonstrate how the framework was used to analyse the problem, and design a solution. We report on findings from empirical evaluation of the design and briefly describe the prototype developed from the design.

In Chapter 9, we summarise the key findings presented in this dissertation and evaluate how the contributions answer the research questions of section 1.2. We end the chapter by discussing potential future work.

## 1.5 Publications arising from thesis work

Table 1.5 describes elements of this work that have been published in peer-reviewed workshop and conference proceedings.

| **Publication** | **Related Chapter** |
|---|---|
| Nthala, N. and Flechais, I., 2017, July. "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. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 123-142). Springer, Cham. | 4,6,7 |
| Nthala, N. and Flechais, I., 2018. Rethinking home network security. In European Workshop on Usable Security (EuroUSEC). | 4,7 |
| Nthala, N. and Flechais, I., 2018. Informal support networks: an investigation into home data security practices. In Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018) (pp. 63-82). | 5,6,7 |

# 2
# Literature Review

## 2.1 Introduction

The aim of this chapter is to: (1) define the terms used througout this dissertation, (2) describe current practice in data security, (3) review current state-of-the-art in home data security and problems therein, and (4) review ways of and current progress in understanding the home context.

## 2.2 Security

*"Security is the state of being free from danger or threat"* [1]. This is similar to Wolfer's interpretation of security as the *absence of threats to acquired values* [224]. These definitions imply some degree of protection of values previously acquired by an entity. However, *free from danger or threat* and *absence of threats* are highly abstract and ambiguous terms, and therefore impractical. Baldwin [23] refocusses Wolfer's definition of security to *a low probability of damage to acquired values.* In practice, the application of this concept of security varies across disciplines (e.g. national security, human security, and computer/information/data security), some of which share basic constructs.

[1] `https://en.oxforddictionaries.com/definition/security`

Baldwin discusses questions that are useful in defining and applying security in a particular domain.

(1) *Security for whom (or what entity)?* The author argues that security should specify the referent object for it to be comprehensible. In national security for example, such an object might include individuals or states; while in information security, this alludes to information assets (i.e. a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently[2]).

(2) *Security for which values?* The referred object might, in principle, have many values—for instance, political independence and territorial integrity in national security, and CIA (confidentiality, integrity, and availability) in information security. A concept of security should therefore specify which values are in question.

(3) *How much security?* The question of how much is enough to protect an asset from a threat poses challenges across disciplines. This entails defining what *enough* means, which realistically cannot be generic across domains. Different environments/contexts have varying needs, and hence different security requirements. The requirements to secure a home with a smart thermostat (e.g. [98]), for instance, cannot be the same with requirements to secure a home with just an Internet-connected computer (e.g. home network security[3]). Thus this is a highly contextual question. In information security, approaches have been developed to aid in assessing and managing security in any given context. One commonly used approach is risk assessment and management, where different methodologies, guidelines, frameworks, and standards have been proposed and developed. Examples include NCSC's component-driven and system-driven risk management[4], ISO/IEC 27005:2011 [1], OCTAVE [13], and AEGIS [75].

(4) *From what threats?* To effectively protect assets, it is important to understand the potential security threats in the given context. Vague reference to threats, such

[2] http://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf

[3] https://www.us-cert.gov/ncas/tips/ST15-002

[4] https://www.ncsc.gov.uk/guidance/introduction-risk-management-cyber-security-guidance

as "threat to my data", poses difficulties in applying appropriate security measures. Questions that would arise from it include, 'is the acquired value under concern confidentiality? or integrity? or availability? or maybe all?' Such ambiguity could lead to inappropriate and/or costly security measures. The concept of threat here refers to anything that poses danger to acquired values.

(5) *By what means?* There could be multiple ways of securing assets against one threat. The process of securing the asset should specify how and why particular measures are preferred over others. This mitigates bias and ensures cost-effectiveness of selected measures.

### 2.2.1 Defining Data Security

*Data security* is often discussed in the sense of *information* and *computer security*. ISO/IEC 27000:2017 [2] defines *information security* as the preservation of *confidentiality, integrity*, and *availability*. The standard states that in addition to these three properties or values of information, other properties such as *accountability, authenticity, non-repudiation*, and *reliability* apply. Whitman [219] expands this definition to indicate the different states in which information is (to be) secured: "to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission".

*Computer Security* can be defined as controls (technical, physical, and procedural) that are put in place to provide confidentiality, integrity, and availability for all components — data, software, hardware, firmware — of computer systems[5]. Gollmann [85] categorises these controls/measures into preventive, detective, and reactive.

Conventional definitions and discussions of *data security* have centred on the above definitions of information and computer security. Kaufman [113] defines data security as ensuring data confidentiality, integrity, and availability through the application of encryption controls, access controls, and data backup procedures. Similarly, Denning [176] defines data security as the science and study of methods

[5]https://study.com/academy/lesson/what-is-computer-security-definition-basics.html

of protecting data in computer and communication systems. Protection alludes to ensuring secrecy (sometimes referred to as confidentiality), privacy, authenticity, integrity, and availability achieved through the application of cryptographic, access, information flow, and inference controls in addition to procedures for backup and restore. The controls and procedures aim to protect data in transit and in storage. Denning introduces an interesting aspect to data security (similar to [127]: data is securely *stored* and *transferred*) – *data must be secured in its different states:* at rest, in motion, and in use.

For the purposes of this research, we define *data security (or security)* and *context* as follows:

- D1: **data security (or security)** deals with measures of protecting data in computer and communication systems.
- D2: **context** refers to any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and a system, including the user and system themselves [57].

Much of the literature on and practice of security has focussed on protecting enterprises against attacks. The practice has grown rapidly over the years, with advances in guidelines, standards, checklists, tools, and other resources devoted to it. Practitioners and researchers have since proposed and embarked on adapting enterprise security practices to non-enterprise environments, like the home [128, 198]. While home users are not as attractive a target as many organisations, they are both commonplace and vulnerable to several attacks. Initial work in exploring the security of home computer users [16, 103, 128] has highlighted the importance of this domain, and yet much more needs to be done to be able to address the scale and complexity of the security challenge. Our study, therefore, is situated in home data security.

However, to effectively explore security practices in the home, we need a solid understanding of what constitutes best practice in security. We, therefore, start with

a review of security practices in section 2.3, briefly describe user-centred security in section 2.4 and then discuss current trends in home security in section 2.5.

## 2.3 Security Practices

As Von Solms [212] states, an *acceptable level* of security can only be introduced and maintained if the *suitable [3]* set of security controls, both technical and procedural, is identified, adopted, and maintained. The challenge is to ascertain what *acceptable level* and *suitable* mean for relevant stakeholders. Identifying which controls should be in place requires careful planning and attention to detail. The actual selection of the controls is dependent on the criteria for risk acceptance, risk treatment options, and the general risk management approach [3].

This evinces two facets of *security practice*: (1) *security behaviour* — the actual implementation of security controls and support function(s), and (2) the *decisions* that precede and lead to the security behaviours. As explained in chapter 1, security behaviours fall into: (a) *security work*, which is highly contextual and specific to technology platforms, comprising behaviours such as installing and using firewalls, antivirus software, patching, data backup, and parental controls; and (b) *security support*, which comprises two subcategories: support seeking and support giving.

### 2.3.1 Security Behaviour

#### 2.3.1.1 Security Work

Security work is highly contextual and specific to technology platforms, comprising behaviours such as vulnerability assessment, installing and using firewalls, antivirus software, patching, data backup, parental, incident management controls, mindful behaviours [14], and security testing [174]. Putting this into the security context, security work spans all stages of a security process or lifecycle (cf. figure 2.1).

Pfau [161] discusses four phases of the security lifecycle (cf. figure 2.1) namely *identify, assess, protect,* and *monitor*. Pfau states that the security lifecycle is built around security policy and standards. *Identification* focuses on knowing and understanding the assets that are to be protected; *Assessment* encompasses reviewing

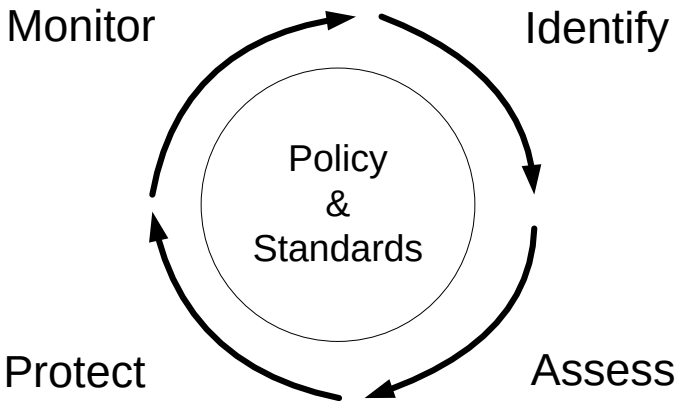


**Figure 2.1:** Pfau's security lifecycle [161, p. 2]

processes and procedures, performing vulnerability assessments, prioritising assets, and many more; *Protection* involves implementation of mitigation strategies, such as firewalls, patching, and awareness and training; and *Monitoring* is concerned with security compliance and verification, and validating the security posture of the context.

#### 2.3.1.2 Security Support

Security support is associated with providing the capability to relevant stakeholders to ensure effectiveness in achieving security work. It is composed of seeking and giving support/help. Forms of support include provision of information, advice, and technical support at all levels of the security life cycle. Support can be provided in-house, as explained in [128], or can be outsourced. Support can be provided locally, or remotely (referred to as 'off-shoring' of computer security if provided from another country [41]).

Examples of security support functions include administrators installing, configuring, and updating anti-malware for other stakeholders, configuring system updates, patching, and incident management. It also includes supporting other stakeholders' behaviour, such as helping them identify phishing emails, and providing targeted user awareness, education, and training.

### 2.3.2 Security Decision-Making

Responsible *stakeholders* in security (for instance an administrator, end user, etc.) make complex decisions, largely under uncertainty [71]. For instance, the process of identifying appropriate and most effective security controls can be very complicated and resource-intensive. It involves understanding threats in a given context, and how they might affect business, organisational, or personal operations; knowing available security controls and how they could be applied to secure assets; and understanding how the security infrastructure can be maintained. Stakeholders, therefore, need to understand how threats, vulnerabilities, and mitigations are composed together to yield security requirements [101]. To cope with these situations, the decisions might involve estimates, representations, and resolving uncertainty at various levels — and might involve a number of trade-offs. By *stakeholder, threat,* and *vulnerability*, we mean:

- D3: **Stakeholder:** person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity [2].
- D4: **Threat:** potential cause of an unwanted incident, which may result in harm to a system or a stakeholder [2].
- D5: **Vulnerability:** weakness of an asset or control that can be exploited by one or more threats [2].

The discussion above shows that security decisions precede security behaviours, and therefore span the entire security life cycle or process. Traditional theory posits that human beings are rational. However, there is evidence that rational decision-making in security is affected by a number of factors. Studies on individual decision processes, with respect to personal information security and privacy, reveal that many factors affect the processes [6, 7]. Among these are limited information, bounded rationality, and psychological distortions.

To make security work, there is need to understand people and their motivations [185]. In this regard, studies have focussed on explaining the determinants of

information security behaviours. Most studies presume that the effects of antecedents on security behaviours are homogeneous. Several such studies are based on behavioural theories such as the Theory of Reasoned Action (TRA) [11], Theory of Planned Behaviour (TPB) [10], Protection Motivation Theory (PMT) [179], and Diffusion of Innovation Model (DoI) [178].

### 2.3.3 Supporting Security Practices

Several techniques have been developed to support security decision-making and security behaviours. These include: security guidelines and principles (e.g. 10 Steps to Cyber Security [142]), checklists (e.g. Home and Office Security [46]), descriptive security-information (e.g. [186, 185]), risk management approaches (e.g. ISO/IEC 27005:2011 [1]), and tools (e.g. NMAP[6] and OpenVAS[7]).

### 2.3.4 Summary

Significant research continues to be carried out in the field of security, particularly on finding ways to deal with the problem of human factors affecting the practice. Advances on the topic have pointed to users' lack of knowledge and lack of user-centeredness in security mechanisms as some of the core problems affecting security practice [8]. Such revelations led to the birth and growth of a new field, *user-centered security* [231]. The field is aimed at finding ways of developing appropriate and effective security approaches that are suited to the user's context. We briefly discuss some of the techniques in section 2.4.

## 2.4 User-Centered Security

This field focusses on building and maintaining user-friendly secure systems, synthesizing security and usability. Zurko and Simon refer to user-centered security as security models, mechanisms, systems, or software that have usability as a primary motivation or goal [231]. We discuss approaches to user-centered security

[6] `https://nmap.org/`
[7] `http://www.openvas.org/`

in section 2.4.1, as presented in [231], and the approach to understanding a context, based on [229, 57, 4], in section 2.4.2.

### 2.4.1 Approaches to User-Centered Security

Zurko and Simon discuss three approaches to user-centered security, most of which are based on concepts from user-centered design [5]: (1) applying usability to secure systems; (2) applying security to usable systems; and (3) user-centered design of security.

The first approach is to apply established procedures for enhancing usability to developing or existing secure systems. Techniques for achieving this include *contextual design* [223], which emphasizes the use of contextual inquiry to yield data on the potential user's work and context to determine product goals; *discount usability testing* [146], which involves user testing with low-tech paper mock-ups to get early rapid feedback on early design concepts; and *in-lab testing* [181], where users perform a set of tasks while being monitored.

The second approach seeks to integrate security services into software that has a strong requirement for usability. Work in this stream focusses on developing techniques, models, and frameworks for applying security to usable systems. Zurko and Simon cite the example of a framework for access control in collaborative environments developed by Shen and Dewan [189].

The last approach relates to the development of user-centered security models and applications. The main focus of the approach is to take into consideration user needs as a primary motivator when defining a model or designing features of a system. Zurko and Simon state that the target user may be an end user, an application programmer, a system or security administrator, or a group of users or social unit.

### 2.4.2 Understanding a Context

As discussed in section 2.4.1, *context* is an important aspect of user-centered security. However, context is a poorly used source of information in the computing environment [57]. As discussed in section 1.1, proposed solutions in home user security fall short of contextual grounding in order to make a meaningful impact on

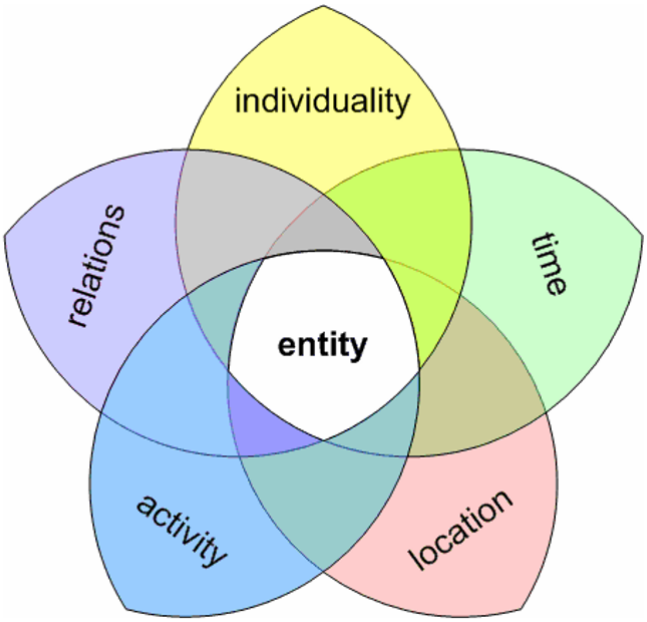


**Figure 2.2:** Fundamental categories of context information (from [229, p. 561])

improving security practice. We, therefore, need to understand what constitutes a context, so that we can use it properly and effectively in our study.

As defined in section 2.2.1 (D2), a context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and a system, including the user and system themselves. There are five general categories of information used to describe a context: *individuality* (i.e. the entity the context is bound to), *activity* (determines the current needs of an entity), *location* (describes location models that classify the physical or virtual residence of an entity), *time* (deals with the temporal dimensions of a context), and *relations* (describes the relations an entity has established with other entities) [229] (cf. Figure 2.2).

## 2.5 Security in the Home

The adoption and use of information technology in homes is rapidly becoming complex, and the number of networked devices available to home users is also on the increase. The advent of smart cities and the Internet of Things continues to diversify the kinds of technology and the level of networking made available to the

home. In 2018, Lueth [131] predicted that the number of IoT devices would grow to 10 billion by 2020, from 7 billion in 2018. Networked devices in the home include laptops/PCs, mobile phones, televisions, tablets, game consoles, routers, networked cars, security systems, smart meters, medical equipment, and many more. Home networks can be wired, wireless, or both, and connect one or more home devices to the Internet through a local Internet Service Provider (ISP).

A survey conducted in the UK in 2007 [79] found that home systems are used for different on-line services including email, web browsing, banking, VOIP/Internet telephony, research/education, chat rooms/forums/social applications, file sharing, instant messaging, shopping, auctions, gambling, and gaming. While technology adoption and use is on the rise, security and privacy breaches and concerns have not been spared. Technology devices and services that are being made available to home users come with a variety of data security issues. Brill of the Federal Trade Commission (FTC) is quoted in [90] saying *"some of them involve sensitive data, home life and where we are moving on a moment-to-moment basis with location-based information... 90 percent of connected devices collect personal information and 70 percent are not encrypting that data. It's a big concern."*

While organisations manage the security and privacy of their data and systems strategically through security policies, the protection of home users is left to the initiative of the users [144]. While home users are not as lucrative a target as many organisations, they are vulnerable to several attacks. Examples of attacks targeting home users include: unauthorised configuration of malicious DNS servers in 4.5 million DSL modems in Brazil with the aim of stealing banking credentials of victims [123] and the Mirai malware attack that affected homes in Germany and UK leading to Internet-service outage to approximately 900 thousand users in Germany and an unknown number in the UK [65]. The focus of this study, therefore, is on securing data for the home user.

### 2.5.1 Understanding the Home

Studies have shown that *home* is a multidimensional concept that is understood differently across disciplines. Questions are raised as to whether the home is a place, a space, feeling, practice, and/or an active state of being in the world [133]. Mallett [133] notes that home is described differently as related to house, family, haven, self, gender, and journeying. Saunders and Williams [184] define the home as a socio-spatial system. The authors argue that the physical environment (e.g. a house) is not a determining factor of a home, but that the physical aspects of the home enable and constrain different relationships and patterns of action. This means that a home cannot be fully defined by a physical entity (e.g. a house). The physical entity is, however, an important attribute that helps to identify and understand relationships and activities that exist and form social and activity aspects of the home.

Saunders and William identify three different social spaces within the home that overlap, namely household, family, and neighbourhood. While studies in sociology have identified varying definitions of the household across societies, we define the household as a 'co-resident domestic group' as defined by Hammel and Laslett [89]. This typically refers to people living in one building. Hammel and Laslett [89] studied the household and presented different categories of family from the perspective of a household, as summarised in Table 2.1. However, Saunders and William note that it is not ideal to link the family to household, arguing that people without the ties of kinship can also belong to the same household. This includes people in shared flats, elderly people in various forms of sheltered accommodation, a family living with a domestic worker, and many more. A household can also be composed of a single individual.

While the family can fall under the household, it is not entirely in this social space. A family can exist within one household or many. Similarly, a family can exist within one neighbourhood or multiple. Neighbourhood (and friends) encompasses geographical proximity such as housing estates, but also social proximity such as common interest groups and other social groupings. We extend the concept

| Category | Composition/Class |
|---|---|
| Solitaries | Widowed<br>Single, or unknown marital status |
| No family | Co-resident siblings<br>Co-resident relations of other kinds<br>Persons not evidently related |
| Simple family households | Married couples alone<br>Married couples with child(ren)<br>Widowers with child(ren)<br>Widows with child(ren) |
| Extended family households[a] | Extended upwards (towards older generations than the family unit)<br>Extended downwards (towards younger generations than the family unit)<br>Extended laterally (towards others of the same generation as the family unit)<br>Combinations of the above three (in this row) |
| Multiple family households [b] | Secondary units UP (older generation than the one heading the household)<br>Secondary units DOWN (younger generation than the one heading the household)<br>Secondary units lateral (same generation as the one heading the household)<br>*Frérèches* [c]<br>Other multiple family households |
| Incomplete classifiable households | *Residual category for groups to which none of the other categories can be associated |

**Table 2.1:** Composition of households [89, p. 96]

[a] a family unit with the addition of one or more relatives other than offspring

[b] where a secondary family unit exists in a household headed by another family unit

[c] two or more married siblings of either sex with accompanying spouses with or without the presence of unmarried siblings

of neighbourhood with a new concept of 'friends' as another defining factor of social relations in the home setting. The social spaces can be viewed as depicted in figure 2.3.

### 2.5.2 Who is "The Home User"?

Many studies, including [16, 120, 103, 167, 39, 144], have referred to the concept of *'the home (computer) user'* without satisfactorily defining this. Most do not define the concept [16, 167, 39, 144], and those that do tend to settle on broad generalities,

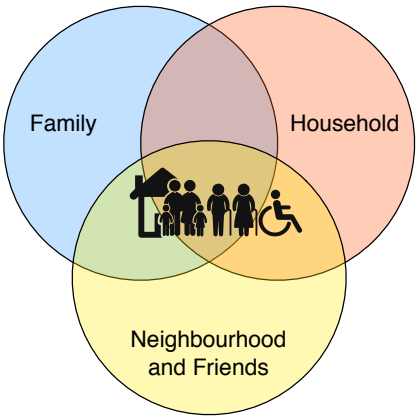


**Figure 2.3:** Model of home user social spaces

e.g. "the distinguishing characteristic is that the users are not professionals in computing" [103], or "a citizen with varying age and technical knowledge who uses Information Communication Technologies (ICTs) for personal use anywhere outside their work environments" [120].

It is evident from this conflict that there is no general understanding of who the home user is. A critical problem with this is that stakeholders might prescribe inappropriate measures for treating security problems in the home. Designers of home security technology are at risk of designing for an *elastic home user* which might lead, for instance, to wrong assumptions that every home user is a security administrator — resulting in security tools that do not fit the context of use. Cooper et al. [48] describe an *elastic user* as an ill-defined user whose characteristics change to suit the needs or views of the designer. Similar assumptions have been made in home security studies [17, 144, 167] that surveyed home users of their administrative security behaviours and awareness.

As discussed in section 2.4.1 and argued by several security studies, including [67, 68, 110], the context of use has a significant impact on data security practices. The user is understood in the context in which they operate. A key challenge to highlight here is that home users can include 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 address this challenge, and drawing from the work of Venkatesh [208, 209, 210, 211], we present a model of the context of home computer users that spans three distinct spaces: social, activity and technological. This breakdown is also supported by work from other researchers who sought to understand, define, or model the home context in relation to computing. Meshkova et al. [136], for instance, present a home environment and context ontology aimed at describing the home environment of each user. The main parts of the ontology are devices and software (*technology*), services (*activities*), and the user. Similar work is presented in [173, 193].

#### 2.5.2.1 Social Space

The social space is complex and has been explored according to Household (people living in one building) and Family (exploring different types of family unit) [89]. 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). As depicted in figure 2.3, social spaces can overlap or not (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.).

As explained in section 2.5.1 and shown in figure 2.3, the social space is composed of three overlapping spaces. From a data security perspective, we can see that these differences can influence the extent to which individuals become involved, motivated, and responsible for data security activities and decisions. The study in [144] 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 [74].

The role of neighbourhood in the wider social context of the home user has largely been explored in the context of housing and planning [94]. Of particular interest

to the problem of home user data security is the neighbourhood concept of *weak ties*, defined as unpretentious everyday contacts, which we theorise may influence how home users communicate about data security issues and share information, expertise, labour, and resources in a variety of informal ways. We also include in the neighbourhood category the role of friends which aims to reflect the role of *strong ties*. While these contacts provide similar opportunities for communication and sharing, there are clear differences in factors such as trust, benevolence, and motivation that warrant further exploration.

#### 2.5.2.2 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. While the activity space from 1996 has evolved, it is interesting to note that these activities are still broadly in the same categories as they were over 20 years ago, as shown in Figure 2.4 from [209], and that some of the aspects that were considered futuristic are still not commonplace.

#### 2.5.2.3 Technology Space

According to Venkatesh [208], and also depicted in Figure 2.2, 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.

#### 2.5.2.4 A Case for Better Understanding Home Security Context?

The model discussed above provides a good starting point in understanding the home context. However, it still does not clarify who the home user is, hence the

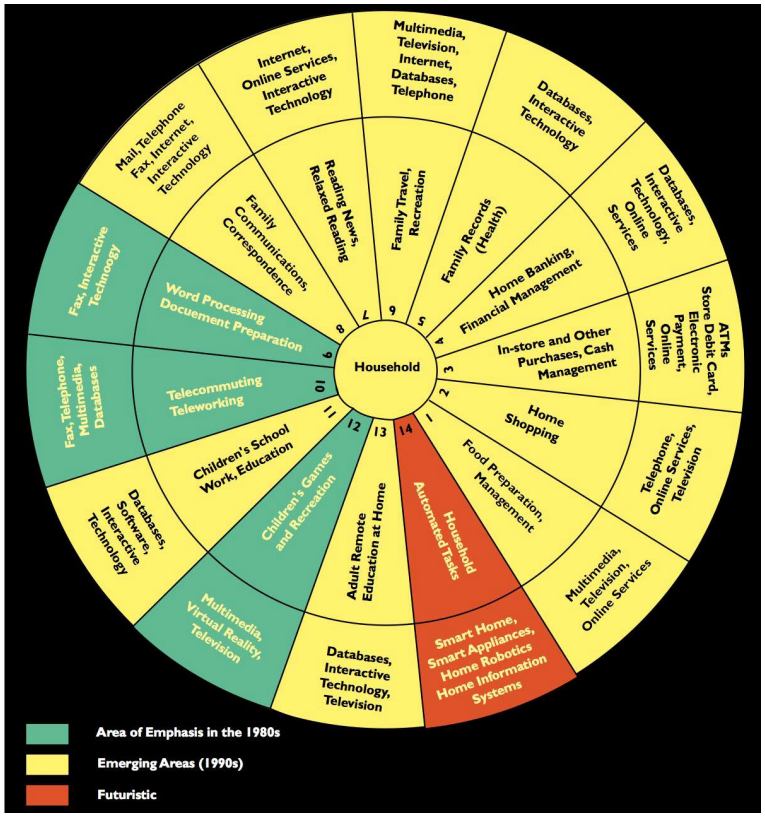


**Figure 2.4:** Everyday life for a household in cyberspace (from [209])

problem discussed in section 2.5.2 still stands. At the same time, it is not grounded in security practices in the home and does not reflect any aspects thereof. Validating and using such a model with security concepts from literature would be difficult for two reasons: (1) not much work has been done to empirically explore the home security context and practices (especially security support practices), and (2) if it were to be used to guide further exploration of home security, it would first need to be empirically validated.

We argue that a more grounded understanding of the context of use in which these types of users operate would provide a general and clear picture of who the home user is. Additionally, understanding important concepts in home security would help to channel efforts appropriately in further exploration of security practices in the home.

### 2.5.3 Threat Model for the Home

The process of securing data and computer systems involves identifying and understanding all possible threats to the systems, regardless of whether or not they

can materialise. Decisions are made to mitigate or accept associated risks based on this understanding and contextual needs. Identifying threats helps to develop realistic and meaningful security requirements. Work, including [225, 20, 162], was done to understand common and known threats to the home.

ITU-T X.1111 states that the home faces threats from both wired and wireless networks. Atamli and Martin [20] discuss a threat model for IoT devices comprised of *threat sources* and *classes of attack vectors* (also referred to as *threats*). Building on this model, we discuss a threat model for the home.

#### 2.5.3.1 Sources of Threats

Narayana Samy et al. [141] identify three main categories of threat sources.

1. **Natural:** events resulting from forces of nature such as floods, earthquakes, tornadoes, landslides, and electrical storms.

2. **Human:** events that are either enabled by or caused by human beings, including unintentional acts and deliberate acts. The three threat sources discussed in [20] implicitly fit into this category.

   (a) *Malicious User:* this is the owner of a device with potential to perform attacks to learn the secrets of the manufacturer, and gain access to restricted functionality. By uncovering the flaws in the system the malicious user is able to obtain information, sell secrets to third parties, or even attack similar systems. This category also includes a user with authorised access to the home network or system with intentions and capability of performing malicious activity for personal benefit or to harm others.

   (b) *Bad Manufacturer:* this is a producer of a device with the ability to exploit the technology to gain information about the users, or other devices. Such a manufacturer can deliberately introduce security holes in its design to be exploited in the future for accessing the user's data and exposing it to third parties. Equally, the production of poorly secured

products results in compromising the user's privacy. In addition and in the context of IoT, a manufacturer can attack other competitors' devices (through deployed devices) to harm their reputation.

(c) *External Adversary:* This is an outside entity that is not part of the system and has no authorised access to it. An adversary would try to gain information about the user of the system for malicious purposes.

3. **Environmental:** incidents or conditions such as pollution, chemical spills, and liquid leakage.

#### 2.5.3.2 Threats

Major threats to the home (organised according to CIA) include [225, 20, 162]:

**A. Confidentiality**

1. **Information disclosure:** an act of revealing information to an entity which does not have permission to see it. This includes accidental exposure, targeted attack, and inference or correlation. An attacker can obtain information by *eavesdropping* or *interception* on the network channel, physical access to the device, or through accessing the device over the network.

2. **Spoofing:** using credentials belonging to others in order to gain access to otherwise inaccessible service. The credentials can be obtained directly from a device, eavesdropping on the communication channel, or phishing.

3. **Elevation of Privilege:** an unprivileged user gaining privileged access to a device/service by installing an impostor in the system that pretends to be another device, which has privileged access in the system.

4. **Unauthorized access:** an illegal entity gains access to an application server, a home application server, or home device by masquerading as a real user.

5. **Shoulder surfing:** an attacker collects information by watching keystroke, reading a remote terminal's screen, or listening to sound from a remote terminal.

6. **Side-Channel:** based on information such as timing analysis of the execution, power consumption, traffic analysis, fault analysis, and electromagnetic analysis of the device, private and confidential data can be inferred.

**B. Integrity**

1. **Data tampering:** an act of deliberately modifying (destroying, manipulating or editing) data through unauthorized channels.

2. **Device tampering:** interference with device parameters to insert an impostor to a system with the intent to use the device maliciously or out of its intended functionality.

3. **Injection and modification of data:** an unauthorized entity inserts, changes, or deletes information transmitted between a remote terminal and an application server. The unauthorized entity can be a person, a program, or a computer. These attacks occur when an attacker adds data to an existing connection with the intent of hijacking the connection or maliciously sending data. This can result in a DoS attack or a man-in-the-middle attack.

4. **Input error:** may be caused by the difficulty of inputting data via a small keyboard or the keypad of a remote terminal.

5. **Signal Injection:** when an attacker injects fake data to the system to change the sensed data, such as transmitting electromagnetic signals to a sensor.

6. **Repudiation:** a sender or receiver denies the fact of having transmitted or received a message, respectively.

**C. Availability**

1. **Denial of service (DoS):** being unavailable when requested by an authorised user. A system must have the ability to continue operating even when some undesired action is being performed by malicious users. This class of attacks can be performed by stealing the device, manipulating its software, or disrupting the communication channel.

2. **Interruption/Communication jamming:** an intentional or unintentional interference overpowering the sender or receiver of a communication link, thereby effectively rendering the communication link useless. This can result in a DoS attack.

3. **Lost remote terminal (end device):** may occur as the remote terminal is carried around by a remote user. This can result in loss or destruction of information stored in the remote terminal.

### 2.5.4 Recommended Home Security Practices

In this subsection, we review well known recommendations for home security. We consider the ITU-T X.1111 recommendation: framework of security technologies for home network and US-CERT guidelines on home network security[8].

ITU-T X.1111 takes a technology-centred approach to home network security. The standard provides a general home network model for security (see figure 2.5), and describes threats and security requirements to the home network. In addition, X.1111 categorizes security technologies by security functions that satisfy the security requirements.

The recommendation presents the following as security requirements in the home: data confidentiality, data integrity, authentication, access control and authorization, non-repudiation, communication flow security, privacy security, and availability. Finally, the security functions to satisfy these requirements are outlined as encipherment (or encryption), digital signatures, access control, data integrity, authentication, notarization, message authentication codes, and key management.

US-CERT provides a range of recommendations for securing the home network[9], most of which are for endpoints. These include use of antivirus, data backup, patching, and mindfulness among others. Another security tip for "securing your home network" (ST15-002) outlines countermeasures to prevent unauthorized access to the home network. These include changing the default username and

[8] `https://www.us-cert.gov/ncas/tips/ST15-002`
[9] `https://www.us-cert.gov/Home-Network-Security`

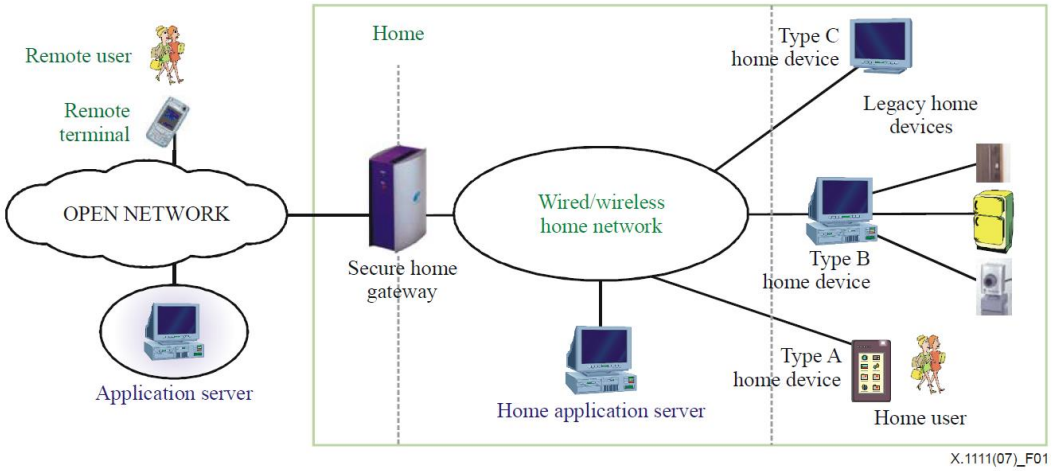


**Figure 2.5:** General home network model for security (from [225, p. 5])

password, changing default SSID, logging out of the router management interface, configuring WPA2, disabling UPnP when not needed, upgrading firmware, disabling remote management, and monitoring for unknown device connections through the router's management website. Similar recommendations for securing home networks include [202, 150].

#### 2.5.4.1 Criticism

It is evident that these recommendations are adapted from enterprise security practices, without much change. In section 2.5.2, we explained that home users have varying skills, capabilities, and needs. The recommendations in subsection 2.5.4 seem to assume that every home user is capable of performing the recommeded tasks. Evidence [62] has already shown that not all users in the home are experts or capable of carrying out most security activities required of them. In an enterprise environment, these are normally dealt with by professionals (administrators). We argue that efforts to support security practices in the home must be designed from a grounded understanding of the home security context, and users' motivations and security management strategies.

### 2.5.5 Security Behaviours in the Home

Much of the work addressing the security of data in the home [17, 79, 167, 144, 106] has focussed on understanding the security behaviours of home users in securing their endpoints. As explained in section 1.2, there are two kinds of security behaviours in the home: security work and security support. Researchers particularly explored the use of endpoint security technologies such as antivirus, updating/patching, backup, password and authentication solutions, and parental controls; and also explored practices, in particular *mindfulness* (e.g. visit only known websites, check if HTTPS, clear browser cookies, and foster cautious email habits).

AOL and the National Cyber Security Alliance conducted a study of online safety of home computer users [17] where 329 home users were interviewed and their computers were analysed. Researchers asked and checked for the availability of virus and spyware protection software, firewalls, parental controls, and the use of encryption for wireless network users. The study found that the majority of those studied lacked core protection. Similarly, Furnell et al. assessed the security perceptions of UK home users [79]. They surveyed 415 home users about their awareness of security threats, usage of system safeguards (firewall, antivirus, anti-spyware, and anti-spam software), and their awareness and understanding of security-specific tools found in contexts such as operating systems and applications. The study found that both novice and advanced home users appeared vulnerable to security risks. The authors concluded with a call for the development of new models of engagement and awareness raising.

Rao and Pati surveyed home users in India to understand their levels of awareness of security threats and usage of security measures (password protection, antivirus, firewall, patching, data backup, and parental controls) [167]. The study revealed poor understanding of security threats, and low levels of adoption of recommended security controls. The authors concluded that security in the home can be improved through awareness and user-friendly security controls.

Ion et al. studied security practices that different experts and non-experts consider to be the most important in protecting their security online [106]. They

conducted 40 semi-structured interviews with security experts, and used the results to design a survey. 231 security experts and 294 non-security experts were surveyed, and the practices of the two groups compared. The studied practices included installing software updates, using antivirus software, account security (using password managers, writing down passwords, changing passwords frequently, and using two-factor authentication), and mindfulness (visit only known websites, check if HTTPS, clear browser cookies, and email habits). The results showed discrepancies between the most important security practices of the two groups. The authors concluded that more work was needed to improve the practices of non-experts, and identified three key recommendations: install software updates, use password managers, and use two-factor authentication for online accounts.

Dourish et al. [62] investigated how users respond to security issues in their daily lives and found that people ask for assistance or delegate security activities to knowledgeable family members (similar to [76]), friends, or roommates. They also found reliance on technology (e.g. SSL for data connections, ssh tunneling for email, or trust wired Ethernet to be more secure than a traditional wireless medium) for protection; others reported delegating security to institutions such as financial companies.

However, other studies [21, 39, 79, 135] and the proliferation of attacks targeting unmanaged endpoints and home network devices [123, 182, 132, 157, 65, 27] show the insufficiency of endpoint-focussed security solutions in the home. In this view, other researchers have recently started looking at ways of securing the home holistically through network security — complementing endpoint security.

Niemietz and Schwenk [147] investigated fingerprinting attacks on router settings in connected homes. To achieve this, they evaluated the security stance of management interfaces on routers from ten different manufacturers, which they claimed were commonly used in homes. The researchers were able to compromise most of the routers. They concluded with recommendations to improve home router security: randomization of default login data, minimal information leakage, use

of SSL/TLS, input validation, use of X-Frame-Options, setting the window name object to a random value, and using cookie flags (httpOnly and secure).

Similarly, Karamanos [112] evaluated the security of routers used in homes through experimentation with different attacks. The attacks included authentication bypass, password guessing and brute force attacks, cross site request forgery, and UPnP exploitation. The researcher managed to conduct the attacks on the selected devices, and recommended: user awareness on account security; and for manufacturers to provide systems with well-implemented security that is transparent to end users. Other recommendations to manufacturers of devices included use of secure kernels, applying software upgrades to the router, packet inspection, and use of lightweight versions of intrusion detection and intrusion prevention systems.

The discussion above clearly shows that a lot of work on exploring security behaviours in the home has focussed on understanding security work as carried out by the *home user*. The studies [17, 79, 167, 106, 112] emphasised the need for the home user to understand security issues and adopt recommended security technologies (with the exception of Niemietz and Schwenk [147] whose recommendations are entirely for device manufacturers). However, as studies in [62, 76] reveal, the home user is not always the administrator. Therefore, any studies seeking to explore security work from such a user population must first understand who the real administrator is. In other words, security work and security support ought to be explored in tandem. Since much has already been done in security work, an exploration of security support practices in great depth is required to guide further work. There is need to understand the different relationships, motivations, sources, and reasoning behind support behaviours.

### 2.5.6 What influences Security Behaviours in the Home?

Research has been conducted to investigate and understand the factors that motivate different security behaviours, mostly endpoint-focussed. The assumption has been that such an understanding could help devise appropriate ways of delivering security

awareness, training, and also to inform the design of security-related technology for home users.

Studies [169, 144] showed that *social influence* has an impact on the security behaviours of home users. Das et al. [54, 55] studied in more detail how this social influence plays a role in the security behaviours of home users. They found that social influence affected the security behaviours of those involved through social processes (observing and learning from friends, social sense-making, pranks and demonstrations, negative experience of others, and device sharing), and conversations about security (a finding similar to that of Rader et al. [166]).

Wash [215] carried out a qualitative study of iterative interviews to investigate the existence of *folk models of security* for home computer users, aiming to increase our understanding of mental models of security for home computer users. The study focussed on finding out how home computer users understand and think about potential threats. Wash identified eight folk models categorised into models of viruses and other malware, and models of hackers and break-ins.

Herley [97] argued that users perform an implicit *cost-benefit analysis* when making a security decision. The cost is the effort required to follow security advice, while the benefit is the avoidance of potential harm that a successful attack might cause. The harm includes monetary loss (if any) that victims endure, but also the time and effort they must spend resolving the situation.

In a study investigating why users accept or reject different advice about secure behaviours, Redmiles et al. [169] found that users reject advice due to *too much marketing information, inconvenience* and *threatening users' privacy.* The study reported that *trust* was a clear factor that influenced the choice of a source of security advice. In addition, the study found that some participants did not practice security because they believed someone else was responsibile for protecting them.

Krol et al. [121] investigated the effectiveness of security warnings through an experiment with 120 participants. The results showed that over eighty percent of the participants ignored security warnings because they had become desensitised by frequent exposure and false alarms, and they thought they could recognise security

risks. The results also showed that the participants misunderstood security threats, e.g. they counted on anti-virus software to protect them from a wide-range of threats, and did not believe that PDF files could infect their machines with viruses. The authors concluded with a call to reduce the number of false positives in security warnings, and to educate users about security threats.

Egelman et al. [63] studied effectiveness of web browser security warnings in preventing phishing attacks. They found that active warnings (which interrupt a primary task) were more effective than passive warnings (without interruption of primary task). The authors concluded with design recommendations for improving effectiveness of warnings: interrupt the primary task, provide clear choices, fail safely, prevent habituation, and alter the phishing website. In a recent study, Reeder et al. [170] performed an experience sampling study of browser security warnings to find reasons for adhering or not to real warnings. They found no single dominant failure in modern warning design that prevents effective decisions. The authors concluded that further improvements to warnings will require solving a range of smaller contextual misunderstandings.

Ng and Rahim studied factors that influence a home computer user's intention to practice computer security [144] using TPB [10]. They surveyed 233 home computer users on the use of antivirus software, data backup, and personal firewall. The study found that "there is a positive relationship between a home computer user's *attitude* towards practising computer security and his/her intention in practising computer security". Attitude refers to a home user's disposition (inclination or tendency) to respond favourably or unfavourably towards practising computer security [144]. Attitude towards a behaviour is related to the subjective values of the behaviour's perceived outcomes — that is, outcome expectancies [10]. Armitage and Conner [19] argued that each behavioural belief links a given behaviour to a certain outcome, or to some other attribute, such as the cost incurred in performing the behaviour. The attitude towards the behaviour is determined by the strength of these associations, and by the beliefs that are salient at the time. The more favourable the attitude towards the behaviour, the stronger is an individual's intention to perform it [19].

In the study by Ng and Rahim [144], *perceived usefulness* was found to be a significant predictor of attitude. Perceived usefulness was defined as the degree to which a home computer user believes performing a particular practice will enhance the security of his/her computer. It was concluded that "usefulness of computer security practices should be stressed as they do influence users' attitude towards practising security" [144]. Similarly, Alkaldi and Renaud [15] carried out an exploratory study to find out reasons people accept or reject password managers. The authors identified several factors including perceived usefulness, negative experience, perceived ease of use, privacy, perception, social needs, and security concerns (similar to Udo [204], who found privacy and security concerns as major barriers for e-commerce). The authors concluded with a call for proper advertisement and reassurance of the trustworthiness of password manager, but also for designers to pay more attention to user experience.

Kirlappos and Sasse [116] studied trust factors that guide user behaviour online. They found the following factors: previous experience with website, logos and certifications, advertisements, social networking references, inclusion of charity names, amount of information provided, website layout, and company information.

In addition to attitude, *subjective norm* is another factor that significantly influences home users' adoption of security measures. This refers to a perception of the social pressure to perform or not to perform the behaviour under consideration, in this case to practice computer security in home computers [144]. Normative beliefs are concerned with the likelihood that important referent individuals or groups would approve or disapprove of performing the behaviour [12]. Family, peer, and mass media influences were discovered to be significant antecedents of subjective norm [144]. The results showed that peer influence contributed more to subjective norm than family influence. Mass media also plays a crucial role in promoting computer security. The study in [144] defined 'mass media' as "media of communication such as newspapers, radio, television, Internet, broadcast emails, official announcements made by authorities, etc. that are designed to reach the mass of the people", a definition obtained from [163]. Some (well-known) Government-led

computer security campaigns include the UK's Cyberstreetwise [196] and the United States' Computer Emergency Readiness Team [206].

Milne et al. [137] applied 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. They wanted to find out factors that 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 the following factors played a role in the decisions of the consumers: self-efficacy, perceived threat and likelihood of threat.

Cocklin [47] used the DoI theory to develop a model which he used to explore factors that influence home user behaviour with respect to operational security measures being applied to a home computer. This was done through an online survey executed through emails. The study targeted home computer users who responded that they took actions to secure their computers and did not rely on a third party. Their population was exclusive of family members who rely on another member to manage the computer. Cocklin found out that there are two pathways that influence the adoption of security functionality in the home PC environment: *decisions can be made based on knowledge and cognitive dissonance over information security issues*, or *directly by intention based on outside influence*. Cocklin concluded that expanding the body of information security knowledge to include individual behavioural aspects can be of benefit to the entire computer security community.

As can be seen from the discussion above, a lot of work has been conducted to identify and understand factors that influence the outcome of security decisions. However, much of the work focussed on individual security behaviours. Little has been done to understand factors that affect security support decisions. We argue that an in-depth understanding of such factors can reveal motivations, beliefs and constraints relevant in supporting security efforts in the home. There is a need to explore motivations, challenges, and limitations of support seekers and providers in order to device approaches that meet the context of the users.

In summary, the following factors were identified to influence the outcome of security decisions in the home: social influence, existing mental models of security, cost/benefit, privacy, convencience, available marketing information, security warnings, risk perception, attitude, subjective norm, perceived usefulness, negative experience, perceived ease of use, social needs, security concerns, trust, self efficacy, and security knowledge.

### 2.5.7 Improving Security in the Home

#### 2.5.7.1 Endpoint-focussed Security Approaches

A key strategy for improving home security practices so far has focussed on *increasing awareness* [39, 97, 122, 169, 149, 47]. Despite the effort put into such an approach, studies [21, 39, 79, 135] and recent events [27, 65, 132] show that home users remain vulnerable, as evidenced by insecure practices and choices to ignore security advice, leading the research community to explore alternatives to increasing awareness.

Dong et al. [61] proposed an economics approach to *designing security solutions for communities* rather than individuals. They argued that incentivizing people to improve the security of a community (from which they benefit) through a shared venture would motivate personal security investment. While maintaining user-centeredness, Gutmann [87] proposed *application of problem structuring methods (PSMs)*, a technique from social planning, to help analyse security problems. The intent is to ensure the most appropriate solution is applied to a problem. Gutmann claimed to tackle a common problem where developers and service providers impose their favourite technology on people, without considering the environmental, social, political, and legal aspects of the overall problem.

Wash and Rader [216] proposed *security story-sharing* to help shape the mental models which inform home security decisions. Through sharing the right stories, and with expert involvement, the authors foresaw changing home user security behaviour. Adding to the body of proposed approaches, Rowe et al. [180] put forward an *approach modelled on public health systems for a shared secure cyberspace*. They argued for a population-centred approach in dealing with cybersecurity issues.

This is a departure from the typical practices in information security, which take an individual focus in trying to understand how systems are compromised and how they can be protected. The authors outlined the technical requirements of a public cyber-health system, with specific focus on how the system would achieve monitoring, prevention, and incident response.

#### 2.5.7.2 Network-focussed Security Approaches

Studies [21, 39, 79, 135] and the proliferation of attacks targeting unmanaged endpoints and home network devices [123, 182, 132, 157, 65, 27] show the insufficiency of endpoint-focussed security solutions in the home. In this view, other researchers have looked at ways of securing the home holistically through network security — complementing endpoint security.

Xu et al. [228] proposed a traffic profiling system for home networks that automatically collects and analyses home network traffic. The system is designed to leverage programmable home routers. The main aim is to analyse and report the behaviour of network devices and also to detect anomalous behaviour. Researchers in [226] put forward an infrastructure that collects data from heterogeneous sources: home network traffic, intrusion detection logs from distributed firewalls, active open DNS resolver scanning, continuous snapshots of Internet routing tables, and geographic databases of Internet end hosts. Their approach integrates all the data and performs traffic analysis to detect attacks.

In a similar pattern, researchers in [227] proposed a Bloom Filter [33] based analytics framework to capture persistent threats towards home routers and identify correlated attacks towards distributed home networks. This is achieved by collecting and analysing inbound and outbound traffic, and traffic within the home. Martin et al. [134] proposed a solution to prevent the exploitation of bugs in outdated software and weak passwords on a home network. Their solution aims at raising an attacker's uncertainty about devices, and enabling the home network to monitor traffic, detect anomalies and filter malicious packets. The proposed infrastructure makes use of a chain of honeypots and deep packet inspection that collects suspicious

packet traces, acquires attack signatures, and installs filtering rules on a home router in a timely manner.

Taylor et al. [200] took a different approach to solving the problem of home security. The researchers put forward a cloud-driven infrastructure which combines software-defined networking (SDN) and proxies with commodity residential Internet routers. They proposed that security management be outsourced from expert service providers. At the centre of the solution is a modification to residential routers to allow them to export management to a remote controller using OpenFlow protocol, and a series of device proxies. Hafeez et al. [88] proposed a cloud-driven, Software as a Service (SaaS) solution that applies SDN to improve network monitoring, security, and management. The proposition utilises a modified gateway running an SDN controller and OpenVswitch to enable remote management of the home network through Cloud Security Service (CSS). Feamster [69] also proposed outsourcing security management of home networks to a third party with expertise. The solution harnesses programmable network switches and distributed network monitoring and inference algorithms.

Lastly, Cruz et al. [53] discussed a cooperative security management infrastructure between ISPs and home users. The researchers proposed adoption of a Distributed Intrusion Detection System (DIDS) architecture. This is to achieve distributed monitoring of service activity and network traffic by specialised components at the remote gateway, and distributed inference and correlation at ISP level to process information from remote gateways. All operation is to be centrally orchestrated on the ISP's infrastructure.

### 2.5.8 Shortcomings in the Approaches

There is evidence [21, 39, 79, 135, 27, 65, 132] that security awareness and the current endpoint-focussed interventions have achieved limited success. The probability of achieving meaningful improvement in home security through *more awareness alone* is minimal. As discussed in section 2.5.5, more or complete information does not

translate into secure actions. Exacerbating the problem is the fact that people get overloaded with information, which makes them resentful and not want to learn [99].

The level of variance in the proposed endpoint-focussed approaches (cf. section 2.5.7.1) (from economics to public health, aiming to solve the same problem of improving security in the home, but justified differently) signifies a big gap in the field. The proposals are not based on empirical evidence, or a grounded understanding of the context in which they are positioned. Interestingly, this is what Gutmann [87] attempts to solve. However, Gutmann's proposal is not a problem-solving technique, but a problem-structuring method. As discussed in section 2.5.7.1, a problem-structuring method helps to analyse and understand a problem, but does not explain or propose how solutions to the problem should be derived (which is what problem-solving techniques do). We believe that positioning similar approaches in a more grounded understanding of the home context would help adapt them more to the context of use.

Most of the proposals to improve network security in the home (cf. section 2.5.7.2) operate from the presumption that home users do not have the expertise or ability to perform security work in the home, and aim to take this responsibility away from home users with designs informed by an understanding of the *threat model* for home networks. The tools and infrastructure propounded aim to take security responsibility away from the *inexperienced* home user. This is in contrast with our initial observations of actual security work in the home during our scoping study and as reported in [62, 76, 169], where social relationships are leveraged to provide tailored and trusted security support. We believe that a grounded understanding of the context would help future efforts in properly situating and justifying these approaches.

While outsourcing security management for home networks may seem ideal (as proposed by a number of approaches in section 2.5.7.2), it comes with its own challenges: privacy concerns to the home user; scalability of such services (Feamster [69] discusses privacy and scalability challenges); cost to the service provider and the home user; and the issue of false positives blocking a home user

from accessing a legitimate service. Most of the proposed approaches recommend major changes to the current infrastructure — interventions that might be costly, complex, and inapplicable in most current environments. With empirical eveidence of what matters in the real context, efforts to outsource would be well aligned with the context and its needs.

## 2.6 Conclusion

The security needs of the home user are much more intricate and nuanced than has been assumed. Home users exist in different environments, with different infrastructure and security needs. In each of the varying contexts, their requirements might differ. The importance of the context in security has been highlighted before [74, 110]. Improving and supporting security in the home should be based on a grounded understanding of the current security practices in the home and their constraints.

Brézillon states that *"users' needs are often intangible, affected by habit, self-image, and even issues of motivation"* [38]. The design of a solution must focus on reducing barriers by analysing what can be known about a user and how to support that information and practice with appropriate interventions. The user must play an active role in defining the context about which the intervention must be aware of [38].

This chapter has highlighted the following needs: (1) to gain a grounded understanding of the home security context and home user (cf. section 2.5.2.4); (2) to explore security support behaviours in great depth (cf. section 2.5.5); (3) to identify factors that affect security support decisions (cf. section 2.5.6); and (4) to ground security support interventions for the home in empirical evidence of the context and practices therein (cf. sections 2.5.4.1 and 2.5.8). The research reported in this dissertation was motivated by this research gap and aimed to gain a grounded understanding of the security context and practices in the home, and applied that understanding to propose a framework for developing appropriate security

technology for the home context. Chapter 3 discusses a research methodology that was used to carry out the research.

# 3 Methodology

In this chapter, we discuss the research methods used to answer the research questions introduced in chapter 1. We first explore how Information Systems (IS), Information Security, and HCI approach empirical research. From this analysis, we present the research methods adopted in this dissertation.

## 3.1 Research Approaches

### 3.1.1 Security Research Approaches

The security domain has long identified the human (especially the end user) as a predominant weakness in properly securing information assets [52]. This has led to a shift from the traditional focus on studying technical measures to exploring security practices of different stakeholders. Researchers have particularly sought to explore use of security-related technology such as firewalls, patching, passwords, and anti-malware. In addition, research has explored mindful behaviours such as checking availability of a padlock or https on a website, using well known websites, and not downloading free files from untrustworthy websites; and lastly study factors that influence or affect the different security behaviours. Work in this area has been the focus of usable security, which aims to bridge the gap between traditional security and usability [24, 183, 159].

The goal of most studies in usable security is usually twofold: (1) to gain an in-depth understanding of security practices in a given context (e.g. [62]), or (2) to gain a broad and general understanding security practices (e.g. [79]). The first takes a qualitative approach, while the second is mostly quantitative.

Qualitatively, researchers have used different methods to study behaviours, attitudes, and factors that influence security decision-making. Kraemer et al. [119] used focus groups [140, 117] and content analysis [64, 104] to identify and explain how human and organisational factors may be related to technical computer and information security vulnerabilities. Content analysis may be used with both qualitative and quantitative data, and commonly used to analyse textual data. Content analysis usually results in a numerical description of features of a given text [109]. It is, however, a purely descriptive method. It describes what is there, but may not reveal the underlying motives for the observed pattern.

Beautement et al. [28] demonstrated the use of interviews and thematic analysis [35, 36], a phenomenological approach, to study security behaviour and attitude. Thematic analysis is seen as a foundational method for qualitative analysis [35]. It is a method for identifying, analysing, and reporting patterns (themes) within data. This method is flexible in that it may be based on prior themes mostly generated from literature (e.g. as applied in [194]), or on themes that emerge during the course of the analysis (e.g. as used in [28, 169]). However, thematic analysis has limited interpretive power beyond mere description, if it is not used within an existing theoretical framework that provides a firm basis or foundation for the analytic claims that are made. Additionally, the flexibility of the approach makes the process of developing guidelines for higher-phase analysis difficult, giving rise to a potential paralysis when deciding what aspects of the data to focus on [35].

Flechais [73] used Grounded Theory [84] to identify factors that affect the design of security. Grounded Theory allows researchers to examine topics and related behaviours from many different angles, leading to comprehensive explanations. It is used to uncover beliefs and meaning that underlie action, and to examine both rational and non-rational aspects of a behaviour [49]. In Grounded Theory,

there is simultaneous involvement in data collection and analysis, creation of analytic codes and categories developed from data only, development of middle-range theories to explain behaviour and processes, memo-making (writing analytic notes to explicate and fill out categories), and theoretical sampling (i.e. sampling for theory construction, not for representativeness of a given population) [44].

Flechais also applied Action Research [26] to research the practical application of a socio-technical security design approach. In this approach, a researcher intervenes into the study context with the study material. Action Research is seen in [26] as a five-phase process composed of problem diagnosis, action planning, action taking, evaluating, and specifying learning.

To get a broad and more general understanding of security behaviours, attitudes, and factors that affect security decision-making, researchers [144, 137, 47] have used surveys [77]. Survey research is useful when a researcher aims to describe or explain the features of a large group or groups. Surveys are commonly employed in descriptive research [114], aimed at estimating specific parameters in a population, and to describe their associations. Security studies have utilised a number of predictive models to study specific security and privacy behaviours of home users, including the Theory of Reasoned Action (TRA) [11], Theory of Planned Behaviour (TPB) [10], Protection Motivation Theory (PMT) [179], and Diffusion of Innovation Model (DoI) [178]. These models are most often extensions of existing social cognitive theories of factors that produce risky behaviour in other decision situations [103].

Das et al. [55] demonstrated how field experiments [187] could be used in evaluating security interventions. They explored how social proof could impact security behaviours of individuals on a large scale: "Field experimentation attempts to simulate as closely as possible the conditions under which a causal process occurs, the aim being to enhance the external validity, or generalizability, of experimental findings" [82, p. 2].

### 3.1.2 IS Research Approaches

For some time, IS research has focussed on studying technical problems associated with the use of IT systems. The IS community has since realised that political, organisational, and social issues have an impact on the effective use of systems [158]. Current efforts have focussed on studying behavioural issues, embracing empirical research methods within the domain with emphasis on *interpretivism* — concerned with the subjective understanding that individuals attribute to their social settings [58].

IS is recognised as a meta-subject that spans multiple disciplines in the social sciences, business, management, computer science, and many more [81]. Research approaches are hence adapted from the different fields to fit the study purpose and context. Among prominent approaches used in the field are Action Research [26], surveys [77], case study [30], ethnography [70], and experimentation [29, 187].

According to Benbasat et al. [30], a case study examines a phenomenon in its natural setting, employing multiple methods of data collection to gather information from one or a few entities (people, groups, or organizations). The boundaries of the phenomenon are not clearly evident at the outset of the research and no experimental control or manipulation is used. The case study approach is used to study practice-based problems where the experiences of the actors are important, and the context of action is critical. It attempts to capture and communicate the reality of a particular context at the point of study [108].

Ethnographic research studies social interactions, behaviours, and perceptions of people in their natural setting. The main aim is to provide rich, holistic insights into people's views, actions, and the natural environment they live in [171]. This is achieved through the collection of detailed observations and interviews, usually lasting long periods.

Experimentation includes strategies such as laboratory or field experiments as well as computer and experimental simulations [154]. It may be used to validate underlying theories, or to study issues surrounding acceptance and transfer of technology. Designs of experiments are guided by theories and facilitated by systems

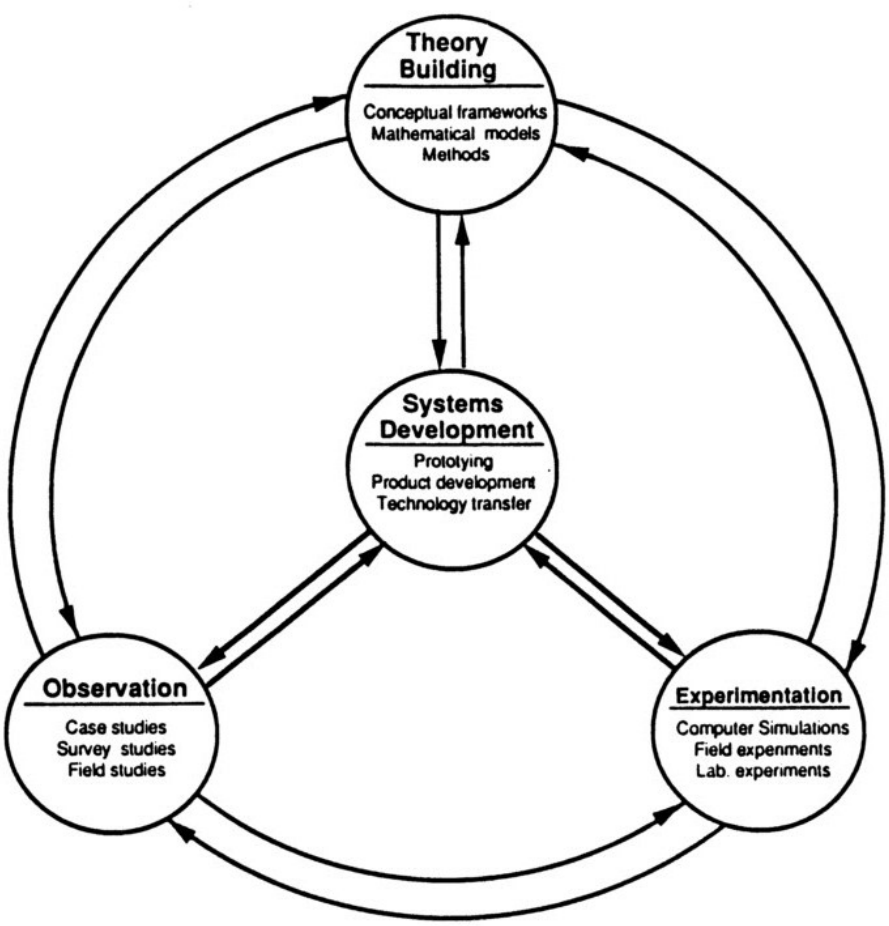


**Figure 3.1:** A Multimethodological approach to IS research (from [154, p. 94])

development where the results may be used to improve the theories or to improve systems [154]. Systems development consists of concept design, systems architectural design, prototyping, product development, and technology transfer [154].

Recent efforts in the field of IS have seen researchers and professionals argue and push for a pluralist methodology [138], which posits that research results will be richer and more reliable if different research methods, preferably from different paradigms, are routinely combined together. Nunamaker et al. [154] propose a multimethodological approach to IS research. The authors argue that focus on traditional (empirical) methodologies alone leads to inconclusive and inapplicable results. They put forward an approach where empirical and technical approaches complement each other. Figure 3.1 shows the multimethodological approach to IS rsearch.

*Theory building* comprises development of new ideas, concepts, frameworks, or models. The theories are usually generic in nature and therefore possess limited practical relevance to the target domain. Nunamaker et al. [154] state that theories may be used to suggest research hypotheses, guide the design of experiments, and conduct systematic observations. *Experimentation* aims to bridge the gap between theory and observations. It may be used to validate underlying theories or to explore issues concerned with technology acceptance.

*Observation* is normally used when little is known about the subject. It helps researchers explore issues for further study or to inform the design of experiments: "It may help researchers to formulate specific hypotheses to be tested through experimentation, or to arrive at generalizations that help focus later investigations" [154, p. 95]. *Systems development* consists of five stages: concept design, constructing the architecture of the system, prototyping, product development, and technology transfer [154]. Nunamaker et al. [154] describe concept design as the adaptation and amalgamation of technological and theoretic advances into potentially practical applications. Prototyping is used as a proof-of-concept to demonstrate feasibility of an idea, concept, or design [154]. Further stages are concerned with full development of production systems, and implementation in a production environment.

### 3.1.3 HCI Research Approaches

HCI is closely related to the design and development of technology. HCI is an interdisciplinary field with three main paradigms: human-factors, classical cognitivism/information processing based, and phenomenologically-situated paradigm [91]. Each encompasses a set of practicies and expectations. Human-factors focusses on optimising man-machine fit. Classical cognitivism/information processing emphasizes (ideally predictive) models and theories, and the relationship between what is in the computer and in the human mind. Phenomenology focusses on the experiential quality of interaction.

Lazar et al. [125] outline seven types of contributions that emerge from HCI research: (1) empirical, (2) artifact, (3) methodological, (4) dataset, (5) theoretical, (6) survey, and (7) opinion contributions. The majority of HCI research contributions fall into either *empirical* — data (qualitative or quantitative) collected through different methods — or *artifact* — the design and development of new artifacts, including interfaces, toolkits, architectures, mock-ups, and envisionments [125].

Widely used methods in HCI include experimental design, ethnography, case study, surveys, and diaries. HCI employs a variety of experimental designs, both laboratory-based and non-laboratory-based. The most frequently used include observations, field studies, interviews/focus groups, and controlled experiments [190]. The choice of an experimental design is context-dependent, and considers factors such as study purpose, time constraints, funding, and availability of participants. Experimental studies have limitations: (1) they require well-defined, testable hypotheses that consist of a limited number of dependent and independent variables, whereas many problems in HCI are not clearly defined or involve a large number of potentially influential factors; (2) they require strict control of factors that may influence the dependent variables which can hardly be satisfied in many HCI studies; and (3) they may not be a good representation of users' typical interaction behaviour, especially lab-based experiments [125].

Surveys have been discussed in section 3.1.1, while ethnography and case study approaches have been explained in section 3.1.2. The last widely used method in HCI research is a diary. This is "a document created by an individual who maintains regular recordings about events in their life, at the time that those events occur" [125, p. 135]. The activities recorded might include scheduled tasks and personal reflections. Diaries are good for studying usage patterns that cross multiple technologies, locations and environments [92]. Diaries are suited for longitudinal studies since such studies require a significant amount of time to gather useful data.

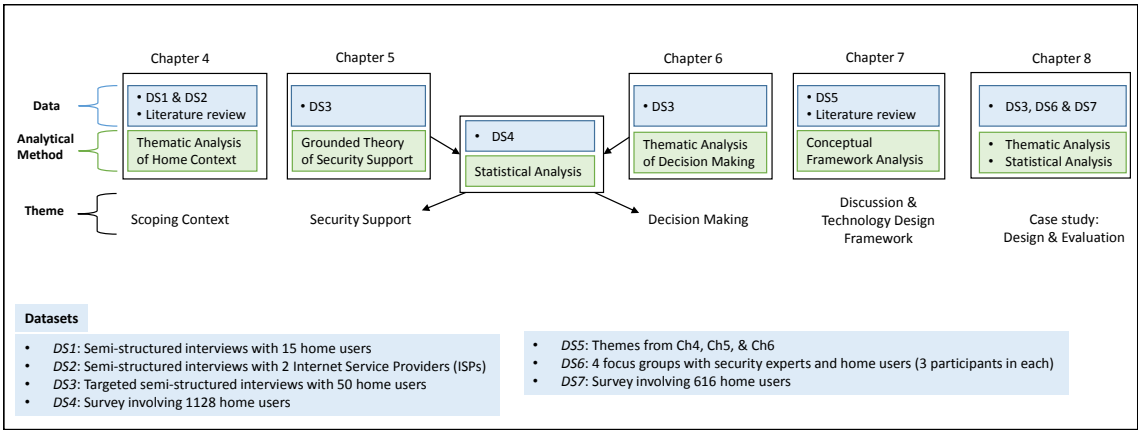


**Figure 3.2:** Research approach

## 3.2 Research Approach

Based on the research questions in chapter 1, the work reported in this dissertation sought to (1) identify important concepts in home security practice — scope the context (RQ1); (2) explore security support behaviours in the home (RQ2); (3) identify factors that influence the outcome of security decision-making (RQ3); (4) propose an approach for supporting security practices in the home (RQ4); and (5) evaluate the approach through empirical application (RQ4).

It is evident that a single research methodology could not answer all the questions. Informed by the discussion of research approaches in related fields presented in section 3.1, we devised a research approach (cf. figure 3.2) that enabled us to address individual questions separately and sequentially. In the next section, we explain why and how the different methods shown in the figure were employed to answer the questions.

### 3.2.1 Research Methodology

In this section, we describe the research strategies and methods used to carry out the work reported in this dissertation. The work was carried out sequentially from the first research question to the last. The sections below describe the methods

adapted for each research question (named according to the primary theme of each question, cf. figure 3.2).

#### 3.2.1.1 Scoping Context (RQ1)

The aim of the study was to identify important concepts in understanding the context of security practices in the home. The phenomenological research strategy, which aims to describe the essence of a lived phenomenon through the lens of several individuals who have shared the experience [126], was ideal in this study. In this strategy, data is analysed by reducing the information to significant statements of quotes and combines the statements into themes (which constitute the concepts in question).

We followed a semi-structured interview protocol, utilising an interview guide to maintain direction while keeping the interview open for both depth and breadth topic exploration. The data was analysed through a combination of both inductive and deductive *thematic analysis*, following the approach described by [35]. It was deductive in that primary themes emerged from our analysis of related previous studies (described in section 2.5.1), and inductive in that the interview data was openly coded for new themes from the views and perceptions of the participants.

Our primary participants in the scoping study were home users as described in section 3.2.3.1. We asked questions about participant demographics, devices and services they use, their concerns about data security, and if they had ever experienced a data security breach before. We further inquired what they did/do to secure their data and who did it; what informs their choice of security measures; their attitude toward data security, which we 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.

Our analysis of the interviews revealed the presence of a shared responsibility between home users and business stakeholders, especially Internet Service Providers (ISPs). We hence decided to engage ISPs (described in section 3.2.3.2) to explore their level of involvement in securing the home. For interviews with ISPs, we

adopted a project management life cycle approach, asking security questions pertaining to each phase (installation/commissioning, operation and maintenance, decommissioning) — an approach ideal for understanding business processes. The aim was to understand the different activities that ISPs undertake to secure homes and the extent of such activities. Prior to delving into details of each phase of the life cycle, we asked the participants questions regarding the services and devices sold and/or rented to customers, and the threats from which the ISPs protect customers.

#### 3.2.1.2 Security Support (RQ2)

Work addressing the second research question aimed to gain an in-depth and generalisable understanding of security support behaviours in the home. To achieve this, we adapted the research methodology proposed by the Productive Security research team of Beautement et al. [28]. In this design, the researcher starts by qualitatively exploring a topic before building to a second, quantitative phase [51].

In phase 1, we conducted 50 targeted semi-structured interviews with the participants described in section 3.2.3.3. The discussions touched on several topics, including factors that influence the outcome of security decisions, common scenarios in which security decisions are made, sources of information to enable decision-making, sources of support and assistance, problems and challenges experienced in security management, and information about successful strategies that users in the home employ to manage security.

As the data was being collected, it was qualitatively analysed using *Grounded Theory* [84] to identify important themes and theories emerging from the data, and to guide subsequent data collection (theoretical sampling). Grounded Theory allows researchers to develop theories to explain behaviours and processes [44]. This makes it the ideal choice for studying security support behaviours and any issues that surround it in the home. Our approach was consistent with that described by Strauss and Corbin [195].

A *survey* tool was developed from the Grounded Theory analysis of the interview data to test a number of significant themes that emerged in phase 2. Scenarios used

in the survey were developed from analysis of anecdotes from the interviews and themes that emerged from the analysis. The aim was to ensure that the participants were presented with scenarios they are familiar with, hence reducing the effect of unknown personal preferences. We made sure that our options to the scenarios were testing the construct under study. Hence, options with factor loadings less than .30 were dropped. The survey involved participants described in section 3.2.3.4. The survey results were statistically analysed and aimed to validate and clarify the findings of the qualitative data analysis, and support the generalisability of these results to a wider home user population.

Descriptive analysis was conducted for different variables on the survey tool. In addition, inferential tests were run on the data including Friedman [78] and Wilcoxon Signed-rank [221] tests for analysis of matched-pair and rank-ordered data. Bonferroni adjustment was applied appropriately where required. These non-parametric tests were selected on the basis of the ordinal nature of our data, where the chances of getting valid results from parametric tests were minimal or unclear. Since our analysis of ranked variables involved multiple comparisons, we conducted Bonferroni tests to control for family-wise error, the probability of making at least one Type 1 error in any of the comparisons (as recommended by Demsar [56]).

#### 3.2.1.3 Factors in Security Decision-Making (RQ3)

This study explored factors that influence the outcome of security decision-making in the home. Our primary aim was to identify (and survey for generalisability) factors that influence the outcome of security support decisions. This was to clarify and complement the support behaviours studied in section 3.2.1.2. To achieve this, we also adopted the two-phase research methodology proposed by the Productive Security research team of Beautement et al. [28].

The first part involved thematic analysis of the 50 targeted semi-structured interviews used in section 3.2.1.2 (involving participants described in section 3.2.3.3). Our focus was on identifying factors that matter in decisions regarding security support. During the analysis, however, we identified other factors related to security

work. Some of these were reported by previous studies. Hence, we confirmed their availability through literature (cf. section 2.5.6). However, two factors related to security work (survival bias and confidence in a security measure) could not be confirmed through related work, and were included in a subsequent confirmatory study together with factors in security support decisions.

The second part aimed to validate factors that influence security support decisions, but also survival bias and confidence in a security measure. We designed a survey with simple response questions to study factors that affect security support decisions. However, we could not explore survival bias and confidence in a security measure through simple response questions because we could not construct questions with direct responses that implied the constructs. This can also be seen in the study by Baron and Hershey [25] who studied outcome bias in decision evauation. Therefore, we designed scenarios from anecdotes and themes from our thematic analysis to study these two factors. The survey involved participants described in section 3.2.3.4. The data was statistically analysed using the same descriptive and inferential statistics as described in section 3.2.1.2.

#### 3.2.1.4 Supporting Security Practices (RQ4)

Research question 4 is twofold: (1) propose approach(es) for supporting security practices in the home; and (2) empirically evaluate the approach. Informed by the multimethodological approach to IS research by Nunamaker [154], we conducted a two-phase study, each addressing one need. In the first phase, a framework for designing security technology for the home was proposed (*theory building*). In the second phase, the framework was applied in a case study which involved diagnosing network security problems (*observation*), and designing and developing a network security toolkit (*systems development*). We explain below how the two phases were executed.

In phase 1, we began by interpreting our findings from studies described in sections 3.2.1.1, 3.2.1.2, and 3.2.1.3 to identify potential improvement areas and opportunities that could be leveraged. A key recommendation that emerged from the

interpretation was to *leverage existing informal support networks* to improve security practices in the home. One area we identified for improvement in order to achieve the recommended approach was to develop appropriate security technology for the home. Our analysis of the literature revealed a critical challenge that designers of security technology face in order to ground their design decisions in relevant contextual information; hence the need for a data-driven framework to guide their decisions.

The traditional and widely used approach to developing conceptual frameworks has been through conceptual analysis [213]. Conceptual analysis techniques focus on quantifying and tallying the presence of a selected concept. Carley [42] argues that this approach results in an overestimation of the similarity of texts since meaning is neglected. Jabareen asserts that this method is inadequate for theorising concepts that emerge from text [107]. Jabareen proposes a Grounded Theory technique called conceptual framework analysis, that aims to generate, identify, and trace a phenomenon's major concepts which altogether constitute its theoretical framework. At the heart of the methodology is a Grounded Theory approach [49].

Data for conceptual framework analysis must represent the practices that are related to the phenomenon and should therefore come from a variety of relevant sources such as articles, books, essays, interviews, guidelines, standards, and practices. The data must effectively represent the relevant context. The analysis is iterative, "requiring a steady movement between concept and data, as well as comparative, requiring a constant comparison across types of evidence to control the conceptual level and scope of the emerging theory" [107, p. 53]. This approach involves eight main phases: (1) mapping the selected data sources; (2) extensive reading and categorizing of the selected data; (3) identifying and naming concepts; (4) deconstructing and categorising the concepts; (5) integrating concepts; (6) synthesis, resysnthesis, and making it all make sense; (7) validating the conceptual framework; and (8) rethinking the conceptual framework. Table 3.1 shows phase 3 of our analysis (excluding data from studies described in sections 3.2.1.1, 3.2.1.2, and 3.2.1.3).

**Table 3.1:** Conceptual Framework Analysis: Identifying and Naming Concepts

| | User Needs | Security Behaviour | Technology | Threats | Security Procedures | Standards & Guidelines |
|---|---|---|---|---|---|---|
| L1 | ✓ | ✓ | ✓ | ✓ | | |
| L2 | ✓ | ✓ | ✓ | | ✓ | ✓ |
| L3 | | ✓ | ✓ | ✓ | | |
| L4 | | ✓ | | | ✓ | ✓ |
| L5 | | | ✓ | ✓ | ✓ | ✓ |
| L6 | | ✓ | ✓ | ✓ | | ✓ |
| L7 | | ✓ | ✓ | | | |
| L8 | ✓ | ✓ | | ✓ | | |
| L9 | ✓ | ✓ | ✓ | | | |
| L10 | ✓ | ✓ | ✓ | ✓ | | |
| L11 | ✓ | ✓ | ✓ | ✓ | ✓ | |
| L12 | ✓ | ✓ | | ✓ | | |
| L13 | ✓ | ✓ | | | | |
| L14 | ✓ | ✓ | ✓ | ✓ | | ✓ |
| L15 | ✓ | ✓ | ✓ | ✓ | | ✓ |
| L16 | ✓ | ✓ | | | | ✓ |
| L17 | ✓ | ✓ | ✓ | ✓ | | ✓ |
| L18 | ✓ | ✓ | ✓ | ✓ | | |
| L19 | ✓ | ✓ | ✓ | ✓ | | ✓ |
| L20 | | ✓ | ✓ | ✓ | | ✓ |
| L21 | | | ✓ | ✓ | | |
| L22 | | ✓ | | ✓ | | |
| L23 | | ✓ | | ✓ | | |
| L24 | | | ✓ | ✓ | ✓ | ✓ |
| L25 | | ✓ | ✓ | ✓ | ✓ | |
| L26 | | ✓ | | ✓ | | |
| L27 | | ✓ | ✓ | ✓ | | |
| L28 | ✓ | ✓ | ✓ | ✓ | | |
| L29 | | ✓ | ✓ | ✓ | | |
| L30 | | | ✓ | ✓ | | ✓ |
| L31 | | | ✓ | ✓ | ✓ | ✓ |
| L32 | | | ✓ | ✓ | | |
| L33 | | ✓ | ✓ | ✓ | | ✓ |
| L34 | | ✓ | ✓ | ✓ | | |
| L35 | | ✓ | ✓ | | | |
| L36 | | ✓ | ✓ | | | ✓ |

L1: [62]; L2: [169]; L3: [53]; L4: [128]; L5: [225]; L6: [103]; L7: [106]; L8: [166]; L9: [144]; L10: [129]; L11: [172]; L12: [37]; L13: [16]; L14: [45]; L15: [215]; L16: [168]; L17: [201]; L18: [116]; L19: [121]; L20: [124]; L21: [220]; L22: [188]; L23: [205]; L24: [191]; L25: [111]; L26: [217]; L27: [66]; L28: [76]; L29: [18]; L30: [200]; L31: [192]; L32: [227]; L33: US-CERT[a]; L34: BT[b]; L35: Microsoft[c]; L36: NSA[d]

[a]https://www.us-cert.gov/ncas/tips/ST15-002
[b]https://home.bt.com/tech-gadgets/computing/tips-protect-your-pc-hackers-malware-11363942012065
[c]https://support.microsoft.com/en-gb/help/4092060/windows-keep-your-computer-secure-at-home
[d]https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-best-practices-for-keeping-home-network-secure.pdf

Our conceptual framework analysis used data from our work (cf. sections 3.2.1.1, 3.2.1.2, and 3.2.1.3), previous studies, available security awareness campaigns, home security guidelines, and best practices that have been developed targeting the home user. This body of work was used to identify, integrate, conceptualise, and theorise core concepts from the home context for designing security-related technologies for the home. The output of this phase was a framework (called *Home-Appropriate Network and Digital Security (HANDS)*) for designing security technology for the home.

In phase 2, we explored problems and practices in securing home networks. This required an approach that is sensitive to context, experiences of participants, and is empirically practical in nature. Based on the discussion in section 3.1, the case study approach was selected as appropriate to the goals of the study. HANDS was applied in the case study focussed on designing a network security toolkit for the home.

Elements of the framework were used to elicit relevant requirements to understand the problem and design a solution. The framework provided structure to and enhanced the *inspiration* and *ideation* phases of the design-thinking process. The resulting conceptual design was evaluated through concept testing [139] composed of 4 focus groups with participants described in section 3.2.3.5 and a survey with 616 participants described in section 3.2.3.6.

Concept testing investigates potential users' reactions to a proposed product. In addition to getting user feedback, we aimed to validate the problems being addressed by the proposed product. The goal was to gather more information about the context of use and user needs, which would be beneficial in reviewing the concept, but also provide more information for functional specification of the product in later stages. Data from focus groups was analysed using thematic analysis. Data from the survey was analysed using the same descriptive and inferential statistical tests described in section 3.2.1.2. The author of this dissertation was the primary designer and researcher in this case study.

### 3.2.2 Ethical Approval

The research reported in this dissertation was reviewed and approved by the Social Sciences and Humanities Inter-divisional Research Ethics Committee at the University of Oxford.

### 3.2.3 Research Datasets

As shown in figure 3.2, six groups of human participants took part in this study. We describe each group in the following sections.

#### 3.2.3.1 DS1: Scoping Context with Home Users

Our scoping study focussed on eliciting and understanding significant themes in home security practice. Participants for the study were recruited through snowball sampling, a method that yields samples through referrals by informants [32]. This was considered as an ideal method cosnidering the sensitivity of security issues, and unwillingness of home users to participate despite public adverts.

The participants comprised 9 male and 6 female participants, with ages ranging from 18 to 34, and an ethnicity of 4 Asians, 5 Whites, 4 Africans, and 2 Black Americans.

#### 3.2.3.2 DS2: Scoping Context with Internet Service Providers (ISPs)

The focus of this study was to explore practices of ISPs in securing connected homes. 8 ISPs were contacted through direct emails and other digital platforms, including LinkedIn. Only 2 accepted to take part in the study. We interviewed 2 participants from the 2 ISPs (1 from each), both responsible for managing security interventions for home customers for each respective ISP. The ISPs operate throughout the UK, and have a combined customer base of over 15 million. They both offer a range of services, including broadband, TV, and communication (phone services).

#### 3.2.3.3 DS3: Security Support and Decision Making Interviews

With this group of participants, we investigated issues of security support behaviours in the home, security work activities, scenarios of security decision-making, security

tasks, and factors influencing security decision-making in the home. Data was collected through semi-structured interviews with 50 home users. We recruited for the interviews by advertising through community centres, newspapers (in print and online), and other social groupings, and by putting up posters at the National Museum of Computing. Each participant was compensated with a £10 Amazon voucher for an approximately sixty-minute session.

Demographics for our 50 participants are shown in figure 3.3. Two participants indicated being both students and employed, while one indicated being both employed and self-employed. 52% of our participants were male, and 48% were female. 44% belonged to the 18-34 age group, and 48% belonged to the 35-64 age bracket. During the interviews, these two age groups were noted to be the ones responsible for making most of the security decisions in the home environment. The other two age groups, 12-17 and 65+, made up 4% of the participants each. 32% of the participants held postgraduate degrees, 24% have graduate degrees, 16% completed undergraduate studies, 4% completed trade/technical/vocational training, 22% completed high school, and 2% did not complete any school level.

#### 3.2.3.4 DS4: Security Support and Decision Making Survey

The survey aimed to confirm and generalise qualitative findings on security support behaviours and factors that influence the outcome of security decisions in the home. Participants were recruited through Prolific Academic (`https://prolific.ac/`), and each participant was compensated with £2.50 for an approximately twenty-minute session.

1128 respondents took part in the survey. After running quality checks on the data, 41 responses were excluded, leaving 1087 responses. Fifty percent of our participants were male, and fifty percent female. Forty seven percent were between the age range of 18-34, fifty percent between 35 and 64, while three percent were above 65 years old. Of all the participants, less than one percent had not completed any education, twenty six percent had completed high school,

| Demographic | Category | # Participants |
|---|---|---|
| ***Age*** | 12-17 | 2 |
| | 18-34 | 22 |
| | 35-64 | 24 |
| | 65+ | 2 |
| ***Gender*** | Male | 26 |
| | Female | 24 |
| ***Highest educational level*** | No schooling completed | 1 |
| | High School | 11 |
| | Trade/technical/vocational training | 2 |
| | Undergraduate | 8 |
| | Graduate | 12 |
| | Postgraduate | 16 |
| ***Ethnicity*** | White | 39 |
| | Hispanic/Latino | 1 |
| | Black/African/Caribbean | 5 |
| | Asian/Pacific Islander | 5 |
| ***Marital Status*** | Single | 28 |
| | Married | 18 |
| | Divorced | 3 |
| | Separated | 1 |
| ***Employment status*** | Employed | 28 |
| | Retired | 3 |
| | Self-employed | 8 |
| | Not working | 2 |
| | Student | 12 |

**Figure 3.3:** DS3 participant demographics

| | | Gender | |
|---|---|---|---|
| | | Male | Female |
| Age | 18 - 34 | 253 | 254 |
| | 35 - 64 | 275 | 269 |
| | 65+ | 12 | 24 |

| Education | Age | | | Gender | |
|---|---|---|---|---|---|
| No schooling completed | 18 - 34 | 35 - 64 | 65+ | Male | Female |
| High school | 131 | 134 | 13 | 137 | 141 |
| Trade/technical/vocational training | 54 | 88 | 9 | 88 | 63 |
| Undergraduate | 148 | 87 | 3 | 126 | 112 |
| Graduate | 102 | 149 | 4 | 114 | 141 |
| Postgraduate | 69 | 83 | 6 | 72 | 86 |

**Figure 3.4:** DS4 participant demographics

fourteen percent had done trade/ technical/ vocational training, twenty two percent had undergraduate degrees, twenty four percent had graduate degrees, and fifteen percent had postgraduate degrees. The demographics of our participants are summarised in figure 3.4.

#### 3.2.3.5 DS6: Design Evaluation — Focus Groups

The focus groups aimed to validate user problems, to get feedback from subject experts, and to test for clarity and completeness of a conceptual statement of the design. 4 focus groups were conducted, each with 3 participants. This included 6 male and 6 female participants in the following age groups: 18 – 34: 7, 35 – 64: 4, and 65+: 1. Of these, 6 were students, 4 employed by different organisations, and 2 not working. All participants were resident in the UK. The participants were recruited through an advert in a newspaper and mass email adverts.

The first focus group consisted of 3 security experts only. The discussion in this group revolved around the clarity of the conceptual statement and how the conceptual design was developed.

The second group comprised 2 software engineering researchers and 1 software developer. The discussion in this group focussed on how they understood the conceptual statement and what informed the design decisions. The last two focus groups comprised all non-technical (not specialised in any computer-related profession) home users. The last two group discussions focussed on problem validation and on testing the conceptual statement for clarity and completeness. All four group discussions lasted about 60 minutes. Each participant was compensated with a £10 Amazon voucher for an approximately sixty-minute session.

#### 3.2.3.6 DS7: Design Evaluation — Survey

The survey aimed to test the acceptance and improvement requirements of the product design with a wider population. The survey utilised the final version of the conceptual statement from the focus groups (cf. section 3.2.3.5). The survey tool included a primary criterion question used to predict consumer acceptance; diagnostic questions to clarify consumer responses and to determine how the concept could be improved; and classification questions to determine market segments. In this dissertation, we report only results related to the functional acceptance of the concept, for which the framework was instrumental in design.

| Employment Status | Age | | | Gender | |
|---|---|---|---|---|---|
| | 18 – 34 | 35 – 64 | 65+ | Male | Female |
| Student | 49 | 3 | 0 | 35 | 17 |
| Employed | 161 | 189 | 8 | 182 | 176 |
| Retired | 0 | 17 | 39 | 29 | 27 |
| Self-employed | 12 | 44 | 2 | 37 | 21 |
| Not working | 44 | 45 | 3 | 29 | 63 |

**Figure 3.5:** DS7 participant demographics

Survey participants were recruited through Prolific Academic. Each participant was compensated with £1 for an approximately seven-minute session. 616 participants took part in the survey. Their age ranges, gender, and employment status are shown in figure 3.5. Of the 616, 5% live in shared houses with co-residents, 6.2% share their houses with friends, 74% live in family houses, and 14.8% live alone.

## 3.3 Validity of Research

Our approach followed recommended qualitative [148, 175] and quantitative [93] validity and reliability practices. We describe these in the subsections below.

### 3.3.1 Validity of Qualitative Studies

The studies involving thematic anaysis, Grounded Theory, and conceptual framework analysis ensured investigator triangulation. In thematic and conceptual framework analysis, two researchers were involved in the analysis. The primary researcher (the author of this dissertation) conducted initial coding and the second researcher (the author's supervisor) reviewed the themes and supporting quotes. Both researchers have a sound background in conducting theoretical and applied human-centered security studies; and one has been extensively involved in security by design research. The two held regular meetings to discuss the findings.

In designing the framework, once we had a draft framework, we engaged *peer reviews*. The work was presented to and discussed with two other researchers working in human computer interaction (HCI) and two researching security. The framework was subsequently reworked based on feedback from the reviews.

In the Grounded Theory study, our approach was consistent with that described by Strauss and Corbin [195]. Three individuals were involved in the analysis. The primary researcher (the author of this dissertation), who conducted the interviews, did the initial open coding of the interview transcripts. To ensure credibility of the codes, the primary researcher engaged a second person with expertise in Grounded Theory studies, who cross-checked all the codes against the interview transcripts. At the same time, a third individual reviewed the initial codes and all quotes supporting each code. Any differences and/or issues arising from the initial coding were discussed and resolved among the three researchers. A codebook consisting of 130 codes emerged from the initial coding. These codes were then applied across other interviews through *constant comparison*, while new codes were added as they emerged and were deemed necessary. In further analysis, the three individuals discussed and grouped the codes into themes (axial coding) and categories (selective coding), based on the properties and dimensions of each theme. Regular coding meetings were held to discuss any emerging codes and to group the codes into families.

In addition to the above, survey results in DS4 and DS7 were analysed and aimed to validate the findings of the qualitative data analysis in DS3 and DS6 respectively, and support the generalisability of these results to a wider home user population.

### 3.3.2 Validity of Quantitative Studies

Prior to running a full survey (DS4 and DS7), a respective survey tool was piloted and tested with seven participants. To ensure we tested for both clarity and usability of the tool (face validity), we developed and tested it on the survey platform it would run on (Unipark[1]). The questionnaire went through three iterations of testing and modification with our participants (four non-experts and three experts — two in usable security research and one in human-centred computing studies).

Two non-experts tested the instrument online, followed by *cognitive interviews* [222]. The participants were asked how they understood and interpreted

[1] `https://ww2.unipark.de/www`

each question; how easy they found it to understand each question and respond; how easy it was to navigate through the whole questionnaire; and how they viewed the general outline of the questionnaire. This was followed by *expert interviews* as applied in [168], where each expert was asked to first test the survey online, and then review each item on the survey tool in terms of biases, question ordering, clarity, sensitivity of questions, and other issues — all in line with the aims of the study. After this phase, the last two non-experts tested the tool, followed by cognitive interviews.

During each of these phases, the tool was updated based on feedback from the interviews. Once a consensus was reached on all issues affecting different aspects of the tool, we published the study on Prolific Academic targeting 1128 UK-only respondents in DS4, and 616 UK-only respondents in DS7.

To check the quality of responses, we applied three kinds of checks. First, we used Prolific's start and finish times to check for *speeders*. During testing of the questionnaire in DS4, the average completion time was fifteen minutes. After publishing the survey on Prolific, we applied demographic filters of the survey platform on the first set of fifty responses to get a representative sample of the demographics. The average completion time remained fifteen minutes, with a minimum of twelve minutes. The minimum acceptable response time was set at ten minutes. In DS 7, we followed a similar procedure, and the minimum limit was set at five minutes. Responses below the limit were rejected. Second, we checked for and rejected *straight-liners* — responses that all have the same answers — and *pattern responses* — answers in a pattern. Third, we included a *binary red herring question*, which read, "I am randomly answering the questions" with a "Yes" or "No" answer. We placed one towards the middle of the questionnaire and another towards the end. Responses bearing a "Yes" to any of these questions were rejected.

Due to the ordinal nature of our data, we tested for reliability of different constructs in DS4 (each measured by a scale of items) on the final questionnaire by computing their ordinal alpha coefficients (Ordinal $\alpha$) [80]. Table 3.2 shows the coefficients of the constructs. Since our test for continuity of care involved repeated measures, we tested for the reliability of the eight pairs of items using Spearman

| **Decision-making factor** | **Coefficient** |
|---|---|
| Survival/outcome bias | .75 |
| Confidence in a security measure | .74 |
| | |
| **Security support theme** | **Coefficient** |
| Offer unsolicited support | .91 |
| Accept unsolicited support | .83 |
| Seek support | .81 |
| Offer solicited support | .94 |
| Duty of care - social responsibility 1 | .71 |
| Duty of care - social responsibility 2 | .76 |

**Table 3.2:** DS4 ordinal alpha coefficients

rank correlation coefficient ($r_s$). There were positive correlations between each of the eight pairs of items, all significant at $p < 0.05$. The Spearman coefficients for the pairs were, $r_s(1085) = .594, .672, .601, .583, 638, .564, .499, .530$ for pairs A through H discussed in section 5.4.2 respectively.

## 3.4 Conclusion

In this chapter, we have reviewed how the related fields of security, IS and HCI approach empirical studies. Based on this analysis, we have discussed the approach that was used to conduct the research reported in this dissertation. We have explained how we employed Thematic Analysis, Grounded Theory and the Case Study approach. Finally, we explained how we ensured validity of the qualitative and quantitative studies we carried out.

# 4

# Home Data Security Context

This chapter presents a conceptual model for a home data security context. Previous work on understanding the home context (cf. section 2.5.2) provided us with a starting point in exploring security in the home. The purpose of the model was to help organise our exploration of security practices in the home.

We briefly describe the research approach, give an overview of the model, and then break it down into individual constructs (spaces). Each space is discussed in line with its contribution to data security practices in the home. Three core spaces make up the model: technology, activity, and social. The content of this chapter is based on [151, 153].

## 4.1 Approach

The work reported in this chapter was conducted using the research methodology described in section 3.2.1.1. The work involved semi-structured interviews with 15 home users and 2 participants from 2 different Internet Service Providers (ISPs). The data was analysed using Thematic Analysis. Our aim was to identify important constructs from experiential data from the home and from literature. We sought to understand how each construct fits into security practice (drawing from our broad understanding of what constitutes best security practice as discussed in section 2.3).

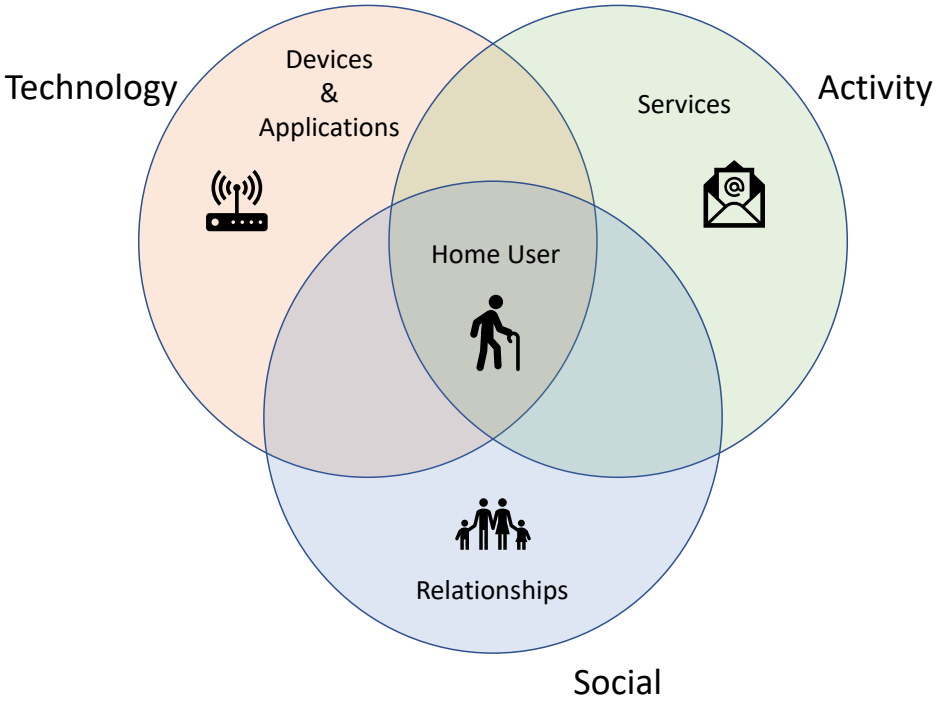


**Figure 4.1:** Home data security context model

## 4.2 Model Overview

As highlighted in section 2.5.2, references to the *home user* are enormous when discussing security practices in the home. The problem, however, is that there is no canonical definition of 'home (computer) user'. Variances in definitions and descriptions of who the home user is might consequently lead to varying understanding and prescription of security interventions targeting the same problem. User-centered security emphasises that the user must be understood in relation to their context. Our review in section 2.4.2 revealed that the first crucial part to understanding a context is to identify entities in the given environment. Our analysis of the interviews and literature led to a model of home security context, shown in figure 4.1. We discuss the elements of the model in the following sections.

## 4.3 Technological Space

This space comprises all the different devices and applications that provide services within the home. Recent advances have seen the technical space of the home being extensively explored in the context of smart homes [83, 118]. The technical stance of a home is highly contextual. Various devices and applications require various security actions from the users including patching, hardening, firmware updates, malware scanning, and updating among others. As explained in section 2.5.2.3, the technical landscape of the home determines the type of threats and vulnerabilities to be considered.

To contextualise the interview questions and align the discussion with the experiences of the participants, the researcher started by eliciting data regarding the devices and services that each participant used in their home. Common devices (owned and/or used by at least 3 participants) in the home included computer, laptop, tablet, smartphone, modem, router, switch, game console, security camera, digital camera, TV, set-top-box, and smart devices (e.g. fit bit). Most of the routers, modems, and set-top-boxes in the participants' homes were sold by or rented from an Internet Service Provider (ISP).

The participants reported buying the devices from different vendors depending on brand preferences, cost, popularity, peer pressure, perceived usefulness, and ease of use.

## 4.4 Activity Space

The activity space defines the digital services and the resulting computer centric pursuits thereof. This includes online/mobile banking, home shopping, entertainment (gaming; watching/streaming/downloading video/TV, music, etc.), home working, home education, home security, and health management. The security needs of each of these differ significantly. Actions from the home user might range from mindful behaviour to use of security technology such as encryption. Hence, the service is another critical entity in the security context of the home.

It is the management of all the devices and services, in both shared and individual use, that lies at the heart of the security challenge for home users. And with the advent of the Internet of Things, the number of devices and services being made available to home users will only increase — but the time, knowledge, and budget that typical home users will allocate to securing their information is likely to remain constant, and small (as reported in section 6.5.1.4).

## 4.5 Social Space

The overarching theme or entity that emerged from the analysis was the role of *relationships* in home data security. This is lightly echoed in the work of Dourish et al. [62] and Forget et al. [76]. Our analysis revealed the impact that business and informal relationships have on home security, especially on security management strategies and responsibility.

The analysis brought to light the importance of understanding 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 4.2): **informal stakeholders**, comprised mainly of social networks that exist in the home environment; and **business stakeholders**, composed of service providers, vendors, governments, and others.

The 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; 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].

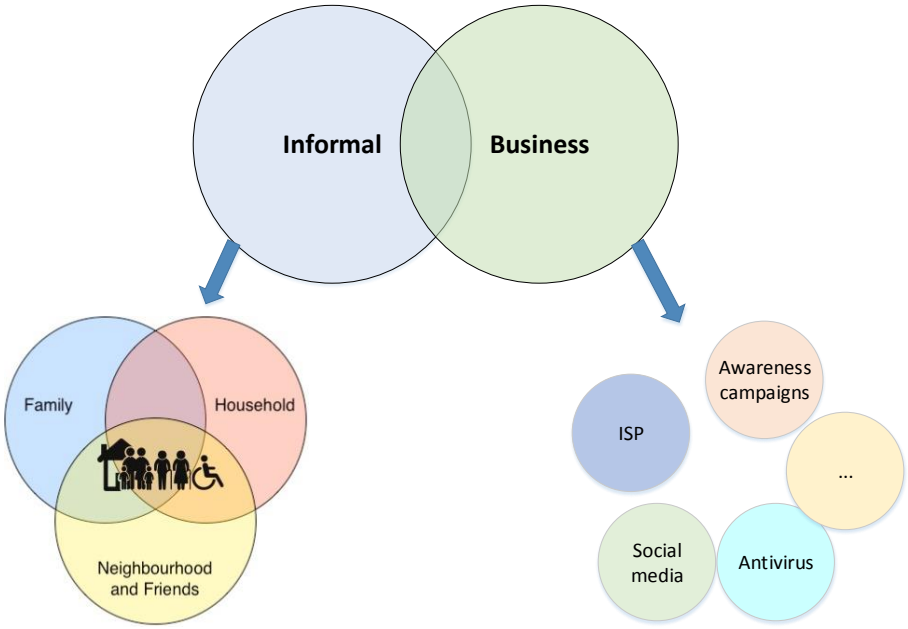


**Figure 4.2:** Home data security stakeholders

*"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].

*"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].

The stakeholders in the business sector usually operate independently of each other. For instance, governments provide awareness campaigns whereas 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.

As discussed in section 2.3, security practices comprise security behaviours and

their preceding decisions. We gathered data on practices aimed at securing data and systems in the home. We found that both business and informal stakeholders play a crucial role in securing the home. Our analysis of the data on security behaviours (from both groups of participants) revealed two separate categories of behaviours which we categorised as: *security work* and *security support*.

*Security work* is highly contextual and specific to technology platforms, comprising mindful behaviours (e.g. check for a padlock or https on a website's url) and use of security-related technology (e.g. firewalls, antivirus software, patching, data backup, and parental controls). The work can be one-off (e.g. configuring a firewall) or routine (e.g. malware scanning). Our findings showed that security work spans different phases of a product's life cycle (commissioning, operation and maintenance, and decommissioning), which is similar to what Distefano et al. [60] discussed. The product can either be a device or service. Products (e.g. a laptop) are purchased and setup (e.g. anti-malware installed and configured), used (e.g. real-time malware scanning) and maintained (e.g. anti-malware updated), and shutdown and disposed of (e.g. accounts deleted, device erased). During our analysis, we identified a number of factors that influence decisions on security work behaviours. Our findings were consistent but much less comprehensive than previous studies (cf. sections 2.5.5 and 2.5.6).

*Security support*, on the other hand, comprises two subcategories: support seeking and support giving. The work of Dourish et al. on delegation [62], and Redmiles et al. [169] on advice seeking and giving fall under security support. Our analysis pointed to a number of support practices in the home, including security advice, technical help, and information provision. Our data was not comprehensive enough to explain the different support activities we found in the home, and neither was the literature.

In the next subsections, we summarise the security pracices we identified from both home users and ISPs (cf. figure 4.3). While figure 4.3 does not show a comprehensive list of all security work in the home, we believe that it gives an indication of a typical home security posture. *Assessment* in this case refers to

| Assessment | Protection | Monitoring | Response |
|---|---|---|---|
| Antivirus | | | |
| | Firewall | Inbound and Outbound Traffic Monitoring for Malware | Adware remover |
| | Harden browser settings | | Report |
| | Data backup | | Network disconnection |
| | Encryption | | |
| | Adblocker | | |
| | Authentication (password, biometric, 2FA) | | |
| | Password manager | | |
| | VPN | | |
| | Delete unused software and apps, cookies, browser history | | |
| | Patching/Updating | | |
| | Parental controls | | |
| | Router firmware upgrade | | |
| | Mindfulness | | |

- Security that ISPs can provide is highlighted in grey

**Figure 4.3:** Security interventions in the home

vulnerability assessment and risk assessment; *Protection* encompasses practices for hardening the security of a system; *Monitoring* refers to practices for detecting security threats; and *Response* includes practices for managing and reporting security incidents. The empty column in figure 4.3 indicates that we did not find any assessment security measures when we interviewed home users and ISPs.

### 4.5.1 Interventions by Informal Stakeholders

'Mindfulness' in figure 4.3 comprises deleting or not opening email attachments from unknown sources, shopping from secure websites (check availability of padlock or https), looking out for phishing emails, making online payments through PayPal, stream legal content only, avoid sharing passwords, and minimising the amount of information shared especially online.

With the exception of the firewall, all other security practices are for endpoints, mainly computers, laptops, tablets, and smartphones. The researcher asked the home users of any security measures taken to secure network devices, including switches, modems, and routers. Of the 15 participants, only two had implemented a firewall on a router.

Our analysis revealed two main reasons our home user participants did not apply security measures to network devices: (1) they assumed the router was secured by the ISP who provided it — *implicit delegation of security responsibility.* One participant said, *"The router comes with everything set properly. We just connect and start using it. Our Internet Service Provider does everything for us. If there is anything to change for security, I think they do all that"* - [P15]; and (2) Home users assumed that network devices are already secure when they are purchased, whether from an ISP or elsewhere — plug and play: *"I bought my router from Amazon, and I think everything is configured in the best way possible. All firewalls are already there. I just connected it and somebody helped me setup our Internet connection"* - [P7]. 2 of the 15 participants used routers purchased elsewhere, other than from an ISP.

We did not ask our participants to assess and report on their technical or security expertise. However, 3 participants reported that they were employed in a security role in their organisation. 4 other participants had technical jobs (including software developer, database engineer, IT support technician) that involved some security tasks. These 7 participants reported learning from their jobs and applying some of their organisational security controls and practices in their homes, and in the homes of those they help. One participant said, *"It's normally the kind of stuff I do at work, except for some of things which use expensive and complicated software"* - [P9].

Overall, 8 participants reported offering security help to their family, friends, and colleagues. 5 of these had offered one-off help, while the other 3 had taken on the responsibility of managing the security of their families or friends. *"I always visit my parents' home to check their devices if they are secure. I just scan them to see if there is a virus. When I see something I don't know, I take the computer to a colleague in our IT Support."* - [P2]. The kinds of security measures that our participants reported to have implemented in their homes, and the homes of those they helped are listed under *Protection* in figure 4.3.

The mode of offering support was either *in-person* or *remotely* via a phone. We identified in-person help where the helpers visited the homes of those who needed help, and/or devices such as laptops, phones, and tablets were brought to the

helpers for their assistance. Remote help on the other hand was reportedly offered where the helpers had no physical access to the devices of those being helped. Most of the 8 participants who had offered help reported having used one or the other, or both means at some point. For instance, *"I call my parents to check if there are any issues affecting their computers. If they complain and I don't understand what they say, I try to make time to go and see what the problem is"* - [P12].

### 4.5.2 Interventions by ISPs

The UK has over 200 ISPs[1]. By the end of 2016, the market providing broadband services to consumers was dominated by four players[2]: BT, Sky, Virgin Media, and TalkTalk. ISPs provide broadband connection to home customers in the following two different ways: (1) through fixed line infrastructure, which provides connectivity via networks of copper (Asymmetric Digital Subscriber Line (ADSL)), fibre-optic, or cable; and (2) using wireless infrastructure, which provides connectivity via mobile networks [155].

ADSL, which is provided through existing Openreach's phone lines, is currently the most widely used connection in the UK[3]. Openreach[4] has an ADSL and fibre-optic infrastructure which most ISPs (including BT, Sky, and TalkTalk) use to deliver brodaband services to their customers. Phone lines are also the most widely used form of last mile connections for most connections on Openreach's fibre network. The use of existing phone lines increases broadband coverage of most ISPs. Virgin Media, on the other hand, offers cable broadband which is faster than ADSL because it uses coaxial cable for the last mile[5]. In recent developments, ISPs have introduced fibre connections to the home, including the last mile (e.g. see Hyperoptic's products and services[6]). ISPs who have been using Openreach's fibre-optic infrastructure have also started launching their own fibre networks (e.g. TalkTalk's FibreNation[7]).

[1] https://www.ispreview.co.uk/isp_list/
[2] https://www.choose.co.uk/guide/home-broadband-market-overview.html
[3] https://www.uswitch.com/broadband/guides/broadband_suppliers/
[4] https://www.openreach.com/
[5] https://www.broadbandchoices.co.uk/ask-our-expert/cable-vs-fibre
[6] https://www.hyperoptic.com/
[7] https://fibrenation.co.uk/

Other ISPs (e.g. EE, Vodafone, O2) provide broadband to homes through mobile networks such as 3G and 4G. Home users can either set up hotspots on their mobile phones or use mobile dongles (or even routers[8]) to provide connectivity to other devices in their homes.

Regardless of the type of broadband infrastructure in use, all ISPs (that provide connectivity to homes) share the responsibility of securing homes. Our analysis of interviews with ISPs revealed that our participants approach the security of their home customers in two ways:

**Duty of Care:** The participants indicated that the ISPs understood their duty to provide cyber care to their customers. In this regard, they provided a generic basic-level of security which included free antivirus, firmware-upgrade (for customers using ISP-provided devices such as modem/router, and set-top-boxes), parental controls, and traffic analysis for suspicious behaviour on traffic going to or exiting a home network (highlighted in grey in figure 4.3). If suspicious traffic patterns were detected, the originating customer's home was disconnected and the customer alerted. Customers were informed of the reasons behind the disconnection and were advised to take necessary actions before they were reconnected.

While both participants indicated the ISP's wish to do more, they indicated that their involvement in home network security was limited by two main factors: (1) *cost*: it was expensive to implement and maintain an infrastructure that took care of the security of all customers; and (2) the router marked the edge of the ISP's *responsibility boundary*—according to regulations and also context (the ISP does not know the needs of the home user). One of the two ISPs engaged did not allow customers to use routers purchased elsewhere for their connection, only the ISP's own. The other ISP, on the contrary, gave customers the freedom to connect their own routers.

**Business Need:** The limitations on how much ISPs could offer as a duty of care provided a business opportunity to ISPs who then offered Security as a Service, in addition to the generic interventions offered under the duty of care.

[8]See example on `https://shop.ee.co.uk/broadband/4g-home-broadband`

Unlike the duty of care, this offering was targeted, and came with specialised support. Aside from offering security as a service, the need for ISPs to maintain their *reputation* in a competitive market forced ISPs to offer some level of security, such as that mentioned under duty of care.

Both participants indicated that they strove to implement solutions (either as a duty of care or as a service) that could *scale well* with growing numbers of their customers. One participant said: *"We need to make sure that whatever we are introducing will be sustainable for our growing number of customers for the next few years"* - [I2].

## 4.6 The Home User

The home user is at the heart of this complex environment. They use devices and applications in the home, which grant them access to various services; and they might have multiple business and/or social relations. Based on this understanding, we refer to the home user as an individual who uses Information Communication Technologies (ICTs) to access digital services in a non-corporate and socio-spatial environment that is composed of three overlapping spaces namely household, family, and neighbourhood & friends.

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.

## 4.7 Security Management in the Home

Often, every home user is assumed to be the administrator of security-related technology in the home. For instance, a survey [17] asked 329 dial-up and broadband users the following questions: how well do you understand the difference between a firewall and anti-virus software; do you believe your firewall is set up correctly? Similar studies include [144, 167] which surveyed home computer users of their administrative security behaviours and awareness.

The average computer user has to worry about tasks that historically have been the concern of system/security administrators. The user has to perform system updates, firmware upgrades, data backup, network monitoring, and incident management among others. These are tasks that are overwhelmingly complex to most and understood by few. Designers of security-related technology cannot plausibly expect such advanced knowledge and skills of potential home users.

Security problems can come from "bugs and flaws in the design and implementation of the system software, firmware, or hardware, unanticipated use of the system for attacks (on either the computer processor or the human processor), and mismatches between computer activities and human expectations" [230]. Our findings from interviews with home users showed that *security administration involved tasks that required varying levels of skills.* We identified activities which most participants were able to do, e.g. setting and updating a password; those that a few were able to do, e.g. scanning for malware on an endpoint device; and those that could only be done by the highly skilled, e.g. configuring a firewall.

Our analysis of interviews with home users revealed that our participants were not always administrators of security-related technology in the home. Security was largely managed through a variety of social relationships (explored in detail in chapters 5 and 6). We identified three groups of technology users in the home in relation to security administration: (1) individuals who self-reported being incompetent in dealing with security issues and relied on others for support; (2) individuals who reported to have higher levels of security competence and provided support to others who perceived themselves as less competent; and (3) those that perceived themselves as competent enough and were administrators for their own devices and services.

In addition to the relationship between *use* of technology and *security administration*, we also identified scenarios (from 6 participants) where security administration was linked to *ownership* of technology. For instance: *"I normally use my friend's laptop. I cannot change any settings or install anything because it*

*is not mine."* - [P8]; *"It is my phone, I can install whatever I want"* - [P2]; and in a flatshare, *"We use his broadband, so whatever settings he wants"* - [P4].

Our analysis of the interviews with ISPs revealed a similar relationship between *use, ownership,* and *security administration*. ISPs felt ownership of the technology and services they provided to their home customers, and therefore took action to administer security on the devices and services. To quote the participants: *"We protect our gateway and the [TV] box itself. We already have the measure in place either at the network layer or at the end device itself to protect it. For a concern to protect our customers' [devices], we provide them the tools that allow them to protect their laptops or their mobile, but of course we cannot enforce it. It is up to our customers"* - [I1]; and *"There is about 1% of customers who have chosen to put their own devices [routers] on the network. Well their security is up to them"* - [I2].

## 4.8 Conclusion

This chapter presented the home data security context model. We discussed the different components of the model, providing relevant data from our empirical studies to clarify what each component means or stands for. In the following chapters, we take a narrow focus on specific issues that affect/influence security in the home. We demonstrate the importance of the context in understanding and planning interventions for supporting and improving security in the home. In the next chapter, we present our findings on security support practices in the home.

# 5

# Security Support in the Home

In this chapter, we present our findings on security support behaviours in the home. We briefly describe the approach taken for the work reported in this chapter. We then report the findings in three main sections: kinds and sources of support, preference for sources of support, and characteristics of security support in the home. The content of this chapter is based on [152].

## 5.1 Approach

The work reported in this chapter was carried out following the methodology described in section 3.2.1.2. The aim was to gain an in-depth and generalisable understanding of security support behaviours in the home. To achieve this, we adapted a 2-phase study. Phase 1 involved semi-structured interviews with 50 UK home users. The data was analysed using Grounded Theory to identify significant themes and theories about security support behaviours in the home. In phase 2, a survey tool was developed from the Grounded Theory analysis and aimed to validate and support generalisability of the qualitative results. We carried out a survey involving 1128 UK participants.

## 5.2 Kinds and Sources of Support

Our analysis of the interviews surrounding security decision-making in the home revealed that our participants constantly needed support in their endeavour to be secure. Previous studies explored support in terms of security advice or information [169, 168, 97, 165]. While this is a common trend, there is evidence [21, 39, 79, 135] of a low success rate of such form of support. We thus set out to first identify the kind of support that is needed or exists in the home regarding security. Our analysis revealed three kinds of support present and/or needed in the home: *provision of information, advice, and technical help.*

**Technical help** involved provision of support in carrying out security work. Users who perceived themselves as not capable of acting on security issues turned to trusted and skilled stakeholders (most commonly among the social circles of the participants) for technical help: *"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]. This also included some aspect of responsibility where someone, who was perceived to be more competent or felt responsible, assumed the responsibility of making security decisions on behalf of others (that is, decided and acted on their behalf). Apart from friends, technical support was reported to also be sought from work colleagues, IT professionals, and relations.

In addition to technical help, home users also sought **advice** from trusted stakeholders (colleagues, IT professionals, relations, friends, and websites). Advice involved provision of an opinion, an off-the-cuff recommendation, or a considered recommendation. For instance, *"It's more of an opinion. I want to ask someone because sometimes there is a tendency to overlook certain things"* - [P1]. An off-the-cuff recommendation did not involve much effort from the provider of the recommendation. The provider simply gave advice from what s/he knew. For instance, *"Usually which antivirus is good? Is it ok if someone installed this kind of software?"* - [P15].

A considered recommendation, on the other hand, required 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].

The final kind of support we found in the home was **provision of information**. This involved sharing experiences and/or operational details of some security tool for example: *"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].

While there might be some differences between information and advice, we noted that participants treated the two as the same. This challenge is also seen in other studies [169, 165] that have been done on this topic, where they interchangeably refer to the two without any difference. To avoid introducing discrepancies in the results, we therefore treated these two as one, and referred to it broadly as security advice. Our analysis pointed out the following examples of advice that our participants talked about:

- Advice on available security tools or controls
- Reviews about a particular security tool or control
- Information on the cost of protection
- Opinion or recommendation for a particular security-related action, e.g. permissions requested by applications
- Advice on privacy settings
- The risks for a specific environment, service, or tool
- Where they can get support with a particular problem

While the above findings seem to suggest that home users always have some form of support available, that is not always the case. 2 participants felt helpless when they were faced with security incidents, and they did nothing. One participant said: *"All my pictures [on my laptop] could not open. There was a message saying my files were corrupt. I had hundreds of pictures, and they were all gone. I did not know what to do."* - [P14]; and the other reported: *"My computer shows a lot of ads when I want to browse the Internet. I have had them for some months now. I don't know how to remove them... I just have to live with them I guess."* - [P17].

## 5.3 Preference for Sources of Support

In our endeavour to propose approaches for effectively supporting security in the home, we thought it ideal to first understand preferences of sources of support in the current security practice. We hence explored three aspects of security support: (1) seeking support from a source; (2) giving unsolicited support to another home user; and (3) accepting unsolicited support from another home user. The support sources and recipients we explored in our survey were the ones that emerged from our analysis of the interviews, reported in section 5.2. In the following subsections, we present our findings in detail.

### 5.3.1 Likelihood of Seeking Support

We asked our survey participants how likely they were to seek advice or help from a source of support that they believed to be more competent than themselves. The sources included relative, friend, work colleague, service provider /manufacturer help desk, and IT repair shop professional. We found that about 80% were likely to seek advice or help from a relative, about 85% from a friend, about 71% from a work colleague, about 58% from a service provider/manufacturer help desk, about 51% from an IT repair shop professional, and about 16% would seek support from other sources. Figure 5.1 summarises these findings.

We also asked the participants to rank these sources in order of preference. A Friedman Test on the ranked order of preference showed that there was a statistically

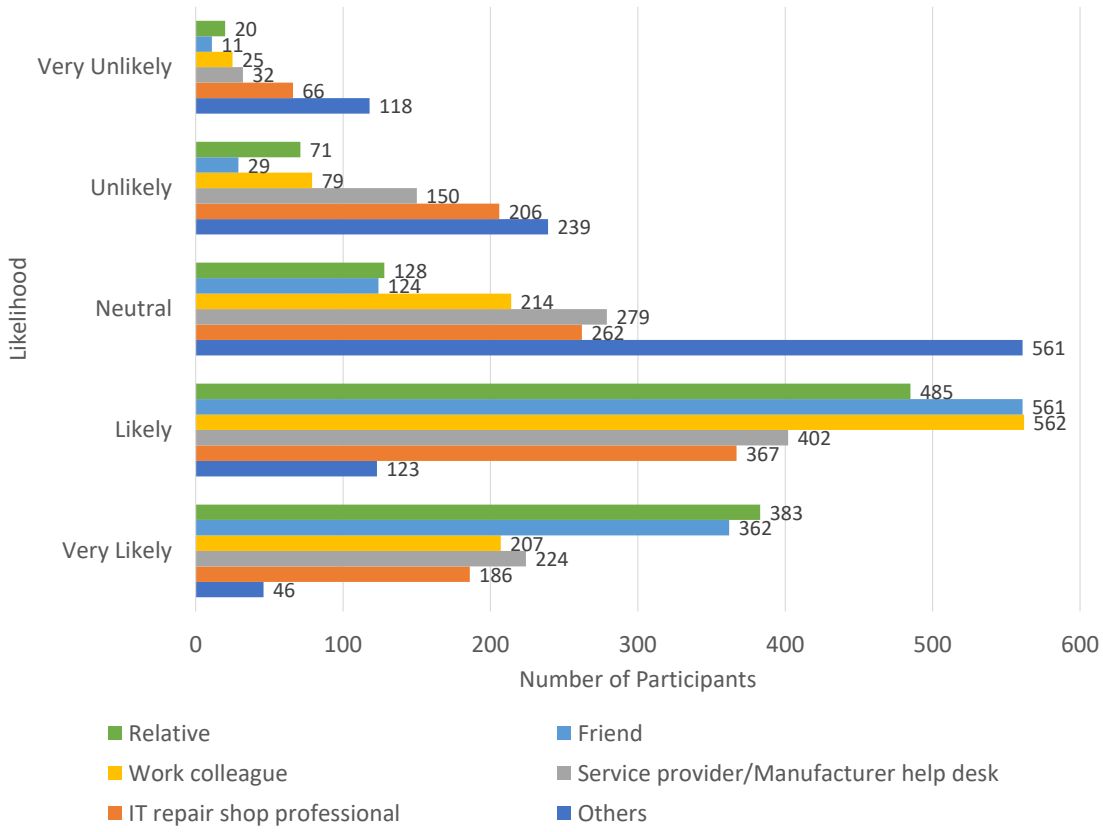


**Figure 5.1:** Likelihood of seeking support

significant difference ($X^2(5) = 2066.482$, $p<.05$). Post hoc analysis with Wilcoxon signed-rank tests was conducted with a Bonferroni correction applied, resulting in a significance level of $p = 0.003$. There was no significant difference between Relatives and Friends ($Z = -0.684, p = 0.494$). The overall ranking in order of preference is as shown below:

1. Relative and Friend
3. Service provider/manufacturer help desk
4. Work colleague
5. IT repair shop professional
6. Others

There was a significant difference ($Z = -5.618, p = 0.000$) in the likelihood of seeking support from a work colleague (71%) and a service provider/manufacturer help desk (58%). However, the rankings indicated a significant difference in reverse: the service provider/manufacturer help desk was preferred to a work colleague. We

hypothesize this might be because (1) some service providers or device manufacturers do not provide support with security, and (2) the range of services and devices available in homes is too broad, and expecting participants to go to many service providers and manufacturers for assistance is contrary to the finding in [62] where users expect one solution to solve multiple security problems.

### 5.3.2 Likelihood of Giving Support

Given the common trend during the interviews where most of the participants indicated that they sought support from friends, relatives, and work colleagues, we wanted to know how likely our participants were to offer support to those that approached them for help. Asked how likely they were to offer advice or technical help when asked by someone they believed to be less competent than themselves in data security, the results showed that about 80% would likely offer support to a relative, 78% are likely to help a friend, 67% are likely to assist a work colleague, and 41% are likely to offer support to any other people who seek it from them. These findings are summarised in figure 5.2.

### 5.3.3 Likelihood of Offering Unsolicited Support

We asked survey participants how likely they were to offer unsolicited advice and technical help to someone they believed to be less competent in security than themselves. Since the interviews showed that this practice was common among relatives, friends, and colleagues, we sought to explore in our survey how widely held such behaviour was. Our survey showed that about 56% of the respondents were likely to offer unsolicited support to a relative, about 47% to a friend, about 27% to a work colleague, and about 12% to others. See figure 5.3 for detailed results.

We also asked the participants to rank who they would likely offer unsolicited support to, in order of preference. A Friedman Test on the ranked order of preference showed that there was a statistically significant difference ($X^2(3) = 2127.517, p<.05$). Post hoc analysis with Wilcoxon signed-rank tests was conducted with a Bonferroni correction applied, resulting in a significance level of $p = 0.008$.

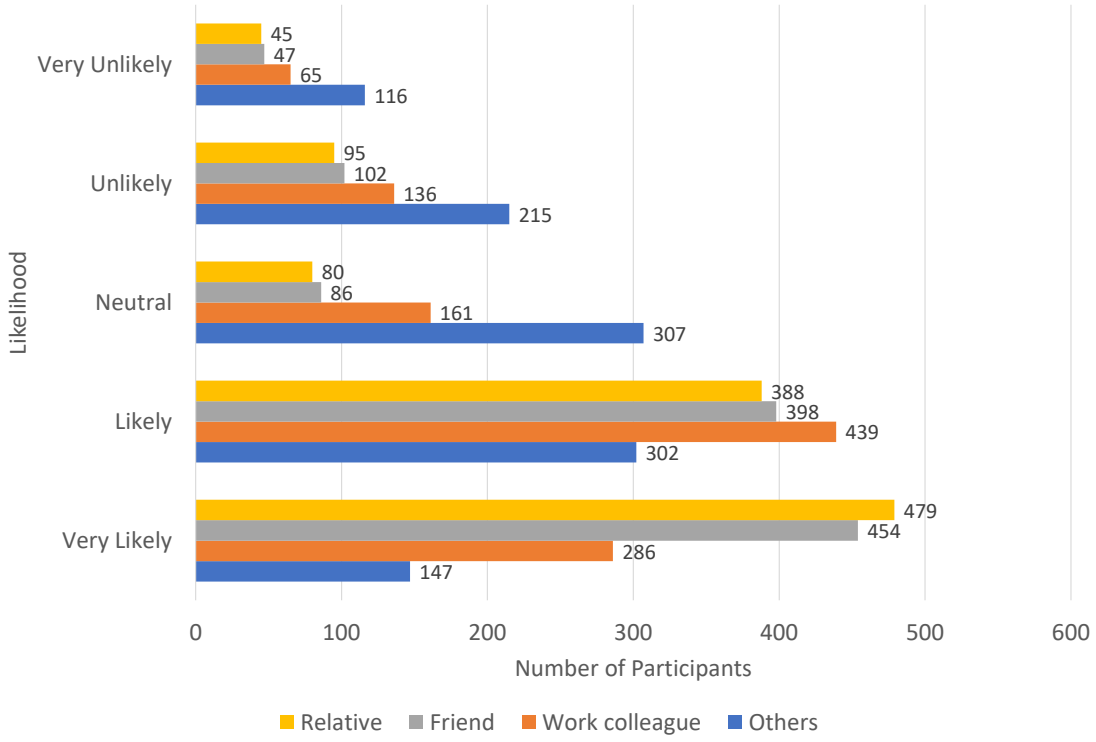


**Figure 5.2:** Likelihood of offering solicited support

The overall ranking in order of preference was as shown below:

1. Relative
2. Friends
3. Work colleague
4. Others

### 5.3.4 Likelihood of Accepting Unsolicited Support

Offering unsolicited support is only one side of the coin. To fully explore the practice, we also asked participants how likely they were to accept unsolicited advice or help with data security from different sources of support. About 63% of respondents reported being likely to accept it from a relative, 63% from a friend, 48% from a work colleague, 44% from a service provider/manufacturer help desk,

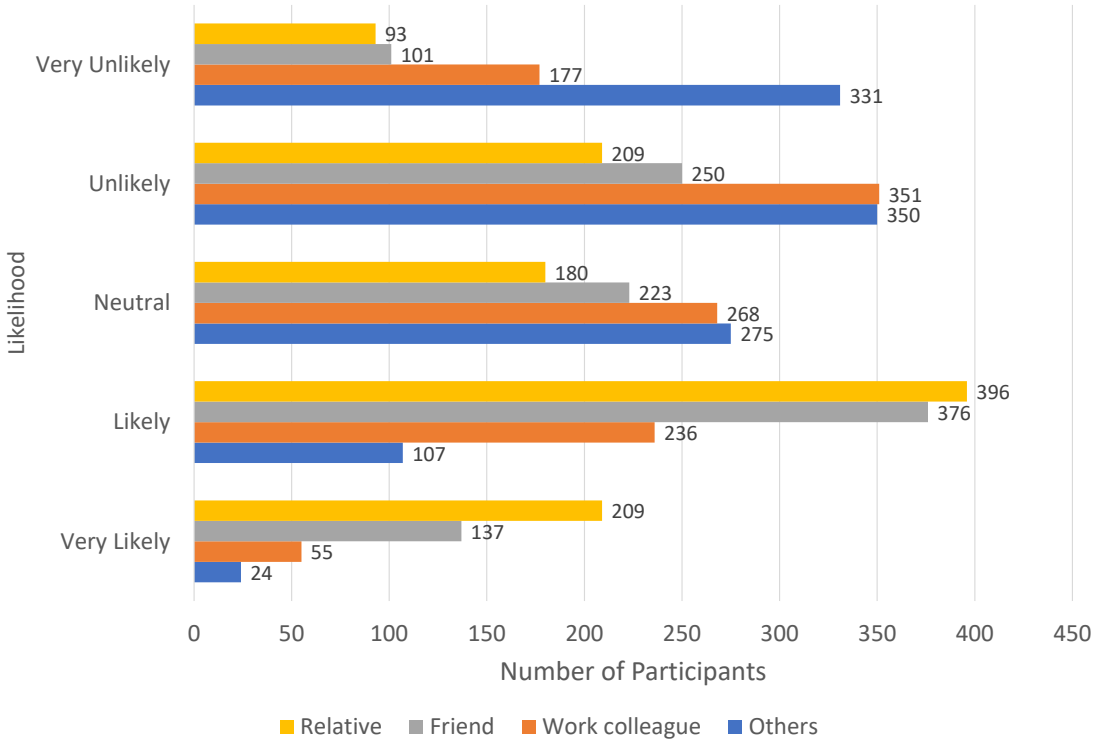


**Figure 5.3:** Likelihood of offering unsolicited support

40% from an IT repair shop professional, and about 12% from other sources. Figure 5.4 shows a summary of the results.

We asked the participants to rank these sources in order of preference. A Friedman Test on the ranked sources of support showed that there was a statistically significant difference ($X^2(5) = 1987.664$, $p<.05$). Post hoc analysis with Wilcoxon signed-rank tests was conducted with a Bonferroni correction applied, resulting in a significance level of $p = 0.003$. There were no significant differences between Relatives and Friends ($Z = -2.153, p = 0.31$), or between Work colleague and Service Provider/manufacturer help desk ($Z = -1.990, p = 0.047$). The overall ranking in order of preference was as shown below:

1. Relatives and Friends

3. Work colleagues and Service provider/manufacturer help desk

5. IT repair shop professional

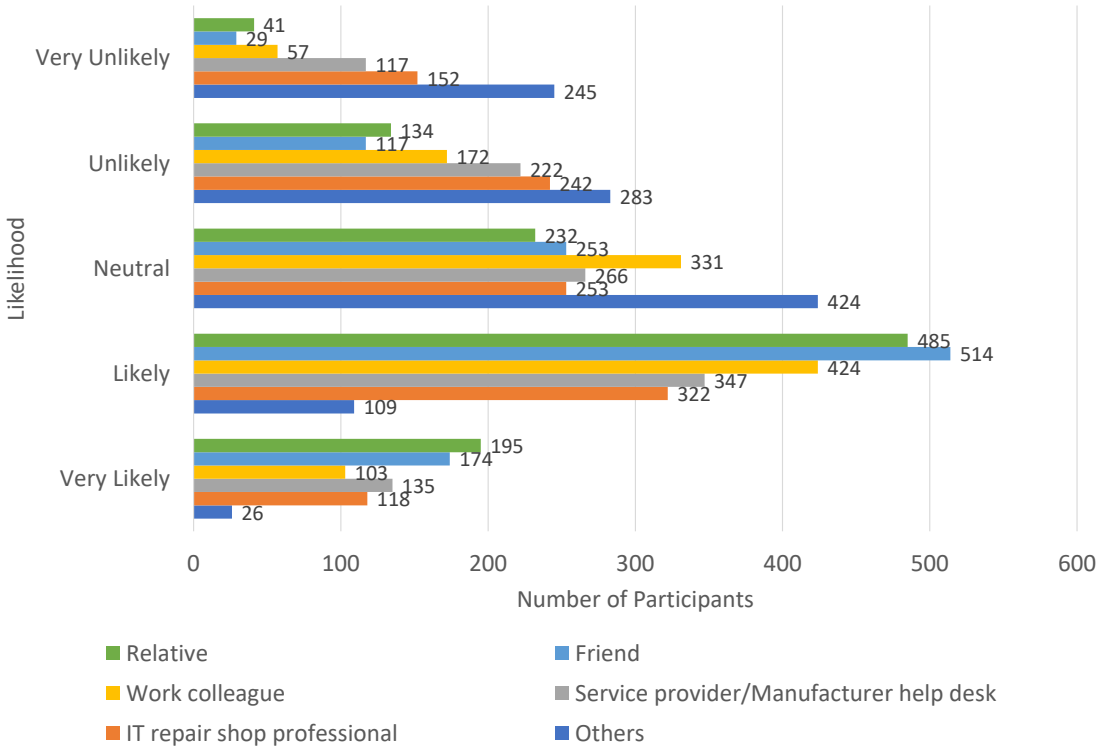


**Figure 5.4:** Likelihood of accepting unsolicited support

6. Others

## 5.4 Characteristics of Support

Our analysis of the interviews revealed that participants mostly had the same sources for advice and technical help. These included family, friends, work colleagues, service providers, and IT repair shop professionals; with family and friends being the most common source. This corroborates other studies [169, 168, 62, 79]. Other sources included search engines (*"I searched online for people with the same problem and got many results. People gave many solutions and I tried several of them until I got one that seemed to work."* - [P23]), and specific websites (*"Sometimes you go to sites that you think are credible like stackoverflow... some credible sites or sites that look credible to me. I just read about what people have experienced and how they went about it."* - [P11]).

None of the fifty interviewees cited any security awareness websites as a source of security advice. We did not expect our participants to recall details of websites they visited for security information, but this is consistent with the findings of Furnell et al. [79], who found that the majority of their respondents had not heard of public awareness websites (including Get Safe Online[1], and Webwise[2]).

Our analysis showed that the preference and choice of a source or recipient of security support in the home was characterised by two main attributes: *duty of care* and *continuity of care*.

### 5.4.1 Duty of Care

Participants consider security support in the home as a moral obligation to ensure the safety or well-being of others. This duty of care is expressed through the following modalities.

#### 5.4.1.1 Delegation

As explained in section 5.2, support for security in the home involved seeking or accepting advice, but also encompassed users taking security responsibility for others to ensure their well-being. We found that some people delegated the responsibility for security to competent and trusted others; a result shared by Dourish et al. [62], who found that people *"delegate to another individual, such as a knowledgeable colleague, family member, or roommate"*. Some of our participants said: *"Me! Mum always. I guess because my husband thinks I'm more knowledgeable about computers and about settings for the internet"* - [P7]; *"Oh! My husband, because he has always been keen on computers and adopting technology, and that is a big part of his work. So he is the one who does that [all security tasks]"* - [P45]; and similarly, *"there is a friend who usually comes here. Mostly he is the one. If the laptop has a virus, I give it to him."* - [P2].

[1]https://www.getsafeonline.org
[2]http://www.bbc.co.uk/webwise

#### 5.4.1.2 Motivation

A second way in which duty of care was expressed was by motivating others to behave securely. This generally included offering unsolicited support (see section 5.3.3). Our interview data showed two aspects of unsolicited support: (1) when somebody noticed a practice they believed to be insecure and they intervened (e.g. *"they just feel like they can send a young person like 'go and check my email', and they give you all the details to check the emails and I'm like, it's supposed to be private."* - [P1]); and (2) when there was nothing specifically wrong but support was offered (e.g. *"My parents, I do advise a lot about different security issues. They are just aware of it"* - [P43]). Unsolicited support without noticing a particular need was common in cases where there was delegation and participants felt responsible for the security of another.

We sought to understand the extent of care and intervention in cases where the participants noticed a practice they believed to be insecure, and crafted the following scenario:

| |
|---|
| Assume you have a sister named Vanessa, and you believe her to be less competent than you in data security. One day you visit her, and while you use her laptop, you notice that her antivirus is not set to automatically scan removable media, such as USB sticks, when they are plugged in. For each of the following options, how much do you agree that it is a good choice?<br>A - *Change the settings of the antivirus to enable auto-scan of removable media, and say nothing.*<br>B - *Change the settings of the antivirus to enable auto-scan of removable media, and tell Vanessa what you have done.*<br>C - *Leave the settings as they are. It is Vanessa's choice to disable auto-scan.*<br>D - *Leave the settings as they are. It is not your responsibility.*<br>E - *Ask Vanessa why auto-scan is disabled.* |

The results showed that 27% of the participants agreed with option A, 68% with option B, 23% with C, 19% with D, and 90% with option E (see figure 5.5 for details). A Friedman Test on the ranked order of preference showed that there was a statistically significant difference ($X^2(4) = 1634.910$, $p<.05$) in the choice of the options. Post hoc analysis with Wilcoxon signed-rank tests was conducted

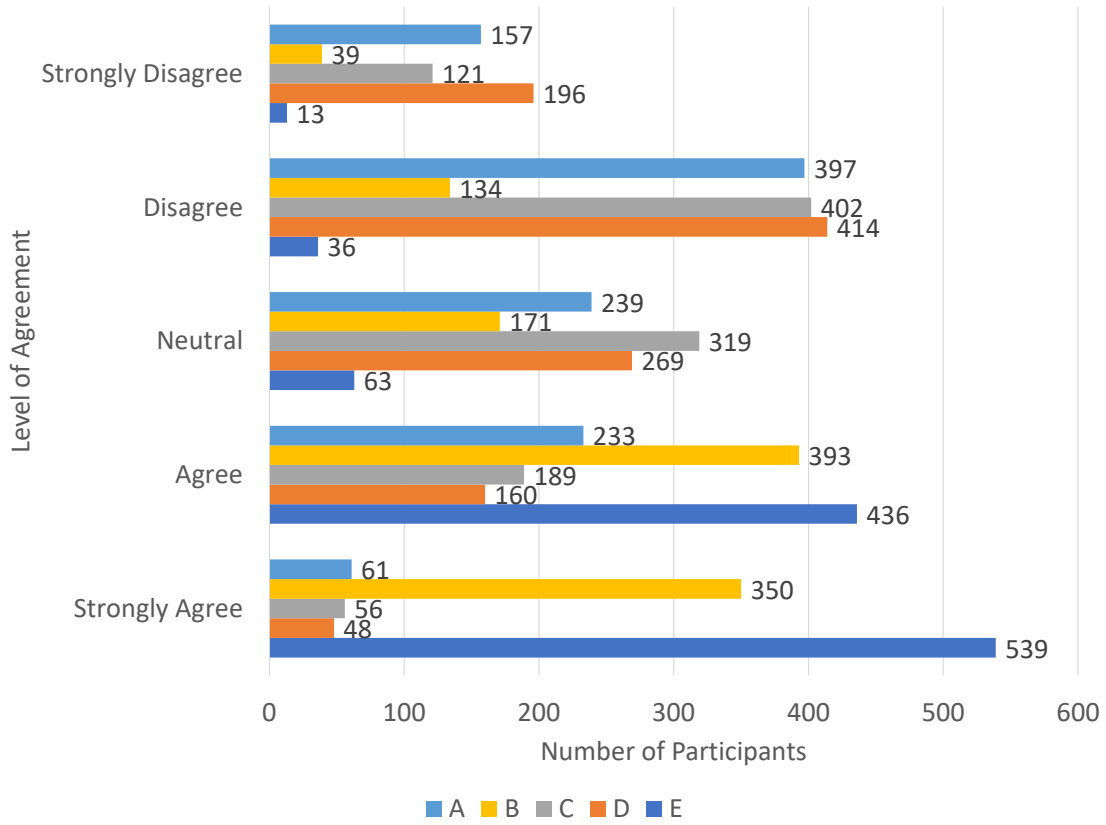


**Figure 5.5:** Duty of care: motivation

with a Bonferroni correction applied, resulting in a significance level of $p = 0.005$. The overall ranking in order of preference was:

1. E: Ask Vanessa why auto-scan is disabled.
2. B: Change the settings of the antivirus to enable auto-scan of removable media, and tell Vanessa what you have done.
3. C: Leave the settings as they are. It is Vanessa's choice to disable auto-scan.
4. A: Change the settings of the antivirus to enable auto-scan of removable media, and say nothing.
5. D: Leave the settings as they are. It is not your responsibility.

#### 5.4.1.3 Social Responsibility

As evidenced in the last scenario in section 5.4.1.2 regarding responsibility towards the security of others, option D received the least agreement (19%), and was ranked lowest. Our interviews revealed that participants considered security support

in the home as an obligation to act for the benefit of *society*. What was more interesting was the scope of this society; who did the participants consider part of their *security/secure society*? "I give it [security advice] to a certain level... I am not an expert in security, but people ask me and I tell them my thoughts... *whoever* asks me... *anyone*.. I mean *colleagues at work, my friends, my relations*" - [P40]. "[I give advice] to help her... [and to] *everyone if I know them* and I am sympathetic to them" - [P36].

More intriguing was an understanding of how much home users were willing to do to ensure that the data of their society was secure. Our analysis of the interviews indicated that even in the absence of security delegation and motivation, the participants saw it as moral to ensure the security of others. We sought to explore the extent of this caring relationship using two different scenarios.

| |
|---|
| Assume you have lived in the same flat with Bob for 2 months. Bob's computer crashed recently, but together you managed to recover his files amounting to 20GB and store them on your 64GB USB stick. While at work, one of your colleagues asks if he can urgently use your USB stick to transfer 15GB of files between computers. He promises to be done in about 30 minutes. You only have Bob's data on your USB stick. You are just about to go for lunch. For each of the following options, how much do you agree that it is a good choice?<br>A - *Move Bob's data to your computer, and let your colleague use the USB stick.*<br>B - *Let your colleague use the USB stick, and sit there and watch him until he finishes.*<br>C - *Let your colleague use the USB stick, there is enough free space. You will get it back when you return from your lunch break.* |

42% of the participants agreed with option A, 27% with option B, and 18% with option C (see figure 5.6 for details). A Friedman Test on the ranked order of preference showed that there was a statistically significant difference ($X^2(2) = 350.721, p<.05$) in the choice of the options. Post hoc analysis with Wilcoxon signed-rank tests was conducted with a Bonferroni correction applied, resulting in a significance level of $p = 0.017$. The overall ranking in order of preference was:

1. A: Move Bob's data to your computer, and let your colleague use the USB stick.

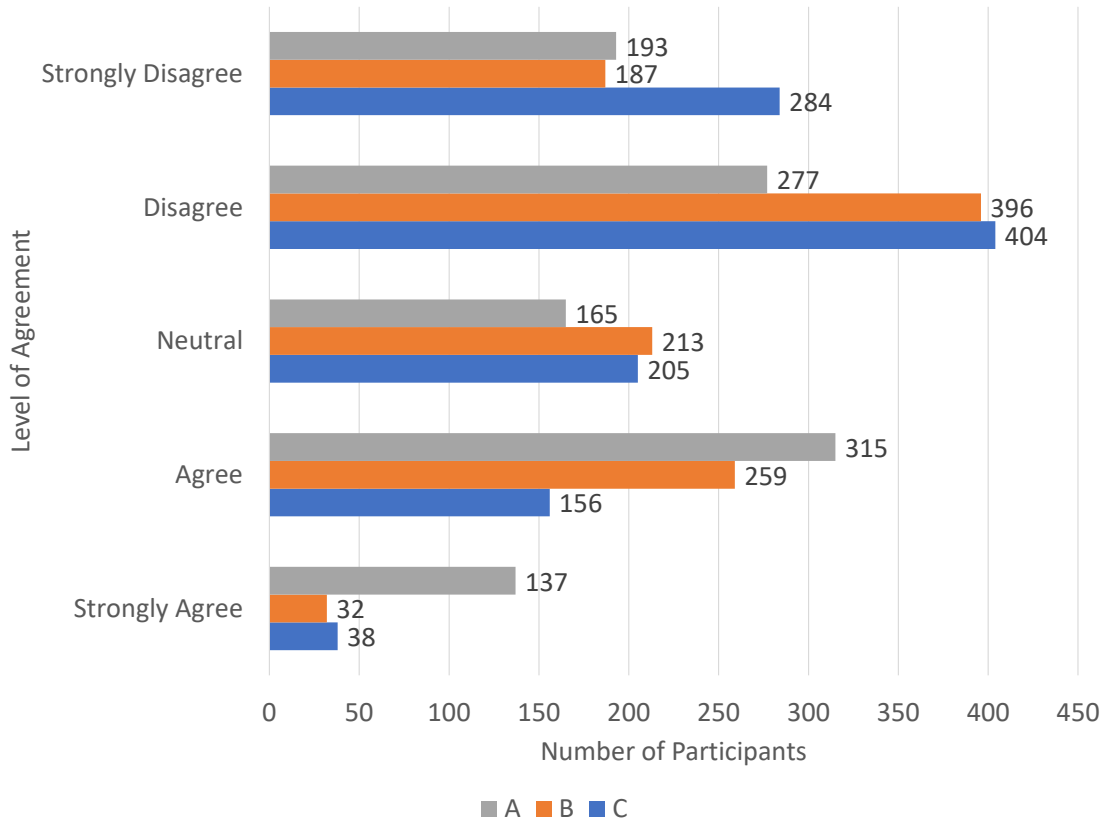


**Figure 5.6:** Duty of care: social responsibility

2. B: Let your colleague use the USB stick, and sit there and watch him until he finishes.

3. C: Let your colleague use the USB stick, there is enough free space. You will get it back when you return from your lunch break.

In the second scenario, we went further to explore if home users cared for the security of others as much as they cared for their own. We modified the scenario above to read as shown below.

In the same scenario where you have recovered 20GB of Bob's files to your 64GB USB stick, but you have another 64GB USB stick holding 20GB of your personal files. For each of the following options, how much do you agree that it is a good choice?
A - *Give your colleague the USB stick with Bob's data. You will get it back when you return from your lunch break.*
B - *Give your colleague the USB stick with your data. You will get it back when you return from your lunch break.*
C - *Move the data from one of the USB sticks to your computer, and let your colleague use the USB stick.*
D - *Let your colleague use either of the USB sticks, and sit there and watch him until he finishes.*

12% of the participants agreed with option A, 21% with option B, 54% with option C, and 21% with option D (see figure 5.7 for details). A Friedman Test on the ranked order of preference showed that there was a statistically significant difference ($X^2(3) = 731.022, p<.05$) in the choice of the options. Post hoc analysis with Wilcoxon signed-rank tests was conducted with a Bonferroni correction applied, resulting in a significance level of $p = 0.013$. There was no significant difference between B and D ($Z = -1.963, p = 0.50$). The overall ranking in order of preference was:

1. C: Move the data from one of the USB sticks to your computer, and let your colleague use the USB stick.
2. B and D: Give your colleague the USB stick with your data. You will get it back when you return from your lunch break, and Let your colleague use either of the USB sticks, and sit there and watch him until he finishes.
4. A: Give your colleague the USB stick with Bob's data. You will get it back when you return from your lunch break.

### 5.4.2 Continuity of Care

The second characteristic of support in the home that we identified from the interviews was continuity of care. Our participants looked for a continuous caring relationship with an identified competent and trusted individual. As section 6.6

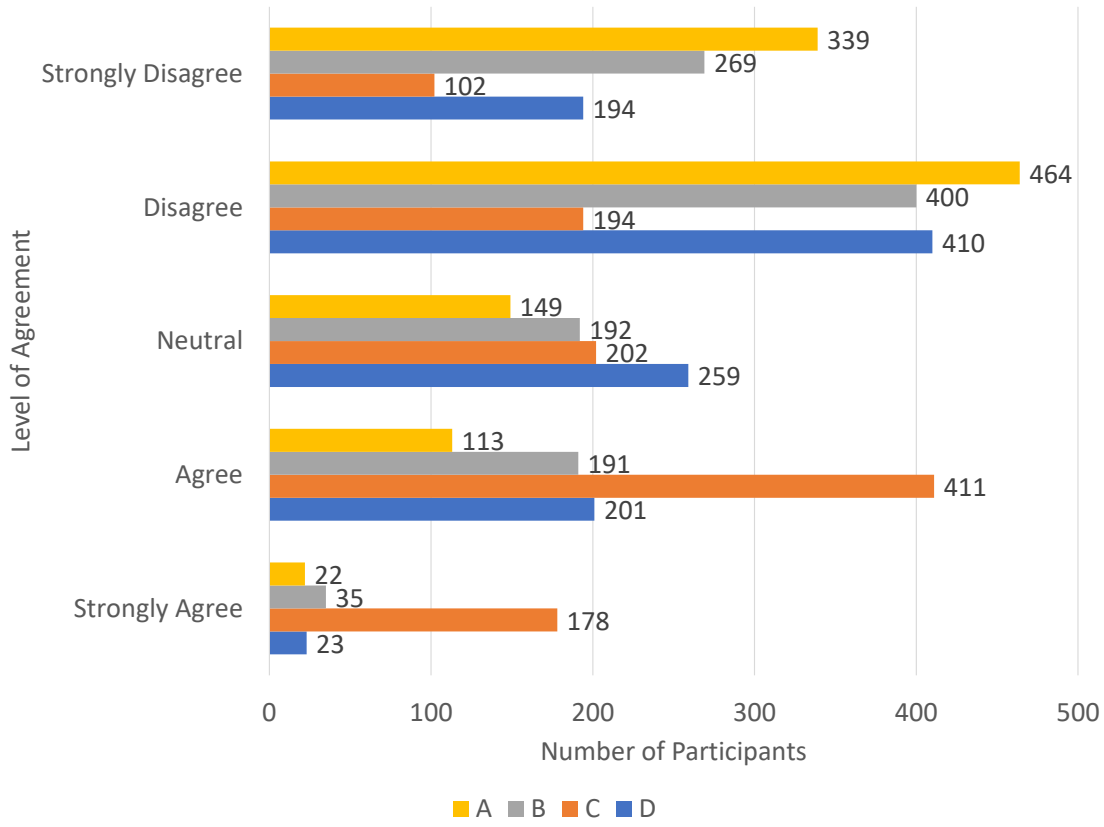


**Figure 5.7:** Duty of care: social responsibility

will show, our participants reported considering the availability of a source (ranked third from competence and trust) when seeking support. From our analysis, two reasons explain this need: (1) in the case of delegation, one needed someone who would be constantly available. Dourish et al. [62] reported that people used to delegate to a "person who had helped them in a previous context, such as in discussing what to get, helping them set up the computer, etc.", and similarly *"I was involved in helping them set up in the first place... I helped a lady buy a computer, I helped her to get it online. So she comes to me all the time for information and she keeps asking me questions. I consult and then go back to her"* - [P36]. (2) If something went wrong as a result of the support someone offered, the victim could easily go back and seek further assistance.

Our study showed that participants were likely to take responsibility for consequences resulting from support they offered: *"I may help to solve the problem"* - [P28]; *"I would consider that as my responsibility, if it was compromised"* - [P47].

To verify how widely shared this belief and practice was, we crafted two scenarios: one without indicating that a compromise was due to advice that the participant might have given; the second indicating that the compromise was due to advice that they had offered beforehand. We presented the participants with the same answers to both scenarios so that we could test the significance of the difference in taking or accepting responsibility. The first scenario read:

> Assume you have a friend, Catherine, who you believe to be less competent than you in data security. She comes to you for help because she had corrupted files on her computer and thinks she has a virus. What would you do?
> A - *Do nothing.*
> B - *Fix it, if you feel you can.*
> C - *Tell Catherine what to do to fix the problem herself, if you know the solution.*
> D - *Tell Catherine to look for help elsewhere if you feel/find that you cannot fix it.*
> E - *Arrange for a trusted contact to fix it, if you feel/find that you cannot.*
> F - *Arrange for a third party to fix it. You offer to pay.*
> G - *Arrange for a third party to fix it. You offer to help pay (share the cost).*
> H - *Arrange for a third party to fix it. You expect Catherine to pay.*

The results showed that 3% of the participants agreed with option A, 87% agreed with B, 70% agreed with C, 81% agreed with D, 73% agreed with E, 7% agreed with F, 7% agreed with G, and 56% agreed with option H.

While maintaining options A - H, we then presented respondents with an updated scenario as follows:

> Assume you have a friend, Catherine, who you believe to be less competent than you in data security. She comes to you for help because she had corrupted files on her computer and thinks she has a virus. You recall that three months ago, Catherine was trying to install a piece of software, but was failing. She asked for your help. You were busy and told her the antivirus was the problem, and to try turning it off. You now notice the antivirus is off. What would you do?

The results showed that 4% agreed with option A, 90% agreed with option B, 74% agreed with option C, 79% agreed with option D, 77% agreed with option E, 21% agreed with option F, 28% agreed with option G, and 40% agreed with option H.

**Test Statistics**[a]

| | A2 - A1 | B2 - B1 | C2 - C1 | D2 - D1 | E2 - E1 | F2 - F1 | G2 - G1 | H2 - H1 |
|---|---|---|---|---|---|---|---|---|
| Z | -.994[b] | -3.035[b] | -4.136[b] | -4.099[c] | -1.262[b] | -15.572[b] | -16.103[b] | -11.571[c] |
| Asymp. Sig. (2-tailed) | .320 | .002 | .000 | .000 | .207 | .000 | .000 | .000 |

a. Wilcoxon Signed Ranks Test. b.Based on positive ranks. c. Based on negative ranks.

**Figure 5.8:** Test for continuity of care

We ran a Wilcoxon signed-rank test against respective pairs of options to check if the changes in the responses were significant. The test showed significant changes in options B, C, D, F, G, and H. These results are summarised in figure 5.8, where the options are presented as $x1$ for options from the first scenario and $x2$ for options from the second scenario, where $x$ represents the respective letter for a given option.

## 5.5 Conclusion

In this chapter, we presented our findings on three aspects of security support in the home: (1) kinds and sources of support; (2) preferences in sources of security support; and (3) characteristics of security support in the home. Our findings revealed the key role of social relationships in home data security. In the next chapter, we present our findings on factors that influence security decision-making in the home, including factors contributing to the security support practices reported in this chapter.

# 6 Factors in Security Decision-Making

In this chapter, we present our findings of factors that influence the outcome of security decisions in the home. We briefly describe the approch taken to carry out the study reported in this chapter. Then, we present an overview of a conceptual model of the factors which emerged from our analysis. Lastly, we report the individual categories and factors. The content of this chapter is based on [151, 152].

## 6.1 Approach

This chapter reports findings from the study described in section 3.2.1.3. The primary aim was to identify and validate factors that influence the outcome of security support decisions. To achieve this, we adopted a two-phase sequential exploratory design.

The first part involved thematic analysis of 50 targeted semi-structured interviews used in chapter 5, but focused on identifying factors that matter in security decision-making. During the analysis, we identified factors related to security support, but also security work. Most of the factors related to security work were reported by previous studies, except *survival bias* and *confidence in a security measure*. In the second part, we validated the factors affecting decisions in security support and the two factors in security work through a survey involving 1128 UK participants.

In this chapter, we present all factors categorised thematically. We report results from our thematic analysis, complemented by respective survey results. For factors that were not included in the survey, we cite relevant previous studies which confirm the factor's availability. We also report numbers of participants who reported to consider such factor(s).

## 6.2 Model Overview

Our analysis of security decision-making in the home highlighted four main categories of factors that influenced the outcome of security decisions: *Stimuli* (cues to action), *Support*, *Stakeholders*, and *Context*. These categories highlight different perspectives of those involved in security decision-making, the catalyst for decisions, and the needs of those involved. Figure 6.1 summarises these categories and the respective factors that fall under each. While it is possible for any single perspective or factor to influence the outcome of decisions, we noticed that, in most cases, a number of factors were in play. As shown in figure 6.1, we identified three possible outcomes of security decisions in the home: *accept risk*, if the risk is known or perceived to be known; *act* — find ways of resolving issues — through seeking help, fixing a problem, or mitigating a risk; and doing nothing based on the perception of *not being responsible* for taking action. Our focus in this chapter is on factors that influence these outcomes of the decisions. We report each of the categories in more detail in the following sections.

## 6.3 Stimuli

Our analysis revealed five different cues that invoke security decision-making: *security concern*, *influence*, *personal negative experience*, *vicarious negative experience*, and an *ad-hoc event*.

### 6.3.1 Security Concern

Security concerns in the home fell into three main categories: (1) *uncertainty*, where the user was not sure about particular aspects of security — reported by

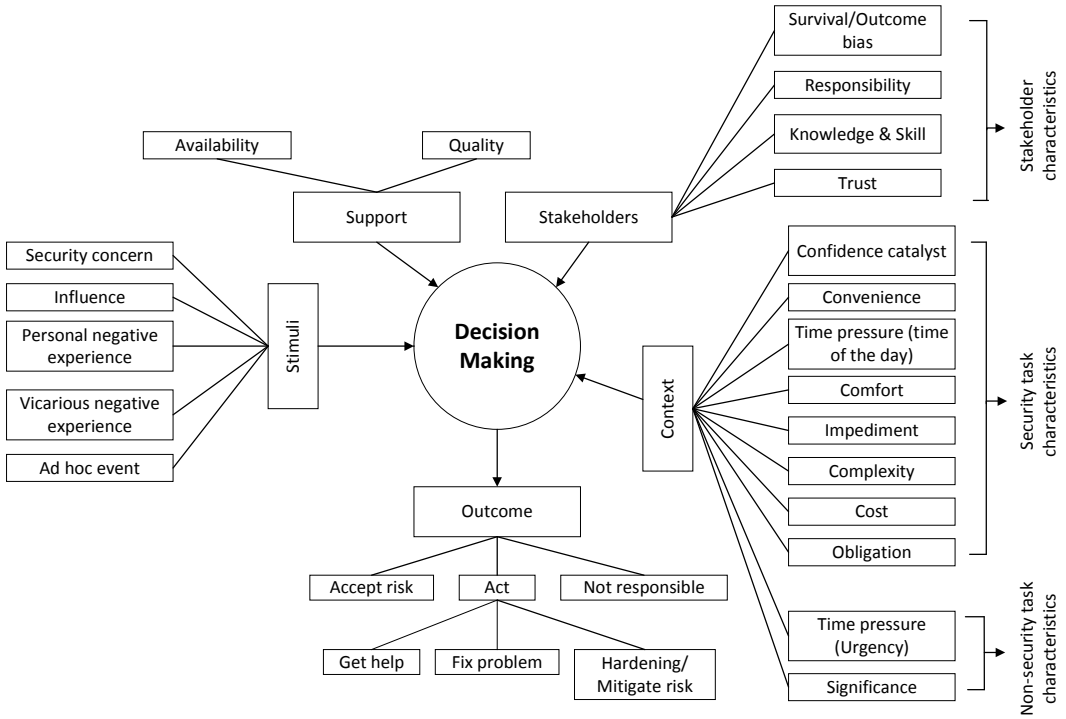


**Figure 6.1:** Home data security decision-making factors model

13 participants; (2) *loss*, where the user was concerned about losing either data or some material thing — reported by 43 participants; and (3) *nuisance*, where the user was concerned about something causing inconvenience or annoyance — according to 9 participants. Loss and uncertainity concerns were also reported in other studies to influence security decisions [15, 204].

Uncertainty included issues like: not being sure about how secure one's credentials were with a service provider; who could access the credentials on the back-end; whether or not to accept access permission requests from applications; and the kind of data that applications access in the background. One participant said, *"I don't know to what extent those apps are doing the right thing"* [P3]. This is similar to the findings in [15].

Loss was noted to be multifaceted with participants referring to both material and non-material loss. Loss of money (which was linked to loss of banking details) from a bank account through unknown transactions, for instance, was a common

concern among 33 participants, with some having experienced a related security breach before.

Other concerns associated with loss included loss of confidentiality, loss of integrity, data loss, data theft, and loss of privacy. Different kinds of data linked to these concerns included health data, pictures, contact details, banking details, communication data, and location data. Participants reported to 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]. This confirmed the results in previous work [177] where loss-framed awareness messages made participants behave more securely online.

Concerns under nuisance included 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"* - [P10].

### 6.3.2 Influence

Similar to the previous findings [169, 144, 54, 55], we found that influence played a role in security decision-making in the home, primarily as a motivating factor to act. 16 participants reported that they were influenced by different stakeholders to act. One said, *"I'm only concerned because people think I should be concerned... Colleagues that I work with, the media say we should all be concerned about our privacy [and security], and that's it really"* - [P4].

### 6.3.3 Negative Experience: Personal or Vicarious

Our findings revealed that 6 participants were motivated to act because they once had a negative experience. This was in line with findings from other studies [15] on individual security behaviour.

4 participants reported having heard about someone's negative experience from which they were motivated to act on their security behaviours. For instance, *"...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"* - [P7].

### 6.3.4 Ad hoc Event

49 participants reported to have been stimulated by ad-hoc occurrences in their contexts. These were occurrences that either made the participants suspicious of what was happening (e.g. slow performance of a computer, which was perceived to be a result of a virus attack), or warned/alerted the individuals of some security issues.

11 participants gave positive reviews and satisfaction with security alerts as an important tool for them to know of any incidents. Examples included receipt of alerts from online accounts such as Google and Facebook. *"I was once alerted that someone logged into my Gmail account in Brazil. I have never been to Brazil. So I followed what Google recommended and changed my password"* - [P2]. *"Facebook always tells me when I login to my account from any device. It tells me the device and location. So I know if someone hacks my account, I will know and change the password"* - [P43].

On the other hand, 38 interviewees reported mixed views regarding security warnings. The participants indicated that most of the time, they did not believe warnings to be true. This confirms the results in [121].

## 6.4 Stakeholder Factors

Our analysis revealed five factors related to stakeholders that influenced the outcome of security decision-making. Four of these factors have been reported by previous studies namely *responsibility, knowledge and skill, trust* and *intuition*. We could not find literature on one factor, *survival/outcome bias*. Therefore, we confirmed its availability through the survey.

### 6.4.1 Security Responsibility

The degree of ownership and responsibility for security for each device and service available to the home varied between manufacturer, service provider, operator, and family member (e.g. mobile phones, social media services, media subscriptions, and

online banking all have different structures of security responsibility). So too did the extent and nature of the security options and interactions available to home users (e.g. ranging from detailed configuration of networking options in routers, to no control over the configuration of set-top boxes).

While some services and devices were provided with robust security "baked-in", the emergent behaviour arising from their combination could itself create security or privacy problems (e.g. account chaining, where reset information for one service was sent to another, allowing an attacker to compromise other services: *"I think most important is bank account of course, and then the email because you can get lots of information from the email. Someone might eventually get hold of my account, and may be in my bank account if he or she can open my email. So there is a lot of information in my email"* - [P6]).

While 14 participants believed in and stuck to individual security responsibility (e.g. *"what I try to do is to try to explain the potential risks, and leave my partner to make a decision herself"* - [P5]), 17 participants reported having one person in the home who was generally responsible for all security decisions and activities. The participants reported that the choice of the one responsible was influenced by perceived competence of the individual: *"Probably my partner more than me. He understands computers a little bit more"* - [P4]. However, 8 participants cited parental responsibility towards protecting their children, but also familial obligations towards protecting elderly relatives according to 5 participants.

The participants reported having considered whether they were responsible for taking a particular action or not. For some actions, stakeholders in the home believed someone, either within their social space or in the business sector, was responsible for keeping their data secure, a finding also reported in [169, 79]. Asked about who they thought was responsible for implementing what they expected 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]; *"[I] 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]; and *"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].

### 6.4.2 Knowledge and Skill

Previous studies [50, 22] explained the role that knowledge and skill about security played in individual security decisions. Similarly, our analysis found that these factors influenced the outcome of individual decisions of our participants. According to 22 participants, the knowledge pertained to knowing the security risks, the security measures, and where one could seek help; whereas the skill was related to how one could do something once they knew it.

For instance, *"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]; and *"And you know some people go as far as doing firewalls and all of that sort of thing, but that's a lot about sophistication I don't have. It's probably good but I don't have it."* - [P11].

The two factors were also revealed to be influential among stakeholders when deciding whether to seek support and where to seek the support. One participant said, *"Because am not an expert so I would call someone who is much more familiar with IT related things."* - [P8]. This is explained in detail in section 6.6 on factors in security support.

We also found that experience was closely linked to knowledge and skill. We identified three perspectives of experience. First, we identified experience in using a security measure, which was perceived as possessing the required skill(s), e.g. *"Only as far as people ask what anti-malware I was using, then I told them, but not more than that."* - [P41].

Second, we found that having experienced a security problem played a role in decision-making. This was perceived as: (1) possessing both knowledge of the risk

and countermeasure, and the skill required to overcome the security risk; or (2) as a failure to handle security properly. For instance, *"On my console possibly because PlayStation, the network, has had several attacks now. But again, I don't use it for anything, you know I don't store photos or anything like that on my console, so it's kind of ok."* - [P36].

Third, we found that professional experience, which was perceived as having both the knowledge and skill to overcome security problems, was a significant attribute. When asked about where they would seek advice or technical assistance with data security, one participant said, *"First of all my boss because he is a computer nerd, he has built his own server"* - [P5]. More details on factors in security support are reported in section 6.6.

### 6.4.3 Trust

Redmiles et al. [169, 168] reported that trust played a role in security decision-making. Our results expanded on their findings and revealed three dimensions of trust: (1) trust in a service or provider; (2) trust in a source of security information (explored further in section 6.6); and (3) trust in a social relation (in the context of using and sharing technology). In (2) and (3), trusted entities included colleagues, IT professionals, family members, peers, and websites providing information in (3). Hence, trust spanned both informal and business stakeholders (cf. section 4.5 for more on security stakeholders).

Two participants said: *"I'm slightly more confident with those that haven't got hacked yet, so I'm more trusting of them"* - [P1]; and *"the most trusted data for me is from the service provider, rather than others"* - [P5].

10 participants reported sharing devices and services in the home as a familial norm or a sign of friendship and trust in each other. In some homes, there were shared devices for all, and, in addition, people also shared their personal devices with each other. Home WiFi connections were shared with relatives, friends, and guests.

We identified the following cues to trust: (1) *brand recognition* - participants reported going for devices and services that were well known and widely used, e.g

*"I tend to use sites that I have used before, and well known sites so that I am not accidentally using a fake site"* - [P38], or *"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].

(2) *Relationship with others* — we found that sharing of devices and services mainly occurred where there was some kind of relationship between those involved, e.g. *"my husband and I trust each other, there is no problem sharing our devices. Our children can also use our laptops when they want to, as long as they ask for permission"* - [P17].

In addition to the two cues, there was also (3) *visual cues* — including https and a padlock, e.g. *"online shopping, I am pretty careful that there is https, and it has the little padlock which is a little bit secure"* - [P46], and a logo (similar to [116]), e.g. *"I guess I am looking at that website to ensure that it looks credible to me. I am slightly reassured by the processing in online shopping where after you have submitted something, it pops up with my bank's logo sort of intermediate extra authentication. That's very reassuring. That means that whatever I am using has got an established relationship with my bank"* - [P33].

### 6.4.4 Intuition

The analysis pointed out that intuition was one of the ways through which 17 of our participants identified security incidents in the home. Without clear visual evidence, the participants reported the ability to identify security incidents as they happened. For instance, *"We both had quick flash screens on our laptops. Since my husband and I were both involved in some political movement at that time, we were very confident that someone was capturing what we were doing on our laptops."* - [P15]. Similarly, *"I had a quick capture screen for like seconds. At that time I was involved in some political campaign for our area. So I knew that someone, especially the secret service were tracking me. I immediately shutdown my computer. And I later deactivated the email account I was using the time I had the screen*

*captured."* - [P10]. We believe this might be in line with claims by home users that they understood security threats in their environment [79].

### 6.4.5 Survival/Outcome Bias

Our analysis of the interviews revealed a tendency for participants to concentrate on practices that had survived security breaches, and to overlook those that had not. This was a reason some participants gave for not implementing recommended security measures. They believed that as long as something bad had not happened yet, they were safe: *"For me, until something happens, I will be safe"* [P4].

Even in the face of a security concern, some participants reported not engaging in security action because: *"I think it's probably the fact that as far as I'm aware of, I haven't had serious breaches of personal data, or data security breaches. Not that I'm aware of, no. I think if I was exposed to something which was quite serious, then I would probably change my look quite a lot"* - [P6]; or *"I don't think I have because I have not had any reason to. That's why personally I just feel like as long as it has not done anything that would cause direct harm to like my information or anything like that, [it is secure]. I haven't felt the need to do any other security check to keep up with any security information because I haven't experienced anything that would cause me to do that. So I feel like until I have that experience with maybe an application, then I might either delete the application, or look for some security measures that I might take"* - [P1].

Survival bias was also discussed under the concept of *visibility of harm*. Given the typical absence of vulnerability assessment tools in the home, and also limited monitoring (see Figure 4.3), the presence of harm was seen as one way of detecting an attack according to responses from 33 individuals. The evidence of harm that our participants reported seeking was either harm to them or to their friends and relatives. *"I have not had any harm in my home network, so I think everything is fine, bullet-proof"* - [P38]. Such evidence was sought in different ways: *"I have not lost money in my account yet, so all should be well"* - [P6]; *"I don't think there is anyone who managed to see the photos in my phone"* - [P44]; *"I lost very important*

*documents some years back, so since then I decided to always use and update an antivirus"* - [P13]; and *"I don't think there is anything I do that can harm anyone. None of my friends has ever told me they suffered because of what I did"* - [P17].

While realising that statistical validation of this factor required some complex and detailed study design as shown in [25], we crafted a scenario to make a preliminary exploration of the availability of this factor. We presented the respondents with two options, both indicating survival/outcome bias. Shown below is the scenario:

> For the past 5 years, your friend John has been downloading free music, videos, and software from different websites including torrent sites without any problem. One day, he reads an article about the dangers of free downloads such as viruses, adware, Trojan horses, worms and spyware. For each of the following options, how much do you agree that it is a good choice for John?
> A - *Continue downloading free files from any website as usual. He has been doing it for 5 years without a problem, chances of being affected are very small.*
> B - *Restrict the downloads to those websites John has already used before. He has used them for 5 years without a problem, he trusts them to be secure.*

The options were evaluated on a 5-point Likert scale ranging from Strongly Disagree to Strongly Agree. The results showed that about 22% agreed with option A, while about 46% of the participants agreed with option B (cf. figure 6.2). While there was a statistically significant difference between options A and B ($Z = -18.058, p < .05$), our aim was to make an *initial exploration of the availability of survival/outcome bias*, and not to study types or levels of survival/outcome bias, or factors that affect the construct.

## 6.5 Contextual Factors

Our analysis showed that the context in which a security decision was made had two primary categories that characterised factors that influence the outcome of decisions: (1) *security task characteristics*, which defined factors related to the required security task which stakeholders took into consideration when making security decisions; and (2) *non-security task characteristics*, which was related to factors about the primary task that a user was required to do. All associated factors

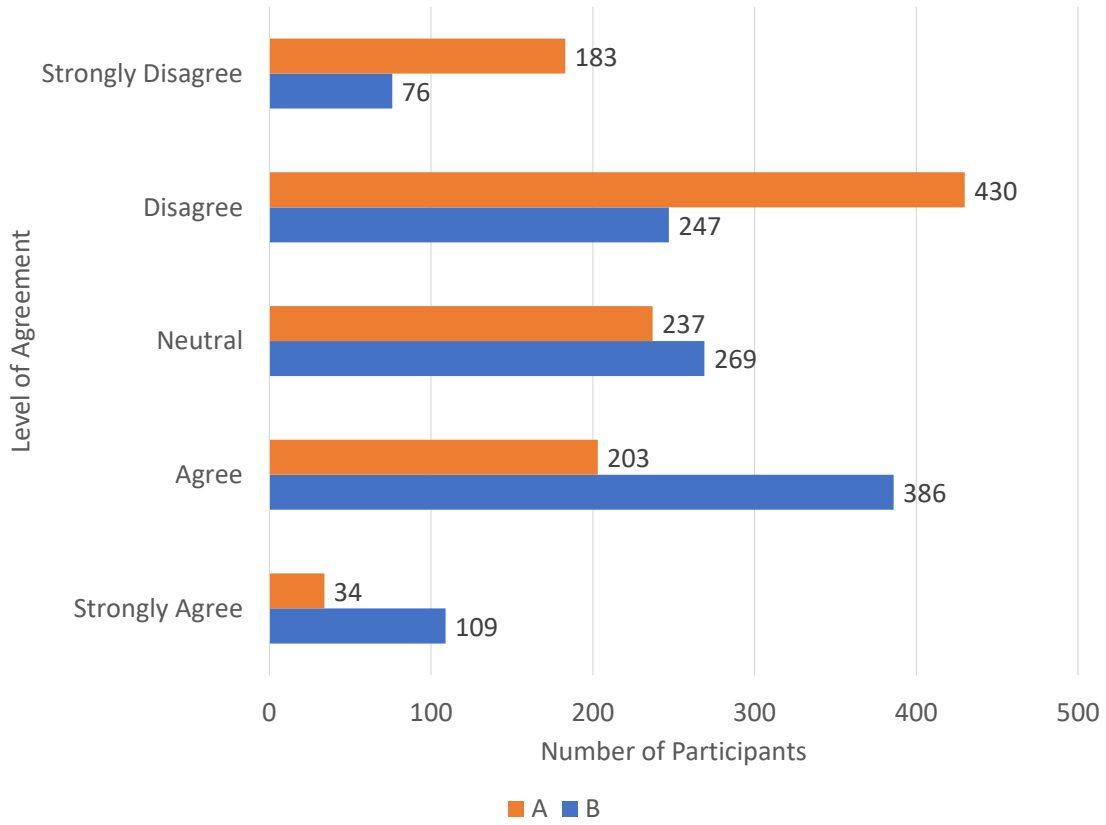


**Figure 6.2:** Survival/Outcome bias

have been reported by related work, except *confidence in a security measure* which we validated through the survey. We report all factors in the following sections.

### 6.5.1 Security task characteristics

#### 6.5.1.1 Convenience/Impediment and Time pressure (time of the day)

12 participants reported that they weighed the convenience of available security countermeasures against the importance of their activities. Similar findings were reported in [199], where the researchers examined the trade-off between security and convenience in password management. When functionality was preferred to security, users were 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].

Our analysis further showed a close relationship between convenience and time pressure. One participant said, *"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].

#### 6.5.1.2 Comfort

The participants indictated that they cared about the security of their data, and took actions to keep it secure. However, 10 of them preferred to do what they wanted comfortably. As one way of ensuring this, they tended to differentiate between more important services and those that were less important. In doing so, much effort was put on securing the most important services. One participant 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]. Similar findings were reported by [15] under the theme 'time (perceived usefulness)'.

#### 6.5.1.3 Complexity

The complexity of a security task in relation to a stakeholder's capability influenced what s/he could do or decide. In most cases, there was an interplay of different factors that influenced the outcome of a security decision. For instance, complexity would be weighed against capability and availability of required support in cases where the stakeholder was not capable of undertaking a decision or action, e.g. *"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]. Unsurprisingly, ease of use had been argued to improve individual security behaviours [96, 15].

#### 6.5.1.4 Cost

We found that the cost associated with security decision-making was threefold (similar to findings in [97]): financial, effort, and time. These were usually weighed against the expected reward after performing a required action. Talking about monetary value, a participant said: *"I would probably just go to them for advice. They are relatively reasonably priced and semi-helpful"* - [P13]. In relation to the effort and time invested in security, one participant said: *"[I wanted] to find out something relatively quickly within the first few pages of search results that had a lot of good reviews and a lot of good feedback and wasn't too expensive, and it would be easy to install. And it has worked pretty well actually."* - [P41].

Our analysis revealed two main ways through which the participants evaluated cost in their context to decide on the appropriate course of action: (1) *perceived value of impact of a successful attack*; and (2) *perceived gain of the attacker*.

46 out of 50 participants reported evaluating the cost or severity of an attack by assessing the value of its perceived impact. Our analysis revealed that the value was highly contextual and was evaluated on the basis of (a) security concerns for the particular home user — according to 46 participants, and (b) personal or vicarious experience — reported by 8 participants.

The participants reported making trade-offs in their security decisions: *"I don't mind exposing my pictures, but my bank details are the most important. I can lose money."* - [P31]. In addition, the concerns were contextual and reactions depended on the estimated value of loss resulting from an attack. A previous personal or vicarious experience played an important role in risk assessment. A common scenario was: *"there are always lots of security warnings and pop-ups when I'm on the internet saying this is not secure. I always ignore the warnings because I know the resources and I have used them before. Some are academic websites and even well known online retail websites that I always shop from like Decathlon. I don't know who sends those warnings, but they are boring"* - [P8] and *"I once had a browser pop-up which said that my computer was infected with a virus, and that Apple had detected it so they wanted to help. They requested for my Apple ID and*

*password. Since I was having a lot of ads, I thought they would help with that so I provided my credentials. I waited for minutes and nothing happened, no feedback. So I just shutdown my computer and changed my password later"* - [P15]. Examples regarding security warnings were shared by a number of our participants.

Our analysis revealed that 26 of the participants evaluated the value of gain for the attacker as a basis for taking security action. The participants reported that: *"Well, I am not an important person, why would someone target me? If I were like the Prime Minister, then I would hire someone like you to take care of my security. But I do not see the need for doing much security-wise. An antivirus is enough"* - [P45]; and *"I don't think I have anything interesting in my home that someone would be interested in. My life is boring"* - [P34].

In addition to cost in security work, our analysis revealed that cost also influenced security support decisions. We confirm this fact and explain it in section 6.6 on factors in security support decisions.

#### 6.5.1.5 Obligation

Security on personal devices for some of those who worked from home was enforced by their organisations: *"Oh that was some forced for me. It's company policy that we need to do that"* - [P6]. Similarly, 17 of the participants reported following security measures for their personal services as a requirement from a service provider.

#### 6.5.1.6 Confidence in a Security Measure

In our analysis of the interviews, we found that where a security measure was in place and the users were confident in its effectiveness, they tended to trust the service or action to be secure: e.g. *"With financial, there was one time when my credit card was charged to two transactions that I did not recognise. I immediately contacted the bank, and I was able to describe why I couldn't recognise them, and the bank believed me and refunded my money... That made me confident in using online shopping, and financial services"* - [P7]; and similarly, *"I am less concerned about banking because I find that the banking services I use to be secure, and I am often reassured by the*

*fact that if something were to go wrong, the bank is likely to compensate me for any fraud or any security breaches that would result in the loss of my money"* - [P21].

The confidence was not always to do with security measures implemented by a service provider however, e.g. *"If they have got work stuff on their laptop, or they are one of those people that have a word document with all their passwords on it, people do that, then I would probably advise them to think about high level security, or at least password-protecting files because I think it's very interesting that there has been an increase in people holding data hostage, and say pay us this, and you can have your files back. That for me would be like, ok you can keep it. I am not that bothered. Any photos I have got are uploaded to the cloud, there is nothing on my desktop that I need that can't be replaced. But for a lot of people, that obviously is not the case"* - [P5].

To explore availability of this factor, we crafted the following scenario:

> Your friend Felicity is a college student. She owns a laptop. She stores assignments and study materials on it. Felicity visits her friend, Laurel, whom she finds watching a very interesting movie. Felicity asks Laurel if she can share the movie with her, as well as some of the music Laurel downloaded. Laurel copies all the files to a USB stick, and hands it over to Felicity. On their way out, Laurel tells Felicity that she thinks her laptop might have a virus because she could not open one of her word documents to study, and this has happened to her a number of times. For each of the following options, how much do you agree that it is a good choice for Felicity?
> A - *Felicity could copy the movie and music to her laptop. Laurel probably got a corrupted file, there is nothing to fear.*
> B - *Felicity could copy the files to her laptop. She has an antivirus which will keep her data secure.*
> C - *Felicity could take and maintain a backup of her files in a USB stick, phone storage, cloud storage, external drive, another computer, etc. She could hence copy the movie and music to her laptop. She can always get the files from the backup when needed.*

We introduced option $A$ to indicate taking no action, here serving the purpose of a control variable. The other two options, $B$ and $C$, were used to test the participants' confidence in the implemented security measures and the subsequent behaviour following from their confidence. These options were also evaluated on

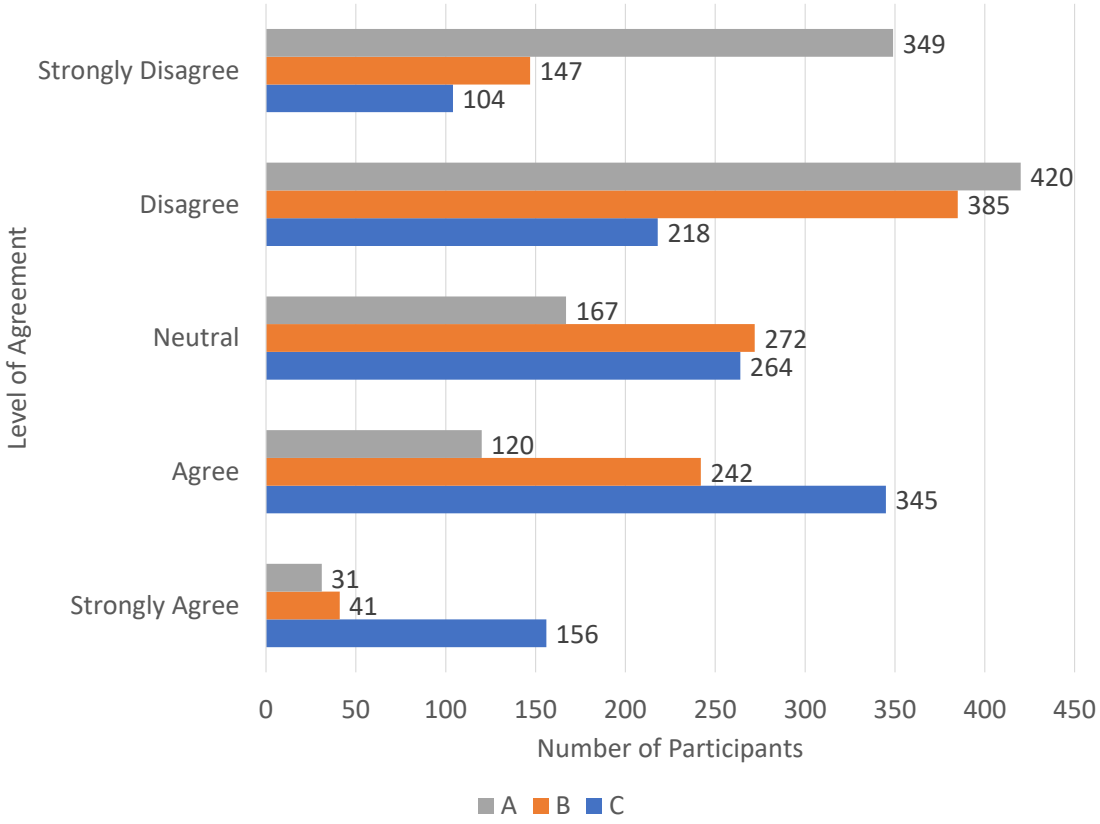


**Figure 6.3:** Confidence in a security measure

a 5-point Likert scale ranging from 'Strongly Disagree' to 'Strongly Agree'. The results (cf. figure 6.3) showed that about 14% agreed with option A, about 26% agreed with option B, and about 46% agreed with option C.

A Wilcoxon signed-rank test showed that the introduction of an antivirus in $B$ resulted in a significant statistical difference between options A and B ($Z = -16.473$, $p = 0.000$). Similarly, the Wilcoxon signed-rank test showed a significant difference between options A and C ($Z = -21.855$, $p < .05$), where a backup was introduced as a security measure. While there was also a significant statistical difference ($Z = -14.497$, $p < .05$) between options B and C, it was not our aim to compare different security solutions, and we hypothesize that this might have occurred due to the participants' perceptions, preferences, needs and experiences.

### 6.5.2 Non-Security Task Characteristics

#### 6.5.2.1 Significance and Time pressure (Urgency)

The significance of a primary task played a big role in security decisions (as also reported in [218]). 11 participants reported to consider the importance of what they were doing or the importance of what they were looking for. They were ready to trade security for something else in order to achieve what they wanted if the situation called for it. For instance: *"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]; or *"most of the times if I search for an app that I want to use, most of the time I end up using it. That's the thing. So whether or not it comes with a lot of security risk, I don't really take too much consideration into it because of the importance, like I need it at that particular point or I need to see what it does at that particular point, I might give it permission quickly"* - [P1].

The analysis revealed that significance of the primary task was assessed with regards to time pressure to complete the task. For instance, *"I think it depends on the circumstance. If it was where you need to urgently get access to the Internet in order to maybe send a message, so to get in touch with someone, then maybe yes [ignore security]"* - [P2].

## 6.6 Factors in Security Support

We were particularly interested in understanding how participants chose where to seek support and/or whether or not to accept any unsolicited support that was offered to them. In this regard, we identified five factors that were used to assess a source and/or the quality of support: perceived competence, trust, availability, cost, and closeness to a source.

### 6.6.1 Perceived Competence

The notion of *better than me* was common among 48 interview participants when talking about a source of security support. We understood this to mean the perceived competence of the source of support. 91% of the survey participants agreed to consider perceived competence in seeking or offering support. The participants reported making a comparison between their self efficacy and the perceived competence of a potential source or recipient of support.

We sought to identify the metrics that were used in this comparison, or in other words, how the different participants understood competence in security. The metrics were identified from our analysis of the interviews, and validated through the survey. Our interview results showed that for some it meant someone who *worked in data security*; 86% of the survey participants agreed with this. For others, it meant someone who *worked for a technical company*, regardless of whether their job was technical or not; 24% of the survey participants agreed to consider this metric. More than that, it also meant someone *whose job was technical*; 24% of the survey participants agreed with this.

Another metric used in assessing someone's competence involved identifying one with *more experience in using technical devices than the one seeking help*; 51% of our survey participants agreed with this. 27% of the survey participants considered someone who *had studied/studies* a technical course. 7% went for someone who was *more educated than the one seeking help*. 78% said they chose someone who *had studied/studies data security*. 39% sought help from those who had *experienced a data security incident before*. Only 4% said they did not consider any of these factors when choosing a source of support. The survey participants were asked to select more than one metric they considered, hence the percentages total more than 100.

In addition to selecting the metrics the participants considered in assessing the competence of a potential source of support, we also asked the participants to rank these metrics in order of preference. A Friedman Test on the metric rankings showed that there was a statistically significant difference ($X^2(7) = 3218.784, p<.05$). Post hoc analysis with Wilcoxon signed-rank tests was conducted with a Bonferroni

correction applied, resulting in a significance level of $p = 0.002$. There were no significant differences between options A and D ($Z = -.339, p = 0.735$), or between A and H ($Z = -1.320, p = 0.187$), or between B and H ($Z = -1.744, p = 0.081$), or between D and H ($Z = -1.646, p = 0.100$); however, B was ranked higher than A ($Z = -4.662, p = 0.000$), and higher than D ($Z = -3.909, p = 0.000$). The overall ranking was:

1. F: He/she works in data security.
2. G: He/she studied or studies data security.
3. C: He/she has more experience than you in using or working with technical devices and services.
4. B: His/her job is technical.
5. A,D,H (A: He/she works for a technical company; D: He/she studied or studies a technical course; H: He/she has experienced a data security incident before.)
8. E: He/she is more educated than you.

### 6.6.2 Trust

Previous studies [169, 168] reported that trust played a role when users chose a source of security advice. Similarly, our study found that trust influenced the choice of a source of support among our participants. Characterising this in our study was the availability of a social relationship between those involved. This was also reflected in the preferences of a source of support, reported in section 5.3. When seeking advice for instance: *"because they are my closest friends and I kind of trust what they have to say. I know that they give me an honest opinion"* - [P29]; and *"they are my parents. So I am their closest relation. I think they trust me a lot"* - [P2]. 89% of the survey participants indicated considering trust when they sought or accepted security advice or help.

### 6.6.3 Cost

Our study confirmed what other researchers [97, 15] reported about the importance of cost in security. We went further to identify two dimensions of cost among our participants that were considered in deciding when and where to seek support. First, *cost to the one seeking help*, which included money, favours, and gifts. Second, there was *cost to the source of support*, which was characterised by effort and inconvenience. These dimensions were evident in reported (from interviews) security support sought and offered among the social relationships of the participants. In the survey, we asked the participants to choose which of the two they took into consideration when choosing a source of support. 49% indicated that they considered the cost to the one seeking support as an important factor, while 36% considered cost to the source of support to be a significant factor.

### 6.6.4 Closeness

When we tried to find out about the sources of security support in the home in our interviews, one thing that was not clear was whether the preference of the sources was determined by (constant) availability of the source, or how close one was to the source. Phrases such as "my friends", "my dad", and "my work colleague" could not explicitly clarify which of the two was in play. When asked why they chose such sources, the common responses were "because they are better than me", "they know me", or "I trust them". We hence separated *closeness* and *availability* and surveyed them as separate factors. 31% of the survey participants indicated that they considered closeness as a significant factor in selecting a source of and accepting support for their security.

### 6.6.5 Availability

Our analysis of the interviews showed a common pattern in the sources of security support, be it advice or technical help. Such consistencies included friend-to-friend, parent-to-child, between couples or within a family, among work colleagues, and client-to-commercial IT services professional. In the survey, we asked the participants

if constant availability of a potential source of support was an important factor. 31% of the participants indicated that they considered availability as a significant factor.

Only 1% of the survey participants indicated that they did not consider any of these factors when selecting a source of security support. We also asked the participants to rank these factors in order of preference. A Friedman Test on the ranked factors showed that there was a statistically significant difference ($X^2(5) = 2444.265, p<.05$). Post hoc analysis with Wilcoxon signed-rank tests was conducted with a Bonferroni correction applied, resulting in a significance level of $p = 0.003$. There was no significant difference between *availability* and *cost to you (money, favour, gifts, etc)* ($Z = -.835, p = 0.404$). The overall ranking therefore was as shown below:

1. Competence
2. Trust
3. Availability and Cost to you (money, favours, gifts)
5. Closeness
6. Cost to the source of advice/help (effort, inconvenience)

## 6.7 Conclusion

This chapter presented a number of factors that influence or affect security decision-making in the home. We presented a general model of the factors, and then detailed each category separately. In the next chapter, we discuss the findings presented in chapters 4, 5, and 6. We present the wider implications, and propose a framework for supporting the design of security technology for the home.

# 7 Discussion and Technology Design Framework

This chapter presents a discussion of the findings presented in chapters 4, 5, and 6. The discussion centres on our understanding of the core issues as presented in these chapters. Based on the discussion, we conclude the chapter with a descriptive framework for designing and evaluating data security-related technology for the home. The content of this chapter is based on [151, 153, 152].

## 7.1 Approach

The first part of this chapter (sections 7.2 through 7.5) presents our interpretation of the findings reported in chapters 4, 5, and 6. The interpretation motivates a need to develop a framework to guide the design of security technology for the home. The last part of this chapter applies conceptual framework analysis [107] to our findings and related work to propose such a framework (see section 3.2.1.4 for a detailed description of the methodology).

## 7.2 Evaluating Security Decisions and Support

This work uncovered that participants in the home look for evidence, specifically impact (see section 6.4.5), of security problems for them to feel motivated to practice

security. The perceived absence of harm (to themselves or their social circles) is seen as evidence of good security decisions. However, harm arises only when an attack is attempted and then successful. A perceived lack of harm is not sufficient evidence to validate a good security decision for the following reasons.

First is the case where harm occurred but was not noticed by the home user. For instance, a user might download malware that steals information in the background without their knowledge. Another instance where the perception of harm can fail is in the situation where a successful attack harms a third party outside the notice of the home user: publicised examples of this are the DDoS attack on DyN DNS servers [27] through compromised IoT devices and the 2014 Lizard Squad attack on XBox live and the Playstation Network [132] through compromised home routers.

Second is the case where harm genuinely did not happen. However, this is not always evidence of a good security decision either. In the case where no attack was attempted, a lack of harm is no evidence of effectiveness. Vulnerabilities might still be exploitable or countermeasures ineffective. Another situation is where an attack was attempted, but was stopped by a third party before material harm occurred. For instance, a home user's credit card details might have been stolen while shopping on an illegitimate website, but the bank stopped the attacker from using the details.

Only in the third case, where attempted attacks are genuinely mitigated down to no harm, does the perceived absence of harm actually demonstrate evidence of a good security decision. We believe that this is strong evidence that survival/outcome bias is a key element in poor security decisions, and that the wider challenge of evaluating a good security decision is a difficult problem for home computer users (and arguably the wider security community).

Related to the difficulties of evaluating good security decisions is the challenge that home users face when evaluating the competence of those they seek support from (see section 6.6). For example, participants reported that the ability to use technical devices better than them was used to support the assessment of competence. However, this is not clear evidence of security competence. This problem is somewhat mitigated when home users seek support from people within their social circles,

where trust and remedial help may be available when problems arise. However, outside of established relationships and remediation, the challenge remains difficult for home users in telling the difference between a genuinely competent individual, an incompetent individual (who may or may not be aware of the fact), and in the worst case a malicious attacker seeking to take advantage by masquerading as a helpful individual.

Home users need to be able to evaluate the quality of a security decision or source of support. In the absence of clear indicators of quality, a variety of different practices have emerged, yet their effectiveness is questionable. A key challenge remains to uncover the means of making quality more evident to non-experts both for security products/practices and for the skills, knowledge, and characteristics of those who offer support. This is a hard challenge, particularly where such indicators might then be spoofed by malicious actors. However we believe it is still important to work at making good security evident to non-experts considering the wide variety of non-malicious situations where they may need to make a decision or seek support.

## 7.3 Security Responsibility and Competence

Our findings highlight another issue: *responsibility for home security* (e.g. in section 6.4.1 regarding users' perceptions of responsibility, or in section 4.5.2 regarding ISPs' duty of care). Home users, ISPs, device manufacturers — and maybe even more — all share in the responsibility of securing the infrastructure in the home. The lack of a clear definition of responsibility boundaries creates ambiguity and leads to diffusion of responsibility, especially for the home user as reported in section 6.4.1. Attached to this problem is the issue of competence and security effectiveness. By its very nature, good (network) security requires competence and expertise, and a key problem is that this is not readily available to homes. The current situation is that ISPs, for instance, that are technically competent to provide network security in the home are unwilling to take on the responsibility, device manufacturers and service providers generally constrain their efforts to their own devices and services and not

the wider home network, and home users that do take responsibility face significant issues in competently resolving their network security needs (see section 4.5).

This is a hard challenge to solve, and we propose three possible options that target the need for clear responsibility that is complemented by competence for securing the home.

The first option is for ISPs and device manufacturers to slowly and appropriately *transfer control* of the home network to home users. The proliferation of mobile apps, for example, has seen a lot of service providers offer a number of services and controls through apps (as reported in [115]). Embedding security functionalities such as configuration management, network monitoring, and incident response tools within the other services could give home users more control over their environments and, with time, take on the responsibility of managing their security. While this might address the issue of responsibility, the question of competence and expertise of home users remains, but might be addressed through improvements in digital assistants, AI agents, and machine learning algorithms.

There are potential risks, however, to the use of mobile apps to transfer security management and control to home users. A number of issues in mobile platforms, Android and iOS, can make it possible for attackers to compromise the security apps and gain control of the home network or gain access to diagnosis information. Developers of security apps must consider a number of issues related to mobile platforms which can impact security of the home. These issues might include: (1) *Android fragmentation*[1] which makes it hard for Google to enforce software updates and requires end users to be vigilant and keep their devices updated — unfortunately, evidence shows that many users do not[2]; (2) *flexibility of Android* which allows users to install apps from unknown sources which makes it possible to install infected apps; and (3) *inadequate vetting of apps* that are published to Play Store which increases chances of malware, capable of creating backdoors in other apps, being downloaded and installed on Android phones[3].

[1] `https://www.techopedia.com/definition/3899/android-fragmentation`
[2] `https://rubygarage.org/blog/ios-vs-android-development`
[3] `https://www.securityweek.com/golduck-malware-infects-classic-android-games`

The second option is to *build an infrastructure to offer security support* to home users. While this could address both issues of responsibility and competence, it is a costly solution. Much of the success of such an approach might depend on economic factors. It is not clear how much home users might be willing to pay (given that cost is a significant factor in security decision-making in the home), and whether other stakeholders could be willing to finance an infrastructure they do not directly benefit from. The main benefit of increasing the security of the home is in the reduction of threats leveraging the home to attack others. It is doubtful whether this is sufficient to attract investment from stakeholders who could benefit from this threat reduction.

Another way can be proposed inspired from a common theme in our data which can be categorised under the idea of *social cure*, where informal support workers play a key role in the digital well-being of their communities. Our findings are consistent with other work in this area, such as Dourish et al. [59], Besmer et al. [31], and Lipford et al. [130] who all point to the key role that *social navigation* and communities play in privacy and security work. Our data shows that some participants regularly rely on a trusted individual to treat their security problems (delegated security responsibility within the home environment), while others seek ad hoc help from wherever they can get it from within their social communities. This is an existing and available source of support, however the issue of competence and ability is less clear. Informal support workers have: (1) an uneven level of security expertise and ability to diagnose security problems; (2) difficulty in providing remote support, usually requiring them to be physically present when helping others; and (3) a genuine problem in procuring, configuring, and deploying security technologies that are tailored to protecting the home beyond the traditional antivirus offering (e.g. use of a firewall in section 6.4.2). On that note, a number of enterprise security tools are made available to home users for free (e.g. nmap and openVAS - cf. section 2.3.3), but: (i) they are typically not tailored to the home; (ii) the expertise needed to use them competently is typically lacking in homes; and (iii) using them is not seen as necessary by home users (see section 4.5.1).

Based on this assessment, our third proposal is therefore to leverage, provide additional resources to, and build competence in these existing informal support networks to target the gaps we have seen in section 4.5.1. This might entail providing informal security workers with: (1) tailored reference material to help them achieve good security practice in the home (for instance, to help remediate the perception that network devices do not need security and provide a common baseline of good network security design); (2) appropriate and tailored tools to help apply good enterprise security practices to the home (increasing the provision of assessment, monitoring, and response options); and (3) practical remote support options to help them perform their tasks conveniently, securely, and in a timely fashion (over and above the reported use of telephones). Because these networks of support are already in use, we believe that these steps will help the existing support workforce to bring about improvements in the quantity, quality, and timeliness of their security work. The end result could have a direct and pragmatic impact on the practical security posture of homes while remaining acceptable to the home user population and fitting in with their existing practices.

As a means of improving the competence of informal support workers, an interesting idea would be to identify key members of social groups, target them with particular security interventions, and let the new behaviours cascade through the social networks organically.

Given the intrinsic and complex social aspects of these existing networks of support, we foresee significant challenges, e.g. better understanding the motivations behind giving and receiving support; mapping out the type and extent of different kinds of security work that individuals are willing to offer to others; or exploring the kind and extent of access individuals are willing to allow to people who they know socially, rather than professionals who are performing a contracted service.

## 7.4 Security Technology

We have seen that most of the security-related technology in the home is for securing the endpoint (cf. figure 4.3). While technical endpoint protection measures are

important, they do not provide comprehensive security on their own as evidenced by the proliferation of network attacks (e.g. [123, 182, 132, 157, 65, 27]). This emphasises the need for *collective security* for all devices and services in the home, as echoed in [118].

The lack of — and need for — network monitoring tools in the home has long been recognised. As discussed in section 2.5.7.2, most of the network security proposals are aimed at performing network monitoring. Similarly, US-CERT states in ST15-002 (see section 2.5.4) that: *"**Monitor for unknown device connections:** Use your router's management website to determine if any unauthorized devices have joined or attempted to join your network. If an unknown device is identified, a firewall or media access control (MAC) filtering rule can be applied on the router. For further information on how to apply these rules, see the literature provided by the manufacturer or the manufacturer's website".* As reported in section 4.5.2, ISPs perform traffic monitoring on inbound and outbound traffic for malware. This is a significant intervention, and would be well complemented with approaches that perform internal network monitoring for malware and other kinds of threats such as unauthorised access to devices and systems in the home.

Monitoring and managing a secure network is a cumbersome task to carry out. Organisations have automated tools that monitor and flag incidents — successful or attempted. The lack of such solutions in the home has forced home users to depend on what they perceive to work best for them in detecting incidents. Relying on harm as a way of detecting incidents may have detrimental consequences, as discussed in section 7.2. Provision of tools that detect and communicate attempted or successful incidents would provide an early warning to home users, and would also provide evidence that, regardless of their assessment of themselves as lacking in value (as discussed in section 6.5.1.4), they are still targets of attacks.

The reliance on intuition to detect incidents and attempts does not give an accurate representation of the issues (cf. section 6.4.4). Wrong assumptions might: (a) lead a home user to abandon a secure service or application for an insecure one; and/or b) cause stress on the stakeholder involved — as reported in section

6.4.4 for instance. The two security-related technologies that have some ground in detecting incidents and attempts are warnings and alerts (cf. section 6.3.4). The success of security warnings, however, is very limited mostly due to a large number of false positives and the frequency of their use, as reported in our study and also extensively studied in [121].

Alerts on the other hand seem to perform better, as reported in section 6.3.4. We postulate that this might be due to their limited and occasional use, as applied in the cited scenarios of Facebook and Gmail. We believe such an approach could be leveraged in detecting and communicating network security incidents. Such a technology could work better if complemented with recommended actions (as reported in section 6.3.4 about the Gmail alerts), that are simple to perform for the home users, or are tailored to include the individuals who typically assist the home users (user-centric). Detecting administrative access and modifications to a network router, for instance, might help prevent potential serious threats. It can allow home users to act on time, either stopping an ongoing attack or hardening their system so that an attempt can not materialise. In the case where an incident is successful, the ability to easily roll back any changes made to the configuration can help home users manage the incident in a timely and cost-effective way. However, more empirical work needs to be conducted to identify and understand the attributes that lead to success of the alerts, as in the cited scenarios.

Overall, security technology in the home should be able to *diagnose* and effectively communicate problems to relevant stakeholders. This would ensure evidence-based practice that would address issues of survival/outcome bias or mere negligence of recommended security practices. This would enhance proactive security practice, other than the current mostly reactive practice. In addition, this would help to ground security decisions in contextual evidence. Diagnostics would involve asset identification, vulnerability assessment and prioritisation, and real-time monitoring of security threats.

There is also a need for *protection technology* that is suited for the home; i.e. adapted to the social context and technology usage models of the home.

Availability of appropriate security technology to complement diagnostics might enhance adoption and use of such among the mostly non-expert communities.

Lastly, the home needs technology that would ensure quick and effective *management of security incidents*. Such technology might include recovery tools, but also incident reporting or support tools. This would aim to address incidents affecting both endpoint and network devices, and provide a platform for home users to report incidents or seek and provide incident management support.

## 7.5 Wider Implications

### 7.5.1 Harmonious Technical Solutions for the Home

Our research has uncovered the key role that social relationships play in home security — serving as informal support networks — and the reasoning behind these informal support networks. We have also revealed factors that influence the outcome of security decisions in the home, novel of which are *outcome bias* and *confidence in security measures*. Our findings also emphasise that there is *a focus on technical endpoint security in the home*, *a lack of tools for assessment, monitoring, and incident response in the home*, and *a fractured structure of security responsibility in the home*. We have also pointed to two potentially useful security-related practices in the home: *careful use of security alerts* and *advances in cheap, open source, and portable security technology.* These findings have implications in the home security domain.

We reported in chapter 4 that homes have a wide range of devices, for various purposes and from different manufacturers. Procurement decisions are influenced by need, cost, features, personal brand preferences, and popularity. Most home infrastructures are therefore inorganic (i.e. they contain technology from different manufacturers, with different compatibility and security requirements). This is in contrast with enterprise practices, where they normally have well defined procurement processes for devices and services. Issues considered in enterprise procurement processes include compatibility with the wider infrastructure, consistency, and manufacturer or supplier support (including patching).

This is in contrast with the practices in the home. For instance, some manufacturers deploy patches automatically, others depend on device owners to patch their devices, and still others do not even make patches available for the devices. Such an environment without procurement procedures (and where it is hard or nearly impossible to implement and maintain one) would benefit from *harmonising technical solutions for the home*. This can be achieved through the development of *open standards*, such as a standard for patch deployment. Harmonious technical solutions for the home would also make it possible to develop technology to enable central management of security activities, as reflected in the need for one solution to solve a number of security problems in the home [62].

### 7.5.2 Contextual Design of Home Security Technology

Evidence has shown poor adoption rates and usage of security technologies by *home users* [17, 79, 167, 144, 106]. However, attacks targeting the home are on the rise (e.g. [27, 65, 132, 123, 157, 182]) either to harm people in the home or to use home connected devices as instruments in attacking others (e.g. Distributed Denial of Service Attacks from compromised home devices on critical infrastructure, or as malware infection vectors). Given the proliferation of connected devices and services in the home, the situation will simply get worse.

While it is generally accepted that security tools must be designed with the context and the user in mind, eliciting appropriate contextual requirements from the home remains a challenge owing to its complexity. As a result, people over-generalise issues about the home. For instance, researchers have described the *home user* in different ways: "the distinguishing characteristic is that the users are not professionals in computing" [103], or "a citizen with varying age and technical knowledge who uses Information Communication Technologies (ICTs) for personal use anywhere outside their work environments" [120]. Such broad generalities are too simplistic and reductive. While research has been looking at the home, design in security has not.

Given the demographic, knowledge, and skill diversity and other nuances in the home, designers of home security technology are at risk of designing for an *elastic home user* and creating *self-referential designs*. Cooper et al. [48] describe an elastic user as an ill-defined user whose characteristics change to suit the needs or views of the designer. Similarly, self-referential design fits the designer's own motivations, goals, skills, and mental models [48]. Expecting home users to know what they ought to do, when to do it, how to do it, and how to do it well (as reported in section 4.5.2) has proven not viable with the current practice. However, similar challenges have been encountered in ubiquitous computing. Researchers and professionals have sought to address this by basing designs of technology on an understanding of the context for which they design. Frameworks, models, and ontologies have been developed to inform the design of such technology (e.g. [95, 136]).

Current security practice has shown that most designers of security technology design for the enterprise environment, not the home. We believe this can be improved if *designers of security-related technology for the home are guided by a framework of the core issues that need to be considered during the early stages of design*. Such a framework could outline issues that, based on the context and current practices in the home, would be beneficial to designing technology that meets the needs and capability of home users. This can be applied, for instance, to the development of technology that creates an enabling environment for informal support workers to carry out their tasks effectively.

In the next section, we apply conceptual framework analysis to our work and related work to propose a data-driven descriptive framework that enables designers to ground their design decisions in relevant contextual information.

## 7.6 Home-Appropriate Network and Digital Security (HANDS) Framework

Section 4.7 reported that a user in a particular home is not always an administrator of security-related technology despite wide assumptions. Three groups of technology users in relation to security administration were reported. In addition, behavioural

models that guide use of technology in the home differ significantly. For instance, adoption and use of an application like Facebook Messenger does not require domain-specific knowledge and skills. On the other hand, to effectively use a security tool such as a firewall requires the user to understand issues such as threats, vulnerabilities, and countermeasures; knowledge which most home users do not have. Hence, the existence of a complex security support infrastructure in the home.

Our findings in chapters 5 and 6 have shown that the less someone knows about security, the more they need help. However, it is important for support providers to know the time and type of help that is needed, but also what tailoring is required to meet the needs.

How then do we design security tools for such an environment with varying users who have different motivations, capabilities, control, and attitudes? More importantly, how can we incorporate models of user behaviour into models of security, so that real user behaviour is taken into account? (A question also posed by Zurko [230].) We heed the call by Zurko and Simon [231], and propose a framework for considering the context of use as a primary design goal at the start of security tool development.

The framework sets out basic issues that designers must consider when evaluating existing solutions (e.g. to make evident problems affecting effective adoption and use of security-related technology) or designing new security technology for the home. The framework describes seven aspects of home data security technology (cf. figure 7.1): *technology, procedures, standards & guidelines, threat model for the home, user needs, existing technology* and *existing behaviours*. The threats and user needs come from established models of threats (e.g. the home threat model discussed in section 2.5.3) and contextual user needs (e.g. the needs discussed in this study, including contextual awareness, integrated solutions, social cure, and ease of use) respectively; whereas the standards & guidelines are available mandatory and non-mandatory security best practice.

The main goal of the framework is to guide designers to come up with a good *design concept* (i.e. home-centred technology shown in figure 7.1). Hence, the

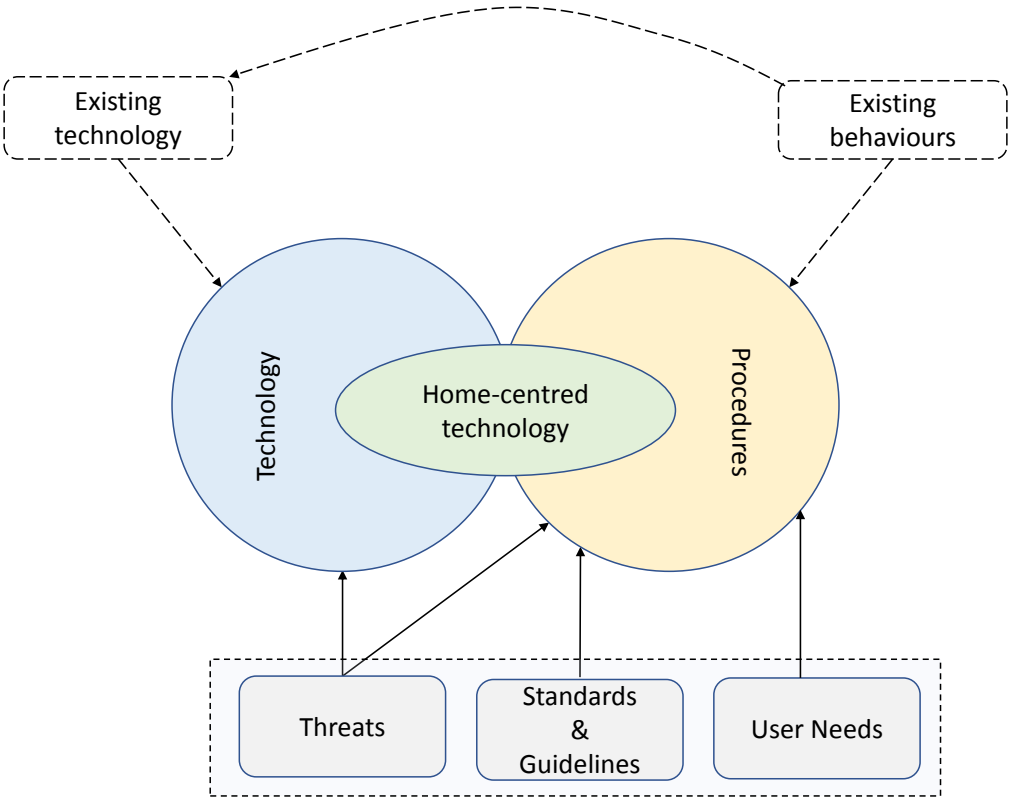


**Figure 7.1:** HANDS framework

scope of the framework is the ABC of user-centered design (i.e "Analysis", "Begin with objectives", and "Conceptual design") [102]. The *analysis* in HANDS involves understanding existing behaviours and existing technology, formulating procedures, and coming up with design ideas. The *objectives* of the analysis are to identify and understand users and the context use necessary for the design of a product.

### 7.6.1 Threats

A preliminary step in the design or evaluation of a secure system is to answer the question *secure against what?* [145]. A threat model answers this question by describing a set of hypotheses about who (or what and how) could attack a system. Swiderski and Snyder [197] describe the purpose of a threat model:

- To improve a design's security by anticipating specific attacks and implementing countermeasures in advance.

- To anticipate the varying outcomes of successful attacks and their possible impact.
- To enable the creation of advance response plans to deal with significant attacks as and when they occur.

It is therefore imperative that designers have a clear picture of threats facing the home. Attention must be paid to threats affecting assets in the home, but also threats introduced by the (new) technology itself. We have discussed the threat model for the home in section 2.5.3.

### 7.6.2 Standards and Guidelines

Unlike enterprise security, the home does not have policies and standards to guide behaviours. However, a number of guidelines have been developed targeting the home (e.g. Get Safe Online[4], US-CERT's Home Network Security[5]). While not mandatory as standards, guidelines provide a framework within which security procedures are implemented. Together with enterprise guidelines and standards, these could be useful reference points for analysing existing user behaviours, grounding them in security best practice. This understanding is beneficial in specifying security procedures for supporting existing behaviours, on whose basis security technology is designed or evaluated.

### 7.6.3 User Needs

Core to the success of security interventions in the home, is the understanding of the home user and designing interventions accordingly. Schneier reports in [185] that "security is all about people... if we are to have any hope of making security work, we need to understand these people and their motivations". Based on our findings and of previous studies, we have identified four core aspects of the home that security technology must pay attention to: *situational awareness, social cure, integrated solutions,* and *ease of use.*

[4]https://getsafeonline.org/
[5]https://www.us-cert.gov/Home-Network-Security

We have uncovered evidence that home users look for *situational awareness* regarding data security (e.g. see section 6.3.4). This includes awareness of: (1) security problems in a given environment, device, or service; (2) available security solutions to resolve diagnosed or detected problems; and (3) usable guidelines or recommendations for security interventions.

Home security technology must take into consideration and provide the capability for informal support workers and support seekers in the home to effectively achieve their goals. The concept of *social cure* has been reported in this study and in [76, 169, 62]. Activities that are done under social cure include delegation of security tasks (e.g. remote monitoring and management of a home network) and social responsibility (e.g. provide unsolicited support to other stakeholders). The technology should facilitate trust relationships among stakeholders, but also allow home users (and any relevant individuals) to be in control of their environments (e.g. assign and revoke access rights to informal support workers).

Dourish et al. [62] state that people expect *one solution to solve multiple security problems — integrated solutions* to a number of problems. Similarly, we have reported that the proliferation of IoT and other Internet-connected devices in the home has made security management a cumbersome task for home users. This calls to attention the centralised management of a number of security tasks in the home.

Lastly, security-related technology for the home must be developed to enable non-experts to effectively carry out security tasks, or to delegate security work. It has previously been reported that lack of *ease of use* perpetrates insecure behaviours [100, 9]. The field of usable security emphasizes matching security principles and demands against user knowledge and motivation.

### 7.6.4 Existing Behaviours

As discussed in section 2.4, understanding the task(s) of a user for which a solution is designed is core to the success of the intervention. Understanding existing behaviours in the target environment includes understanding how users structure their activities as revealed in their thoughts, intentions, and how they orient their tasks. This helps

frame the goal(s) of and tasks to be supported by design. This process involves the use of contextual inquiry [231] to yield data on user work as a basis for design.

### 7.6.5 Existing Technology

Most of the security problems in the home are not new. They are similar to those in enterprise environments. The two environments, however, vary on how they approach and support security interventions. We have mentioned in section 2.3.3 some tools that are available in the enterprise environment for supporting security activities. Some of these could be adapted to the home environment, or provide guidance or a benchmark for the design of new technologies for the home. Identification of existing technologies can be through existing behaviours, or other tools available in practice aimed at achieving a specific security goal. Existing technologies span security assessment, protection, monitoring, and incident management.

### 7.6.6 Technology

Technology refers to an artefact that solves a security problem in question (i.e. helps to protect assets from associated threats). This could either be: (1) a new technology designed from an understanding of the threat model and existing technologies[6]; or (2) applying existing security technology to the home environment[7].

The threat model informs design or selection of technology in two ways: (1) it informs about threats that the technology is aiming to protect against; and (2) it informs about threats introduced by the technology itself. For example, outsourcing the management of home network security as described in [69] would protect against spoofing and denial of service. At the same time, the proposed solution might expose data from the home to disclosure to entities that are not otherwise permitted to access it. Consideration must therefore be given to both cases to ensure the final

[6]For instance, most of the proposed approaches discussed in section 2.5.7.2 are said to have been developed from an understanding of the home threat model, with some using the performance of existing technology as a benchmark.

[7]For instance, as shown in [53] where the functionality of an ISP's IDS/IPSs are extended to protect the home network.

solution does not introduce significant security problems into the home environment, and, if it does, they should be dealt with accordingly.

### 7.6.7 Procedures

A procedure could be defined as an established or official way of doing something. Enterprises have and enforce procedures that are aimed at achieving particular security goals. Such procedures are developed from security policies, standards, and guidelines. In the home, however, there are rarely security policies. Homes have heterogeneous and unregulated security behaviours. As Peltier [160] states, there is no generally accepted standard for a proper way to write procedures. It depends on how they currently are or what will work best to provide the target audience with what they need.

We believe that the understanding of user needs, existing behaviours, and the threat model could be used to derive security procedures in a given home context. The resulting procedures can help to determine whether and how technology will support the practice in question. Peltier [160] provides guidelines in writing security procedures.

Existing behaviours provide a basis for procedures, informed by the user needs. Behaviours and user needs ensure that procedures are in line with what the user wants to achieve (security goal), and how they want it done. For instance, *"I call my parents to check if there are any issues affecting their computers. If they complain and I don't understand what they say, I try to make time to go and see what the problem is"* - [P49]. From this, the main aim or activity could be stated as 'security monitoring', which is done both remotely and locally on another entity's computer. A section of the procedure would look like figure 7.2.

The example in figure 7.2 is aimed at demonstrating what procedures can look like, but is not comprehensive. In this example, the specific security goal is not stated, technical capabilities are not explained, tools used are not given, stakeholders and their level of involvement is not outlined either. All this and more information can help make procedures more comprehensive, but also more

*Monitoring Activities*

1. Devices must be regularly monitored to detect potential security problems and to track ongoing effectiveness of protective security measures.
2. Any security issues discovered must be securely reported to authorised personnel.
3. The health status of devices must be regularly reported to authorised personnel.

*Authorised Personnel*

1. Device owner.
2. Support provider(s) trusted and assigned by the device owner.

**Figure 7.2:** Sample security procedure

daunting. Contextual inquiry must aim to gather as much information as possible to make the procedures thorough and comprehensive.

Threats, on the other hand, define potential dangers from which assets are being protected, but also threats introduced by the procedures. If there were an activity in the procedure above which required the stakeholders involved to share information over the phone as is the current practice, for instance, threats such as information disclosure through eavesdropping would need to be considered. The value of the information shared over the phone would determine if significant threats are introduced; e.g. sharing credentials over the phone might have a more detrimental impact, in case of a successful attack, compared to sharing application error messages or codes.

The final procedures must determine whether, where, and how technology would be applied to support the practice in question. It might be possible to find that a practice would be better supported by non-technical means.

### 7.6.8 Home-Centred Technology

Home-centred technology refers to security technology that takes into consideration technical, social, and organisational needs and nuances of the home context. The

resulting technology can be persuasive in nature, designed following a user-centred approach; and aimed at enabling, motivating, or to constrain user behaviour or attitudes.

In the example given above, an existing monitoring technology such as an IDS can be adapted to the given context. Additional features would be designed to enable the responsible stakeholder to conduct remote monitoring on concerned machines. At the same time, the owners of the machines would be given the ability to assign and revoke access rights to/for particular individuals they assign the responsibility to. Both device owners and the support worker would be alerted in real time of any issues detected on the devices and also the health status of the devices.

## 7.7 Conclusion

In this chapter, we discussed the findings presented in chapters 4, 5, and 6. We divided our discussion according to three main themes we saw emerging from the findings: (1) evaluating security decisions and support; (2) security responsibility and competence; and (3) security technology. Based on the discussion, we put forward three recommendations for improving security practices in the home: (a) leverage the informal security support infrastructure; (b) make the quality of security evident to non-experts; and (3) prioritise security efforts and develop appropriate tools. We finally presented a descriptive framework for designing and evaluating security technology for the home. The framework describes eight aspects of the home environment that a designer must take into consideration: the home threat model, standards & guidelines, user needs, existing behaviour, existing technology, technology, procedures, and home-centred technology.

# 8

# Case Study: Home Digital Security Technology

In this chapter, we demonstrate an application of the framework developed in section 7.6 to the design of a network security toolkit for the home. We start by briefly describing the approach taken to carry out the work reported in this chapter. We then motivate the problem, describe the application of the framework, report findings of an evaluation study, briefly describe the system prototype developed from the design, and close by discussing the application and results.

## 8.1 Approach

As discussed in sections 7.2 and 7.4, our work identified several challenges faced by home users in securing their homes, including difficulties in identifying security problems, evaluating security risks, and managing security incidents. We build on this work, and propose a solution to some of the problems.

We demonstrate how each component of HANDS was applied to the design of a network security toolkit. The resulting toolkit was evaluated through concept testing, comprising 4 focus groups (of 3 participants in each) and a survey involving 616 participants. The methodology for this study is described in section 3.2.1.4.

## 8.2 Motivation

Evidence has shown poor adoption rates and usage of security technologies by *home users* [17, 79, 167, 144, 106]. However, attacks targeting the home are on the rise, either to harm people in the home or to use home connected devices as instruments in attacking others (e.g. Distributed Denial of Service Attacks from compromised home devices on critical infrastructure, or malware infection vectors). Given the proliferation of connected devices and services in the home, the situation will simply get worse.

Security efforts in the home have focussed on securing endpoints (see sections 2.5.7.1 and 4.5.1). Even so, much work has focussed on securing home computers; yet more devices, some without management interfaces, have penetrated the home in recent years (mainly due to the advent of the Internet of Things). Recent attacks have targeted and exploited insecure devices in the home, and affected both homes and the critical infrastructure. Grossklags et al. [86] state that the overall protection level of a network depends on the sum of contributions normalised over the number of all participants. This emphasises the need to find ways of holistically securing the network in the home.

In this chapter, we report on a case study where HANDS was used to support the conceptual design of a network security toolkit for the home, aimed to support the practices of home users in securing their networks. In the next sections, we demonstrate how the different components of HANDS were applied to the design thinking process.

## 8.3 Existing Behaviours and Technologies

To scope and target our efforts appropriately, we created two personas and a scenario from our data. The personas and scenario were developed using the approach described in [48, 214, 164]. The scenarios were developed from different situations which emerged from our interview data — similar to the approach described in [34].

We validated the personas and scenario using our quantitative research dataset involving home users (see section 3.2.3.4). Our personas were as follows:

1. **Alice, 45, the Incompetent User**

   Alice is a high school teacher. She has spent her professional life teaching languages. She likes researching and trying new teaching methods. Because of her work, she spends some hours everyday on the Internet doing research and downloading teaching aids. She is familiar with basic use of technology, but is not interested in learning more.

   Quote: "I told you my friend, ..., because he is a Computer Engineer, mostly he has to put some security." - P2

   Key facts:

   - lives in a home with a broadband connection
   - considers herself incompetent to appropriately secure the home network
   - is sensitive to suspicious activities
   - seeks and accepts help from trusted, competent stakeholders

2. **Jane, 28, the Support Provider**

   Jane is an academic administrator at a business school. She studied business management and worked as an office administrator at a telecommunications company before joining the business school. She stays with her partner, who is greatly into new technology. Through him, Jane is familiar with technology, and is willing to explore new innovations.

   Quote: "I always visit my parents' home to check their devices if they are secure. I just scan them to see if there is a virus. When I see something I don't know, I take the computer to a colleague in our IT Support." - P1

   Key facts:

   - has experience using some security technologies
   - considers herself to be somehow competent in security

- is comfortable to help those she considers less competent
- feels obliged to help her family and friends

Our scenario read as follows:

*"Alice lives with her husband in their family home. They have a broadband connection in the house, to which their guests are allowed to connect. They have a number of devices connected to the home network. When Alice notices suspicious behaviours on any device, she calls her daughter Jane for help. Alice explains to Jane what she has noticed. If Jane identifies a problem from the details Alice provides, she guides Alice to fix it. If Alice cannot fix it, Jane arranges to visit her parents to fix the problem herself.*

*If Jane cannot diagnose the problem over the phone, she makes time to visit Alice and check the affected device. If she finds a problem, she either fixes it if she can, or seeks help from her partner or from IT support at her work place. In addition to expecting calls from Alice for help, Jane regularly calls or visits her parents to check if everything is fine on the network."*

From our scenario and analysis of the interview data, we identified two kinds of tasks that the users perform: *security tasks*, and *enabling tasks*. The security tasks are aimed at achieving specific security goals. These include diagnosing security problems in the home network (comprised of identifying vulnerabilities and performing real-time security monitoring), evaluating security risks, and fixing security problems (which consists of managing vulnerabilities and managing incidents).

Enabling tasks include seeking and giving help. They aim to support home users in performing the security tasks. The forms of help include performing health checks on devices and helping to fix problems. These tasks are completed locally, where the support provider has physical access to concerned devices, and remotely through phone calls. Where problems cannot be understood/diagnosed through on-call support, the support provider is forced to visit the concerned homes. This practice is common where security responsibility is permanently delegated to the

**Table 8.1:** Existing behaviours and technologies

| Task | Existing technology/tools | Stakeholder(s) |
|---|---|---|
| Diagnose problems | Vulnerability assessment tools<br>Network monitoring tools<br>Situational awareness tools | Alice, Jane |
| Evaluate security risks | Vulnerability management tools<br>Risk management methodologies, guidelines, standards, and frameworks | Jane |
| Fix problems | Vulnerability management tools<br>Incident management tools<br>Guidelines and recommendations | Alice, Jane |
| Seek/give help | Phone call | Alice, Jane |

support provider. On the other hand, where ad hoc support is sought, visits are usually made to the support provider.

We summarise the tasks, responsible stakeholders, and existing technologies/tools identified from the context under study and those we identified from practice that achieve the tasks in question in table 8.1.

## 8.4 Technology

To identify features that were required for the toolkit, we analysed existing technology against user tasks. In this, we considered two questions: (1) does the existing technology have security features to support the user tasks? and (2) what new features are required? The output from this was a list of security features that could satisfy the user and contextual needs: (1) vulnerability identification, assessment and management; (2) real-time network monitoring; and (3) incident management. We then analysed these features against the home threat model, and considered the following questions: (a) do the features solve the problems posed by the home threat model? and (b) do the features introduce new threats into the home network?

Our analysis showed that vulnerability identification, assessment and management can help protect against a number of threats. It can detect flaws that

can enable information disclosure, DoS, spoofing, data and device tampering, and elevation of privilege. Real-time monitoring can detect ongoing attacks including DoS, unauthorised access, and device tampering. Incident management, on the other hand, can help minimise the impact from threats including DoS and lost remote terminal. We could only identify threats introduced by the features from the perspective of how they can be implemented and used, which we discuss under procedures (cf. section 8.5).

## 8.5 Procedures

Based on existing behaviours, we expounded each task into a security procedure for achieving the security goal. We developed procedures for all the five tasks explained in section 8.3. During this process, reference was made to relevant security guidelines and standards. We also considered the user needs and how they can be fulfilled in the procedure. A sample procedure for *diagnosing network vulnerabilities* is shown below. In developing this procedure, we made reference to ISACA's Vulnerability Assessment guidelines[1].

---

*Diagnosis Activities*

1. All devices connected to the network must be identified
2. Each device must be scanned for vulnerabilities
3. A detailed report of the vulnerability status of each device should be generated
4. Authorised personnel should be alerted of the vulnerability or health status of all devices on the network
5. Authorised personnel must review the scan results and create a system baseline

[1]https://cybersecurity.isaca.org/info/cyber-aware/images/-ISACA_WP_Vulnerability_Assessment_1117.pdf

*Authorised Personnel*

The authorised personnel could be local to the home network or remote.

1. Device owner/Home administrator (e.g. *Alice*)

2. Support provider(s) trusted and assigned by the device owner

   (a) Permanent (e.g. *Jane*) or

   (b) Ad hoc (e.g. *Jane's trusted and more competent stakeholder*)

---

From this procedure, a number of issues were considered including one's ability and effort to perform each of the stated activities. The activities were grouped into two: (a) ones that can be better accomplished with the support of a tool, e.g. scanning for vulnerabilities (also recommended in the respective guideline); and (b) those that can be accomplished without tool support, e.g. reviewing scan results. Two additional features were identified that the resulting technology would need to have: (1) provision of situational awareness; and (2) support for remote diagnosis and management of the home network security.

Analysing the procedure and new features in relation to the home threat model raised two important questions: (1) how do we make sure that only authorised personnel perform these activities? — what if an attacker gets hold of the tool, and goes scanning home networks or even public networks for vulnerabilities they can exploit? and (2) What new possible threats are introduced or exacerbated by remote access? — what if an attacker hijacks the communication? A discussion around these questions led to the addition of two more security features: (1) strong authentication and authorisation; and (2) channel protection through strong encryption.

## 8.6 Home-Centered Technology

The final ideation process aimed at consolidating all the features identified, and specifying how the technology must operate in light of the procedures. We brainstormed and generated several ideas. Figure 8.1 shows part of our idea board during one of the sessions. We discussed, eliminated, and consolidated some of the ideas. Finally, we developed the following preliminary conceptual statement to guide concept testing.

Conceptual statement: *"Company Z offers an app for diagnosing problems in your network and a device to help you configure security on your home network. The app will show you all devices connected to your home network, security problems for each device, and give you advice on how you can resolve the problems. The device will enable you to easily (and without a need for technical expertise) configure security in your network, it will alert you when a problem arises in the network, and it will enable you to seek remote support or delegate security management of your home network to someone you trust. Z also offers 24/7 personalised on-call help when you need it."*

## 8.7 Evaluation: Concept Testing

In this section, we report results of concept testing aimed to evaluate the conceptual design described above. The study tested functional acceptance of the features developed with the aid of the framework. We report core results from the focus groups and the survey.

### 8.7.1 Focus Group Results

The primary goal of the focus group discussions was to test the conceptual statement for clarity and completeness. In addition, we aimed to validate problems which informed the design, but also to gather new insights that might help improve the concept (cf. section 3.2.3.5). Our results were consistent with those reported in chapters 4 and 5: security practices among our participants were more end-point focussed; and our participants managed the security of their networks individually

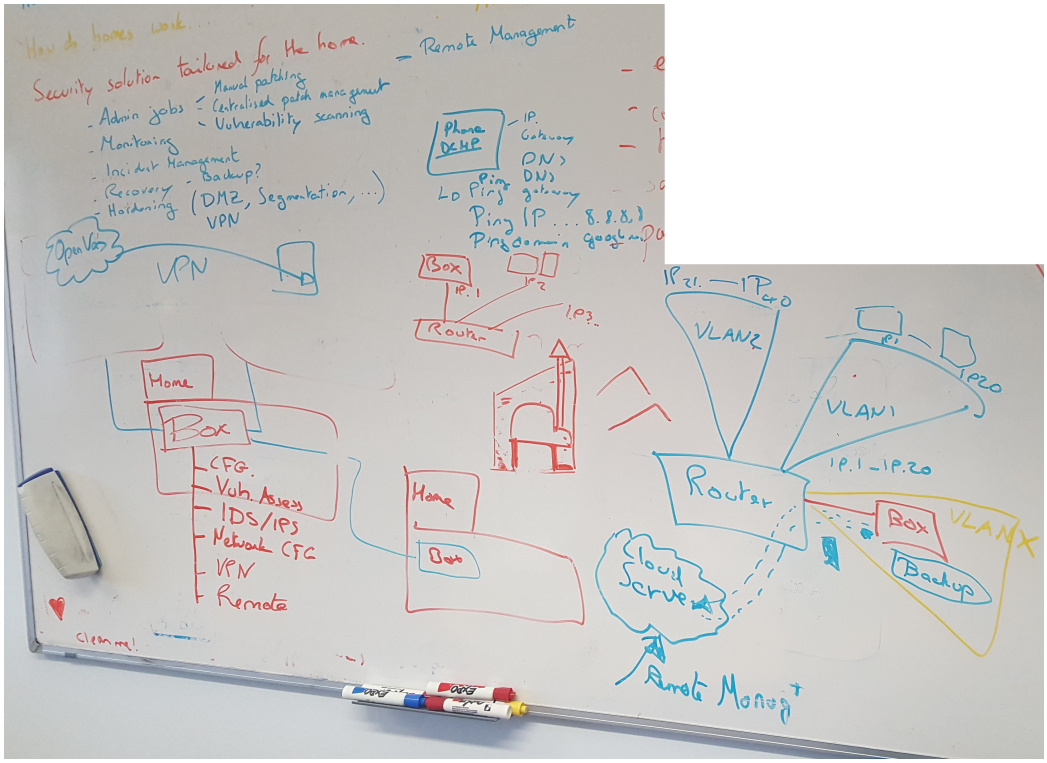


**Figure 8.1:** Designers' idea board

or through social relations, e.g. *"I understand a bit [about security], but my parents don't. I do sometimes help them with their computers"* - [P3].

One of the burning questions that was echoed from almost all the participants was, *"what am I not doing that I don't know about?"* - [P4]. This question could be silently heard from: *"I do not know if there are any problems that I should be fixing. We are told to change passwords, and I have done it. Is there anything else I should do?"* - [P7]; or *"...I have done what I know"* - [P11]. In addition, we identified supporting information that we could leverage to improve the design:

- Remembering to perform a routine security task is hard (*"I always remember when something happens"* - [P1])
- Complexity of available tools (*"I probably would appreciate some statistics about my home network... something visual. I know there are some command line tools. I have tried using them, but it's largely very uninteresting and needs more time and effort"* - [P5])

- Feeling a false sense of security (*"I haven't been hacked, but if there was already malware on my network and they are sniffing data and sending out to another server, I don't know about that"* - [P3])
- False positives (*"I tried two software for scanning for malicious websites, but they were just giving me false warnings and I uninstalled them"* - [P8])

The core output of this phase was an updated conceptual statement:

*"Imagine an app that shows you security problems in all devices connected to your home network, and gives you guidelines on how to fix them. Simply download and install the app, and click a button to see all devices on your network, and any security problems. The app comes with a small device that allows you to monitor your home network for malicious activities in real time, sending you alerts and helping you fix problems simply with a click of a button. The device also allows you to offer remote help to your friends and family, and gives you access to a 24/7 support network when you have problems."*

### 8.7.2 Survey Results

The survey aimed to test acceptance and improvement requirements of the proposed product with a wider population (cf. section 3.2.3.6). 616 participants took part in the survey. Of the 616, 5% lived in shared houses with co-residents (no social connection), 6.2% shared their houses with friends, 74% lived in family houses, and 14.8% lived alone. Figure 8.2 shows devices and services which the participants used in their homes.

**Managing Security:** We first wanted to understand our participants' involvement in digital security practices in the home. We hence wanted to know who managed security for the home networks of the participants. 87% reported to be responsible for managing their own security, while 13% indicated that they depended on others. 35.6% of the participants helped others to secure their devices and networks.

**Product Acceptance:** We presented the conceptual statement to our participants, and inquired about a number of issues related to acceptance of the proposed product. We asked the participants that assuming the product was reasonably priced, how

| Device | No. of participants | Service | No. of participants |
|---|---|---|---|
| Mobile phone | 614 | Online/Mobile banking | 568 |
| Telephone | 458 | Online shopping | 594 |
| Tablet/iPad | 481 | Social networking | 541 |
| Laptop | 541 | Communication | 450 |
| Desktop computer | 333 | Education | 217 |
| Game console | 373 | Entertainment | 488 |
| TV | 585 | Working from home | 249 |
| Camera | 408 | Remote working | 121 |
| Wearable device | 177 | Home security | 98 |
| Network router | 488 | TV streaming | 432 |
| Other | 28 | Health services | 156 |
| | | None of the above | 1 |

**Figure 8.2:** Devices and services used by participants

likely would they be to consider buying it? 63% indicated that they were likely to consider it (cf. figure 8.3). Their preference of features is shown in figure 8.4. The full names of the features, as shown on the survey tool were as follows: diagnosing security problems; guidance on fixing problems; monitoring for problems in real time; central management of all devices on the network; remote management of home networks for security support; and 24/7 access to a support network.

We asked the participants to rank the features in order of importance to them. A Friedman test on the rankings showed a statistically significant difference ($X^2(5) = 813.194$, $p < .05$). Post hoc analysis with Wilcoxon signed-rank tests was conducted on all pairs of the features, with Bonferroni correction applied. The new significance level was $p = 0.008$. There were no significant differences between guidance on fixing problems and monitoring for problems in real time ($Z = -3.415$, $p = 0.01$), and between remote management of home networks for security support and 24/7 access to a support network ($Z = -3.412$, $p = 0.01$). The overall ranking was as follows:

1. Diagnose security problems

2. Guidance on fixing problems and Monitoring for problems in real time

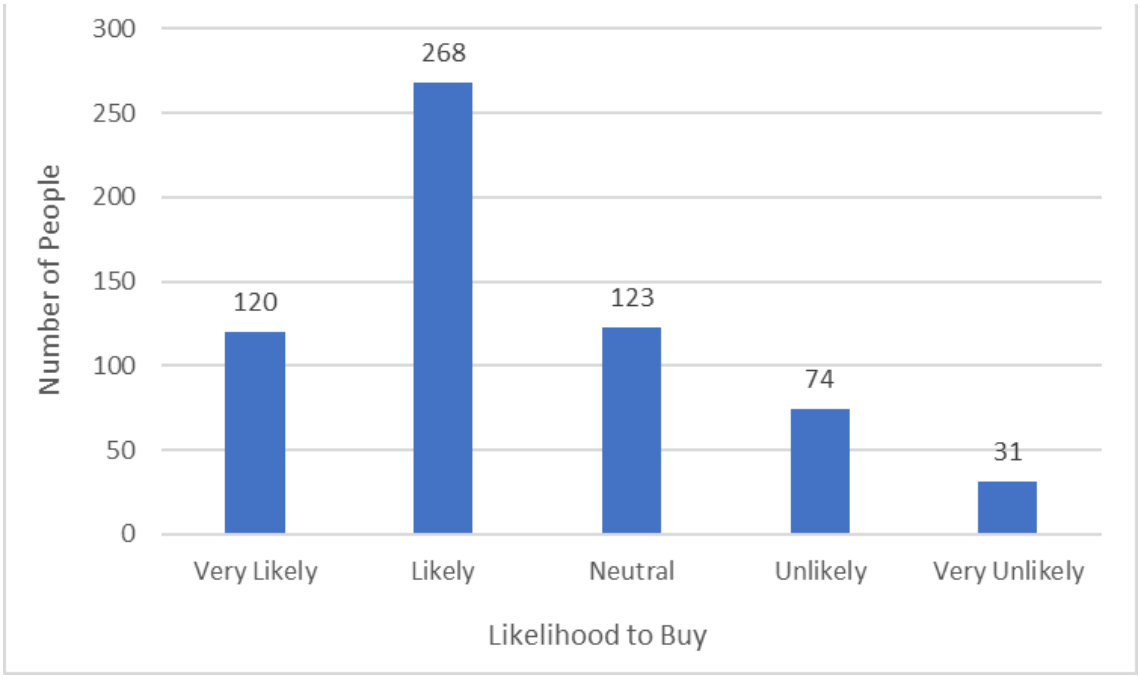


**Figure 8.3:** Likelihood to buy the product

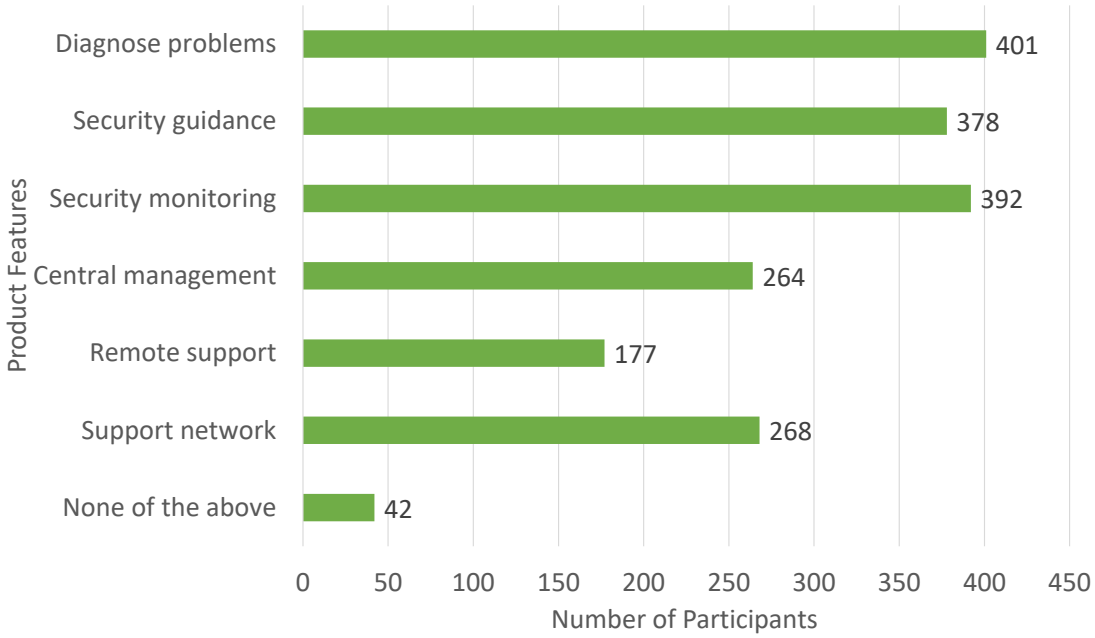


**Figure 8.4:** Preference of features by participants

4. Central management of all devices on the network

5. Remote management of home networks for security support, and 24/7 access to a support network

Another way to gauge acceptance level of the proposed product was to measure willingness of the target users to recommend the product to others and understanding who they could recommend it to. 58.6% of the survey participants showed likelihood to recommend the product to others, whereas 24.8% indicated neither likelihood nor unlikelihood to recommend (i.e. they were neutral). 72.2% indicated that they could recommend it to their family members, 68% to their friends, 36% to their work colleagues, and 7% to any other stakeholders.

**Product Rejection and Improvement:** We sought to understand from those who would not consider buying the product why they indicated so. The aim was to understand whether the reasons were due to design flaws. The information was elicited through an open-ended question. The main reasons given included:

- Privacy concerns (*"Who is receiving the data from my devices other than me? I would want to know that before considering purchase and whether my data remains mine and is encrypted end to end"* - [SP102])

- *"Already use other similar products"* - [SP397]

- *"It sounds like a good quality product but I prefer to use free security products as I am on a tight budget"* - [SP246]

- Brand recognition (*"If it had the backing of a major supplier/provider of online security for example Microsoft"* - [SP70])

- *"Don't have enough 'at risk' devices to warrant it"* - [SP281]

We also asked the participants of changes they thought would most improve the product and the following were the core things that were indicated:

- Product accessibility — not just an app, but also a desktop version, a web interface, and text messages for sending alerts.

- Ability to lock or disconnect devices from the network.
- *"Ability to link devices to the app, instead of the app linking all the devices on the same network, as I believe this can be slightly intrusive."* - [SP133]

## 8.8 System Prototype

Development of a working prototype of the security toolkit was outside the scope of the application of HANDS. However, this was done as part of Innovate UK's 2018 Cyber Security Academic Startup Accelerator Programme[2]. The prototype was developed under the banner of Security Monitoring and Administration Residential Toolkit (SMART). The author of this dissertation was the sole developer of the SMART Box and SMART cloud instance. He was one of two who developed the SMART Mobile App. In this section, we give a brief description of how the results from the design and evaluation informed a working prototype that is commercially viable.

### 8.8.1 Architectural Model

Design specifications from the conceptual design and findings from evaluation reported in section 8.7 enabled us to develop an architectural model for the proposed product (cf. figure 8.5).

### 8.8.2 Prototype Overview

The prototype aimed to demonstrate four core security features: host discovery; diagnose security problems; guidance on fixing problems; and monitoring for problems in real time. All functionalities are done centrally on the SMART box. They provide user feedback and interaction through the SMART App. We built in the capability to perform remote monitoring and get remote alerts, as an enabling functionality for support providers. The system operates as follows:

**Host discovery:** Once the SMART box is connected to a home network (through a wired connection), it first searches for the gateway on the network and obtains its

[2]https://gtr.ukri.org/projects?ref=133737

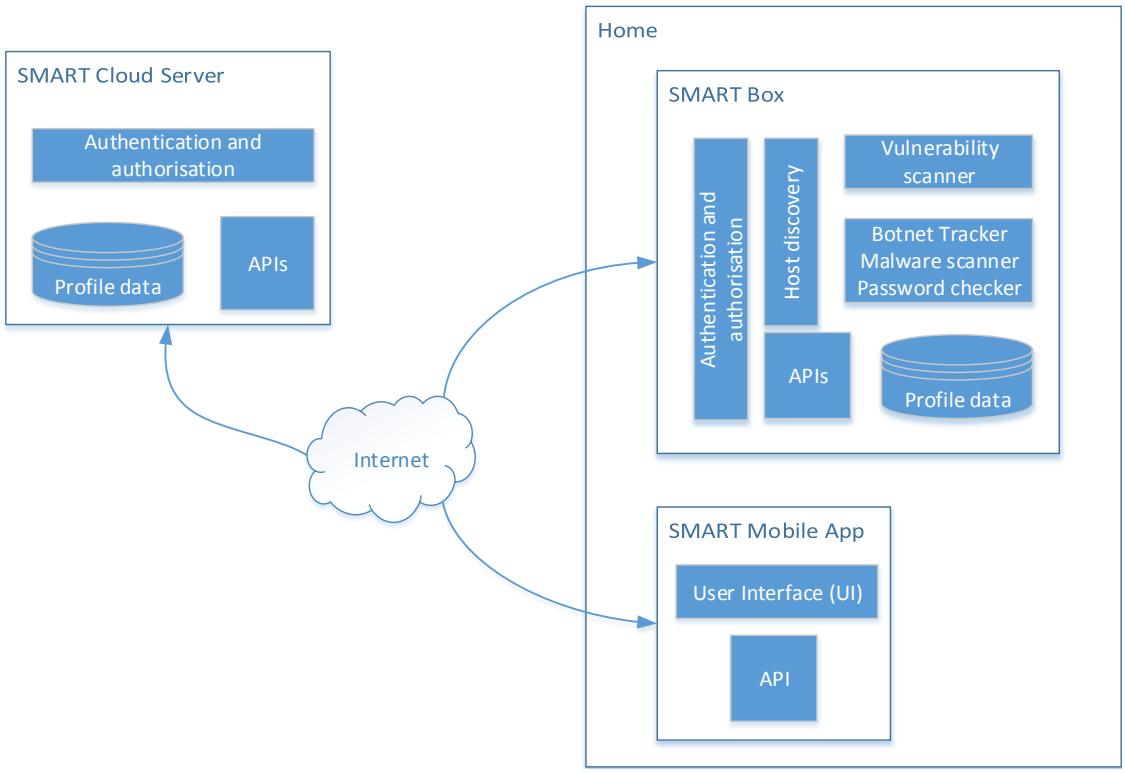


**Figure 8.5:** SMART architectural model

MAC and IP addresses. It then performs host discovery to find all active devices on the network. The box automatically creates a home profile in its local database and the SMART cloud server, using the MAC address of the gateway as its unique ID.

**Diagnose security problems:** This involves vulnerability scanning of all devices on the network using OpenVAS, an open-source pentesting tool running on the box.

**Guidence on fixing problems:** We developed automated scripts to process the output from vulnerability scanning and to log them accordingly in the home's profile. The profile includes vulnerability details, affected device, threat that can exploit the vulnerability, and *recommended action to mitigate the threat*. An alert is sent to the user's app for attention.

**Monitoring for problems in real time:** We developed three security scripts, running nmap, to automate the following real time security tasks: (1) check if any device in the home is part of a Zeus botnet; (2) perform network malware scanning on all devices on the network; and (3) check for weak network accessible passwords on all devices on the network. Real time alerts are sent to the user's app upon detection.

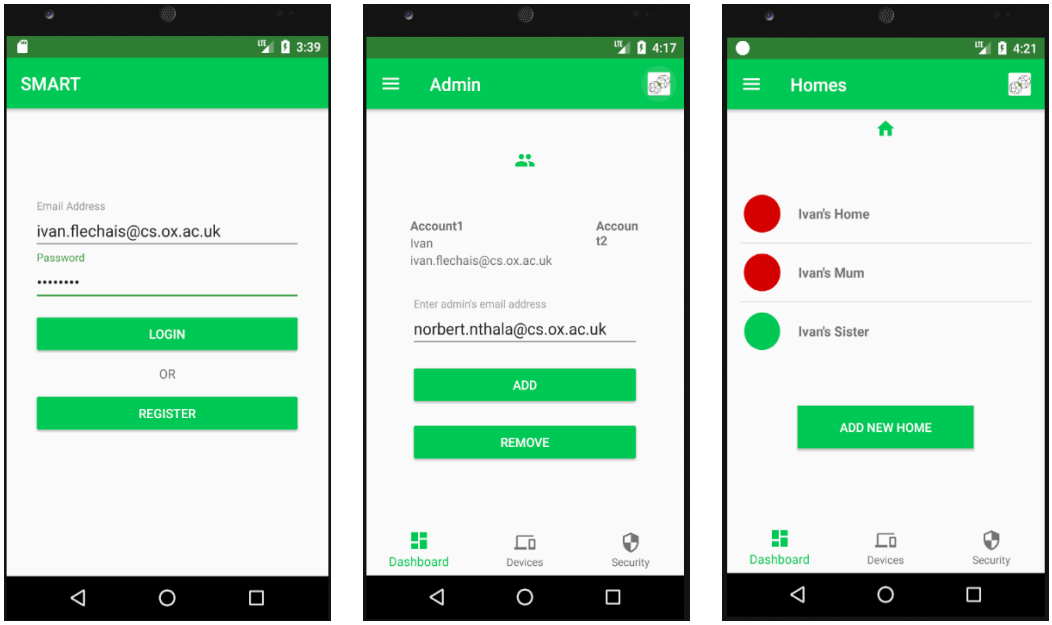


**Figure 8.6:** Login, administrator, and homes screenshots for the SMART app

**Authentication and Authorisation:** Once a user connects the box to the network and installs the SMART app, they create a user account and pair with their home using the MAC address of the home's gateway (the user becomes the primary administrator for the home with superuser rights). This user can grant and revoke administrative access to two other users.

**Remote Monitoring and Alerts:** We included a feature to allow home users to delegate security monitoring activities for their home and to seek ad hoc support, as explained above. When one is made an administrator for a home, they are able to perform scans and get alerts of detections.

**User Interface (UI):** Users can create a user account, register a home, view security status of homes they administer, and add/revoke security administration rights through the UI (see figures 8.6 and 8.7 for sample screenshots). On the list of homes, the colour green shows no security issues detected in that home, while red indicates that there is a problem requiring attention in the home.

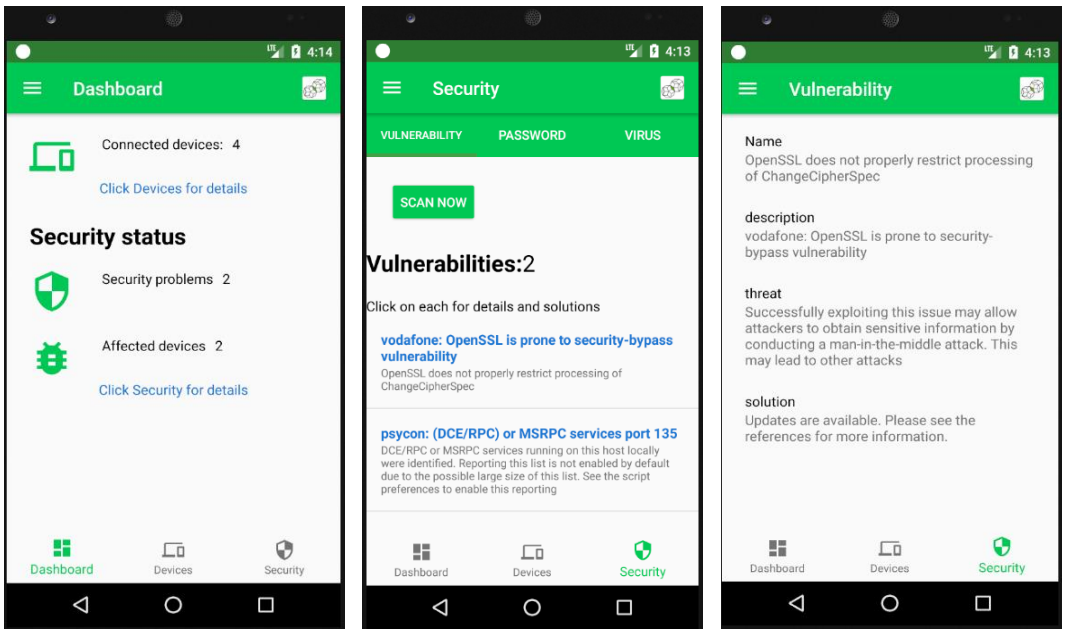


**Figure 8.7:** Dashboard and security screenshots for the SMART app

## 8.9 Discussion

### 8.9.1 Framework and Design Evaluation

Security awareness campaigns have long advocated for the adoption and usage of security tools in the home. Subsequent studies have surveyed the usage patterns of such technologies, including firewalls, data backup, firmware upgrade, software updates, patching, two factor authentication, and many more [106, 17, 79]. The evidence, however, shows otherwise. One of the reasons reported in section 6.5.1.3 is that most technologies do not conform to the nuances and needs of the home, including the required technical expertise.

In section 7.4, we recommended that security technology for the home must aim to support, enhance, and complement existing practices if success is to be achieved. The development and application of a framework to foster such practice moves us towards that goal. The evaluation reported in section 8.7 has shown that home users are willing to acquire technology to support their practices, if it meets their needs and fits into their daily life style and practices. HANDS has shown some potential to help fit technology into the home context discussed in chapter 4, focussing mainly

on getting the functional and operational details right early on during the design.

The functional and operational acceptance of the product reported in section 8.7 demonstrates the potential that the framework has. Neither the reasons for rejection nor the proposed improvements discredit the initial design. We can attribute this to the fact that the design was grounded in the practices and needs of the home, but also in security best practice.

From the case study, it can be noted that the framework does not introduce a new technique or approach for technology design; but complements existing design techniques such as personas and scenarios. HANDS was used to provide scope, structure, and clarity to relevant issues that designers had to focus on. In addition, the framework attempts to propose a way in which security best practice can ably contribute to practices in the home as shown in section 8.5.

From our experience applying the framework, we noticed two issues. First, just as adoption and usage of security tools in the home requires a set of skills, there is even more to the design of such tools. The design called for a range of skills including information security, user experience, and design thinking. Second, it is significant to understand different characteristics of the home and to consider them during the design. These include household composition and its influence on security behaviours, and the impact of security technologies on life style in the home. We could identify a handful of the characteristics from our analysis, and the time spent to understand them was significant.

### 8.9.2 Prototype Evaluation

As explained in section 8.8.2, selection of features for the prototype was based on the results of design evaluation presented in section 8.7. During development of the SMART mobile app, we engaged home users in designing the user interface by using wireframes[3]. Four home users were asked to individually draw how they wanted the interface of the app to look like. Then, all four diagrams were put together and we asked the participants to evaluate and discuss the designs. Finally,

[3] https://www.justinmind.com/blog/why-wireframing-your-interface/

we asked them to consolidate their feedback and work as a group to produce a final design of the interface.

During preliminary testing of SMART, we noticed that our participants (who were different from those involved in interface design) were able to easily: (1) navigate the interface, (2) understand the menu, and (3) understand *some* of the messages (or output) after running security scans. For instance, the participants could easily interpret messages regarding detection of a weak password on any of the connected devices on the network. The messages simply read: *"No weak passwords found"* or *"Device <devicename> has a weak password for <username>. Threat: device can be accessed by an attacker on the network or remotely. Solution: change password"*. Similarly, messages regarding malware and botnet detection were easy to understand as they indicated: *which device was infected*; *a threat stating that an attacker could gain access to the device, network and data*; and *a solution to disconnect the device from the network and scan it with anti-malware*. Modules running the password checker, botnet tracker, and malware scanner were developed to run NMAP[4]. The messages displayed to the user (upon execution of these modules) were our own custom texts designed based on the fixed set of possible outcomes from these modules.

The vulnerability assessment module was running OpenVAS[5], one of the most widely and highly rated vulnerability assessment and management tools. All messages displayed to the user from this module were raw messages presented by OpenVAS. We could not customise the messages due to the dynamic nature and size of OpenVAS databases from which the messages were served. Some of these messages, however, were not easy to understand for less competent home users (e.g. see figure 8.7). For other messages, e.g. those indicating that an update was available for software on one of the connected devices, the users could understand. This challenge underpins the need to develop security tools (e.g. alternative vulnerability assessment tools to OpenVAS) that are specifically targeted

[4]`https://nmap.org/`
[5]`http://www.openvas.org/`

for the home and communicate results using simple language (messages), but without losing their original meaning.

A second challenge we observed with some of our participants was related to their inability to carry out the recommended tasks/solutions, even when they understood the message. For instance, one participant did not know how to change a weak administrative password of a router. We can argue that the provision of security tools alone cannot change the security competence of home users. More needs to be done to improve competence in the home, as discussed in section 7.3.

As reported in section 4.7, *security administration involves tasks that require varying levels of skills.* Chapter 5 revealed that home users solve this challenge by delegating security tasks to or seeking help from competent individuals. There will almost always be a need for someone to fix even the most complex and highly technical security problems in the home (e.g. the one shown in figure 8.7). We considered filtering messages from OpenVAS to display only the less technical ones to the home user. However, we realised that this could not resolve the security problems in the home. It could actually lead to a false sense of security (survival bias — see sections 6.4.5 and 7.2).

Despite its shortfalls, SMART presents two opportunities. First, one of the objectives for developing the tool (see sections 8.3 and 8.5) was to allow less competent users to delegate security assessment and monitoring to and seek ad hoc support from more competent stakeholders. A user of the SMART app can add another registered user to run security assessments and receive security alerts — see figure 8.6. This is in line with current practice in the home (see sections 4.7 and 5.2), but also with the recommendation in section 7.3 to *leverage, provide additional resources to* and build competence in the existing informal support networks to target the gaps we have seen in section 4.5.1.

Second, our findings showed that home users are motivated to act when they are alerted or warned of the existence of a security problem (see section 6.3.4). We believe that the alerts from SMART can stimulate users to act or seek help. A potential problem exists here. Frequent alerts can make users to become accustomed

to the alerts and stop acting on them (similar to security warnings [121]), or can overwhelm users with the messages and they can stop using the tool (see section 7.4). Use of the alerts, therefore, needs careful planning and implementation.

## 8.10 Conclusion

In this chapter, we demonstrated the application of HANDS to the design of a network security toolkit. We presented findings from an evaluation study of the design, briefly described a working prototype that was developed from the design, and lastly discussed the case study.

# 9 Conclusions

The technical infrastructure in the home is becoming increasingly complex, partly due to advent of the Internet of Things. Many homes are becoming digital and connected. At the same time, security attacks targeting the home are on the rise. Attackers aim to compromise insecure devices in connected homes to mount attacks on the critical infrastructure, to benefit from valuable data available in the home, or to harm home users.

The proposed solution for securing the home has been increased security awareness [39]. Evidence [21, 135] and recent events [27, 65, 132], have shown limited success of awareness campaigns in improving home security. In response to this, the research community has sought to explore new ways of addressing the problem. A range of endpoint and network security approaches, e.g. [61, 180, 53, 69], have been proposed, built on interdisciplinary theories. Whilst this is a useful step, some of the approaches have already been criticised for a number of shortfalls, including privacy violation, cost, and lack of scalability. The proposed approaches have varying motivations, but common is *lack of expertise of the home user* in managing security for the home.

In order to devise more appropriate and effective security solutions, we believe that secure (and security) systems in the home need to be designed from an empirical and grounded understanding of home users, the context of use in which

they operate, and how they make data security decisions. The research reported in this dissertation took a step in that direction.

The research question addressed in this dissertation was: **'How can home data security practices be well *understood* and supported to help security entities design appropriate home user security approaches, and home users to make appropriate data security decisions?'** The question was broken down into the following four subquestions:

1. Which concepts are important in understanding security practices in the home?

2. What kind of security support behaviours exist in the home?

    - What are the characteristics of security support in the home?
    - Where do home users get security support?

3. What influences security decision-making in the home?

4. How can appropriate and effective home data security practices be supported?

We summarise the key findings in the next section.

## 9.1 Key Findings

### 9.1.1 Evaluating Quality of Security

Chapter 6 showed two challenges that home users face pertaining to quality of security: (1) assessing the quality of security work; and (2) evaluating quality of sources of support.

First, our findings revealed that home users rely on *absence of harm* as evidence of good security. Chapter 7 highlighted that the absence of harm is not always reflective of good security. For instance: (a) harm might occur but not be noticed by a home user; or (b) harm might not occur because no attempt was made. Only where an attack was attempted and successfully mitigated is the absence of harm evident of good security.

Second, chapter 6 revealed that the quality of a source of security support is dependent on perceived competence, trust, availability, cost (time, effort, financial), and closeness. Perceived competence is assessed based on the following factors: one works in data security; one studied or studies data security; he/she has more experience in using or working with technical devices and services; his/her job is technical; he/she works for a technical company; he/she studied or studies a technical course; he/she has experienced a data security incident before; and he/she is more educated.

Home users need to be able to evaluate the quality of a security decision or source of support. In the absence of clear indicators of quality, a variety of different practices have emerged, yet their effectiveness is questionable. A key challenge remains to uncover the means of making quality more evident to non-experts both for security products/practices, and for the skills, knowledge, and characteristics of those who offer support.

### 9.1.2 Security Responsibility

Often, the home user is presumed to be the security administrator in the home. The average computer user has to worry about chores that historically have been the concern of system/security administrators. The user has to perform system updates, firmware upgrades, data backup, network monitoring, and incident management among others. These are chores that are overwhelmingly complex to most and understood by few.

Contrary to this belief, chapters 4 and 5 revealed that the home user is not always the security administrator in the home. Security is largely managed through a variety of social relationships. Many home users seek ad hoc support from or even completely delegate security administration to friends, family members, colleagues, or computer professionals. Security support behaviours in the home are characterised by duty of care (delegation, motivation, or social responsibility), and continuity of care.

In addition, chapter 4 revealed a fractured structure of responsibility in home security. The degree of ownership and responsibility for security for each device and

service available to the home varies between manufacturer, service provider, home user, and even more. The lack of a clear definition of responsibility boundaries creates ambiguity and leads to diffusion of responsibility, especially for the home user.

### 9.1.3 Security Technology

Chapter 4 showed that current security efforts in the home are focussed on securing the endpoint, despite proliferation of attacks targeting insecure devices in home networks. Even so, evidence [17, 79] has shown poor adoption and usage rates of security technology in the home. Chapter 6 reported a number of contextual and user experience factors that affect adoption and usage of security technology in the home: convenience, significance, ease of use of technology, and complexity of security task. Chapter 7 pointed out that part of the problem is that available security technology does not fit the context of use in the home. Most designers of security technology design for the enterprise environment, not the home.

Chapter 7 proposed a data-driven descriptive framework (HANDS) for designing appropriate technology for the home. HANDS was applied to the design of a network security toolkit for the home in chapter 8. Evaluation of the design showed significant acceptance of the proposed product. The results showed that home users are willing to acquire technology to support their practices, if it meets their needs and fits into their daily life style and practices.

## 9.2 Evaluation

In this section, we discuss how the contributions from this thesis answer the four sub-questions which guided the research reported in this dissertation. We also evaluate the validity of the research reported in this dissertation.

### 9.2.1 Which concepts are important in understanding security practices in the home?

The aim of this question was to scope the security context in the home and position the related work appropriately. Based on the literature review in chapter 2 and a scoping study, important concepts (themes) were identified which, collectively,

helped to define the security context and related practices in the home. A context model was developed and presented in chapter 4. We demonstrated its applicability and usefulness by using it to situate and organise previous studies in home security, making evident a research gap which led to the work reported in chapters 5 and 6.

Although the model was high level, it provided structure to the interpretation of findings, but also contributed to the development of HANDS in chapter 7. The model also provided motivation to the case study in chapter 8.

### 9.2.2 What kind of security support behaviours exist in the home?

Based on Grounded Theory analysis of interviews, three kinds of security support behaviours were identified: (1) technical help; (2) advice; and (3) information provision. Identification of these was aimed at situating all security support issues within the boundaries of support practices. Furthermore, the question sought to explore sources and characteristics of security support in the home. From the analysis, two characteristics of security support were identified: (a) duty of care; and (b) continuity of care. An understanding of the characteristics was useful in categorising support activities (such offering unsolicited support, accepting unsolicited support, etc.), which was instrumental in exploring preference and sources of support.

As reported in chapter 5, this theory of security support in the home was validated through a large scale survey of home users. In addition, the case study in chapter 8 applied this understanding to the design of a new security technology which was subsequently validated in an empirical study.

### 9.2.3 What influences security decision-making in the home?

It was noted in chapter 2 that a significant amount of work was covered by other researchers. Much of the work focussed on understading factors that affect decisions related to security work. Some researchers used existing predictive theories, including PMT and TPB, to explore security behaviours in the home. Antecedents from

these theories are studied as factors. Howe et al. [103] argued for the importance of understanding factors that matter to people, if security were to be improved in the home. While some of the factors reported in chapter 6 were similar to findings from related work, the results in this dissertation add a new perspective of understanding to the related work, including the model of factors that influence security decision-making in the home.

Core to the results were factors which influence security support decisions (cf. section 6.6). These complement the work in chapter 5. The factors reported in chapter 6 were useful in the development of the framework in chapter 7 and in the case study in chapter 8.

### 9.2.4 How can appropriate and effective home data security practices be supported?

This question's focus was on finding ways of helping home users know what to do, when to do it, how to do it, and how to do it well. Chapter 7 interpreted the findings from chapters 4, 5 and 6, and synthesised the results with related work to put forward three recommendations for improving security practices in the home in chapter 7.

First, we proposed to leverage the existing informal security support infrastructure. We discussed how this could be achieved, but also outlined potential challenges.

Second, based on results of current security practices in the home in chapter 4, we discussed how prioritising security efforts and developing appropirate technology would benefit the home. We further proposed a framework to help designers ground their design decisions in relevant contextual information.

Third, we discussed the need to develop metrics to make the quality of security more evident to non-experts.

The three reccommendations were collectively demonstrated in the case study in chapter 8. The author of this dissertation was the primary designer and researcher in the case study. He was also the sole developer of the SMART Box and SMART cloud instance. He was one of two who developed the SMART Mobile App. The

success of the case study showed the value held by these recommendations, and is indicative of success of the research reported in this dissertation.

### 9.2.5 Validity of Research

We ensured validity of the research reported in this dissertation in three different ways as discussed by Carter et al. [43]: method triangulation, data source triangulation, and investigator triangulation.

First, we used *different research methods*. This was achieved in two ways. (1) To understand the home security context and practices to answer research questions RQ1, RQ2, and RQ3 (see section 1.2), we used qualitative methods (semi-structured interviews, Thematic Analysis, and Grounded Theory) followed by a survey which validated the qualitative findings (see sections 3.2.1.1, 3.2.1.2 and 3.2.1.3 for details). (2) To investigate how security practices in the home can be supported to answer research question RQ4 (see section 1.2), we also used qualitative methods (Conceptual Framework Analysis, Design, Focus Groups, and Thematic Analysis) followed by a quantitative method (survey) to validate qualitative results (see section 3.2.1.4 for details).

Second, we *triangulated data sources*. To understand the home security context and practices, we collected data from literature, home users and ISPs (see sections 3.2.1.1, 3.2.1.2 and 3.2.1.3 for details). To investigate how security practices in the home can be supported, we collected data from literature, software engineering researchers, security experts, and home users (see section 3.2.1.4 for details).

Third, we ensured *investigator triangulation* as explained in section 3.3.1. Two investigators were involved in the Thematic Analysis and Conceptual Framework Analysis studies. Three investigators were involved in the Grounded Theory study.

## 9.3 Research Question Evaluation

The evaluation of research sub-questions in sections 9.2.1, 9.2.2, 9.2.3, and 9.2.4 show that the research question which was posed in section 1.2 — **How can home data security practices be well understood and supported to help**

**security entities design appropriate home user security approaches, and home users to make appropriate data security decisions?** — has been answered. Chapter 4 introduced a security context model for understanding security practices in the home. The model was then used to explore security practices in the home in chapters 5 and 6. Chapter 7 interpreted the findings in chapters 4, 5 and 6, and proposed a data-driven framework (HANDS) to help designers of security technology for the home to ground their design decisions in relevant information. Chapter 8 illustrated an application of HANDS in a case study and its success through evaluation.

As discussed in section 9.2, the contributions also answered the research sub-questions. RQ1 was answered by presenting the home security context model in chapter 4. RQ2 was answered by reporting the kinds, sources, source preferences, and characteristics of security support in chapter 5. RQ3 was answered by presenting the model of factors that influence the outcome of security decisions in the home in chapter 6. RQ4 was answered by: (1) recommending to leverage existing informal support networks of security in the home; (2) proposing HANDS in chapter 7; and (3) demonstrating applicability of HANDS, and evaluation of the design in chapter 8.

## 9.4 Research Limitations

Despite the successes reported above, this thesis has limitations. First, all participants were residents of the UK. This might raise questions regarding generalisability of our results. However, we have documented the procedure we followed in this research, which makes it possible for other researchers to replicate it elsewhere.

Second, common to all qualitative studies, researcher bias is a concern. A single researcher (the author of the dissertation), trained to conduct research interviews, conducted all the 65 interviews. The researcher avoided leading questions, and ensured participants felt comfortable to respond to questions. The researcher avoided interrupting participants and probed for more information when required. To further mitigate bias, two/one other researcher(s) reviewed and were part of the

data analysis to enhance consistency in data coding (see chapter 3 for details). Our research design explicitly aimed to mitigate potential bias by also running extensive surveys to test how generalisable the qualitative findings were.

Third, given that security is a sensitive topic, social desirability could bias some of the responses to the survey described in section 3.2.3.4, specifically for the two scenarios developed to study survival/outcome bias and confidence in a security measure. To mitigate this, we took three measures. (1) We did not reveal at the onset that the main purpose of the survey was to study security practices of the participants. Instead, we stated that the aim was to understand decision-making in the daily use of technology. (2) We employed a self-administered questionnaire [143], hence there was no interviewer and a high degree of anonymity. (3) We used indirect (structured, projective) questioning [72] in those two scenarios, where respondents answered from the perspective of another person.

Fourth, our data consisted of only what people said. This made it hard to understand how our results translated into actual behaviour in the home. Future work would aim to employ relevant approaches to study these behaviours in context, and also to evaluate the SMART prototype.

Fifth, most of the work reported in the case study in chapter 8 was conducted in an academic environment. Of particular interest was the evaluation and applicability of the framework. The evaluation did not include a representative sample of professional designers, who are the target population for this work.

Last, the work in chapter 8 only tested the conceptual design. The adoption and usage of the actual product could be affected by a number of developmental factors, such as usability [15]. However, we believe that the overhead of fixing some usability attributes is less compared to resolving functional and operational failures post development. In addition, as can be noted from the case study, some usability attributes were tackled early on. During the development of the SMART prototype, we engaged target users in the design of the user interface by using wireframes.

## 9.5 Directions for Future Work

The study has pointed to a number issues worth further exploration. In this section, we describe three potential areas that could build on the contributions presented in this dissertation.

### 9.5.1 Evaluating the Quality of Security

Chapter 6 revealed a number of challenges which home users face in evaluating the quality of their security decisions and their sources of support. The study has revealed and discussed factors that people in the home use to conduct such evaluations. This could be a good starting point for work focussed on developing and evaluating indicators of quality of security in the home. As discussed in section 7.2, it is important to identify and find ways of dealing with challenges that would emerge from the use of such indicators, but also to identify and leverage opportunities that such an intervention could present. Unlike indicators targetting administrators in organisational settings (e.g. [203, 40]), most home users are not security professionals. Such work would focus on non-experts.

### 9.5.2 Harmonising Technical Solutions for the Home

In section 7.5.1, we highlighted the importance of harmonising technical solutions for the home. Our study and Dourish et al. [62] emphasise the call for centralised management of security in the home. In addition, Koppel et al. [118] make two important recommendations for improving security in the home: (1) end users must be able to implement security and privacy settings for the collective population of devices in the smart home; and (2) information should be provided to end users to help them reason about collective (network) security. From our experience developing SMART, we noted that this is hard to achieve given the heterogeneity of devices made available to homes. Most devices required custom APIs to be able to retrieve network and status information. For some devices, this was completely not possible. Future work could focus on finding ways of harmonising technical solutions for the home. One possibility is to explore the development and use of open standards.

### 9.5.3 Information Healthcare

Information security for home users is a problem that has a number of analogies to healthcare. First, attack vectors have been compared to biological threats before (e.g. in the naming of the computer virus). Second, a number of attacks exist that are perpetrated by exploiting the insecurity of a small proportion of the home user population (e.g. home devices being compromised in order to DDoS online services). Third, securing this small proportion of users benefits others too: by securing this population, the benefits apply to all by reducing the number of possible attacks — much in the same way vaccinations help through herd immunity.

While security in the home tends to be treated as an awareness and compliance issue, the health sector is holistic, focussing on the wider functioning unit to promote well-being and not merely the absence of disease, e.g. the first article of the World Health Organization's constitution: *Health is a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity.* Our study revealed how different factors (e.g. security responsibility, risk, and economic factors) are relevant to the problem of home data security, and we argue that, instead of focussing on minimising threats and harm, we need to view all these factors from the perspective of making security an enabler in the home.

In healthcare, *primary care* relates to the work of health professionals who act as a first point of contact. For more specific needs, *secondary* and *tertiary care* refer to services that provide advanced care. *Public health* focuses on threats to populations, and its methods aim to detect, prevent and treat threats on a much broader basis. There are clear distinctions between public health and patient-focussed approaches, but the key is that they operate in concert with one another.

To conclude, in the light of the discussion above, we propose the need to explore a combination of "public health" and "patient-focussed" approaches that complement one another to protect home data. We also need to explore the concepts of primary and secondary *data care* services for homes, continuity of care (to foster trust), and investigate participation opportunities from families and communities. The work of Rowe et al. [180], which proposes a *population-centred*

*approach* in dealing with cybersecurity issues, falls within this proposal and could provide a good starting point.

# Appendices

# A
# Study Details

## A.1 Interview Demographic Form

1. *Age*: a) 12 - 17, b) 18 - 34, c) 35 - 64, d) 65+

2. *Gender:* a) Male, b) Female

3. *Location:* a) Rural, b) Suburban, c) Urban

4. *What is the highest level of school you have completed?*

a) No schooling completed, b) Nursery, c) High School, d) Trade/technical/vocational training, e) Undergraduate, f) Graduate, g) Postgraduate

5. *Choose one option that best describes your ethnic group or background:*

a) White, b) Hispanic/Latino, c) Black/African/Caribbean, d) Asian/Pacific Islander, e)Other:

6. *Choose the technology devices you own/use in your home:*

a) Mobile Phone, b) Telephone, c) Tablet/iPad, d) Laptop, e) PC, f) Game Console, g)TV, h) Camera, i) Wearable device, j) Other:

7. *Choose the services you use:*

a) Online/Mobile banking, b) Online shopping, c) Social networking, d) Communication, e) Education, f) Entertainment, g) Work, h) Home security, i) TV streaming, j) Health services, k) Other:

8. *How would you rate your general skills in using technology devices, services, and applications?*

a) Novice, b) Competent, c) Expert

9. *How would you rate your general skills in computer security and privacy (e.g. understanding threats, vulnerabilities, and countermeasures)?*

a) Novice, b) Competent, c) Expert

10. *Would you briefly describe the composition of your household?*

*A. Marital status:* a) Single, b) Married, c) Widowed, d) Divorced, e) Separated

*B. Number of people in your household:*

*C. Relationship with other residents:*

*D. Age ranges of other residents:*

E. Employment status: a) Student, b) Employed, c) Retired, d) Self-employed, e) Not working

## A.2 DS3 Interview Guide

### A.2.1 Introductory questions

1. Can you rank these services in order of importance, from the most important to the least important?

### A.2.2 Data Security Concerns and Breaches

2. Do you have any data security concerns with these devices/services/applications?

3. Have you or people you know experienced any data security breaches in the past?

### A.2.3 Security Controls/Tasks

4. What was done to address the data security concerns, and breaches? Who did this?

5. Do you think this was enough to keep your data secure? If not, why?

6. Did you face any problems with the solution?

7. Have you ever adopted or avoided a device/service/application for data security

| | | | |
|---|---|---|---|
| Open problems in security decision making | Data security concerns | Factors influencing security decisions | Home responsibility |
| Evaluating the effectiveness or quality of security solution | Loss | Convenience | Source of Support |
| Unable to have a relevant solution | Loss of control | Cost | Relative |
| Good Security Practices | Loss of money | Ease of use | Friend |
| Guidelines and rules for security decision making | Loss of Privacy | Experience | Service provider |
| Ask the more knowledgeable | Nuisance | Experience in using a security measure | IT shop |
| Disconnect from the internet when not needed | Uncertainty | Experienced a security breach | Work colleague |
| Follow advice from a service provider | Security practice | Professional experience | Online forum |
| Use a tier system of passwords | Insecure practices | Knowledge and skill | Search engine |
| Don't give out personal details to someone you don't know | Secure Practices | Professional - education | Technical help |
| Responsibility | Non-security-technology practices | Professional job-related experience | Awareness |
| Attitude - Giving advice and post breach reaction | Pre-emptive practices | Obligation | Identifying risks |
| Attitude - Problems arising from well-intended individuals | Pro-active Damage Limitation | Survival/Outcome bias | News |
| Attitude - Responsible stakeholders | Reactive practices | Perceived Competence | Devices |
| Boundaries of responsibility | Security-technology practices | experience in using or working with technical devices and services | Services |
| Understanding responsibility | Reactive - Incident Management | Level of education | Anecdotes |
| Abrogate responsibility | Noticing a breach | Personal negative experience | Incident reporting behaviour |
| Noticing responsibility | Risk attitude | Studied or studies a technical course | Security evaluation |
| Taking responsibility | It's not a risk | Studied or studies data security | Cost of protection |
| Stakeholders | Not understanding the risk | Technicality of a job | Where to get support |
| Support | Risk evaluation | Works for a technical company | Reviews |
| Characteristics of Support | Perceived value of impact | Works in data security | Available security tools or measures to a problem |
| Continuity of Care | Perceived gain for attacker | Significance | Unsolicited support |
| Duty of Care | Security incidents experienced | Time pressure (Urgency) | Solicited support |
| Delegation | Identifying incidents | Trust | Trust evaluating practices |
| Motivation | Harm | Sharing devices, services and passwords | Relationship with others |
| Social Responsibility | Security alert | Extent of sharing | Knowledge and skill level |
| Types of support | Security warning | Purpose of sharing | Closeness to source |
| Advice | Intuition | Trust cues | Visual cues |
| Types of advice | Support giving | Availability heuristic | Kinds of information |
| Opinion | Support seeking | Brand recognition | Confidence in security measure |
| Recommendation | Availability of support | Interaction | Reviews about a security tool |
| Information | Quality of support | | |

**Table A.1:** Grounded Theory Codebook

reasons? What prompted you to do this?

8. Have you ever changed settings or abandoned/uninstalled a device/service/application for data security reasons? What prompted you to do this?

9. Is there a particular time when you had data security concerns with a device/service/application but you chose to continue using the device/service/application? Why did you do so?

10. Who is generally responsible for making data security decisions in your home? Why?

11. In the particular scenarios you have mentioned, who made these data security

decisions? Why? Were there any difficulties in deciding what to do?

12. If you were to make these decisions for your friend, what would you do? Why?

### A.2.4 Capability and Support

13. Are there any guidelines or rules you follow when making data security decisions? Where do these come from? In the scenarios you mentioned, did you follow these? If not, why?

14. What kind of information/resources do you need when you want to make a data security decision?

15. Where or from who do you seek such information/resources?

16. If you needed advice or technical assistance with data security, where would you seek it?

### A.2.5 Delegation

17. Have you ever given advice/recommendation about data security to other people? Who were they? What kind of advice/recommendation did they want? How much effort did you put in (what did you do)?

18. Why do you think they chose to seek advice/recommendation from you? Why did you give advice/recommendation?

19. Have you made data security decisions and acted on them on behalf of someone? For who was this done? What kind of decisions were these? Why did you do it?

20. If you have given bad advice/recommendation or wrongly decided and acted on behalf of someone and something happened, what would you do? Has this ever happened to you?

### A.2.6 Attitude towards data security

21. Can you give me examples of what you consider good and bad data security (measures/practices)?

22. Who do you think is responsible for implementing this kind of data security in the different devices/services/applications you use?

23. Do you personally follow these measures? If not, why?

24. Do you think any of your actions in using the devices/services/applications could expose other people to data security risks? What are some of these actions and how do you think they might affect others? What do you do about it?

## A.3 DS4 Survey Tool

### A.3.1 Demographics

1. Please select your age range: a) 18 - 34, b) 35 - 64, c) 65+

2. Please select your gender: a) Male, b) Female

3. What is the highest educational level you have completed?

a) No schooling completed, b) High school,

c) Trade/technical/vocational training, d) Undergraduate, e) Graduate, f) Postgraduate

### A.3.2 Survial/Outcome Bias

For the past 5 years, your friend John has been downloading free music, videos, and software from different websites including torrent sites without any problem. One day, he reads an article about the dangers of free downloads such as viruses, adware, Trojan horses, worms and spyware. For each of the following options, how much do you agree that it is a good choice for John?

*(Responses: I strongly agree, I agree, Neutral, I disagree, I strongly disagree)*

A. Continue downloading free files from any website as usual. He has been doing it for 5 years without a problem, chances of being affected are very small.

B. Restrict the downloads to those websites John has already used before. He has used them for 5 years without a problem, he trusts them to be secure.

How would you rank the options from the scenario above in order of preference?

### A.3.3 Assessing Other's Security Competence

How do you assess if someone is more competent than you in data security? (Please select all that apply.)

A. He/she works for a technical company.

B. His/her job is technical.

C. He/she has more experience than you in using or working with technical devices and services.

D. He/she studied or studies a technical course.

E. He/she is more educated than you.

F. He/she works in data security.

G. He/she studied or studies data security.

H. He/she has experienced a data security incident before.

I. None of the above.

How would you rank the options selected in the question above in order of preference?

### A.3.4 Seeking Support

Assuming you believe each of the following to be more competent than you in data security, how likely are you to seek advice or help with data security from him/her? *(Responses: Very Likely, Likely, Neutral, Unlikely, Very Unlikely)*

A. Relative

B. Friend

C. Work colleague

D. Service provider/Manufacturer help desk

E. IT repair shop professional

F. Others

How would you rank the options in the question above in order of preference?

### A.3.5 Accepting Unsolicited Support

Assuming you believe each of the following to be more competent than you in data security, how likely are you to accept unsolicited (not asked for) advice or help with data security from him/her?

*(Responses: Very Likely, Likely, Neutral, Unlikely, Very Unlikely)*

A. Relative

B. Friend

C. Work colleague

D. Service provider/Manufacturer help desk

E. IT repair shop professional

F. Others

How would you rank the options in the question above in order of preference?

### A.3.6 Giving Solicited Support

Assuming you believe each of the following to be less competent than you in data security, if they ask you for advice or help with data security, how likely are you to offer it?

*(Responses: Very Likely, Likely, Neutral, Unlikely, Very Unlikely)*

A. Relative B. Friend

C. Work colleague D. Others

### A.3.7 Quality Check

I am randomly answering the questions.

A. Yes B. No

### A.3.8 Giving Unsolicited Support

Assuming you believe each of the following to be less competent than you in data security, how likely are you to offer unsolicited (not asked for) advice or help with data security to him/her?

*(Responses: Very Likely, Likely, Neutral, Unlikely, Very Unlikely)*

A. Relative B. Friend

C. Work colleague D. Others

How would you rank the options in the question above in order of preference?

### A.3.9 Assessing the Quality and Source of Support

Which of the following do you take into consideration when seeking data security advice or help from someone? (Please select all that apply)

A. Competence

B. Availability

C. Trust

D. Closeness to you

E. Cost to you (money, favours, gifts, etc)

F. Cost to the source of advice/help (effort, inconvenience, etc)

G. None of the above

How would you rank the options in the question above in order of preference?

### A.3.10 Confidence in a Security Measure

Your friend Felicity is a college student. She owns a laptop. She stores assignments and study materials on it. Felicity visits her friend, Laurel, whom she finds watching a very interesting movie. Felicity asks Laurel if she can share the movie with her, as well as some of the music Laurel downloaded. Laurel copies all the files to a USB stick, and hands it over to Felicity. On their way out, Laurel tells Felicity that she thinks her laptop might have a virus because she could not open one of her word documents to study, and this has happened to her a number of times. For each of the following options, how much do you agree that it is a good choice for Felicity?

*(Responses: I strongly agree, I agree, Neutral, I disagree, I strongly disagree)*

A. Felicity could copy the movie and music to her laptop. Laurel probably got a corrupted file, there is nothing to fear.

B. Felicity could copy the files to her laptop. She has an antivirus which will keep her data secure.

C. Felicity could take and maintain a backup of her files in a USB stick, phone storage, cloud storage, external hard drive, another computer, etc. She could hence

copy the movie and music to her laptop. She can always get the files from the backup when needed.

How would you rank the options in the question above in order of preference?

### A.3.11 Duty of Care

Assume you have a sister named Vanessa, and you believe her to be less competent than you in data security. One day you visit her, and while you use her laptop, you notice that her antivirus is not set to automatically scan removable media, such as USB sticks, when they are plugged in. For each of the following options, how much do you agree that it is a good choice?
*(Responses: I strongly agree, I agree, Neutral, I disagree, I strongly disagree)*
A. Change the settings of the antivirus to enable auto-scan of removable media, and say nothing.
B. Change the settings of the antivirus to enable auto-scan of removable media, and tell Vanessa what you have done.
C. Leave the settings as they are. It is Vanessa's choice to disable auto-scan.
D. Leave the settings as they are. It is not your responsibility.
E. Ask Vanessa why auto-scan is disabled.

How would you rank the options in the question above in order of preference?

### A.3.12 Quality Check

I am randomly answering the questions.
A. Yes B. No

### A.3.13 Continuity of Care - Scenario 1

Assume you have a friend, Catherine, who you believe to be less competent than you in data security. She comes to you for help because she had corrupted files on her computer and thinks she has a virus. What would you do?
*(Responses: I strongly agree, I agree, Neutral, I disagree, I strongly disagree)*

A. Do nothing.

B. Fix it, if you feel you can.

C. Tell Catherine what to do to fix the problem herself, if you know the solution.

D. Tell Catherine to look for help elsewhere if you feel/find that you cannot fix it.

E. Arrange for a trusted contact to fix it, if you feel/find that you cannot.

F. Arrange for a third party to fix it. You offer to pay.

G. Arrange for a third party to fix it. You offer to help pay (share the cost).

H. Arrange for a third party to fix it. You expect Catherine to pay.

### A.3.14 Continuity of Care - Scenario 2

Assume you have a friend, Catherine, who you believe to be less competent than you in data security. She comes to you for help because she had corrupted files on her computer and thinks she has a virus. You recall that three months ago, Catherine was trying to install a piece of software, but was failing. She asked for your help. You were busy and told her the antivirus was the problem, and to try turning it off. You now notice the antivirus is off. What would you do?

*(Responses: I strongly agree, I agree, Neutral, I disagree, I strongly disagree)*

A. Do nothing.

B. Fix it, if you feel you can.

C. Tell Catherine what to do to fix the problem herself, if you know the solution.

D. Tell Catherine to look for help elsewhere if you feel/find that you cannot fix it.

E. Arrange for a trusted contact to fix it, if you feel/find that you cannot.

F. Arrange for a third party to fix it. You offer to pay.

G. Arrange for a third party to fix it. You offer to help pay (share the cost).

H. Arrange for a third party to fix it. You expect Catherine to pay.

## A.4 DS7 Survey Tool

### A.4.1 Demographics

1. Please select your age range: a) 18 - 34, b) 35 - 64, c) 65+

2. Please select your gender: a) Male, b) Female

3. What is your employment status?

a) Student, b) Employed,

c) Retired, d) Self-employed, e) Not working

4. What is your household composition?

a) Shared house with co-residents, b) Shared house with friends, c) Family house, d) Live alone

5. What devices do you have in your home?

a) Mobile phone, b) Telephone, c) Tablet/iPad, d) Laptop, e) Desktop computer, f) Game console, g) TV, h) Camera, i) Wearable device, j) Network router, k) Other

6. Which of the following services do you use?

a) Online/Mobile bankinge, b) Online shopping, c) Social networking, d) Communication, e) Education, f) Entertainment, g) Working from home, h) Remote working, i) Home security, j) TV streaming, k) Health services, l) None of the above

### A.4.2 Behavioural Questions

Who manages data security on your devices in the home?

a) Do it myself, b) Depend on someone to help

Do you help others secure their devices and networks?

a) Yes, b) No

### A.4.3 Product Acceptance

Imagine an app that shows you security problems in all devices connected to your home network, and gives you guidelines on how to fix them. Simply download and install the app, and click a button to see all devices on your network, and any security problems. The app comes with a small device that allows you to monitor your home network for malicious activities in real time, sending you alerts and helping you fix problems simply with a click of a button. The device also allows you to offer remote help to your friends

and family, and gives you access to a 24/7 support network when you have problems.

Assuming the price was reasonable, how likely would you be to consider buying this product?
*(Responses: Very Likely, Likely, Neutral, Unlikely, Very Unlikely)*

Why would you not consider buying the product?

How likely would you be to recommend this product to someone?
*(Responses: Very Likely, Likely, Neutral, Unlikely, Very Unlikely)*

Who would you recommend the product to?
a) Family, b) Friends, c) Work colleagues, d) Others

### A.4.4 Feature Preference

What do you like most about the product? (Please select all that apply.)
A. Diagnosing security problems
B. Guidance on fixing problems
C. Monitoring for problems in real time
D. Central management of all devices on the network
E. Remote management of home networks for security support
F. 24/7 access to a support network
G. None of the above

How would you rank the features above in order of preference to you?

### A.4.5 Improvement

What changes would most improve the product?

## A.5 DS4 Summary Statistics

**Survival/Outcome Bias:**

| | *Strongly Agree* | *Agree* | *Neutral* | *Disagree* | *Strongly Disagree* |
|---|---|---|---|---|---|
| A. | 34 (3.1%) | 203 (18.7%) | 237 (21.8%) | 430 (39.6%) | 183 (16.8%) |
| B. | 109 (10%) | 386 (35.5%) | 269 (24.7%) | 247 (22.7%) | 76 (7%) |

**Confidence in a Security Measure:**

| | *Strongly Agree* | *Agree* | *Neutral* | *Disagree* | *Strongly Disagree* |
|---|---|---|---|---|---|
| A. | 31 (2.9%) | 120 (11%) | 167 (15.4%) | 420 (38.6%) | 349 (32.1%) |
| B. | 41 (3.8%) | 242 (22.3%) | 272 (25%) | 385 (35.4%) | 147 (13.5%) |
| C. | 156 (14.4%) | 345 (31.7%) | 264 (24.3%) | 218 (20.1%) | 104 (9.6%) |

**Assessing Other People's Security Competence:**

How do you assess if someone is more competent than you in data security? (Please select all apply.)

| | | | |
|---|---|---|---|
| A. He/she works for a technical company | 255 (23.5%) | F. He/she works in data security | 938 (86.3%) |
| B. His/her job is technical | 255 (23.5%) | G. He/she studied or studies data security | 846 (77.8%) |
| C. He/she has more experience than you in using or working with technical devices and services | 559 (51.4%) | H. He/she has experienced a data security incident before | 428 (39.4%) |
| D. He/she studied or studies a technical course | 289 (26.6%) | I. None of the above | 47 (4.3% |
| E. He/she is more educated than you | 75 (6.9%) | | |

**How would you rank the options in the question above in order of preference?**

| | *0 (No rank)* | *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* |
|---|---|---|---|---|---|---|---|---|---|
| A. | 36 (3.3%) | 38 (3.5%) | 47 (4.3%) | 106 (9.8%) | 176 (16.2%) | 180 (16.6%) | 233 (21.4%) | 188 (17.3%) | 83 (7.6% |
| B. | 32 (2.9%)) | 38 (3.5%) | 41 (3.8%) | 116 (10.7%) | 201 (18.5%) | 269 (24.7%) | 229 (21.1%) | 131 (12.1%) | 30 (2.8% |
| C. | 21 (1.9%) | 96 (8.8%) | 73 (6.7%) | 231 (21.3%) | 252 (23.2%) | 164 (15.1%) | 140 (12.9%) | 96 (8.8%) | 14 (1.3% |
| D. | 32 (2.9%) | 16 (1.5%) | 38 (3.5%) | 103 (9.5%) | 173 (15.9%) | 254 (23.4%) | 249 (22.9%) | 190 (17.5%) | 32 (2.9% |
| E. | 39 (3.6%) | 11 (1%) | 15 (1.4%) | 24 (2.2%) | 41 (3.8%) | 36 (3.3%) | 65 (6%) | 188 (17.3%) | 668 (61.5 |
| F. | 8 (.7%) | 730 (67.2%) | 163 (15%) | 71 (6.5%) | 38 (3.5%) | 33 (3%) | 20 (1.8%) | 18 (1.7%) | 6 (.6 |
| G. | 18 (1.7%) | 115 (10.6%) | 634 (58.3%) | 138 (12.7%) | 55 (5.1%) | 45 (4.1%) | 32 (2.9%) | 25 (2.3%) | 25 (2.3% |
| H. | 22 (2%) | 42 (3.9%) | 68 (6.3%) | 284 (26.1%) | 124 (11.4%) | 74 (6.8%) | 84 (7.7%) | 208 (19.1%) | 181 (16.7 |

**Assessing the Quality and Source of Support:**

Which of the following do you take into consideration when seeking data security advice or help from someone? (Please select all that apply)

| | | | |
|---|---|---|---|
| A. Competence | 993 (91.4%) | E. Cost to you (money, favours, gifts, etc) | 530 (48.8%) |
| B. Availability | 334 (30.7%) | F. Cost to the source of advice/help (effort, inconvenience, etc) | 394 (36.2%) |
| C. Trust | 971 (89.3%) | G. None of the above | 11 (1%) |
| D. Closeness to you | 339 (31.2%) | | |

**How would you rank the options in the question above in order of preference?**

| | *0 (No rank)* | *1* | *2* | *3* | *4* | *5* | *6* |
|---|---|---|---|---|---|---|---|
| A. | 6 (.6%) | 660 (60.7%) | 273 (25.1%) | 79 (7.3%) | 39 (3.6%) | 17 (1.6%) | 13 (1.2% |
| B. | 22 (2%) | 21 (1.9%) | 77 (7.1%) | 293 (27%) | 283 (26%) | 232 (21.3%) | 159 (14.6%) |
| C. | 4 (.4%) | 321 (29.5%) | 541 (49.8%) | 118 (10.9%) | 62 (5.7%) | 32 (2.9%) | 9 (.8%) |
| D. | 28 (2.6%) | 20 (1.8%) | 71 (6.5%) | 212 (19.5%) | 195 (17.9%) | 224 (20.6%) | 337 (31% |
| E. | 21 (1.9%) | 50 (4.6%) | 82 (7.5%) | 234 (21.5%) | 252 (23.2%) | 248 (22.8%) | 200 (18.4%) |
| F. | 24 (2.2%) | 14 (1.3%) | 38 (3.5%) | 140 (12.9%) | 232 (21.3%) | 304 (28%) | 335 (30.8%) |

**Offer Unsolicited Support: ranking the recipients in order of preference?**

| | *0 (No rank)* | *1* | *2* | *3* | *4* |
|---|---|---|---|---|---|
| A. | 4 (.4%) | 756 (69.5%) | 196 (18%) | 97 (8.9%) | 34 (3.1%) |
| B. | 5 (.5%) | 216 (19.9%) | 746 (68.6%) | 113 (10.4%) | 7 (.6%) |
| C. | 5 (.5%) | 96 (8.8%) | 123 (11.3%) | 812 (74.7%) | 51 (4.7%) |
| D. | 12 (1.1%) | 18 (1.7%) | 17 (1.6%) | 58 (5.3%) | 982 (90.3%) |

**Accept Unsolicited Support: ranking the sources in order of preference**

| | *0 (No rank)* | *1* | *2* | *3* | *4* | *5* | *6* |
|---|---|---|---|---|---|---|---|
| A. | 7 (.6%) | 405 (37.3%) | 192 (17.7%) | 211 (19.4%) | 119 (10.9%) | 119 (10.9%) | 34 (3.1%) |
| B. | 8 (.7%) | 220 (20.2%) | 403 (37.1%) | 167 (15.4%) | 203 (18.7%) | 76 (7%) | 10 (.9%) |
| C. | 9 (.8%) | 95 (8.7%) | 134 (12.3%) | 456 (42%) | 127 (11.7%) | 235 (21.6%) | 31 (2.9%) |
| D. | 10 (.9%) | 232 (21.3%) | 149 (13.7%) | 129 (11.9%) | 332 (30.5%) | 186 (17.1%) | 49 (4.5%) |
| E. | 8 (.7%) | 123 (11.3%) | 191 (17.6%) | 93 (8.6%) | 227 (20.9%) | 378 (34.8%) | 67 (6.2%) |
| F. | 12 (1.1%) | 11 (1%) | 13 (1.2%) | 22 (2%) | 67 (6.2%) | 81 (7.5%) | 881 (81%) |

**Seek Support: ranking the sources in order of preference**

| | *0 (No rank)* | *1* | *2* | *3* | *4* | *5* | *6* |
|---|---|---|---|---|---|---|---|
| A. | 10 (.9%) | 361 (33.2%) | 205 (18.9%) | 229 (21.1%) | 119 (10.9%) | 132 (12.1%) | 31 (2.9%) |
| B. | 8 (.7%) | 243 (22.4%) | 393 (36.2%) | 173 (15.9%) | 198 (18.2%) | 62 (5.7%) | 10 (.9%) |
| C. | 10 (.9%) | 98 (9%) | 138 (12.7%) | 410 (37.7%) | 166 (15.3%) | 236 (21.7%) | 29 (2.7%) |
| D. | 11 (1%) | 232 (21.3%) | 159 (14.6%) | 151 (13.9%) | 305 (28.1%) | 196 (18%) | 33 (3%) |
| E. | 9 (.8%) | 145 (13.3%) | 176 (16.2%) | 97 (8.9%) | 235 (21.6%) | 357 (32.8%) | 68 (6.3%) |
| F. | 14 (1.3%) | 6 (.6%) | 9 (.8%) | 17 (1.6%) | 52 (4.8%) | 90 (8.3%) | 899 (82.7%) |

**Continuity of Care - Scenario 1:**

| | *Strongly Agree* | *Agree* | *Neutral* | *Disagree* | *Strongly Disagree* |
|---|---|---|---|---|---|
| A. | 12 (1.1%) | 24 (2.2%) | 116 (10.7%) | 452 (41.6%) | 483 (44.4%) |
| B. | 389 (35.8%) | 561 (51.6%) | 80 (7.4%) | 42 (3.9%) | 15 (1.4%) |
| C. | 146 (13.4%) | 613 (56.4%) | 188 (17.3%) | 114 (10.5%) | 26 (2.4%) |
| D. | 327 (30.1%) | 556 (51.1%) | 100 (9.2%) | 77 (7.1%) | 27 (2.5%) |
| E. | 263 (24.2%) | 535 (49.2%) | 192 (17.7%) | 81 (7.5%) | 16 (1.5%) |
| F. | 11 (1%) | 66 (6.1%) | 131 (12.1%) | 464 (42.7%) | 415 (38.2%) |
| G. | 20 (1.8%) | 72 (6.6%) | 148 (13.6%) | 442 (40.7%) | 405 (37.3%) |
| H. | 153 (14.1%) | 459 (42.2%) | 281 (25.9%) | 130 (12%) | 64 (5.9%) |

**Continuity of Care - Scenario 2:**

| | *Strongly Agree* | *Agree* | *Neutral* | *Disagree* | *Strongly Disagree* |
|---|---|---|---|---|---|
| A. | 14 (1.3%) | 29 (2.7%) | 98 (9%) | 491 (45.2%) | 455 (41.9%) |
| B. | 424 (39%) | 549 (50.5%) | 62 (5.7%) | 37 (3.4%) | 15 (1.4%) |
| C. | 200 (18.4%) | 604 (55.6%) | 160 (14.7%) | 98 (9%) | 25 (2.3%) |
| D. | 240 (22.1%) | 615 (56.6%) | 131 (12.1%) | 69 (6.3%) | 32 (2.9%) |
| E. | 252 (32.3%) | 584 (53.7%) | 161 (14.8%) | 61 (5.6%) | 29 (2.7%) |
| F. | 63 (5.8%) | 168 (15.5%) | 219 (20.1%) | 367 (33.8%) | 270 (24.8%) |
| G. | 65 (6%) | 235 (21.6%) | 211 (19.4%) | 331 (30.5%) | 245 (22.5%) |
| H. | 90 (8.3%) | 347 (31.9%) | 315 (29%) | 241 (22.2%) | 94 (8.6%) |

# Bibliography

[1] ISO/IEC 27000:2011(E). Information technology – Security techniques – Information security risk management. Standard, International Organization for Standardization, Geneva, CH, 2011.

[2] ISO/IEC 27000:2017(E). Information technology. Security techniques. Information security management systems. Overview and vocabulary. Standard, International Organization for Standardization, Geneva, CH, 2016.

[3] ISO/IEC 27002:2017(E). Information technology. Security techniques. Code of practice for information security controls. Standard, International Organization for Standardization, Geneva, CH, 2016.

[4] Gregory D Abowd, Anind K Dey, Peter J Brown, Nigel Davies, Mark Smith, and Pete Steggles. Towards a better understanding of context and context-awareness. In Gellersen HW, editor, *International symposium on handheld and ubiquitous computing, Lecture Notes in Computer Science*, volume 1707, pages 304–307. Springer, Berlin, Heidelberg, 1999.

[5] Chadia Abras, Diane Maloney-Krichmar, and Jenny Preece. User-centered design. *Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications*, 37(4):445–456, 2004.

[6] Alessandro Acquisti and Jens Grossklags. Privacy attitudes and privacy behavior. In L.J. Camp and S. Lewis, editors, *Economics of information security. Advances in Information Security*, volume 12, pages 165–178. Springer, Boston, MA, 2004.

[7] Alessandro Acquisti and Jens Grossklags. Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3(1):26–33, 2005.

[8] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[9] Anne Adams, Martina Angela Sasse, and Peter Lunt. Making passwords secure and usable. In H. Thimbleby, B. O'Conaill, and P.J. Thomas, editors, *People and Computers XII*, pages 1–19. Springer, London, 1997.

[10] Icek Ajzen. From intentions to actions: A theory of planned behavior. In J. Kuhl and J. Beckmann, editors, *Action Control. SSSP Springer Series in Social Psychology*, pages 11–39. Springer, Berlin, Heidelberg, 1985.

[11] Icek Ajzen. Theory of reasoned action. In E. Kazdin, editor, *Encyclopedia of psychology*, volume 8, pages 61–63. Oxford University Press, 2000.

[12] Icek Ajzen and Thomas J Madden. Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of Experimental Social Psychology*, 22(5):453–474, 1986.

[13] Christopher J. Alberts and Audrey Dorofee. *Managing Information Security Risks: The Octave Approach*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2002.

[14] Eirik Albrechtsen. A qualitative study of users' view on information security. *Computers & Security*, 26(4):276–289, 2007.

[15] Nora Alkaldi and Karen Renaud. Why do people adopt, or reject, smartphone password managers? In *1st European Workshop on Usable Security (EuroUSEC)*, Darmstadt, Germany, 2016. Internet Society.

[16] Catherine L Anderson and Ritu Agarwal. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3):613–643, 2010.

[17] AOL/NCSA. Online Safety Study. `https://library.educause.edu/resources/2004/1/aolncsa-online-safety-study`. [Online; accessed on August 25, 2017].

[18] Nalin Asanka Gamagedara Arachchilage and Melissa Cole. Design a mobile game for home computer users to prevent from "phishing attacks". In *International Conference on Information Society (i-Society 2011)*, pages 485–489. IEEE, 2011.

[19] Christopher J Armitage and Mark Conner. Efficacy of the theory of planned behaviour: A meta-analytic review. *British Journal of Social Psychology*, 40(4):471–499, 2001.

[20] Ahmad W Atamli and Andrew Martin. Threat-based security analysis for the internet of things. In *2014 International Workshop on Secure Internet of Things (SIoT)*, pages 35–43. IEEE, 2014.

[21] Kregg Aytes and Terry Connolly. Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing (JOEUC)*, 16(3):22–40, 2004.

[22] Maria Bada and Angela Sasse. Cyber security awareness campaigns: Why do they fail to change behaviour? In *1st International Conference on Cyber Security for Sustainable Society*. arXiv:1901.02672, Coventry, UK, 2015.

[23] David A Baldwin. The concept of security. *Review of International Studies*, 23(1):5–26, 1997.

[24] Dirk Balfanz, Glenn Durfee, Diana K Smetters, and Rebecca E Grinter. In search of usable security: Five lessons from the field. *IEEE Security & Privacy*, 2(5):19–24, 2004.

[25] Jonathan Baron and John C Hershey. Outcome bias in decision evaluation. *Journal of Personality and Social Psychology*, 54(4):569, 1988.

[26] Richard L Baskerville. Investigating information systems with action research. *Communications of the AIS*, 2(3es):4, 1999.

[27] BBC. Smart home devices used as weapons in website attack. `http://www.bbc.co.uk/news/technology-37738823`, 2016. [Online; accessed on 03-April-2017].

[28] Adam Beautement, Ingolf Becker, Simon Parkin, Kat Krol, and Angela Sasse. Productive security: A scalable methodology for analysing employee security behaviours. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 253–270. USENIX Association, 2016.

[29] Izak Benbasat. Laboratory experiments in information systems studies with a focus on individuals: a critical appraisal. *The information systems research challenge: Experimental research methods*, 2:33–47, 1989.

[30] Izak Benbasat, David K Goldstein, and Melissa Mead. The case research strategy in studies of information systems. *MIS Quarterly*, 11(3):369–386, 1987.

[31] Andrew Besmer, Jason Watson, and Heather Richter Lipford. The impact of social navigation on privacy policy configuration. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 7:1–7:10, New York, NY, USA, 2010. ACM.

[32] Patrick Biernacki and Dan Waldorf. Snowball sampling: Problems and techniques of chain referral sampling. *Sociological methods & research*, 10(2):141–163, 1981.

[33] Burton H. Bloom. Space/time trade-offs in hash coding with allowable errors. *Commun. ACM*, 13(7):422–426, July 1970.

[34] Susanne Bodker. Scenarios in user-centred design-setting the stage for reflection and action. In *Proceedings of the 32nd Annual Hawaii International*

*Conference on Systems Sciences. 1999. HICSS-32. Abstracts and CD-ROM of Full Papers*, pages 11–pp. IEEE, 1999.

[35] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[36] Virginia Braun, Victoria Clarke, and Gareth Terry. Thematic analysis. *Qualitative Research in Clinical and Health Psychology*, 24:95–113, 2014.

[37] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):18–26, 2011.

[38] Patrick Brézillon. Using context for supporting users efficiently. In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences, 2003*, pages 9 pp.–. IEEE, 2003.

[39] P Bryant, SM Furnell, and AD Phippen. Improving protection and security awareness amongst home users. *Advances in Networks, Computing and Communications 4*, page 182, 2008.

[40] Shawn A Butler. Security attribute evaluation method: a cost-benefit approach. In *Proceedings of the 24th International Conference on Software Engineering*, pages 232–240. ACM, 2002.

[41] Pascale Carayon. Human factors of complex sociotechnical systems. *Applied Ergonomics*, 37(4):525–535, 2006.

[42] Kathleen Carley. Coding choices for textual analysis: A comparison of content analysis and map analysis. In *Sociological Methodology*, volume 23, pages 75–126. American Sociological Association, Wiley, Sage Publications, Inc., 1993.

[43] Nancy Carter, Denise Bryant-Lukosius, Alba DiCenso, Jennifer Blythe, and Alan J Neville. The use of triangulation in qualitative research. *Oncology Nursing Forum*, 41(5):545–547, 2014.

[44] Kathy Charmaz and Linda Liska Belgrave. Grounded theory. In George Ritze, editor, *The Blackwell Encyclopedia of Sociology*. American Cancer Society, 2015.

[45] Erika Chin, Adrienne Porter Felt, Vyas Sekar, and David Wagner. Measuring user confidence in smartphone security and privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, pages 1:1–1:16. ACM, 2012.

[46] Anton Chuvakin. Basic Security Checklist for Home and Office Users. `https://www.symantec.com/connect/articles/basic-security-checklist-home-and-office-users`, 2001. [Online; accessed on 19-November-2017].

[47] Arthur Wm. Conklin. *Computer Security Behaviors of Home Pc Users: A Diffusion of Innovation Approach*. PhD thesis, The University of Texas at San Antonio, 2006. AAI3227760.

[48] Alan Cooper, Robert Reimann, and David Cronin. *About face 3: the essentials of interaction design*. John Wiley & Sons, 2007.

[49] Juliet Corbin and Anselm Strauss. *Basics of qualitative research: Procedures and techniques for developing grounded theory*. Sage Publications, Inc., Thousand Oaks, CA, US, 4th edition, 2014.

[50] Lynne Coventry, Pamela Briggs, John Blythe, and Minh Tran. Using behavioural insights to improve the public's use of cyber security best practices. Technical report, Government Office for Science, London, UK, 2014.

[51] John W Creswell and Vicki L Plano Clark. Designing and conducting mixed methods research. *Australian and New Zealand Journal of Public Health*, 31(4):388–388, 2007.

[52] Robert E Crossler, Allen C Johnston, Paul Benjamin Lowry, Qing Hu, Merrill Warkentin, and Richard Baskerville. Future directions for behavioral information security research. *Computers & Security*, 32:90–101, 2013.

[53] Tiago Cruz, Paulo Simões, Edmundo Monteiro, Fernando Bastos, and Alexandre Laranjeira. Cooperative security management for broadband network environments. *Security and Communication Networks*, 8(18):3953–3977, 2015.

[54] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 143–157, 2014.

[55] Sauvik Das, Adam DI Kramer, Laura A Dabbish, and Jason I Hong. Increasing security sensitivity with social proof: A large-scale experimental confirmation. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, pages 739–749. ACM, 2014.

[56] Janez Demšar. Statistical comparisons of classifiers over multiple data sets. *Journal of Machine Learning Research*, 7(Jan):1–30, 2006.

[57] Anind K Dey. Understanding and using context. *Personal and ubiquitous computing*, 5(1):4–7, 2001.

[58] Gurpreet Dhillon and James Backhouse. Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, 11(2):127–153, 2001.

[59] Paul DiGioia and Paul Dourish. Social navigation as a model for usable security. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, SOUPS'05, pages 101–108, New York, NY, USA, 2005. ACM.

[60] Alessandro Distefano, Antonio Grillo, Alessandro Lentini, and Giuseppe F Italiano. Securemydroid: enforcing security in the mobile devices lifecycle. In

*Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, page 27. ACM, 2010.

[61] Zheng Dong, Vaibhav Garg, L Jean Camp, and Apu Kapadia. Pools, clubs and security: designing for a party not a person. In *Proceedings of the 2012 Workshop on New Security Paradigms*, pages 77–86. ACM, 2012.

[62] Paul Dourish, Rebecca E Grinter, Jessica Delgado De La Flor, and Melissa Joseph. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6):391–401, 2004.

[63] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1065–1074. ACM, 2008.

[64] Satu Elo and Helvi Kyngäs. The qualitative content analysis process. *Journal of advanced nursing*, 62(1):107–115, 2008.

[65] ENISA. "Mirai" malware, attacks Home Routers. `https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers`, 2016. [Online; accessed on 03-April-2017].

[66] Michael Fagan and Mohammad Maifi Hasan Khan. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 59–75, 2016.

[67] Shamal Faily and Ivan Fléchais. Analysing and visualising security and usability in IRIS. In *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*, pages 543–548. IEEE, 2010.

[68] Shamal Faily and Ivan Fléchais. A meta-model for usable secure requirements engineering. In *Proceedings of the 2010 ICSE Workshop on Software Engineering for Secure Systems*, pages 29–35. ACM, 2010.

[69] Nick Feamster. Outsourcing home network security. In *Proceedings of the 2010 ACM SIGCOMM workshop on Home networks*, pages 37–42. ACM, 2010.

[70] David M Fetterman. Ethnography. In *Handbook of applied social research methods*, pages 473–504. Sage Publications, Inc, Thousand Oaks, CA, US, 1998.

[71] Thomas Finne. Special feature: The three categories of decision-making and information security. *Computers and Security*, 17(5):397–405, 1998.

[72] Robert J Fisher. Social desirability bias and the validity of indirect questioning. *Journal of consumer research*, 20(2):303–315, 1993.

[73] Ivan Fléchais. *Designing secure and usable systems*. PhD thesis, University College London, London, UK, 2005.

[74] Ivan Flechais and M Angela Sasse. Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-science. *International Journal of Human-Computer Studies*, 67(4):281–296, 2009.

[75] Ivan Flechais, M Angela Sasse, and Stephen Hailes. Bringing security home: a process for developing secure and usable systems. In *Proceedings of the 2003 workshop on New security paradigms*, pages 49–57. ACM, 2003.

[76] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. Do or do not, there is no try: user engagement may not improve security outcomes. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 97–111, 2016.

[77] Floyd J Fowler Jr. *Survey research methods*. Applied social research methods series, v. 1. Sage publications, Inc, 2013.

[78] Milton Friedman. A comparison of alternative tests of significance for the problem of m rankings. *The Annals of Mathematical Statistics*, 11(1):86–92, 1940.

[79] SM Furnell, P Bryant, and Andrew D Phippen. Assessing the security perceptions of personal internet users. *Computers & Security*, 26(5):410–417, 2007.

[80] Anne M Gadermann, Martin Guhn, and Bruno D Zumbo. Estimating ordinal reliability for likert-type and ordinal item response data: A conceptual, empirical, and practical guide. *Practical Assessment, Research & Evaluation*, 17(3), 2012.

[81] Robert D Galliers and Frank F Land. Choosing appropriate information systems research methodologies. *Communications of the ACM*, 30(11):901–902, 1987.

[82] Alan S Gerber and Donald P Green. Field experiments and natural experiments. In Robert E. Goodin, editor, *The Oxford Handbook of Political Science*. Oxford Handbooks, 2008.

[83] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. Home sweet home? investigating users' awareness of smart home privacy threats. In *Symposium on Usable Privacy and Security (SOUPS 2018). Baltimore, MD*. USENIX, 2018.

[84] Barney G Glaser, Anselm L Strauss, and Elizabeth Strutzel. The discovery of grounded theory; strategies for qualitative research. *Nursing research*, 17(4):364, 1968.

[85] Dieter Gollmann. Computer security. *Wiley Interdisciplinary Reviews: Computational Statistics*, 2(5):544–554, 2010.

[86] Jens Grossklags, Nicolas Christin, and John Chuang. Secure or insure?: a game-theoretic analysis of information security games. In *Proceedings of the 17th international conference on World Wide Web*, pages 209–218. ACM, 2008.

[87] Peter Gutmann. Applying problem-structuring methods to problems in computer security. In *Proceedings of the 2011 workshop on New Security Paradigms Workshop*, pages 37–44. ACM, 2011.

[88] Ibbad Hafeez, Aaron Yi Ding, Lauri Suomalainen, Alexey Kirichenko, and Sasu Tarkoma. Securebox: Toward safer and smarter iot networks. In *Proceedings of the 2016 ACM Workshop on Cloud-Assisted Networking*, pages 55–60. ACM, 2016.

[89] Eugene A Hammel and Peter Laslett. Comparing household structure over time and between cultures. *Comparative studies in society and history*, 16(01):73–109, 1974.

[90] E Erin Harrison. The privacy Puzzle. `https://www.ftc.gov/system/files/documents/public_statements/630791/141222privacypuzzleinsidecounsel.pdf`, 2016. [Online; accessed on 16-June-2016].

[91] Steve Harrison, Deborah Tatar, and Phoebe Sengers. The three paradigms of HCI. In *Alt. Chi. Session at the SIGCHI Conference on human factors in computing systems San Jose, California, USA*, pages 1–18, 2007.

[92] Eiji Hayashi and Jason Hong. A diary study of password usage in daily life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2627–2630. ACM, 2011.

[93] Roberta Heale and Alison Twycross. Validity and reliability in quantitative studies. *Evidence-Based Nursing*, 18(3):66–67, 2015.

[94] Cecilia Henning and Mats Lieberg. Strong ties or weak ties? neighbourhood networks in a new perspective. *Scandinavian Housing and Planning Research*, 13(1):3–26, 1996.

[95] Karen Henricksen, Jadwiga Indulska, and Andry Rakotonirainy. Modeling context information in pervasive computing systems. In Friedemann Mattern and Mahmoud Naghshineh, editors, *International Conference on Pervasive Computing*, pages 167–180. Springer, Berlin, Heidelberg, 2002.

[96] Tejaswini Herath, Rui Chen, Jingguo Wang, Ketan Banjara, Jeff Wilbur, and H Raghav Rao. Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Information systems journal*, 24(1):61–84, 2014.

[97] 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*, pages 133–144. ACM, 2009.

[98] Grant Hernandez, Orlando Arias, Daniel Buentello, and Yier Jin. Smart nest thermostat: A smart spy in your home. *Black Hat USA*, pages 1–8, 2014.

[99] Rebecca Herold. *Managing an information security and privacy awareness and training program*. Auerbach Publications, Boca Raton, FL, 2005.

[100] Morten Hertzum, Niels Jørgensen, and Mie Nørgaard. Usable security and e-banking: Ease of use vis-a-vis security. *Australasian Journal of Information Systems*, 11(2), 2004.

[101] Hanan Hibshi, Travis D Breaux, Maria Riaz, and Laurie Williams. A grounded analysis of experts' decision-making during security assessments. *Journal of Cybersecurity*, 2(2):147–163, 2016.

[102] Ursula Holmström. User-centered design of security software. In *Proceedings of Human Factors in Telecommunications (HFT)*, pages 4–7, Copenhagen, Denmark, 1999.

[103] Adele E Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska, and Zinta Byrne. The psychology of security for the home computer user. In *2012 IEEE Symposium on Security and Privacy (SP)*, pages 209–223. IEEE, 2012.

[104] Hsiu-Fang Hsieh and Sarah E Shannon. Three approaches to qualitative content analysis. *Qualitative Health Research*, 15(9):1277–1288, 2005.

[105] Internet Live Stats. Internet Users. `http://www.internetlivestats.com/internet-users/`. [Online; accessed on 25-August-2017].

[106] Iulia Ion, Rob Reeder, and Sunny Consolvo. "... no one can hack my mind": Comparing expert and non-expert security practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 327–346, 2015.

[107] Yosef Jabareen. Building a conceptual framework: philosophy, definitions, and procedure. *International Journal of Qualitative Methods*, 8(4):49–62, 2009.

[108] A Milton Jenkins. Research methodologies and MIS research. In *Research Methods in Information Systems*, volume 103, page 117, BV, Amsterdam, Holland, 1985. Elsevier Science Publishers.

[109] Helene Joffe and Lucy Yardley. Content and thematic analysis. In David F. Marks and Lucy Yardley, editors, *Research Methods for Clinical and Health Psychology*, pages 56–68. SAGE Publications, 2004.

[110] Ronald Kainda, Ivan Flechais, and AW Roscoe. Security and usability: Analysis and evaluation. In *International Conference on Availability, Reliability, and Security, 2010 (ARES'10)*, pages 275–282. IEEE, 2010.

[111] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 39–52, 2015.

[112] Emmanouil Karamanos. Investigation of home router security. Master's thesis, KTH, Communication Systems, CoS, 2010.

[113] Lori M Kaufman. Data security in the world of cloud computing. *IEEE Security & Privacy*, 7(4), 2009.

[114] Kate Kelley, Belinda Clark, Vivienne Brown, and John Sitzia. Good practice in the conduct and reporting of survey research. *International Journal for Quality in Health Care*, 15(3):261–266, 2003.

[115] Eunice Kim, Jhih-Syuan Lin, and Yongjun Sung. To app or not to app: Engaging consumers via branded mobile apps. *Journal of Interactive Advertising*, 13(1):53–65, 2013.

[116] Iacovos Kirlappos and M Angela Sasse. Security education against phishing: A modest proposal for a major rethink. *IEEE Security & Privacy*, 10(2):24–32, 2012.

[117] Jenny Kitzinger. Qualitative research: introducing focus groups. *British Medical Journal (BMJ)*, 311(7000):299–302, 1995.

[118] R Koppel, A Blythe, V Kothari, and S Smith. Security for the collective reality of the smart home. In *Workshop on the Human Aspects of Smarthome Security Privacy (WSSP 2018), Baltimore, MD, USA*, 2018.

[119] Sara Kraemer, Pascale Carayon, and John Clem. Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, 28(7):509–520, 2009.

[120] Elmarie Kritzinger and Sebastiaan H von Solms. Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29(8):840–847, 2010.

[121] Kat Krol, Matthew Moroz, and M Angela Sasse. Don't work. Can't work? Why it's time to rethink security warnings. In *2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, pages 1–8. IEEE, 2012.

[122] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. Teaching johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2):7, 2010.

[123] Kaspersky Lab. The Tale of One Thousand and One DSL Modems. `https://securelist.com/the-tale-of-one-thousand-and-one-dsl-modems/57776/`, 2012. [Online; accessed on 19-November-2017].

[124] Fanny Lalonde Levesque, Jude Nsiempba, José M Fernandez, Sonia Chiasson, and Anil Somayaji. A clinical study of risk factors related to malware infections. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 97–108. ACM, 2013.

[125] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. *Research methods in human-computer interaction*. Morgan Kaufmann, Cambridge, MA 02139, United States, 2 edition, 2017.

[126] Sarah Lewis. Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice*, 16(4):473–475, 2015.

[127] Ming Li, Wenjing Lou, and Kui Ren. Data security and privacy in wireless body area networks. *IEEE Wireless Communications*, 17(1), 2010.

[128] Ying Li and Mikko T Siponen. A Call For Research On Home Users' Information Security Behaviour. In *Proceedings of 2011 Pacific Asia Conference on Information Systems (PACIS 2011)*, pages 1–12, 2011.

[129] Huigang Liang and Yajiong Xue. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems*, 11(7):394–413, 2010.

[130] Heather Richter Lipford and Mary Ellen Zurko. Someone to watch over me. In *Proceedings of the 2012 New Security Paradigms Workshop*, NSPW '12, pages 67–76, New York, NY, USA, 2012. ACM.

[131] Knud Lasse Lueth. State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. `https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/`, 2018. [Online; accessed on 16-June-2019].

[132] Phil Lunsford and Mrs Constance Boahn. How the Lizard Squad Took Down Two of the Biggest Networks in the World. `http://www.infosecwriters.com/Papers/JRollins_Lizard_Squad.pdf`, 2015. [Online; accessed on 09-June-2016].

[133] Shelley Mallett. Understanding home: a critical review of the literature. *The Sociological Review*, 52(1):62–89, 2004.

[134] Vincentius Martin, Qiang Cao, and Theophilus Benson. Fending off IoT-hunting attacks at home networks. In *Proceedings of the 2nd Workshop on Cloud-Assisted Networking*, pages 67–72. ACM, 2017.

[135] Marilia S Mendes, Elizabeth Furtado, Guido Militao, and Miguel F de Castro. 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*, pages 391–403. Springer, 2015.

[136] Elena Meshkova, Janne Riihijarvi, Petri Mahonen, and Christoforos Kavadias. Modeling the home environment using ontology with applications in software configuration management. In *International Conference on Telecommunications, 2008 (ICT 2008).*, pages 1–6. IEEE, 2008.

[137] George R Milne, Lauren I Labrecque, and Cory Cromer. Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, 43(3):449–473, 2009.

[138] John Mingers. Combining is research methods: towards a pluralist methodology. *Information Systems Research*, 12(3):240–259, 2001.

[139] William L Moore. Concept Testing. *Journal of Business Research*, 10(3):279–294, 1982.

[140] L Morgan David. Focus groups as qualitative research. *Qualitative Research Methods Series*, 16(2), 1997.

[141] Ganthan Narayana Samy, Rabiah Ahmad, and Zuraini Ismail. Security threats categories in healthcare information systems. *Health Informatics Journal*, 16(3):201–209, 2010.

[142] NCSC. 10 Steps to Cyber Security. `https://www.ncsc.gov.uk/guidance/10-steps-cyber-security`, 2016. Online; accessed on 10-November-2017.

[143] Anton J Nederhof. Methods of coping with social desirability bias: A review. *European Journal of Social Psychology*, 15(3):263–280, 1985.

[144] Boon-Yuen Ng and Mohammad Rahim. A socio-behavioral study of home computer users' intention to practice security. *Proceedings of 2005 Pacific Asia Conference on Information System (PACIS 2005)*, pages 234–247, 2005.

[145] Maria Nickolova and Eugene Nickolov. Threat model for user security in e-learning systems. *International Journal Information Technologies and Knowledge*, 1(1):341–347, 2007.

[146] Jakob Nielsen. Guerrilla HCI: Using discount usability engineering to penetrate the intimidation barrier. *Cost-justifying Usability*, pages 245–272, 1994.

[147] Marcus Niemietz and Jörg Schwenk. Owning your home network: Router security revisited. *arXiv preprint arXiv:1506.04112*, 2015.

[148] Helen Noble and Joanna Smith. Issues of validity and reliability in qualitative research. *Evidence-Based Nursing*, 18(2):34–35, 2015.

[149] Mariam Nouh, Abdullah Almaatouq, Ahmad Alabdulkareem, Vivek K Singh, Erez Shmueli, Mansour Alsaleh, Abdulrahman Alarifi, Anas Alfaris, et al. Social Information Leakage: Effects of Awareness and Peer Pressure on User Behavior. In Theo Tryfonas and Ioannis Askoxylakis, editors, *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 352–360, Cham, 2014. Springer International Publishing.

[150] NSA. Best Practices for Keeping Your Home Network Secure. `https://dodcio.defense.gov/`, 2014. [Online; accessed on 10-November-2017].

[151] Norbert Nthala and Ivan Flechais. "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. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 123–142. Springer, 2017.

[152] Norbert Nthala and Ivan Flechais. Informal support networks: an investigation into home data security practices. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 63–82, 2018.

[153] Norbert Nthala and Ivan Flechais. Rethinking home network security. *European Workshop on Usable Security (EuroUSEC)*, 2018.

[154] Jay F Nunamaker Jr, Minder Chen, and Titus DM Purdin. Systems development in information systems research. *Journal of Management Information Systems*, 7(3):89–106, 1990.

[155] Parliamentary Office of Science & Technology (POST). Uk broadband infrastructure. Technical report, Houses of Parliament, London, UK, 2015.

[156] Office for National Statistics. Internet access - households and individuals 2015. `http://www.ons.gov.uk/ons/dcp171778412758.pdf`. [Online; accessed on 05-June-2016].

[157] Krebs on Security. Lizard Stresser Runs on Hacked Home Routers. https://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/, 2015. [Online; accessed on 19-November-2017].

[158] Craig M Parker, Evalyn N Wafula, Paula MC Swatman, and Paul A Swatman. Information systems research methods: The technology transfer problem. In *Proceedings of the 5th Australian Conference on Information System*, pages 197–208, 1994.

[159] Bryan D Payne and W Keith Edwards. A brief introduction to usable security. *IEEE Internet Computing*, 12(3):13–21, 2008.

[160] Thomas R Peltier. *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. Auerbach Publications, New York, 1st edition, 2016. 312 pages.

[161] Robert Pfau. The security lifecycle. Technical report, SANS Institute, 2003.

[162] Davar Pishva and Keiji Takeda. Product-based security model for smart home appliances. *IEEE Aerospace and Electronic Systems Magazine*, 23(10), 2008.

[163] Oxford University Press. *The World Encyclopedia*. Oxford University Press, New York, N.Y., 5th edition, 2001.

[164] John Pruitt and Jonathan Grudin. Personas: practice and theory. In *Proceedings of the 2003 Conference on Designing for User Experiences*, pages 1–15. ACM, 2003.

[165] Emilee Rader and Rick Wash. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, 1(1):121–144, 2015.

[166] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 6:1–6:17, New York, NY, USA, 2012. ACM.

[167] Umesh Hodeghatta Rao and Bishwa Prakash Pati. Study of internet security threats among home users. In *Fourth International Conference on Computational Aspects of Social Networks (CASoN 2012)*, pages 217–221. IEEE, 2012.

[168] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. How i learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 666–677. ACM, 2016.

[169] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 272–288. IEEE, 2016.

[170] Robert W Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. An experience sampling study of user reactions to browser warnings in the field. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI'18, pages 512:1–512:13, New York, NY, USA, 2018. ACM.

[171] Scott Reeves, Ayelet Kuper, and Brian David Hodges. Qualitative research methodologies: ethnography. *British Medical Journal (BMJ)*, 337(7668):512–514, 2008.

[172] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. Why doesn't Jane protect her privacy? In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 244–262. Springer, 2014.

[173] Helen J Richardson. A 'smart house' is not a home: The domestication of ICTs. *Information Systems Frontiers*, 11(5):599, 2009.

[174] Robert Richardson. 2008 CSI/FBI computer crime and security survey. In *Computer Security Issues Trends*, pages 1–30. Computer Security Institute, 2008.

[175] Andreas M Riege. Validity and reliability tests in case study research: a literature review with "hands-on" applications for each research phase. *Qualitative Market Research: An International Journal*, 6(2):75–86, 2003.

[176] Dorothy Elizabeth Robling Denning. *Cryptography and data security*. Addison-Wesley Longman Publishing Co., Inc., 1982.

[177] Nuria Rodríguez-Priego and René van Bavel. The effect of warning messages on secure behaviour online: Results from a lab experiment. EUR - Scientific and Technical Research Reports, Joint Research Centre (Seville site), Seville, Spain, 2016.

[178] Everett M Rogers. *Diffusion of innovations*. Simon and Schuster, New York, 4th edition, 2010.

[179] Ronald W Rogers. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, 91(1):93–114, 1975.

[180] Jeff Rowe, Karl Levitt, and Mike Hogarth. Towards the realization of a public health system for shared secure cyber-space. In *Proceedings of the 2013 workshop on New security paradigms workshop*, pages 11–18. ACM, 2013.

[181] Richard Rubinstein, Harry M Hersh, and Henry F Ledgard. *The human factor: Designing computer systems for people*. Digital Press Burlington, MA, 1984.

[182] Mary-Ann Russon. Two London IP Addresses Hijack Over 300,000 Home Routers. `http://www.ibtimes.co.uk/two-london-ip-addresses-hijack-over-300000-computers-1438719`, 2014. [Online; accessed on 19-November-2017].

[183] M Angela Sasse and Ivan Flechais. Usable security: Why do we need it? How do we get it? In L. Cranor and S. Garfinkel, editors, *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly, 2005.

[184] Peter Saunders and Peter Williams. The constitution of the home: towards a research agenda. *Housing Studies*, 3(2):81–93, 1988.

[185] Bruce Schneier. *Beyond Fear Thinking Sensibly about Security in an Uncertain World*. Copernicus Books, New York, 2003.

[186] Bruce Schneier. *Secrets & Lies: Digital Security in a Networked World*. John Wiley & Sons, 2015.

[187] William R Shadish and Thomas D Cook. The renaissance of field experimentation in evaluating interventions. *Annual Review of Psychology*, 60:607–629, 2009.

[188] Richard Shay, Iulia Ion, Robert W Reeder, and Sunny Consolvo. My religious aunt asked why i was trying to sell her viagra: experiences with account hijacking. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2657–2666. ACM, 2014.

[189] HongHai Shen and Prasun Dewan. Access control for collaborative environments. In *Proceedings of the 1992 ACM conference on Computer-supported cooperative work*, pages 51–58. ACM, 1992.

[190] Ben Shneiderman, Catherine Plaisant, Maxine Cohen, Steven Jacobs, Niklas Elmqvist, and Nicholas Diakopoulos. *Designing the User Interface: Strategies for Effective Human-Computer Interaction*. Pearson, 6th edition, 2016.

[191] Diomidis Spinellis, Spyros Kokolakis, and Stefanos Gritzalis. Security requirements, risks and recommendations for small enterprise and home-office environments. *Information Management & Computer Security*, 7(3):121–128, 1999.

[192] Mariusz Stawowski. The principles of network security design. *Information Systems Security Association (ISSA) Journal*, pages 29–31, 2007.

[193] Barbara Steward. Living space: the changing meaning of home. *British Journal of Occupational Therapy*, 63(3):105–110, 2000.

[194] Detmar W Straub and Richard J Welke. Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, pages 441–469, 1998.

[195] Anselm Strauss and Juliet Corbin. *Basics of qualitative research: Procedures and techniques for developing grounded theory.* Sage Publications, Inc., Thousand Oaks, CA, US, 2nd edition, 1998.

[196] Cyber Streetwise. Cyberstreetwise. `https://www.cyberstreetwise.com`, 2016. [Online; accessed on 15-April-2016].

[197] Frank Swiderski and Window Snyder. *Threat Modeling (Microsoft Professional)*, volume 7. Microsoft Press, 2004.

[198] Shuhaili Talib, Nathan L Clarke, and Steven M Furnell. An analysis of information security awareness within home and work environments. In *International Conference on Availability, Reliability, and Security, 2010 (ARES'10)*, pages 196–203. IEEE, 2010.

[199] Leona Tam, Myron Glassman, and Mark Vandenwauver. The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, 29(3):233–244, 2010.

[200] Curtis R Taylor, Craig A Shue, and Mohamed E Najd. Whole home proxies: Bringing enterprise-grade security to residential networks. In *IEEE International Conference on Communications (ICC), 2016*, pages 1–6. IEEE, 2016.

[201] Faye P Teer, SE Kruck, and Gregory P Kruck. Empiracal study of students' computer security practices/perceptions. *Journal of Computer Information Systems*, 47(3):105–110, 2007.

[202] Kim Thomas. Building a secure home network. Technical report, SANS Institute, 2001.

[203] Jose M Torres, Jose M Sarriegi, Javier Santos, and Nicolás Serrano. Managing information systems security: critical success factors and indicators to measure effectiveness. In *International Conference on Information Security*, pages 530–545. Springer, 2006.

[204] Godwin J Udo. Privacy and security concerns as major barriers for e-commerce: a survey study. *Information Management & Computer Security*, 9(4):165–174, 2001.

[205] Blase Ur, Jonathan Bees, Sean M Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Do users' perceptions of password security match reality? In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 3748–3760. ACM, 2016.

[206] US-CERT. Home Network Security. `https://www.us-cert.gov/Home-Network-Security`, 2016. [Online; accessed on 10-November-2016].

[207] U.S. Department of Commerce, Economics and Statistics Administration. Computer and internet use in the united states: 2013. `http://www.census.gov/content/dam/Census/library/publications/2014/acs/acs-28.pdf`. [Online; accessed on 05-June-2016].

[208] Alladi Venkatesh. A conceptualization of the household/technology interaction. In *NA - Advances in Consumer Research*, volume 12, pages 189–194. UT : Association for Consumer Research, 1985.

[209] Alladi Venkatesh. Computers and other interactive technologies for the home. *Communications of the ACM*, 39(12):47–54, 1996.

[210] Alladi Venkatesh. Digital home technologies and transformation of households. *Information Systems Frontiers*, 10(4):391–395, 2008.

[211] Alladi Venkatesh, Erik Kruse, and Eric Chuan-Fong Shih. The networked home: an analysis of current developments and future trends. *Cognition, Technology & Work*, 5(1):23–32, 2003.

[212] Rossouw Von Solms. Information security management (3): the code of practice for information security management (bs 7799). *Information Management & Computer Security*, 6(5):224–225, 1998.

[213] Lorraine Olszewski Walker, Kay Coalson Avant, et al. *Strategies for theory construction in nursing*. Pearson/Prentice Hall Upper Saddle River, NJ, 6th edition, 2005.

[214] Jennifer L Ward. Persona development and use, or, how to make imaginary people work for you. Technical report, University of Washington, Washington, USA, 2010.

[215] Rick Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 11:1–11:16, New York, NY, USA, 2010. ACM.

[216] Rick Wash and Emilee Rader. Influencing mental models of security: a research agenda. In *Proceedings of the 2011 workshop on New Security Paradigms Workshop*, pages 57–66. ACM, 2011.

[217] Rick Wash and Emilee Rader. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security*, SOUPS '15, pages 309–325. USENIX Association, 2015.

[218] Ryan West. The psychology of security. *Communications of the ACM*, 51(4):34–40, 2008.

[219] Michael E. Whitman and Herbert J. Mattord. *Principles of Information Security*. Course Technology Press, Boston, MA, United States, 4th edition, 2011.

[220] George Whitson. Computer security: theory, process and management. *Journal of Computing Sciences in Colleges*, 18(6):57–66, 2003.

[221] Frank Wilcoxon and Roberta A Wilcox. *Some rapid approximate statistical procedures*. Pearl River: American Cyanamid Co. Lederle Laboratories, revised edition, 1964.

[222] Gordon B Willis. *Cognitive interviewing: A tool for improving questionnaire design*. Sage Publications, 2004.

[223] Dennis Wixon, Karen Holtzblatt, and Stephen Knox. Contextual design: an emergent view of system design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 329–336. ACM, 1990.

[224] Arnold Wolfers. " national security" as an ambiguous symbol. *Political Science Quarterly*, 67(4):481–502, 1952.

[225] ITU-T X.1111. Framework of security technologies for home network. Standard, International Telecommunication Union, Geneva, Switzerland, 2007.

[226] Kuai Xu, Feng Wang, Richard Egli, Aaron Fives, Russell Howell, and Odayne Mcintyre. Object-oriented big data security analytics: A case study on home network traffic. In *International Conference on Wireless Algorithms, Systems, and Applications*, pages 313–323. Springer, 2014.

[227] Kuai Xu, Feng Wang, and Xiaohua Jia. Secure the internet, one home at a time. *Security and Communication Networks*, 9(16):3821–3832, 2016.

[228] Kuai Xu, Feng Wang, and Michael Lee. Hometps: Uncovering what is happening in home networks. In *2012 IEEE Consumer Communications and Networking Conference (CCNC)*, pages 40–41. IEEE, 2012.

[229] Andreas Zimmermann, Andreas Lorenz, and Reinhard Oppermann. An operational definition of context. In *International and Interdisciplinary Conference on Modeling and Using Context*, pages 558–571. Springer, 2007.

[230] Mary Ellen Zurko. User-centered security: Stepping up to the grand challenge. In *21st Annual Computer Security Applications Conference*, pages 14–pp. IEEE, 2005.

[231] Mary Ellen Zurko and Richard T Simon. User-centered security. In *Proceedings of the 1996 Workshop on New Security Paradigms*, pages 27–33. ACM, 1996.