

Master's thesis

Fredrik Løvaas Theien

The Security Awareness of Smart Home Users in Norway

Master's thesis in Information Security

Supervisor: Vasileios Gkioulos

June 2020

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical
Engineering
Dept. of Information Security and Communication
Technology



Norwegian University of
Science and Technology

Fredrik Løvaas Theien

The Security Awareness of Smart Home Users in Norway

Master's thesis in Information Security
Supervisor: Vasileios Gkioulos
June 2020

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology



Abstract

A smart home may be a relatively new concept for many people. Under ideal circumstances, interactions between users and smart home devices should be done securely, or at least with some level of risk understanding. However, security awareness may not have matured in most people yet. Therefore, this thesis will seek to identify the current security awareness level of smart home users in Norway, as well as analysing their risk perceptions, to help professionals create efficient awareness training programs. These objectives include the identification of usage patterns, user motivations and routines which may impose risk amplification in their daily lives. To achieve the desired results, I utilised a quantitative methodology to assess the security awareness levels of smart home users in Norway. My results showed that the awareness level of smart home users in Norway is quite decent, especially for smart home enthusiasts. There was also a difference in how invested in the smart home ecosystem one are, and their security awareness level. Furthermore, I showed that the most common pitfalls included lack of network segmentation and password reuse. Lastly, my results suggest that loss of login credentials, unauthorised access to personal information, and malware are among the highest perceived risks for a smart home user.

Sammendrag

Et smarthus kan være et relativt nytt konsept for mange. Under ideelle omstendigheter bør samhandling mellom brukere og smarthusapparater gjøres sikkert, eller i det minste med en viss grad av risikoforståelse. Imidlertid er det ikke sikkert at sikkerhetsbevissthet har modnet hos folk flest ennå. Derfor vil denne avhandlingen forsøke å identifisere dagens sikkerhetsbevissthetsnivå for smarthusbrukere i Norge, samt analysere deres risikooppfatninger, for å hjelpe fagpersoner med å lage effektive opplæringsprogrammer for bevissthet. Disse målene inkluderer identifisering av bruksmønstre, brukermotivasjoner og rutiner som kan medføre økt risiko i brukernes daglige liv. For å oppnå de ønskede resultatene benyttet jeg en kvantitativ metodikk for å vurdere sikkerhetsbevissthetsnivået til smarthusbrukere i Norge. Resultatene mine viste at bevissthetsnivået til smarthusbrukere i Norge er relativt anstendig, spesielt for smarthusentusiaster. Det var også en forskjell i hvor investerte en er i smarthusøkosystemet, og deres sikkerhetsbevissthetsnivå. Videre viste jeg at de vanligste fallgruvene for økt risiko inkluderer blant annet mangel på nettverkssegmentering og gjenbruk av passord. Til slutt antyder resultatene mine at tap av påloggingsinformasjon, uautorisert tilgang til personlig informasjon og skadelig programvare er blant de høyest oppfattede risikoene for en smarthusbruker.

Contents

Abstract	iii
Sammendrag	v
Contents	vii
Figures	ix
Tables	xi
1 Introduction	1
1.1 Topic covered by the project	1
1.2 Keywords	1
1.3 Problem description	1
1.4 Justification, motivation and benefits	2
1.5 Research questions	2
1.6 Planned contributions	2
1.7 Structure of the thesis	3
2 Background and definitions	5
2.1 Smart homes	5
2.1.1 Definition	5
2.1.2 Smart home technologies	5
2.1.3 Smart home resident roles	6
2.2 Security awareness	7
2.2.1 Definition	7
2.2.2 Levels of security awareness	7
3 Related work	9
3.1 RQ1: What is the current security awareness level of smart home users in Norway?	9
3.2 RQ2: What are the most common pitfalls of smart home users in Norway which impose risk amplification?	10
3.3 RQ3: What do smart home users in Norway perceive being the highest security risks when using smart home devices?	11
4 Method	15
4.1 Choice of methods	15
4.2 Study population and sampling	16
4.3 Data collection	16
4.4 Data analysis	17
4.4.1 Analysis procedure	17

4.5	Ethical and legal considerations	18
5	Results	19
5.1	Demographics	19
5.1.1	Age	19
5.1.2	Gender	20
5.1.3	Highest completed education level	20
5.1.4	County	21
5.2	Background	22
5.2.1	How smart are the homes?	22
5.2.2	Household smart home administrators	22
5.2.3	Professional / hobby based background	24
5.2.4	Knowledge of subjects	24
5.3	Security awareness of the respondents	25
5.3.1	Use of Smart Home Devices	25
5.3.2	Credential management	29
5.3.3	Knowledge of smart home security aspects	31
5.3.4	Risk perceptions of the respondents	32
5.4	Bivariate analysis	33
5.4.1	Age differences	33
5.4.2	Education differences	35
5.4.3	Reasons for changing security and privacy settings	36
5.5	Control group analysis	38
5.5.1	Demographics	38
5.5.2	Analysis of differences to the main sample	40
5.5.3	Differences in the knowledge of certain topics and aspects	43
5.6	Specifications by the respondents in feedback	46
6	Discussion	47
6.1	Sample representativeness for smart home users in Norway	47
6.2	RQ1: What is the current security awareness level of smart home users in Norway?	48
6.3	RQ2: What are some of the most common pitfalls of smart home users in Norway which impose risk amplification?	50
6.4	RQ3: What do smart home users in Norway perceive being the highest security risks when using smart home devices?	51
6.5	Limitations	52
7	Conclusion	55
7.1	Future work	56
	Bibliography	57
A	Main questionnaire form	61
B	Control group questionnaire form	69
C	Bivariate analysis of age differences	79
D	Bivariate analysis of education differences	81
E	Analysis of changing settings and knowing data flow	83
F	Control group analysis	85

Figures

5.1	Age distribution	20
5.2	Highest completed education level	21
5.3	County population distribution	21
5.4	Household administrators of their smart home	23
5.5	The respondent's background in IT or technology	24
5.6	The respondent's knowledge of three different subjects	25
5.7	The respondent's routines towards updates their devices	26
5.8	The respondent's routines towards turning off features and services they do not use	27
5.9	The respondent's routines towards connecting smart devices to a separate home network segment	27
5.10	The respondent's routines towards changing their security and privacy settings	28
5.11	The respondents preference for cable or wireless when connecting their smart devices to the internet	29
5.12	The respondent's routines towards changing standard passwords	30
5.13	The respondent's routines towards using password managers	30
5.14	The respondent's routines towards using a password on multiple devices/services	31
5.15	Knowledge of different security aspects relating to smart homes	32
5.16	Respondents risk evaluation of different risk scenarios	34
5.17	ANOVA of age up against other variables	34
5.18	Age differences when it comes to knowledge of smart device security	35
5.19	Age differences when it comes to knowledge of risks by buying used smart devices	35
5.20	Age differences when preferring cable or wireless to connect to the internet	36
5.21	ANOVA of education up against the use of password managers	36
5.22	Education differences when it comes to using password managers	37
5.23	ANOVA of whether knowledge of data flow affects changing security and privacy settings	37
5.24	ANOVA of whether knowledge of data flow affects changing security and privacy settings	38

5.25	Age distribution of the control group in comparison with the main sample	39
5.26	Gender distribution of the control group	39
5.27	Highest completed education level of the control group	40
5.28	County population distribution of the control group	41
5.29	The part of the sample who reported to owning one or more smart devices	41
5.30	The knowledge of the control group respondents regarding different topics	43
5.31	Differences between the samples in the usage of a separate segment of the home network for smart devices	44
5.32	Differences between the samples in preferring cable or wireless to connect smart devices to the internet	45
5.33	Differences between the samples in using the same password on multiple devices/services	45
C.1	Descriptive statistics of age up against other variables	79
C.2	Post-hoc tukey of age categories up against other variables	80
D.1	Descriptive statistics of education up against the use of password managers	81
D.2	Post-hoc tukey of education categories up against the use of password managers	82
E.1	Descriptive statistics of changing privacy and security settings and knowledge of data flow	83
E.2	Post-hoc tukey of changing privacy and security settings and knowledge of data flow	83

Tables

5.1	Number of people who specified what smart device types they own	22
5.2	What types of smart devices the respondents own	23
5.3	Descriptive statistics of perceived risk from 8 risk scenarios	33
5.4	Number of people in the control group who specified what smart device types they own	42
5.5	What types of smart devices the respondents in the control group own	42
F.1	Descriptive statistics of perceived risk from my control group based on 8 risk scenarios	85
F.2	Frequencies of the control groups routines towards updating their electronic devices	86
F.3	Frequencies of the control groups routines towards turning off features and services they do not use	86
F.4	Frequencies of the control groups routines towards changing the privacy and security settings of their smart devices	86
F.5	Frequencies of the control groups routines towards using password managers	86
F.6	Frequencies of the control groups routines towards using the same password on multiple devices/services	87

Chapter 1

Introduction

1.1 Topic covered by the project

These days, more and more people are filling their homes with smart devices that ought to make their lives easier. However, many of these devices connect to the internet, which can impose a plethora of risks and attack vectors. Even the devices that do not connect to the internet have risk factors as well. Therefore, the topic of this thesis will look at the security awareness of people who utilises smart home Internet of Things (IoT) devices, as well as identify risks perceptions these users have when living in a smart home. I will explain the background of the topics further in chapter 2.

1.2 Keywords

Security awareness, Smart home, IoT, Risk perceptions.

1.3 Problem description

A smart home is a relatively new concept for many people. Ideally, the users should securely interact with the devices and understand the risk involved with doing so. However, this security awareness may not have matured in most people yet. This thesis will, therefore, seek to identify the current security awareness level of smart home users, as well as analyse risk perceptions that they might have, in order to enhance current security awareness programs, help vendors prioritise security features, and overall increase security awareness of consumers. These objectives include the identification of usage patterns and user motivations that can impose risk amplification in their daily lives, and also which self-reported security aspects that are considered most important to people. I also want to look at the balance between functionality and risk awareness to identify if the risk is accepted or if the users are oblivious to the risk.

1.4 Justification, motivation and benefits

With more and more households using smart home devices in their homes, the potential risk increases. In many aspects, the market for smart devices is increasing faster than what security can keep up with. In 2016 the DNS provider Dyn was targeted by one of the most significant DDoS attack in history [1]. The origin of this attack was an IoT botnet comprising, among other things, smart home devices like IP cameras, printers, and baby monitors. The botnet got access to the devices through brute-forcing default credentials that had not been changed by the user. Incidents like this reveal the severity of the issue. Some issues impact smart home owners in particular. For example, they have more devices to keep up to date, more devices to keep track of credentials on, larger attack surface, and higher consequence if an attacker gets access to ones home network. Therefore, this thesis will be about uncovering if users are aware of these types of issues and assess how they perceive these risks. These results will hopefully help both consumers to be more aware of the risks of owning a smart home, as well as provide security professionals with some data on how to prioritise awareness training. It will also help vendors explore what the consumers think are the most important things to focus on securing.

1.5 Research questions

Based on my problem description, I have identified a couple of research questions I want to explore when performing my project. The research questions are the following:

1. What is the current security awareness level of smart home users in Norway?
2. What are the most common pitfalls of smart home users in Norway which impose risk amplification?
3. What do smart home users in Norway perceive being the highest security risks when using smart home devices?

1.6 Planned contributions

In this section, I have compiled the contributions that are made in this thesis into tasks that were performed during this thesis. These tasks are as follows:

Task 1: Identification of definitions to smart homes and security awareness.

Task 2: Identification of related work regarding my research questions mentioned in section 1.5.

Task 3: Analysis of the current security awareness level of smart home users in Norway.

Task 4: Analysis of current usage patterns, motivations, and routines with negative security impact of smart home users in Norway.

1.7 Structure of the thesis

The report will start with a brief elaboration of the two main topics of my thesis in chapter 2. This elaboration is done to provide a foundation to build on and to make sure we are on the same page regarding certain concepts concerning the thesis. Further, in chapter 3 I will identify and explain the related work surrounding the concepts of my research questions in particular, in order to identify what has already been researched, and what parts of my research questions need further analysis. Moving on to chapter 4, I will describe the methodology I used to achieve the results, as well as why I chose the methods I used. The results I got from the method are presented in chapter 5, followed by a discussion on the results in chapter 6, which also include specific limitations to my thesis. Lastly, I summarise my thesis in the conclusion chapter 7 along with possible avenues for future work.

Chapter 2

Background and definitions

This chapter will introduce a brief background of the different topics my thesis will be about and provide definitions to make sure the reader understands the basic concepts. These topics are smart homes and security awareness.

2.1 Smart homes

Identifying the concepts regarding smart homes is essential to my thesis in order to help define the boundaries of the concept and agree on a common viewpoint.

2.1.1 Definition

According to IoT Agenda [2], a smart home is defined as:

“a residence that uses internet-connected devices to enable the remote monitoring and management of appliances and systems, such as lighting and heating.”

A smart home aims to provide the homeowners a sense of security, comfort, convenience and energy efficiency by allowing them to control smart devices through a smart home app on their smartphone or other networked devices [2]. Smart devices can often also operate together, sharing information between the devices and taking actions based on that information and the user’s preferences. The devices also exchange data with internal and external actors. These interactions can take place in mobile applications on end-user equipment such as smartphones and tablets, as well as remote services in the Cloud [3].

2.1.2 Smart home technologies

Smart home technology first came with the introduction of the communication protocol X10. This protocol utilised the existing electrical wiring of a home to send signals with information and commands to the automated devices. This innovation did not come without problems; however, as it was seen as unreliable at

times since electrical wiring was not designed to be free from radio-band noise, which could cause loss of signal. In 2005, a technology that combined electrical wiring with wireless signals was introduced. Other protocols, including Zigbee and Z-Wave, have since emerged to counter some of the problems with X10 [2]. Since then, smart home technology has entered most aspects of our daily lives, and recently, companies like Amazon, Google and Samsung have entered the market with their systems. Some examples of smart device types are:

- **SmartTV's:** which connects to the internet to access content such as video or music and some also include voice and gesture recognition.
- **Smart lighting systems:** which can be remotely controlled and customised to detect when people are in the room, and adjust lighting level as needed.
- **Smart thermostats:** which can monitor, remotely control and automatically adjust the home temperature.
- **Smart locks and garage door openers:** Which can control access, and also automatically detect the residents, so the door opens.
- **Smart security cameras:** which monitors their homes while away.
- **Household system monitors:** which can detect anomalies and turn of systems to prevent further damage in case of an electrical surge, or water failures.
- **Kitchen appliances:** which can automatically make coffee in the morning, or a refrigerator which keep track of expiration dates and can make shopping lists.
- **Robot vacuums or lawnmowers:** which can be remotely controlled and scheduled to perform their tasks automatically.
- **Smart voice assistants:** which can take commands by voice and control other devices.

2.1.3 Smart home resident roles

The paper by Mennicken and Huang [4] seeks to understand how smart home technologies are integrated into homes, as well as their effects on the residents. They conducted a qualitative study involving smart home providers and consumers. The main results were motivations for home automation, phases of making a smart home, and the different roles of the residents. Especially interesting is the identification of different roles within the household. Technologically competent people can generally be identified as home technology drivers, who show a keen interest in home automation. Household members with no technical background, but still have the primary responsibility of the home automation are categorised as home technology responsible. Most other users are categorised as passive users, except for guests and children.

2.2 Security awareness

This part will focus on briefly describing security awareness (SA) as a concept, and focuses on the aspects that are relevant to the work I will be doing in my thesis.

2.2.1 Definition

To understand and define security awareness, we need to look at awareness as a concept. Awareness has its roots in the behavioural theory of psychology and refers to the state resulting from the acquisition of knowledge, norms, or practises [5]. The acquisition is a personal process connected to intimate factors that characterise not only the individual but the overall group. There are three elements of this process [5]:

- **Knowledge:** which indicated the process by which an individual learns the existing standards, norms, and procedures that are desirable to ensure both the environment and operations.
- **Attitude:** which is connected to the consciousness of an individual and refers to the perception the latter has about the object of interest. In the case of security, it comes from the belief that security norms are useful. The group culture deeply influences the attitude.
- **Behaviour:** which is the actions that are taken based on the consciousness of an individual, which are the consequence of the shared values of a group.

The security awareness is, therefore, the concept of awareness explicitly applied to the field of security, and especially cybersecurity.

2.2.2 Levels of security awareness

According to an article by Shaw et al. [6], the level of security awareness (SA) can be broken down into three different levels:

- **Level 1 SA: perception** the ability to sense and detect potential security risks, and to achieve an understanding of the presence or awareness of a threat.
- **Level 2 SA: comprehension** the ability to comprehend, understand and assess the dangers posed by different threats. This ability includes ensuring that users know how to integrate information from multiple sources and interpret them in the right direction.
- **Level 3 SA: projection** the ability to project or predict the future course of security attacks. The ability to anticipate future situational events indicates that users have the highest level of understanding of their surroundings [6].

Chapter 3

Related work

This chapter will go over related work that has been previously done on the topic of my thesis. I will systematically go through the research questions and uncover topics that are relevant to them when talking about the literature that is out there. I will delve into each of the research questions to figure out to what extent information in the literature can provide answers to the research questions I identified, and which areas or research questions the literature provides insufficient information.

3.1 RQ1: What is the current security awareness level of smart home users in Norway?

The paper by Kang et al. [7], makes use of mental models to assess the participant's knowledge of the Internet, and how the level of knowledge affect their privacy and security decisions. People with more articulated mental models perceived more privacy threats, possibly because of better knowledge on where the specific threats could occur. However, the study did not find any connection between people's technical background and the security measures taken to control their security and privacy online. Mental models could be an exciting method to consider when assessing the knowledge of a smart home, and the relation this has to a participant's security awareness levels.

The aim of the paper by Drevin et al. [8] is to introduce a value-focused assessment methodology when identifying ICT security awareness aspects. The approach focuses on identifying the stakeholders that would be impacted by the decisions and questioning them about their values related to the area of interest. These values are then used to identify objectives like maximising the confidentiality and integrity of data. For my thesis, it could be interesting to consider taking a value-based approach when assessing security awareness and especially the risk perceptions of smart home users.

In a study by McReynolds et al. [9] they focus specifically on the privacy concerns, expectations and security awareness of using connected toys and gadgets

for the home that can listen to a person speak. As they are waiting for voice commands, they are similar to voice assistants in that they blend into the background and are always listening. The study consisted of interviews with parent-child pairs in which they interacted with familiar connected toys. The results were that the children were often unaware that others might be able to hear what was said around the toy, and many parents voiced privacy concerns.

Another paper by Gerber et al. [10] also focuses on the privacy threats of a smart home. They found that most people were unable to state even a single privacy consequence, and most people listed quite general privacy issues like profiling and data collection but also threats not related to privacy in particular.

There exist prior studies that also focus on security awareness in Norway, specifically. Gunleifsen [11] addresses the level of security awareness, perception, and culture of users of ICT in Norway and whether it can be improved. The paper covers different aspects of security awareness, such as general security knowledge, self-evaluation of risk, and different behavioural patterns in regards to WiFi connections, authentication routines and phishing awareness. The findings can be summarised with the fact that the level of security awareness can be significantly improved; however, the results were better than similar national studies.

A study by Ghiglieri et al. [12] focused on exploring consumer awareness and attitudes of Smart TV related privacy risks. The study was conducted in three steps with questionnaires. The first aimed to assess the awareness of privacy-related risks of using a Smart TV, which showed a meagre level of awareness. The main findings of the second part include that the consumers were generally unwilling to give up the functionality of a Smart TV for the sake of privacy. Lastly, respondents were asked to choose between five different SmartTV Internet connection options, in which two retained functionality, however, included using extra time and effort to preserve privacy. The results from this showed that they were willing to use some extra time and effort, but only if the functionality was not impaired.

Another paper also focuses on the consumer perspective, regarding awareness of botnet activity of consumer IoT devices. In the study by McDermott et al. [13] they assessed user ability to detect threats in their smart devices. The conclusion was that it was challenging for the consumers to detect and be aware of whether or not a device was infected without any apparent signs. Interestingly, they also discovered that there was no correlation between the level of technical knowledge and the ability to detect these infections.

3.2 RQ2: What are the most common pitfalls of smart home users in Norway which impose risk amplification?

Not many papers focus specifically on the mistakes or bad habits of smart home users. However, these bad habits could somewhat be inferred by combining security awareness research and vulnerability assessments on smart homes.

In a recent article, Awad and Ali [14] seeks to identify possible security risks in order to understand the current security status of smart homes. They apply the operationally critical threat, asset, and vulnerability evaluation (OCTAVE) methodology, which focus on information assets concerning different information containers. The main results from this assessment were a list of threats ordered by risk score. The highest scoring threats were related to unauthorised access and execution of operations, as well as loss of control.

Another article, by Denning et al. [15], also highlights security risks associated with using home technologies. The article explores the landscape of technological attacks on smart homes, identified key features in devices that make them more vulnerable and human assets at stake. Using these three concepts, they applied their framework to three example technologies, a wireless webcam toy, a wireless scale, and a home automation siren. This framework can be used to determine risk areas of different devices, and therefore also potential pitfalls the users can fall into.

A paper by Caviglione et al. [16] analyses the human-related aspects of security and privacy threats in smart environments and reviews the significant risks arising from using such devices, emphasising networking. It takes a role-based approach, focusing on vendors, customers, operators and deployers. The results show that each group have their pitfalls, and for customers, this is projected as a lack of awareness. This, in turn, affects the other roles as customers will not demand better security on their products since they are unaware of the insufficiency. It also emphasises that security should come from the other groups than customers since awareness campaigns have had little effect.

3.3 RQ3: What do smart home users in Norway perceive being the highest security risks when using smart home devices?

First, let us look at some studies about risk perception in general. A quantitative empirical study by Schaik et al. [17] analysed the perceptions of risk several students had towards a set of 16 different security risks. The results of the study concluded that the highest perceived risks were identity theft, keyloggers, cyberbullying, and social engineering. It also identified predictors of perceived risk, which were voluntariness, immediacy, catastrophic potential, dread, the severity of consequences and control, as well as Internet experience and frequency of Internet use. Control was also a significant predictor of precautionary behaviour.

Another paper, written by Conti and Sobiesk [18], aims to identify user perceptions on web-based information disclosure. The paper assumes that we face a growing tension between privacy concerns of individuals and financial motivations of organisations, and seeks to explore these issues through querying students about their risk perceptions. The results can be summarised that the students believe that an honest man has nothing to fear, which were mostly contradictory

to beliefs of security and privacy professionals. This result is similar to the issue raised by Solove [19], where he tries to break the argument apart and counter it.

Some studies have also been conducted with a focus on risk perception in smart homes, like the article by Zeng et al. [20]. It focused on the disjointed perception of risk between the end-users and security experts and was conducted using semi-structured interviews with 15 people living in smart homes. Similarly to many other studies mentioned in this chapter, it utilised mental and threat models to assess security awareness. The results included a gap in threat models due to limited technical understanding and awareness of some security issues but limited concern. The study also revealed that the participants have varied threat models and do not share a common set of concerns when it comes to risk perceptions. However, some of the threats were video/audio recording, adversarial remote control, network attack, spying by other users in the household, and account/password hacking.

As the previous paper slightly touches on, there also seem to be a concern that people in the same household violate each others privacy. The paper by Ur et al. [21] focuses specifically on how the deployment of connected locks and security cameras in a smart home may impact a teenager's privacy and in turn the relationship between parent and teen. They conducted a series of interviews with teenagers and parents and investigated reactions to audit logs of family members. The parents wanted audit logs with photos, but teenagers preferred only text logs or no logs at all and were averse to include photos.

Another paper [22] written by students at the University of Tromsø touches on risks related to the procurement of a smart home, specifically about perceived risk from privacy and security issues. They asked questions about how much users trust that the data security and privacy are safeguarded in a smart home system, and how much this affect their willingness to procure a smart home. The conclusion is that most respondents are either sceptical or unsure as to whether the smart home safeguards their privacy and security. It also shows that most people do take into consideration the privacy and security of the smart home system before procuring it for themselves.

A study by Brush et al. [23] sought to get insight into the challenges and opportunities of home automation in order for smart homes to become amenable for broader adoption. They conducted a series of home visits to households with home automation and identified four barriers. These were high cost of ownership, inflexibility, poor manageability, and difficulty of achieving security. For the security barrier, the participants were especially worried that remote access to their smart devices introduced security risk, even though the functionality was very appealing.

There have also been some studies regarding risk perceptions of IoT security in other aspects of society, especially regarding critical social services. In particular, a study by Asplund and Nadjm-Tehrani [24] presents the perceptions and attitudes on the security of IoT and relates them to the current challenges of IoT in general. The paper demonstrated optimism in the utility of such devices; however, there

was a lack of consensus regarding the risks. It also showed that many people did not believe there are any significant risks associated with IoT since the risk factors are already accounted for in regular system design.

In another article by Gerber et al. [25] peoples privacy risk perceptions were assessed in relation to, but not limited to, smart homes. They found that when users assess their risk perception, they are more likely to perceive higher risk from more specific scenarios, whereas abstract scenarios were deemed less severe. This could mean that people do not seem aware of specific privacy risks when confronted with an abstract risk scenario.

Chapter 4

Method

This chapter will go over the methods I used when performing the study and will cover how to identify, construct, and conduct the study population and sampling, the data collection, and the data analysis. First of all, I give the reasoning for the methods that I chose, and how they are appropriate for the research questions and the procurement of the desired results.

4.1 Choice of methods

The paper by Rahim et al. [26] reviews approaches to assessing cybersecurity awareness. The authors captured 23 studies from 2005 to 2014 and categorised them by assessment method, target audiences, coverage of assessment and assessment goals, among other things. It found that very few studies focused on youngsters and on the issue of protecting personal information, while most studies are focused on organisations. The value in this paper is a taxonomy of methods which can be used as inspiration. One of the target audiences are home users, which is what my thesis will focus on, and most of these studies used a survey-based questionnaire, which could indicate that this is a good option. However, it can also mean that there should be some diversity in the methodology targeting these groups. Other papers, which had similar goals to mine, used questionnaires for the most part.

In the sections below, I argue for the use of this method to answer my research questions.

RQ1: What is the current security awareness level of smart home users in Norway?

A quantitative method is appropriate for investigating the security awareness level since one can quantify the specific levels with numbers. This method can lead to a more accurate representation of their security awareness, rather than if I had to infer it by qualitative analysis.

RQ2: What are some of the most common pitfalls of smart home users in Norway which impose risk amplification?

When using a questionnaire, one can ask questions that seek to uncover different usage patterns and user behaviours. Risk experts mostly know what types of behaviour that can impose risk amplification. Therefore, using predefined answers will be able to uncover the common pitfalls of smart home users.

RQ3: What do smart home users in Norway perceive being the highest security risks when using smart home devices?

By identifying related work on risk perceptions, I have uncovered a sizeable amount of potential risk scenarios which can be used to verify what risks are perceived as the highest by the respondents. These results can be presented to the respondents as a series of risk scenarios where they will rank them on a Likert scale to determine their perceived risk.

Final thoughts

In addition to the thoughts above, I may also need to include a question where the respondent can voice their thoughts freely on the questionnaire in order to fully cover these research questions, and possibly other things I may have missed. This solution will slightly reduce the negative aspects of a survey-based data collection in comparison to a semi-structured interview.

4.2 Study population and sampling

The data gathering methodology will include a questionnaire given to a sample of the Norwegian population. I utilised non-probability sampling since the target group comprises people who own and use smart home devices in their daily lives. Furthermore, the sample was constructed as a convenience sample due to the difficulty of reaching out to other sample types. When creating the sample, it is essential to note that the response rate is about 10-15 per cent; therefore, the sample size must be ten times the expected response.

4.3 Data collection

To collect the data for my thesis, I used a questionnaire as the primary quantitative research method. In order to answer the research questions, I created several hypotheses' to aid in measuring the security awareness level, as well as the most common pitfalls and highest perceived risks. Since this is a quantitative approach, I used close-ended questions, which means that responses are predefined. The distribution vector was through a Facebook group for smart home enthusiasts in Norway, which contained between eight and nine thousand people at the time of

distribution. The tool for creating the questionnaire was Nettskjema, which is an NTNU affiliated resource. In addition to the primary data collection, I also collected data from a control group to compare results. The distribution vector for this sample was my network on Facebook, so it may contain bias. The questions for this sample was reformatted to be receptive for respondents who do not own any smart devices, although they still try to measure the same aspect. Some of the questions that cannot easily be changed to fit both groups were made only to be answered by people who own smart home devices.

When creating the questions, I relied on a couple of sources as guidance. In order to assess the security awareness, I relied on a document from ENISA called “Security and Resilience of Smart Home Environments: Good practices and recommendations” [3]. In Annex D of this document, they go over topics for user awareness and best practises for the consumer. This annex explains how to choose, operate, and use online services for smart home devices securely. I have based the questions on these practises collecting the necessary data about the user’s security awareness level. I also used other sources [14] [16] [17] to create questions from. Especially when it comes to finding risk scenarios, which I will ask the respondents to rate according to their perception of the risk. Additionally, I also brainstormed topics for questions.

The final questionnaires that were used for the primary sample and the control group are included in Annex A and Annex B.

4.4 Data analysis

When analysing the data, it is crucial to understand that biases may exist and that an either-this-or-that dichotomy is not necessarily the best way to think about it. According to a book by Leedy and Ormrod [27], quantitative researchers may use a constructivist framework when approaching a research question, while qualitative researchers usually think in a postpositivist manner. However, many also acknowledge that both absolute truths may exist, and that self-constructed beliefs and biases are legitimate objects of study in itself. This way of thinking is usually labelled as pragmatism and realism and is the general mindset I will focus on while analysing the data. The number of respondents (N) of each sample was 222 for the primary sample, and 43 for the control group.

4.4.1 Analysis procedure

For analysis, I used the statistical program IBM SPSS, as well as Excel spreadsheets and other minor tools. In the following sections, I will give a summary of the statistical methods that I used in the analysis.

I started analysis of every question with a descriptive analysis, seeking to identify the distribution in percentage and count. Further, I have performed a univariate analysis of individual questions and visualised the results mostly in regular

vertical bar charts; however, I also used tables and stacked horizontal bar charts where appropriate.

After these questions were analysed, I performed a bivariate analysis of multiple questions to search for differences and similarities between, for example, categorical groups and continuous variables. I did this to test the hypothesis that there were differences between the groups. The null hypothesis I used was that there is no significant difference between the groups. When doing the analysis, the yes and no answers were given the values of yes = 1 and no = 2. In questions where knowledge was analysed, I gave the knowledge levels the values of 1 to 4. I have used ANOVA (analysis of variance) to check for statistical significance, in which I used the standard $P = 0.05$. P stands for probability and indicates how probable it is that the results are due to chance alone. When P is less than 0.05, it means that the probability of this result being due to chance is less than 5%, and provides a good argument for discarding the null hypothesis. I started by performing ANOVA with demographics data as the independent variable, which was cross-checked with all the relevant questions. Then I moved on to other variables I found could be interesting to look at during the univariate analysis.

I analysed the control group in the end and performed a univariate analysis of the questions which I compared to the results in the primary sample. I first looked at the demographics and background of the sample to get an overview of how it looked. Then I went through every question and compared the distribution to the primary sample and noted the questions that had the most substantial divergent answers and reported on those.

Many have criticised the use of ANOVA of ordinal data like Likert-scales, small sample sizes, unequal variances, and non-normal distributions, and says that parametric statistics cannot be used because of this. However, a Paper by Norman [28] breaks down these arguments and shows that parametric statistics are robust, and can be used without concern for getting wrong answers. This position is also consistent with empirical literature dating back nearly 80 years [28].

4.5 Ethical and legal considerations

This thesis will collect data about respondents who need to be anonymous. I also need to consider the privacy aspect of the information I collect. For legal considerations, I need to avoid collecting data which can turn out to be identifiable if put together since the data should be anonymous. The project was reported to the Norwegian Center for Research Data (NSD), and the project was approved. Initially, I wanted to let the people leave their email addresses if they wished to receive the report when finished since I assumed many people in my sample would think it would be interesting to read. However, I later removed this option in order to make the questionnaire completely anonymous.

Chapter 5

Results

This chapter will introduce the results of the data analysis. I will touch on some topics for discussion for some of the results; however, most of the discussion will take place in chapter 6. This chapter will start by describing the demographics and background of the primary sample. Further, I will present the results from the univariate analysis that assess the security awareness of the respondents. Next, I present my findings from the bivariate analysis, and lastly present and compare the results from the control group sample.

5.1 Demographics

The following section will describe the demographics of my samples, as well as compare relevant groups to each other and the Norwegian national population. Out of the total of 222 people who answered, one person did not want to specify any demographic data.

5.1.1 Age

In the age distribution of my sample, none of the respondents reported being under 20 years old. 33 (14.9%) of the respondents answered being between 20 and 29 years old, and a whole 102 (45.9%) responded that they are between 30 and 39 years old, which is the largest age group of our sample. Further, 56 (25.2%) people answered being between 40 and 49 years old, which is the second-largest age group. Lastly, 24 (10.8%) of my sample is between 50 and 59 years old and 6 (2.7%) people being 60 or older.

As we can see from figure 5.1, we have a reasonably middle-aged sample compared to the national population [29], which has a sizeable difference in younger and older people compared to my sample.

Since the number of respondents being 60 or older in my sample only comprise 6 respondents, I will merge that category with 50-59 years going forward, resulting in a single category of 50 or older. This will result in the category comprising

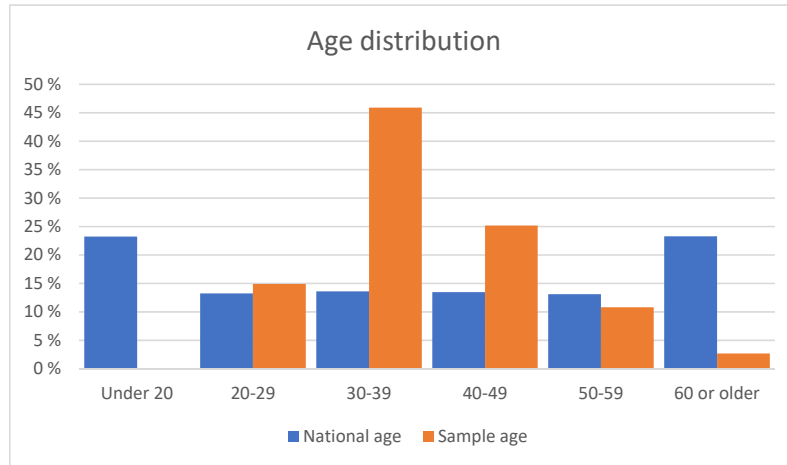


Figure 5.1: Age distribution

30 respondents, which should be the minimum for further analysis between the groups.

5.1.2 Gender

The gender distribution of my main sample is all men. There was also one respondent who did not want to specify; however, there are no women in my sample. This gender distribution makes it impossible to use in further analysis other than for sample description. This distribution is a huge deviation from the national average of approximately 50% of each gender.

5.1.3 Highest completed education level

None of the respondents answered that they had only primary school education or no education, and only one person did not want to specify their education level. 48 people (21.6%) answered that they had completed high school, while 55 of the respondents (24.8%) has completed vocational college. 76 people (34.2%) has completed at least four years of university or college, and 42 (18.9%) has completed university or college for longer than four years.

From figure 5.2 above, we can see that my sample contain a higher share of people with higher education compared to the national population [30]. The most interesting fact is that the data shows a huge difference when it comes to people reporting to having a vocational education.

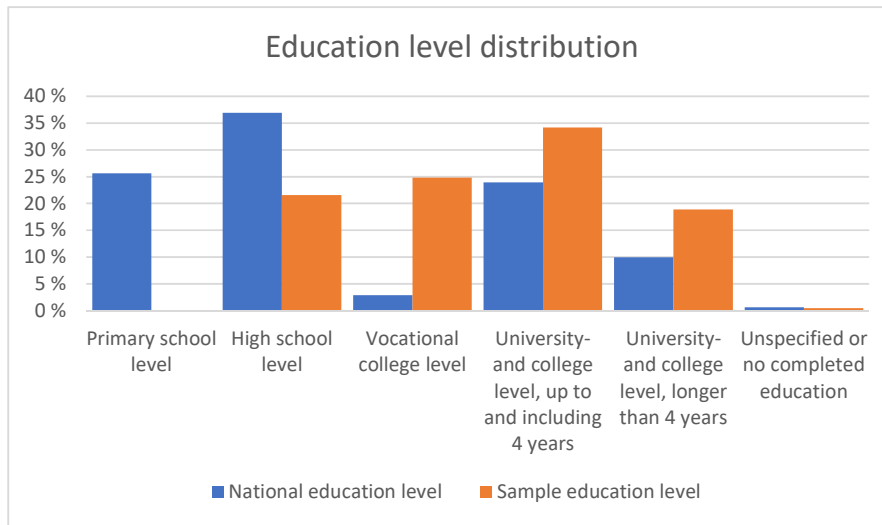


Figure 5.2: Highest completed education level

5.1.4 County

There were two people who did not want to specify which county they lived in. The sample distribution in figure 5.3 below shows that it is very close to the national distribution [29]. The only significant outlier is that my sample has a bit more people from Rogaland (14%), compared to the national level (9%).

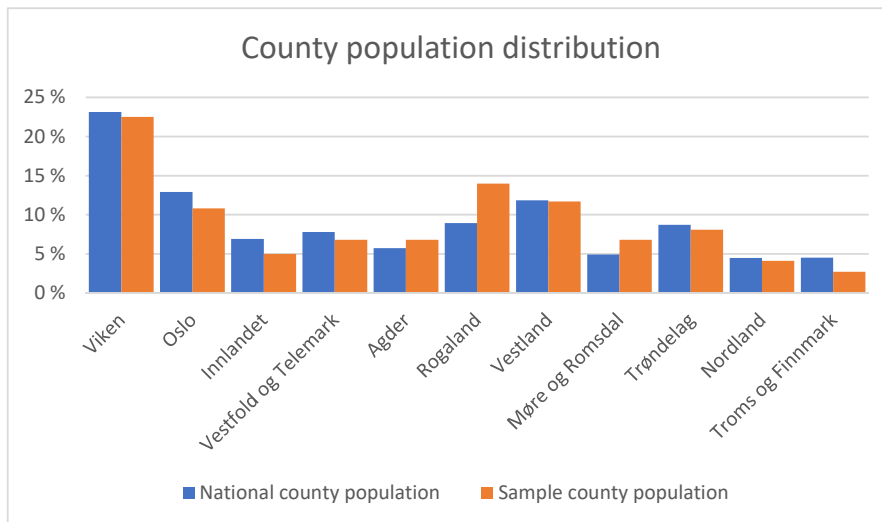


Figure 5.3: County population distribution

It should be mentioned that most of the categories from my sample has less than 30 answers, which might impact the comparability of the numbers. For example, Troms og Finnmark only has 6 respondents in my sample, and Nordland

has 9 respondents. At the other end of the spectrum lies Viken with 50 respondents and Rogaland with 31 respondents.

5.2 Background

5.2.1 How smart are the homes?

In order to investigate how invested people are in the smart home ecosystem, I chose to include a question that aimed to assess which smart device types the respondents own. In table 5.1 below is an overview of the number of respondents that answered this question.

Case summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Smart devices	219	98.6%	3	1.4%	222	100.0%

Table 5.1: Number of people who specified what smart device types they own

Out of the three that did not answer, two of them specified in the free text that they used a KNX system with control of heating, lighting, and ventilation, as well as motion sensors among other things. Multiple people who answered, also specified in the free text that they used a KNX system, and many others specified that they had a smart home with basically “everything”. One respondent answered that they had no smart devices. The table below shows the frequency of which types of smart devices the respondents owned.

Here, N shows how many responses of each category there was. People were allowed to make multiple choices, so the total amount of answers amounts to 2310. Considering that 219 people answered this, we can see that on average, every respondent chose a little over ten device types. The per cent of cases shows us the per cent of the respondents who chose each category. We observe that it was prevalent for the respondents to have a Smart TV (84%), smart dimmers (82.6%) and switches (80.8%), as well as motion sensors (80.8%). It was however uncommon for people to have smart kitchenware, with only 18.7% responses. Only two categories were not chosen by at least 50% of the respondents.

Several people also specified further devices in the free text section.

5.2.2 Household smart home administrators

I asked a question regarding whether or not the respondents were the administrators of their smart home. My hypothesis in advance was that the vast majority were the smart home administrators of their household solely since I collected my sample from a social media group of smart home enthusiasts. As we can see from figure 5.4 below, this turned out to be correct.

Smart device types frequencies				
		Responses		Percent of Cases
		N	Percent	
Smart devices	Voice assistant	155	6.7%	70.8%
	Speaker	158	6.8%	72.1%
	Robot vaccum	123	5.3%	56.2%
	Smart hub	169	7.3%	77.2%
	Smart TV	185	8.0%	84.5%
	Smart screen	69	3.0%	31.5%
	Router	143	6.2%	65.3%
	Door lock	149	6.5%	68.0%
	Light bulbs	163	7.1%	74.4%
	Smart dimmer	181	7.8%	82.6%
	Smart switch	177	7.7%	80.8%
	Kitchenware	41	1.8%	18.7%
	Surveillance	138	6.0%	63.0%
	Alarms	111	4.8%	50.7%
	Motion sensors	177	7.7%	80.8%
Thermostat	171	7.4%	78.1%	
Total		2310	100.0%	1054.8%

Table 5.2: What types of smart devices the respondents own

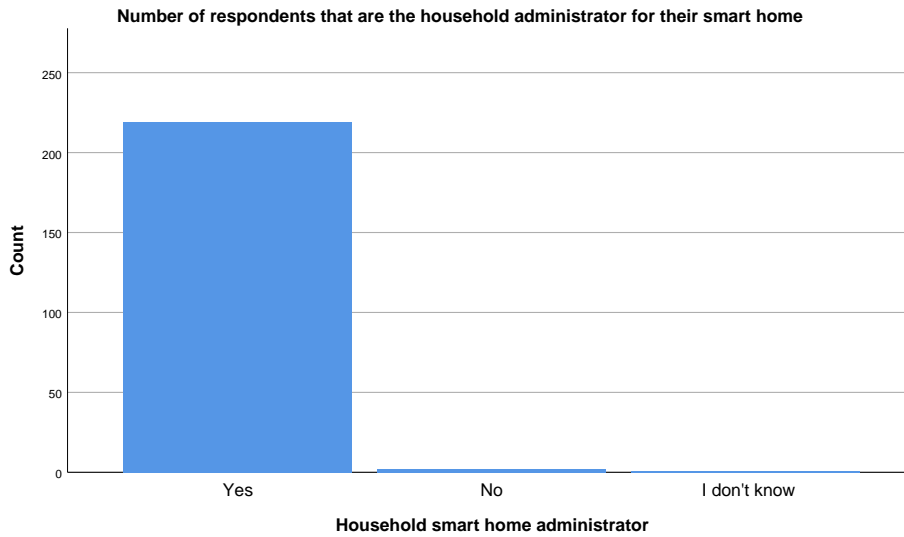


Figure 5.4: Household administrators of their smart home

Out of the total of 222 people who answered, 219 (98.6%) of the respondents said that they were the smart home administrator of their household. Only 2 people said no, and the last one said that they did not know. This shows us that

the people in this study are active users and not passive ones.

5.2.3 Professional / hobby based background

I asked a question to figure out if the respondents had a background in technology, either a professional one or as a hobby. I hypothesised that most people would have a background in technology since that is how one gets exposed to and interested in devices like those in a smart home. From figure 5.5 below, we can see that most people do have a background in technology. Out of the total

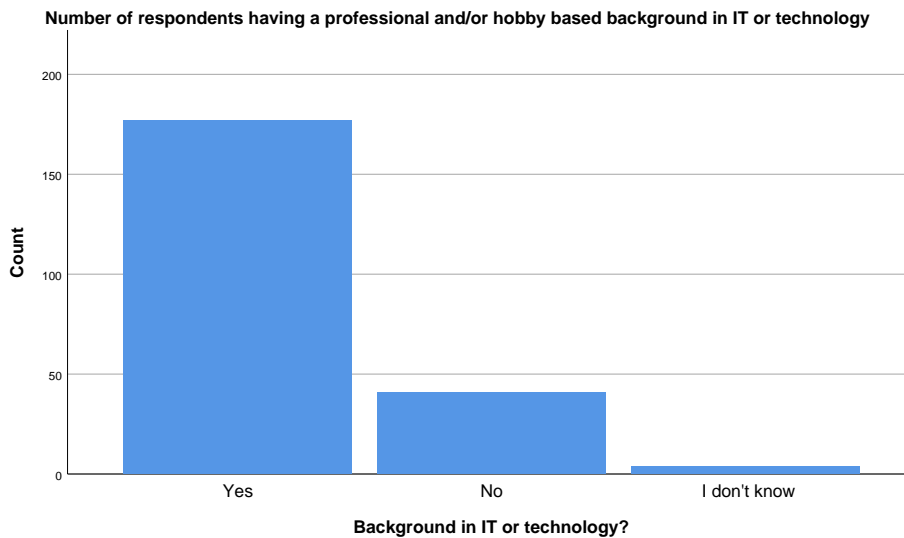


Figure 5.5: The respondent's background in IT or technology

of 222 people who answered this question, 177 respondents (79.7%) said yes, and 41 people (18.5%) answered no. The last four people said that they did not know. This shows us that the sample consists of many people from a technological background.

5.2.4 Knowledge of subjects

In addition to the previous questions, I also wanted to assess the respondent's knowledge of certain subjects relating to smart home security. This is, of course, only self-reported knowledge. I hypothesised that they know a lot about technology and smart homes, but not that much about data security. We can see that the hypothesis was mostly correct based on figure 5.6 below.

159 (71.6%) of the respondents answered that they know technology well, while another 51 (23%) claims to know it. This amounts to 94.6% of the respondents alone. Regarding data security, 90 people (40.5%) said they know it well, while 88 people (39.6%) responded that it was known to them. This is considerably less than with technology but still reasonably good as it amounts to around

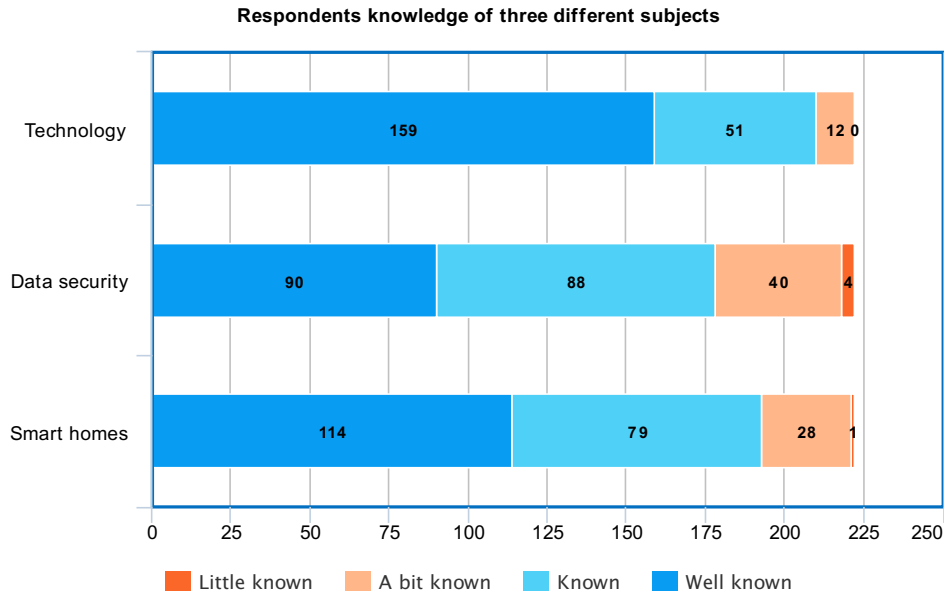


Figure 5.6: The respondent's knowledge of three different subjects

80.2%. Lastly, 114 respondents (51.4%) answered that smart homes were well known to them, while 79 people (35.6%) responded that it was known. These results are more than data security, however still significantly less than technology. While still being partly correct in my hypothesis, it was surprising that the knowledge of smart homes was not closer to technology for a sample specifically interested in smart homes. This result could have many explanations, such that there are people that joined the Facebook group in order to learn, so they might not be experts yet. Another explanation could be that they underestimate their expertise, and overestimate what they do not know. This concept has been proven to be the case in multiple studies previously [31] [32].

5.3 Security awareness of the respondents

In this section, I will perform a univariate analysis of the questions in the primary survey that includes data that can be used to describe the security awareness of the sample. This analysis is broken down into four parts: the respondents use of smart home devices, their credential management, knowledge of different smart home security aspects, and risk perceptions based on a few given risk scenarios.

5.3.1 Use of Smart Home Devices

The first question aims to identify the respondent's routines when it comes to regularly updating their smart devices. I initially hypothesised that most people do

update their devices, but that the majority wait a while before doing so. The results are visualised in figure 5.7 below. A total of 138 people (62.2%) answered

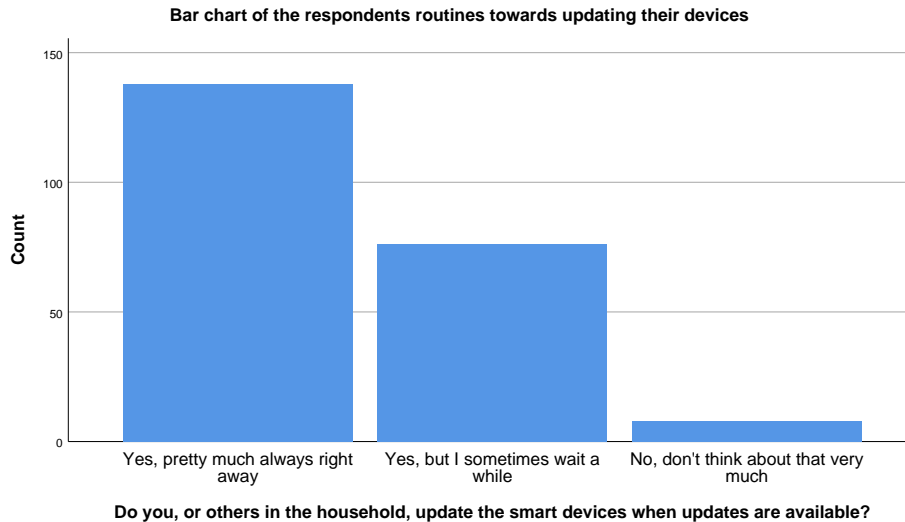


Figure 5.7: The respondent's routines towards updates their devices

that they pretty much always update their devices right away, and 76 people (34.2%) said they do update their devices regularly; however, they sometimes wait a while. Only 8 people (3.6%) responded that they do not think about updating their devices that much. These results did not confirm my hypothesis and showed that the majority try to update their devices regularly, even though a significant portion (34.2%) sometimes waits a while before doing so.

The next question aimed to quantify how many people interact with the settings and turn off features and services they do not use regularly. My initial hypothesis for this question was that most people did not turn off features they do not use. The results from this question are displayed in figure 5.8 below. For this question, 147 people (66.2%) confirmed that they turned off features and services they did not use, and 68 of the respondents (30.6%) denied doing so. Only 7 people (2.3%) did not know whether they did so or not. This is the opposite result of what I had as my hypothesis and shows that most people are mindful about what services they keep running that they do not need. However, this also shows that almost one-third of my sample could have an amplified risk profile due to this.

Some [3] consider it best practise to segment their home network when one has multiple device types that access the network, for example connecting smart devices to the network. Therefore, I asked the question if the respondents used a separate segment of their home network for their smart devices. My initial hypothesis was that most people did not segment their network for this purpose. The results are visualised in a bar chart in figure 5.9 below. The answers show us that 90 people (40.5%) use a separate segment of their home network when

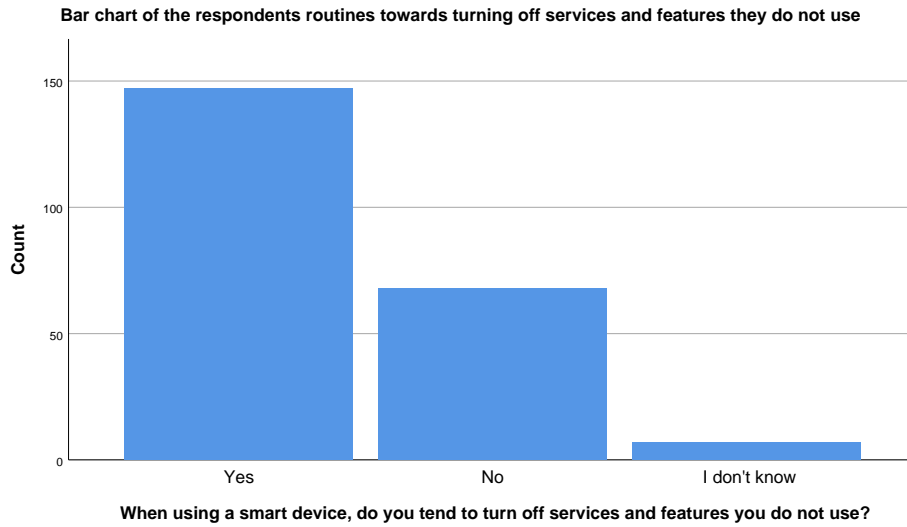


Figure 5.8: The respondent’s routines towards turning off features and services they do not use

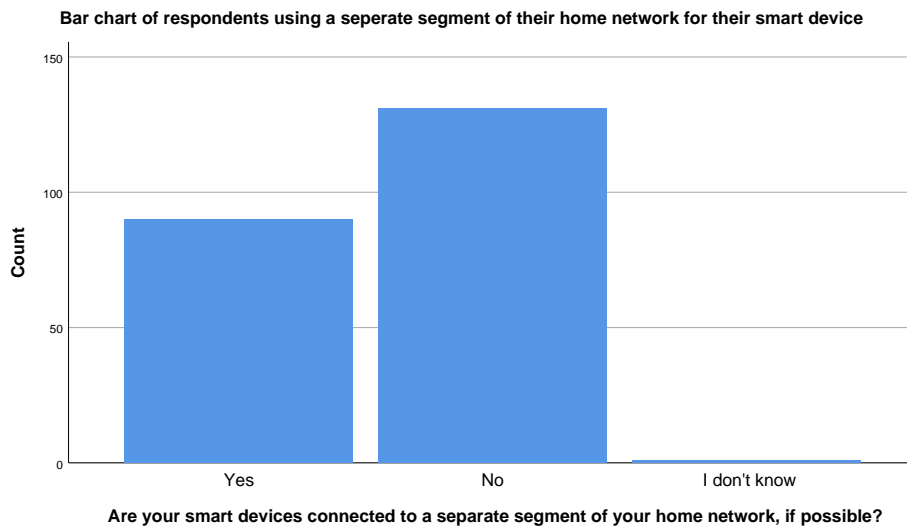


Figure 5.9: The respondent’s routines towards connecting smart devices to a separate home network segment

connecting their devices to the network, and 131 people (59%) does not. Only 1 person answered that they did not know. This confirms my hypothesis; however, it was a bit closer than initially expected. The results could indicate that most people either do not know that this is best practise, or that they lack the necessary networking knowledge to make it happen, despite it being much easier for a consumer to do than before.

Another aspect I wanted to explore in regards to smart home device usage was the respondent's routines towards changing their security and privacy settings. A significant part of security awareness is the conscious decisions one make about security and the risks one choose to accept or not. Privacy concerns have gotten some attention from the media lately [33] [34], so I hypothesise that the majority actually change or at least validate their privacy and security settings, either to give out more or less information. The results are visualised in figure 5.10 below. From the sample, we observe that 125 people (56.3%) answered that they do

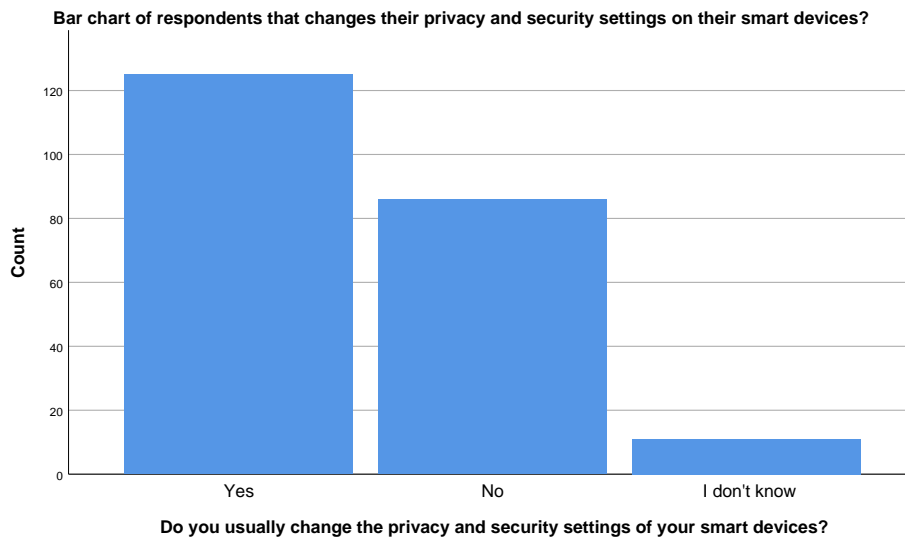


Figure 5.10: The respondent's routines towards changing their security and privacy settings

change the privacy and security settings on their smart devices, and 86 people (38.7%) answered that they did not. Only 11 people (5%) responded that they did not know. This confirms my hypothesis that the majority care about changing their privacy and security settings, although not by a large margin. Even though almost 40% does not change their settings, we do not know whether this is an accepted risk, or just due to not knowing what data is being shared or not caring. This issue could be interesting to look at further as bivariate analysis.

Lastly, for device usage, I wanted to explore the respondent's preference in what they use to connect their smart devices to the internet, and asked them if they preferred cable or wireless where possible. I hypothesised that they would largely prefer wireless since it would be easier to set up, and less hassle without cables lying around. Of course, some devices only connect using one of the methods, and that is why I included "where possible" in the answers. The results are shown in figure 5.11 below. Surprisingly, 142 people (64%) preferred cable, and 46 people (20.7%) preferred wireless. Also, 31 respondents (14%) answered that it was not important to them how they connected their devices to the internet. The last 3 people answered that they had some other thoughts on the matter, with one of

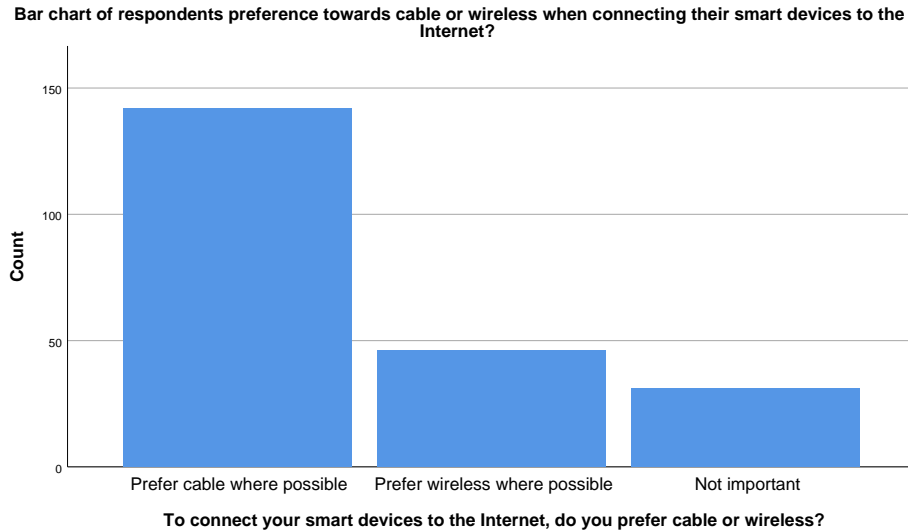


Figure 5.11: The respondents preference for cable or wireless when connecting their smart devices to the internet

them specified in the free text that their devices were not connected to WAN, and another that none of his smart home devices is allowed access to internet. The last person did not include any additional thoughts. According to ENISA [3], the best practice is to use cable where possible, so this is not a pitfall many people fall victim to.

5.3.2 Credential management

One thing I wanted to explore about peoples password routines was whether they changed the default password on the smart devices after purchase. Many products prompt the user to set or change the password after initialisation. Therefore, my hypothesis is that a large majority do change the default password on recently purchased devices. The results are displayed in figure 5.12 below. A total of 186 people (83.8%) answered that they did change the default password, while 21 (9.5%) said they did so only if the device did not come with a unique password when purchased. Only 14 people (6.3%) answered that they did not change the password, and the last person was not sure. This result shows that my hypothesis was correct in that a vast majority do change the default password, and it was, in fact, over 90% of the respondents in total.

Next, I wanted to know if the sample used a password manager to store their password in. Once again, this was asked as a binary type yes/no question; however, I allow an option for people who do not know about password managers. My hypothesis was that most people do not use password managers, and also that a significant number does not know of the service in the first place. The results from the question are visualised in figure 5.13 below. 111 of the respondents

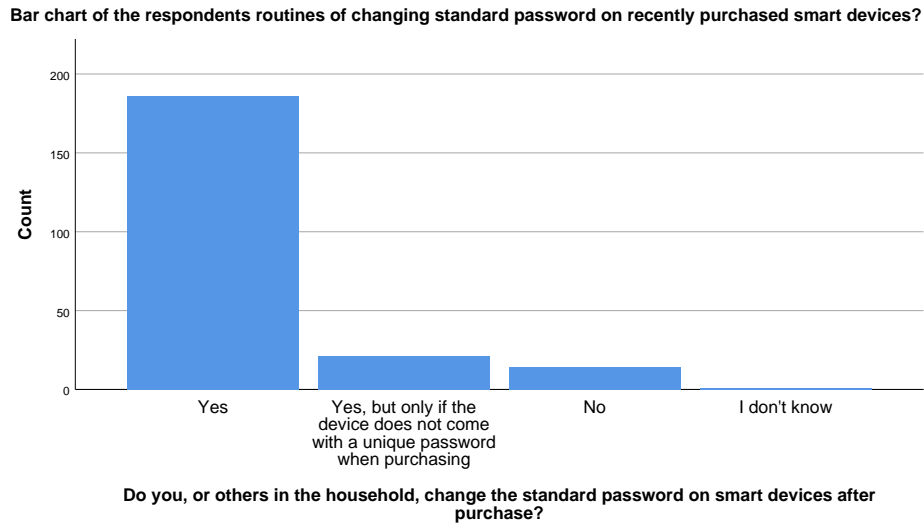


Figure 5.12: The respondent's routines towards changing standard passwords

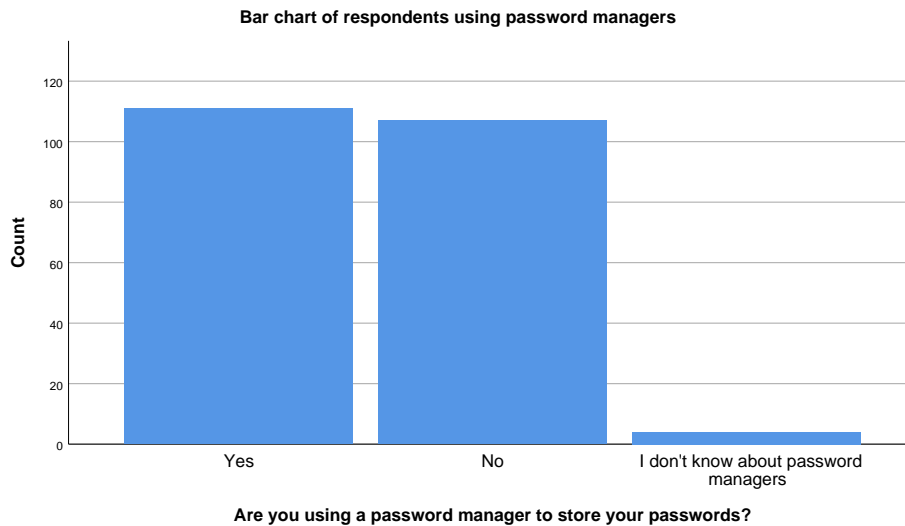


Figure 5.13: The respondent's routines towards using password managers

(50%) answered that they do use a password manager to store their passwords in, and 107 people (48.2%) do not. Only 4 people (1.8%) admitted to not knowing of password managers. It was surprising that exactly half used a password manager, so my hypothesis was proven wrong. It was also interesting to see that so few people did not know about the service. This could be because they did not want to admit not knowing about it, and just answered no instead. Moreover, technically that is still the truth, so this might be a limitation for this question.

In the last question regarding credential management, I wanted to assess the

respondent's routines when it comes to password reuse. Password reuse could lead to higher consequence if the credentials were to get compromised due to an event. Suddenly, an intruder would not only gain access to one service or device but possibly multiple. I hypothesised that the majority understands the risks of password reuse, and therefore do not use the same passwords. The results are shown in figure 5.14 below. The descriptive statistics show us that only 17 people

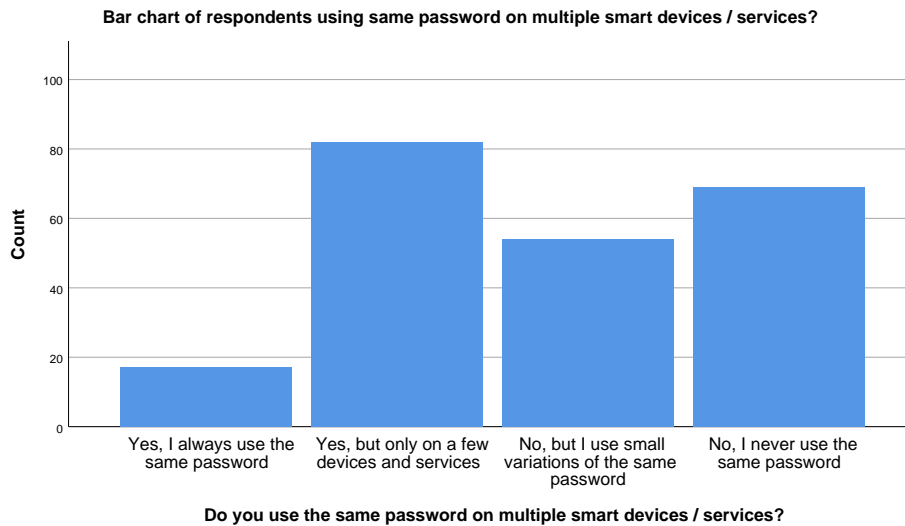


Figure 5.14: The respondent's routines towards using a password on multiple devices/services

(7.7%) admitted to always using the same password, while 82 people (36.9%) reused their password only on a couple of services and devices. Furthermore, 54 people (24.3%) responded that they did not reuse the same password; however, they used small variations of the same base password. Lastly, the remaining 69 people (31.1%) never used the same password. This shows us that a worrying number of people reuse their password, although the majority of them only reused it on a few services, which would reduce the potential impact of a credential leak. My hypothesis was mostly true; however, a sizeable portion used variations of the same password, which is not ideal but could be adequate depending on the strength of the base password. This could also make it easier to remember if one does not use a password manager, while at the same time retaining password strength.

5.3.3 Knowledge of smart home security aspects

I asked the respondents to rate their knowledge of three different aspects relating to the security awareness of smart homes, ranging from little known to well known. The results are displayed in figure 5.15 below. Regarding their self-proclaimed knowledge of the data flow between the smart devices and the inter-

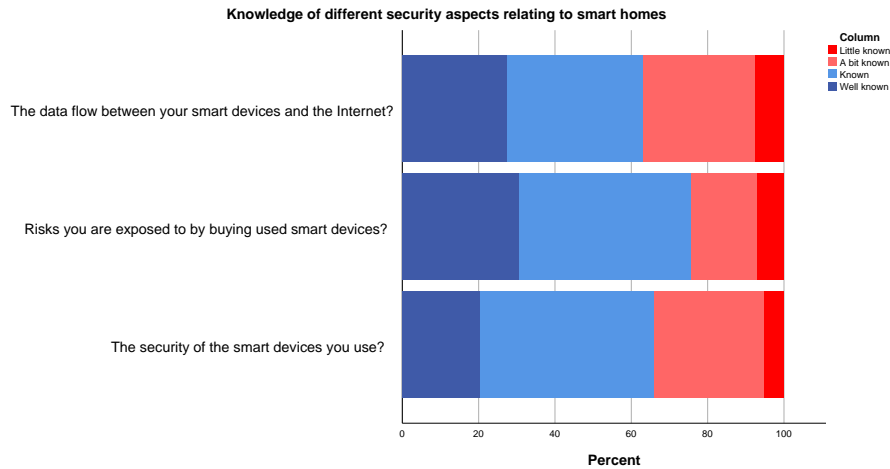


Figure 5.15: Knowledge of different security aspects relating to smart homes

net, 140 people (63.1%) claimed that it is known or well known to them, while 82 people (36.9%) claimed to know little or just a bit. When it comes to risks they are exposing themselves to when buying used smart devices, 168 people (75.6%) claims that it is either known or well known, while only 44 people (24.4%) claims to know little or just a bit. The last question was how well the respondents know the security of the smart devices they use, in which 146 people (65.8%) claims to either know it or know it well, while 76 people (34.2%) claims to know little or just a bit. We can see from the stacked bar chart, and the descriptive statistics the majority claims to at least know of these security awareness aspects, in which risks when buying used devices stand out as slightly more known among the respondents.

5.3.4 Risk perceptions of the respondents

In the last set of questions, I asked the respondents to assess their perceived risk according to a set of risk scenarios. The respondents could choose a risk score from 1 to 6, where 1 equals to low risk, and 6 equals to high risk. In table 5.3 below, the mean scores are listed for all scenarios, together with the standard deviation of the respondents.

We can see from table 5.3 that most risk scenarios have a mean score of between approximately 2.5 and 2.9, and a standard deviation of 1.2 to 1.5. The risk scenario that stands out the most is breaking into the house, as it only has a mean score of 1.97, the lowest of the bunch, together with the lowest standard deviation at 1.192. At the upper end, we have the loss of login details at a mean of 2.9, with a standard deviation of 1.502.

The results are displayed graphically in figure 5.16 below, and is displayed based on the percentage of answers each risk score got.

Descriptive Statistics of Perceived Risk					
	N	Min	Max	Mean	Std. Dev.
1. One or more of your smart devices gets infected by malicious software	222	1	6	2.77	1.235
2. An unauthorized person gets access to login details for one or more smart devices	221	1	6	2.90	1.502
3. An unauthorized person breaks into the house and steals your smart devices	222	1	6	1.97	1.192
4. An unauthorized person takes control of your smart devices and uses them to attack others	222	1	6	2.49	1.361
5. An unauthorized person intercepts the network traffic to your smart devices	222	1	6	2.71	1.382
6. One or more smart devices are accidentally rendered unusable	222	1	6	2.68	1.366
7. An unauthorized person gets remote access to one or more of your smart devices	222	1	6	2.75	1.391
8. An unauthorized person accesses personal information through your smart devices	222	1	6	2.82	1.531

Table 5.3: Descriptive statistics of perceived risk from 8 risk scenarios

5.4 Bivariate analysis

In this section, I will perform bivariate analysis on my primary sample. I started by analysing demographics as the independent variable, which includes age, education level, and county. Based on the previous analysis in section 5.1.2, I was not able to do bivariate analysis on gender, and in my analysis, there were no significant findings regarding county as an independent variable.

5.4.1 Age differences

In my analysis of the differences in age groups I found that there were significant differences between the groups in mainly three different questions. The result of the ANOVA in figure 5.17 below, shows us that the answers between the groups are significantly different since I am using the threshold of $P = 0.05$. If we look

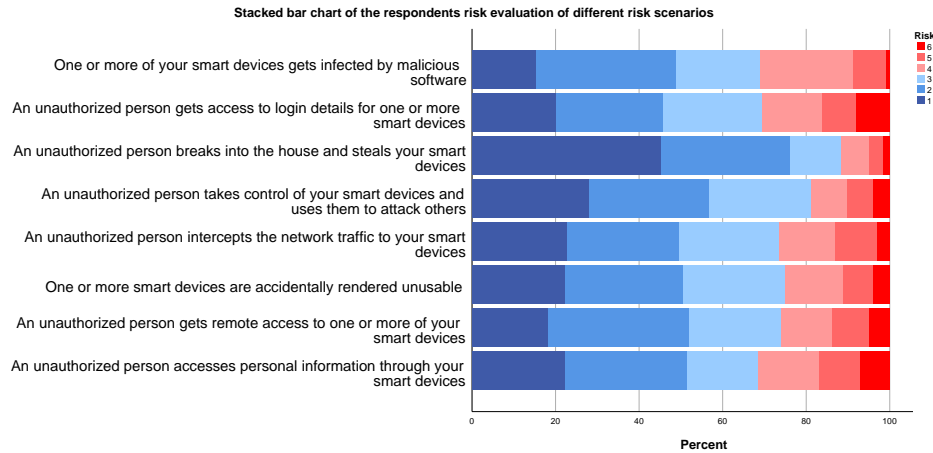


Figure 5.16: Respondents risk evaluation of different risk scenarios

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
To connect your smart devices to the Internet, do you prefer cable or wireless?	Between Groups	8.365	3	2.788	4.776	0.003
	Within Groups	126.694	217	0.584		
	Total	135.059	220			
Knowledge of the security of the smart devices you utilise?	Between Groups	5.584	3	1.861	2.836	0.039
	Within Groups	142.434	217	0.656		
	Total	148.018	220			
Knowledge of risks you expose yourself to by buying used smart devices?	Between Groups	8.407	3	2.802	3.788	0.011
	Within Groups	160.552	217	0.740		
	Total	168.959	220			

Figure 5.17: ANOVA of age up against other variables

further at the descriptive statistics I have included in the appendix C.1, we can see that the age group that is older than 50 is more likely to score higher in their knowledge of the risks of buying used smart devices with a mean score of 3.2, as well as the security of their smart devices with a mean score of 3.47. When looking at Tukey's post-hoc test, we see that the difference between people older than 50 is significant at the 0.05 level in comparison to people between 20-29 and 30-39 in both those questions. This table is included in appendix C.2. This variance can further be visualised in bar charts in figure 5.18 and 5.19.

When it comes to the differences between people who prefer cable or wireless when connecting their smart home devices to the internet, we also see that those older than 50 do significantly more often prefer wireless to cable. This variance is visualised in figure 5.20.

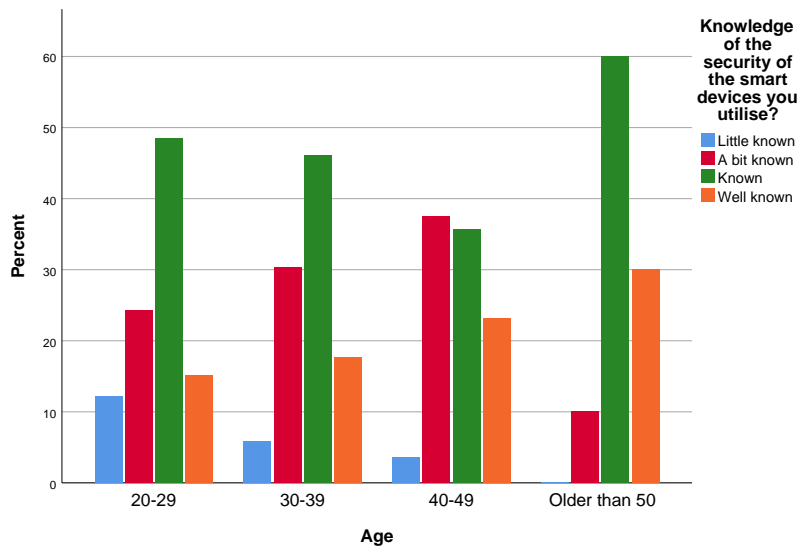


Figure 5.18: Age differences when it comes to knowledge of smart device security

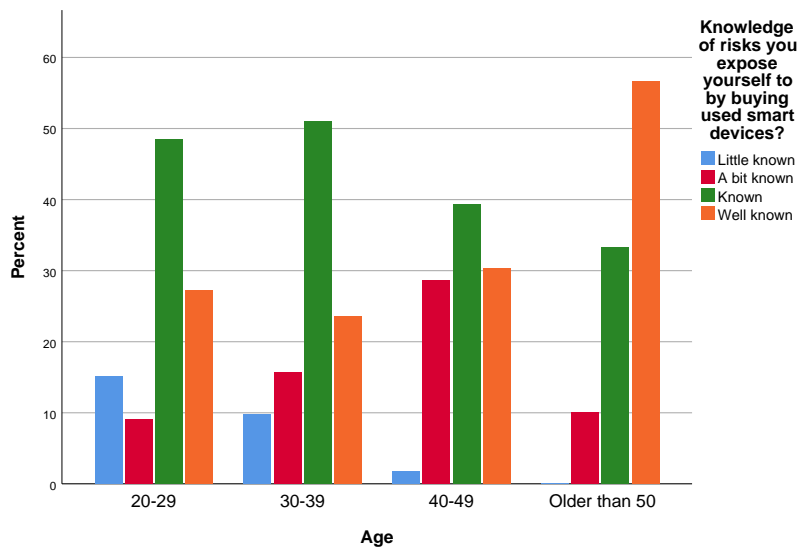


Figure 5.19: Age differences when it comes to knowledge of risks by buying used smart devices

5.4.2 Education differences

In the analysis of educational differences, my main findings included variance in whether people used a password manager or not. As is presented in figure 5.21, the difference has a significance of 0.028, which means there is only 2.8% probability that this difference is due to chance alone. This is also under the set threshold of 0.05. When looking further at the descriptive statistics in appendix

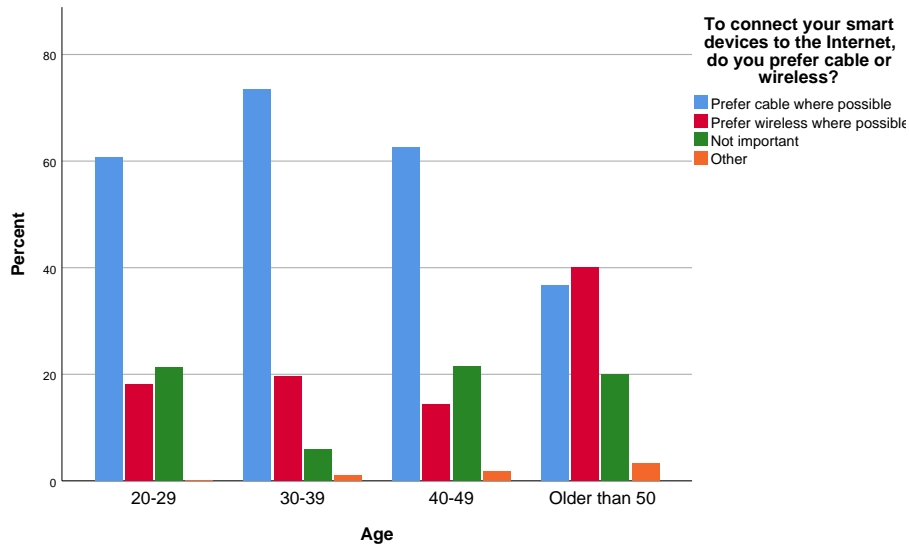


Figure 5.20: Age differences when preferring cable or wireless to connect to the internet

ANOVA

Are you using a password manager to store your passwords?

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2.593	3	0.864	3.094	0.028
Within Groups	60.602	217	0.279		
Total	63.195	220			

Figure 5.21: ANOVA of education up against the use of password managers

D.1, we see that the mean value is lower for people with university education. As mentioned in the method chapter, yes = 1 and no = 2, so this could mean that university graduates are more likely to answer yes. This difference is further visualised in a bar chart in figure 5.22 below.

When looking at the post-hoc Tukey test in appendix D.2, however, none of the mean differences between the education groups are significantly different. The results should, therefore, be taken with a grain of salt, even though the ANOVA results show up as significant.

5.4.3 Reasons for changing security and privacy settings

Back in section 5.3.1 I presented how many people changed the security and privacy settings on their smart home devices. Looking further into this question, I wanted to know if those who answered no knew about the contents of the data they are sending and if that risk was accepted. I took the independent variable, which was if they changed the security and privacy setting or not, and compared

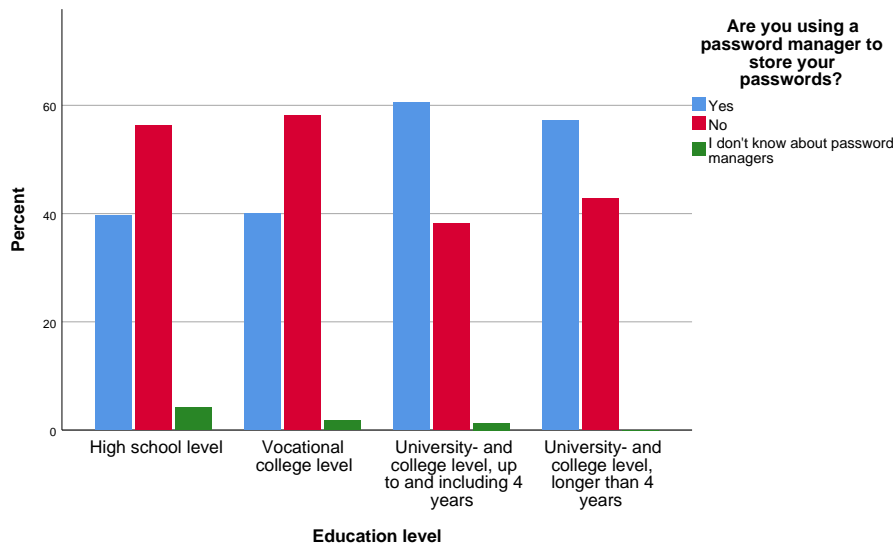


Figure 5.22: Education differences when it comes to using password managers

their knowledge of the data flow of their smart devices. The ANOVA in figure 5.23 shows us that there is a difference between the groups of the independent variable that is significant at 0 and that the dependent variable has an effect on the independent one.

ANOVA

Knowledge of the data flow between your smart devices and the Internet?

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	16.148	2	8.074	10.319	0.000
Within Groups	171.347	219	0.782		
Total	187.495	221			

Figure 5.23: ANOVA of whether knowledge of data flow affects changing security and privacy settings

When we look at the descriptive statistics in appendix E.1, we see that the mean value of data flow knowledge for those who said yes to changing their settings is at 3.06, while it is 2.55 for those who said no. When looking at the post-hoc Tukey test, in appendix E.2, we see that the mean difference between saying yes or no is 0.517, which is also significant at the 0.05 level. This difference is further visualised in the bar chart 5.24 below.

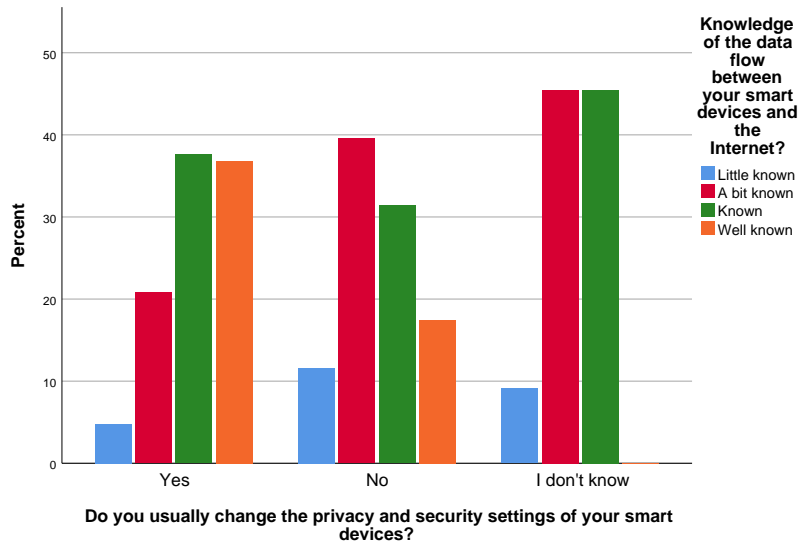


Figure 5.24: ANOVA of whether knowledge of data flow affects changing security and privacy settings

5.5 Control group analysis

In this section, I will go over the findings of my control group analysis. The number of respondents for the control group was 43 people.

5.5.1 Demographics

Before presenting the results, I will describe the control group sample demographics and compare them to the primary sample.

Age

A visual representation of the age distribution and comparison to the main sample is included in figure 5.25 below. In the control group sample, a total of 35 people (81.4%) responded to being between 20 and 29 years old. This means that the control group is overwhelmingly made up of young people, especially compared to the primary sample.

Gender

When it comes to the gender distribution, it seems much closer to 50/50, especially in comparison to the main sample, which had all males except for one person who preferred not answering. The distribution is shown in figure 5.26 below. In this sample, 26 people (60.5%) responded that they were male, while 17 people (39.5%) said they were female. This is much closer to the national average than the primary sample.

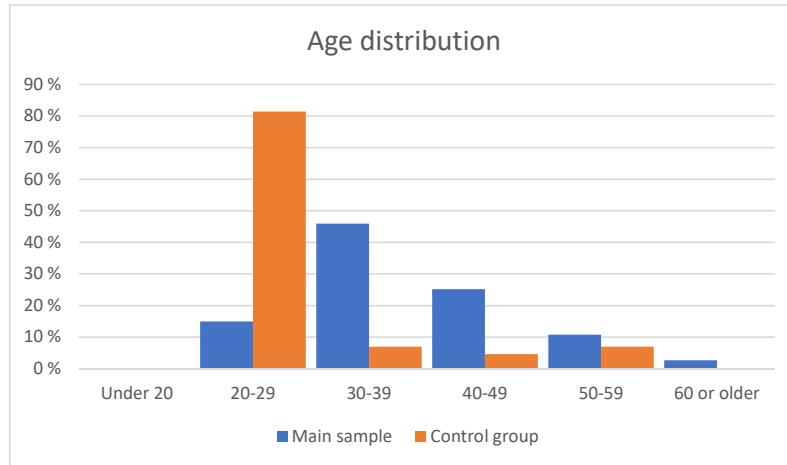


Figure 5.25: Age distribution of the control group in comparison with the main sample

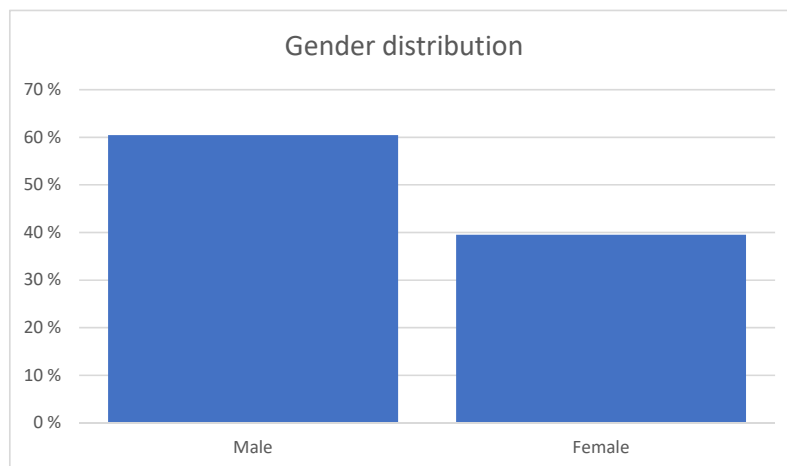


Figure 5.26: Gender distribution of the control group

Highest education level

Regarding the education level, both similarities and differences are observed. As we can see in figure 5.27 below, there is about the same share of people with

high school education and slightly more people with higher education. The big difference, however, is the people who answered to having a vocational college education. In the control group sample, none of the respondents had a vocational

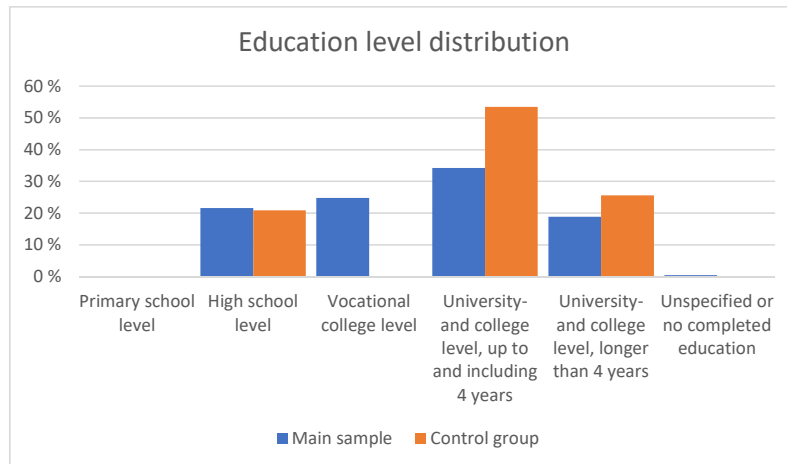


Figure 5.27: Highest completed education level of the control group

college education, while it amounted to about a quarter of the respondents in the main sample.

County

The county population distribution of the control group is visualised in figure 5.28 below. Compared to the main sample it seems to have much more people from Innlandet county. About 30% responded to living in Innlandet, compared to 5% in my main sample, and 7% nationally. Due to the low sample size and the high number of possible answers, these results may not be very representative, as some categories do not even have a single answer.

5.5.2 Analysis of differences to the main sample

To start, in order to make the control group sample available to more people than just smart homeowners, I included an additional question where I asked if they owned any smart devices. The results from this question can be seen in figure 5.29 below. Out of the 43 total respondents, 35 people (81.4%) answered that they owned smart devices, while 8 people (18.6%) did not. Those who answered yes received additional questions regarding smart home devices, compared to the ones who answered no. In retrospect, I realised I should have specified smart

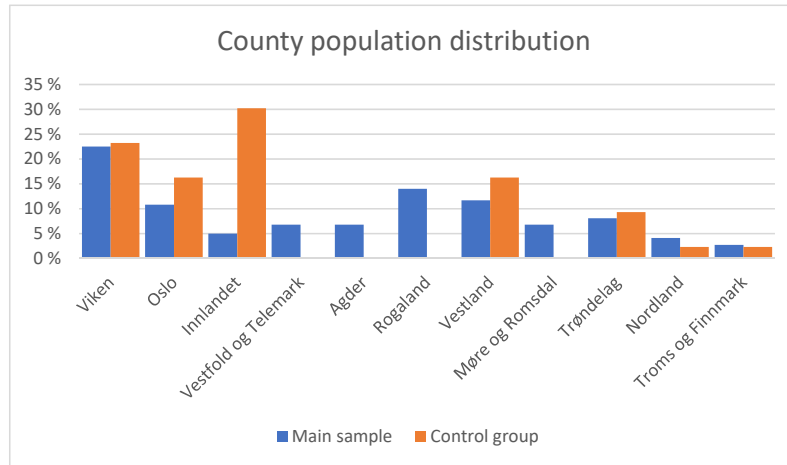


Figure 5.28: County population distribution of the control group

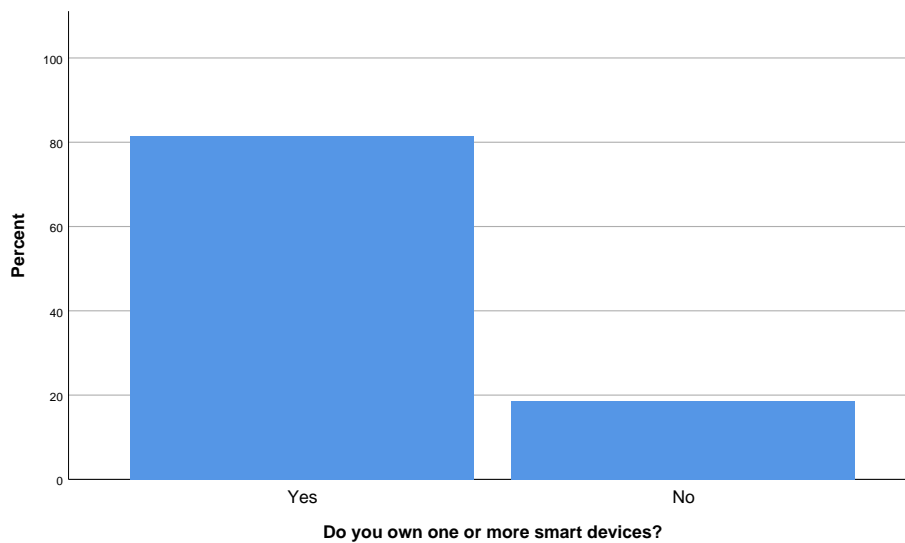


Figure 5.29: The part of the sample who reported to owning one or more smart devices

home devices, and not just smart devices, since it may be people who misinterpret the question to include regular smartphones or other devices. Therefore, the percentage of people owning smart home devices could be lower than the displayed results.

Differences in smart device types owned

For those 35 people who said they owned smart devices, I asked what types of smart devices they owned. In table 5.4 below is an overview of the number of respondents that answered this question. Out of the 9 missing cases, 8 of them

Case Summary						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Smart devices	34	79.1%	9	20.9%	43	100.0%

Table 5.4: Number of people in the control group who specified what smart device types they own

did not receive the question due to not owning smart devices as described in the previous section. The last person did not specify any device types; however, he described in the free text that he owned a smartphone and tablet. This confirms that at least one person misunderstood the definition. Table 5.5 below shows us the frequencies of different smart device types people own. We can see that the

Smart device types frequencies				
		Responses		Percent of Cases
		N	Percent	
Smart devices	Voice assistant	8	6.8%	23.5%
	Speaker	20	17.1%	58.8%
	Robot vacuum	9	7.7%	26.5%
	Smarthub	1	0.9%	2.9%
	Smart TV	21	17.9%	61.8%
	Smart screen	2	1.7%	5.9%
	Router	16	13.7%	47.1%
	Door lock	4	3.4%	11.8%
	Light bulbs	7	6.0%	20.6%
	Smart dimmer	6	5.1%	17.6%
	Smart switch	4	3.4%	11.8%
	Kitchenware	5	4.3%	14.7%
	Alarms	5	4.3%	14.7%
	Motion sensors	3	2.6%	8.8%
Thermostat	6	5.1%	17.6%	
Total		117	100.0%	344.1%

Table 5.5: What types of smart devices the respondents in the control group own

total number of responses is 117 since people can make multiple choices. Considering there were 34 people who answered, this means that on average, people only chose between three and four device types each. The three most popular

device types were smart speakers (58.8% of the time), smart TV's (61.8% of the time), and routers (47.1% of the time). The answers show us that most people in this control sample have much more basic smart homes with much fewer device types than in our primary sample. People in the main sample had, on average, a little over ten device types, and maybe even more if we consider free-text answers. Speaking of free-text answers, one person in the control group sample also specified that they owned a robot lawnmower, and one person said they had a smart washing machine.

5.5.3 Differences in the knowledge of certain topics and aspects

Another aspect in which I received results that were different from the main sample was when assessing the respondents knowledge of certain security issues regarding smart devices and knowledge of technology, data security, and smart homes. The results are shown in a stacked bar chart in figure 5.30 below. In the

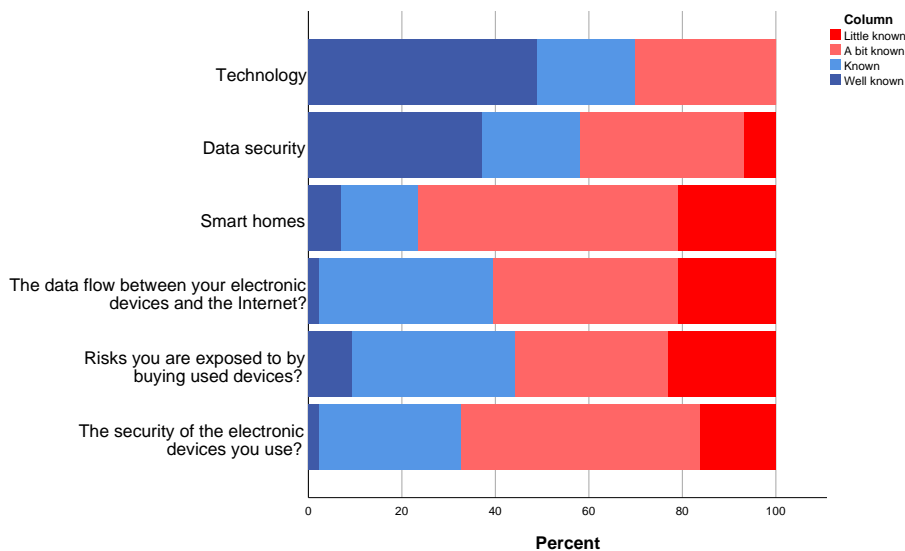


Figure 5.30: The knowledge of the control group respondents regarding different topics

last three questions, the word smart devices are exchanged with electronic devices to make people with no smart home devices able to answer, while still retaining the same aspect that is analysed. When comparing the results to the main sample in figure 5.6 and 5.15, we see that on average, the control group reports overall lower knowledge in each of the six aspects.

Differences in use of devices

When comparing the two samples, I found some interesting differences in device usage. When analysing the question about if their smart devices were on a separate

segment of their home network, I saw that only 6 people (17.1%) that answered this question from the control group used a separate segment, compared to 41% from the main sample. Also, 7 people (20%) said they did not know, compared to 0.5% from the main sample. The ones who said no were fairly similar in size for both samples. The results is visualised and compared in figure 5.31 below.

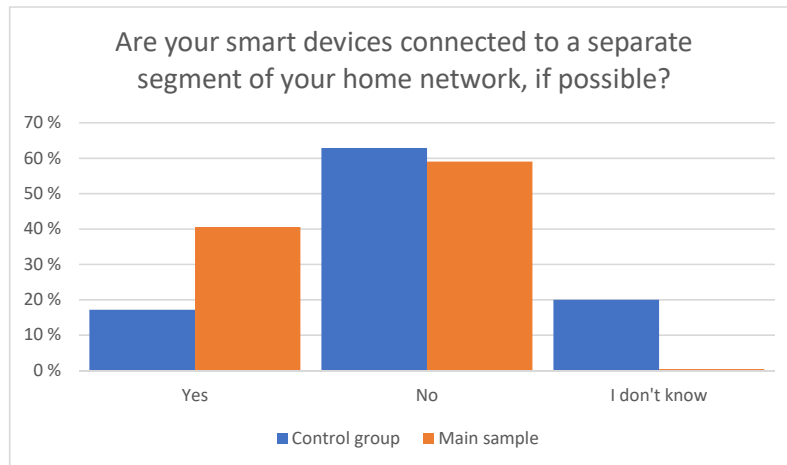


Figure 5.31: Differences between the samples in the usage of a separate segment of the home network for smart devices

I also found an interesting difference between the samples when it comes to a preference towards using wireless or cable to connect to the internet. For the control group sample, 10 people (28.6%) answered that they preferred cable where possible, to the 64% of the main sample. On the other hand, 23 people (65.7%) from the control group preferred wireless, compared to 21% of the main sample group. The results are visualised in figure 5.32.

Both of these questions were answered only by people who owned smart home devices.

Differences in credential management

Other findings in differences between the samples included a question regarding credential management. This question aimed to figure assess if the respondents used the same password on multiple devices and services. The results can be viewed in figure 5.33 below. I observed that around the same amount of people used the same password; however, 28 people (65%) from the control group sample admitted to using the same password on a few services and devices, compared to

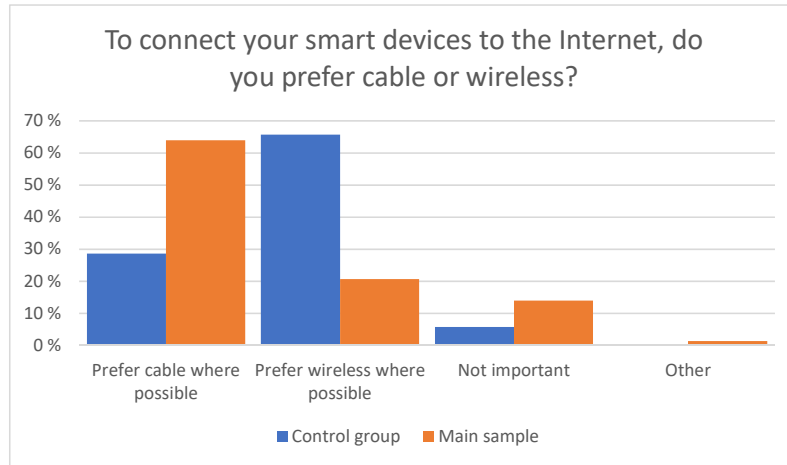


Figure 5.32: Differences between the samples in preferring cable or wireless to connect smart devices to the internet

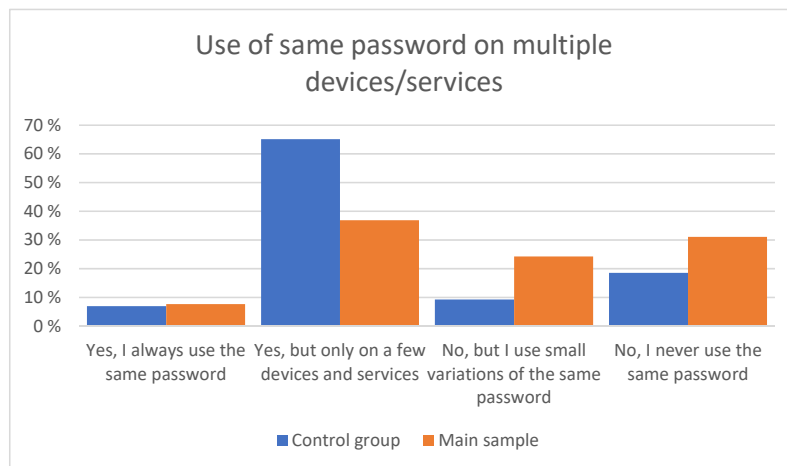


Figure 5.33: Differences between the samples in using the same password on multiple devices/services

the 37% from the primary sample. This also means that fewer people from the control group answered that they do not use the same password.

These results are the most significant differences in the analysis of the questions. For the rest of the questions regarding credential management and use of devices, I have included frequency tables in appendix F. These results are mostly similar to the main sample; however, they all seem to follow a similar trend of slightly less security awareness.

Differences in risk perception

I also looked at the differences in risk perception between the samples based on the 8 risk scenarios that were analysed in section 5.3.4. Looking at the descriptive statistics, I found that overall, the control group sample perceived the risk from these scenarios slightly higher than the main sample. The descriptive statistics can be viewed in table F.1 in the appendix.

5.6 Specifications by the respondents in feedback

Many of the respondents mentioned that a lot of the questions assumed the devices needed to be connected to the internet. However, multiple people specified that they strive towards having smart devices that are not connected directly to the internet, and that many solutions do not require internet connection. Many also specified that they run a local system that is linked with the cloud through a gateway. One respondent also specified that they use a security solution that is named Europe's best. Another said that they work as a pentester and that they use the smart home as a lab for breaching services. In the control group survey, some people specified that they have consciously decided to not have any smart home devices, due to the added risk involved.

Chapter 6

Discussion

This chapter will focus on discussing the different results from the previous chapter. The chapter will focus on separating immaterialities, details, doubts, and other things to be able to conclude. The discussion is structured around the samples and the three research questions of my thesis, and the discussion is conducted with those in mind. Lastly, the limitations of the study as a whole will be discussed.

6.1 Sample representativeness for smart home users in Norway

In the previous chapter, I went through the demographics data and saw that only peoples residency was similar to the overall population, based on SSB data [29]. For the age distribution, there was a massive overweight of people between 30 and 49 years old, and way fewer older people above 60 and younger people below 20. In addition to this, my sample only contained men, and had an abnormally high number of people who have done vocational college. Whether this sample is representative of the overall smart home users in Norway is hard to say since I only collected data from a single Facebook group. I of course also collected data from a control group, which showed a different demographic makeup, especially in gender and age, but also education, eluding to the fact that the primary sample may not be representative to every smart home user. On the other hand, the sample may be representative for those especially interested in the smart home ecosystem, since my results in section 5.2.1 show that the main sample has, on average, much smarter homes. The control group sample mostly said they had generic smart home devices like a SmartTV, and not fully integrated smart home systems. The primary sample also reported overall higher technical knowledge than the control group.

6.2 RQ1: What is the current security awareness level of smart home users in Norway?

For my first research question, the aim was to assess the security awareness of smart home users in Norway. To answer this, I asked a series of questions in the form of an online survey to people in a smart home enthusiast Facebook group for Norwegian smart home users, although anyone could join and therefore take part in the survey. In fact, from my results, one person claimed to not owning any smart home devices. When trying to assess the security awareness of the smart home users, I focused on their use of the smart devices, their credential management routines, knowledge of specific security aspects, and their risk perceptions. The questions that aim to answer these aspects were mostly based on the best practises for security awareness by ENISA [3]. Initially, I came in with the hypothesis that their routines regarding the use of smart home devices carried significant risk, and that their security awareness is generally low. However, as I argue in the subsequent sections, this turned out to not be entirely accurate.

For example, when asking about their routines when updating their devices, I observed that 62.2% update them right away, and another 34.2% do so, but sometimes wait a while. Only 3.6% did not think about it that much, which is a tiny amount of people. This shows us that the overwhelming majority of people care about updating their devices, even though approximately one third still wait a while before updating. The results are similar for the control group; however, there are slightly fewer people updating right away (46.5%) and slightly more people (41.9%) sometimes waiting a while.

Another example is when I asked if they turn off services and features they do not use, which resulted in about two thirds (66.2%) confirming that they did so. This also denied my initial hypothesis that this was something the respondents mostly did not do. My results are also consistent with the control group sample, which showed that 60.5% do and 32.6% do not, while the rest did not know.

In addition to the questions mentioned previously, I also asked if they change their privacy and security settings on their smart devices. Moreover, most people (56.3%) do, while 38.7% do not. This is also mostly consistent with the control group, where 45.7% do, and 48.6% do not, which is a difference in about 10%.

Another aspect was whether the respondents preferred to use cable or wireless when connecting their smart home devices to the internet. According to ENISA [3], the best practice is to use cable where it is possible due to the smaller attack surface. My initial hypothesis was that the sample would prefer wireless since this is easier to set up and use, while also being more visually pleasing by not having cables lying around. This turned out to be false however, as 64% preferred cable, only 20.7% preferring wireless, and the rest answering that it was not important to them. This was also one of the questions I was curious about regarding my control group, since the two samples have a different technical background, and the control group on average having less smart home devices. The results from the control group showed a complete opposite distribution, were 65.7% preferred

wireless and 28.6% preferred cable. It could be that these differences are due to the discrepancies in technical knowledge and how smart their homes are since, according to my results, most people in the control group only had basic smart home devices. Another finding was that there were differences in the age groups when it comes to internet connection preference. People older than 50 almost equally preferred cable and wireless, while the other age groups heavily preferred cable, which may indicate that older people do not think about the security aspects while choosing. Another possible explanation is that the reason why older people choose to implement smart home devices in their homes is mainly to make their lives more comfortable, and wireless connection is a much easier and more intuitive option for connecting to the internet.

On the other hand, I also asked if the respondents used a separate segment of their home for their smart home devices. A separate segment for smart home devices is considered best practise so that these devices do not have direct contact with the personal devices of the household, like smartphones, laptops, and tablets. My results show that most people do not connect these devices to a separate segment, where 59% answered no, and 40.5% answered yes. The difference here is not very large; however, there is room for improvement. This difference is especially jarring when it comes to the control group, which only had slightly more people saying no, but this difference was minuscule. However, the big difference is shown when many people (20%) in the control group said they did not know, which may indicate that they do not know how to segment their network in the first place.

Another indication of their security awareness level is how they manage their credentials. When asked about their routines of changing the default password on recently purchased devices, they overwhelmingly said that they do, with 83.8% saying yes. On the other hand, when asked about using password managers, about half of the respondents said yes and no. For the control group, fewer people were saying yes, and more people saying that they do not know about password managers, following the narrative that the control group are slightly behind the primary sample in overall terms of security awareness. Furthermore, there seems to be a significant variance in the respondent's education level and whether they use a password manager. Around 60% of people with university education use password managers, compared to only around 40% of people with high school or vocational college level.

Another classic indication of bad credential management is whether they use the same password on multiple services and devices. In my results, only a few people (7.7%) admitted to using the same password everywhere, while 36.9% reused their password on a couple of services. On the one hand, this is certainly not ideal but seems decent when compared to the control group, in which 65.1% used the same password on a couple of services and devices as is displayed in figure 5.33. On the other hand, a study by Gkioulos et al. [35] also asked the question of using the same password on applications, distributed on three different competence groups. The results show that, depending on the competence group, between

about 70-90% responded with saying that they either always use different passwords or use small variations of the same password for different applications. The limitations of this question, however, is that no answer identify if people use the same password on only some services, which might change the results.

Knowledge of particular smart home security aspect can be an indicator of sufficient or insufficient security awareness. I asked about the respondent's assessment of their knowledge when it comes to the data flow between their devices and the internet, risks when buying used devices, and the security of the smart devices they use. The respondents showed a decent understanding, with over 60% answering that it was either well known or known, with almost 80% saying so with risks about used devices. Additionally, it turns out that older people are slightly more knowledgeable about the security of the devices they use and the risks of buying used devices, which is surprising. The control group, however, show lesser understanding at about 40% of the respondents answering that it is well known or known to them.

6.3 RQ2: What are some of the most common pitfalls of smart home users in Norway which impose risk amplification?

The second research question I will be answering in my thesis deals with common pitfalls that smart home users in Norway fall into that increases the risk they expose themselves to in their daily lives. In many ways, this question can also be seen as an extension of the first one, as the main findings that impose risk amplification can explain this.

One of the main issues I saw from my results was that people generally do not segment their network so that their smart home devices are not in direct contact with their other personal devices. Based on my results, only 40.5% answered that they had done segmentation, while 59% said they did not. In the control group, this was even more of an issue, with only 17.1% saying that they did so, and 20% answering that they did not know. These results could mean that some people do not know how to segment their network, even though it has become much easier to do for a consumer with little technical knowledge over the years. I argue that this is not necessarily an issue of lack of knowledge aside from knowing that this is best practise, but rather a lack of initiative or priority to learn how to do.

Another pitfall seems to be the reuse of passwords. My results show that while only 7.7% admitted to always using the same password, 36.9% admitted to using the same password on just a couple of services. A study by Gkioulos et al. [35] asked a similar question for passwords on applications, and the results show that, depending on the competence group, between about 70-90% responded to only using different passwords or variations of the same one. However, they only asked about the extremes; if one uses the same password on all applications or none. Therefore, I argue that this is a significant pitfall for smart home users in Norway

since if their credentials are leaked on another service, there exists a significant risk that their smart home may be compromised. Credential stuffing is widely used as a method for cybercriminals to test compromised credential on a variety of services to see if they have been reused [36]. Moreover, while people seem to know the risks of password reuse, people do it regardless due to the fear of forgetting their passwords and wanting to be in control of all their credentials [37].

Regularly updating the devices, one use is also vital to secure the smart home. When it comes to updating smart home devices, my results show that only 3.6% do not think about doing that. Furthermore, another 34.2% sometimes wait a while before updating the devices, leaving them potentially insecure for a while. Considering that studies have shown that at least 15% of home routers are unsecured [38], this is a significant pitfall one can fall into. Additionally, for my control group, the results show that a slightly higher share of people either do not think about it (7%) or sometimes wait a while (41.9%).

6.4 RQ3: What do smart home users in Norway perceive being the highest security risks when using smart home devices?

The last research question aimed to uncover some of the perceptions smart home users in Norway had about the risks to their smart home. To achieve this, I asked the respondents to rate their perceived risk of eight risk scenarios. Out of these eight scenarios, there was a few which the respondents perceived as being slightly higher risk than the others.

First off, we have loss of login credentials, which turned out to be the highest perceived risk of the respondents at a mean value of 2.9 in the primary sample on a scale from 1 to 6. It is interesting to note that the highest mean value is still lower than the half point between the minimum and maximum possible values. This could show that most people do not perceive most of the risks as anything serious. For the control group, the mean value is at 3.14, which is the second-highest of the bunch. While this is among the risks they perceive as highest, it is also interesting that so many people choose to reuse their passwords as discussed in the previous chapter. In a paper by Van Shaik et al. [17], which focused on risk perceptions of cybersecurity and precautionary behaviour, they found that the highest risks perceived were risks associated with identity theft and keylogging. This assumes the loss of login credentials and is in accordance with the results in my thesis.

Further, my results show that unauthorised access to personal information through smart devices are perceived as the second-highest risk across all respondents of my primary sample. Here, the mean risk value is 2.82, while in the control group, this risk scenario is perceived to be of the highest risk, with 3.23 as a mean score. On the one hand, studies show that privacy and the loss of personal in-

formation are of high priority among consumers, like in the study by Van Shaik et al. [17], where identity theft was shown as the highest risk. Identity theft can be made possible by stealing personal information and using that to impersonate another person. Other risks that were perceived as high risk in this study was social engineering and phishing, which could be enhanced by collecting personal data. On the other hand, a study by Zeng et al. [20] shows that most people are worried for the physical security of their smart home, while general privacy issues are perceived as secondary issues. When comparing these results to mine, we observe that physical security issues are perceived to be much lower risk.

The last risk scenario I want to highlight is related to the infection by malware on the smart home devices. This scenario was perceived to be the third-highest risk according to both the main sample and the control group, with a mean score of 2.77 and 3.11, respectively. This could be because this is somewhat known to the respondents, as most people have heard about or previously interacted with computer viruses and similar malicious software, and it is easier to assess the risk based on previous knowledge and experience.

Interestingly, the risk scenario that deals with the control of devices to attack others is second to last in perceived risk by the respondents. Given the amount of media coverage of distributed denial of service (DDoS) attacks from botnets originating from the Internet of Things (IoT), one would think this would be higher on the risk priority list. One thing that could explain this is that many in the primary sample prefer using devices that run locally so that the probability of this risk is much lower. However, this risk scenario is second to last in the control group as well, which has shown to have slightly less knowledge and use more generic smart home devices that connect to the internet. When formulating the question, I aimed to make it as understandable as possible since many people do not know what a botnet is and what a DDoS attack is. A negative aspect of this could be that some respondents did not catch the implication that this was about botnets, thus downplaying the risk as a result.

6.5 Limitations

Most studies are not perfect, and mine is no exception. In this section, I will elaborate on a few on the overall limitations of my thesis. First off, the low sample size of the control group (43 respondents) makes it hard to say that the comparisons between the main sample and the control group are completely significant, although it can serve as an indication. Secondly, the control group was collected through my connections on Facebook, which may contain bias. Another limitation is that the main sample was only collected from one source, which may contain bias. The source was from a Facebook group of smart home enthusiasts from Norway, which is not uniquely representative for every smart home user in Norway. This was my main reason for wanting a control group to double-check my data, although this control group had limited quality. On the other hand, this limitation was somewhat remediated with a series of questions on demographics to be able

to describe my samples adequately, and also questions to assess the background knowledge of the respondents, as well as how smart their homes were. This data showed the difference in the samples when it comes to background knowledge and how many smart devices they owned.

Further, there was an overall assumption in the survey that smart home devices are connected to the internet, which is the main area I wanted to cover. However, many of the respondents specified that there were solutions that could run locally and move through a hub, which multiple people said that had implemented due to the security concerns of IoT devices. I may have needed additional questions or choices for some questions in order to cover the field of smart homes fully. Another issue that could have limited my results was insufficient definitions of what I mean by risk when asking the respondents of their perceived risk of various scenarios. This issue was fixed in the control group survey, and although the risk was slightly higher across the board, the variance in distribution and the ranking of the risks remained very similar.

Chapter 7

Conclusion

Smart homes are a relatively new concept, and thus the security awareness have not yet matured in most people. The aim of this thesis was therefore to assess the security awareness level of smart home users in Norway in order to help both the consumers and security professionals enhance their awareness, and help them prioritise awareness training. Based on this, three research questions were outlined:

- What is the current security awareness level of smart home users in Norway?
- What are some of the most common pitfalls of smart home users in Norway which impose risk amplification?
- What do smart home users in Norway perceive being the highest security risks when using smart home devices?

After conducting the survey, I found that the results suggests the security awareness level of smart home users in Norway are quite decent, especially for the smart home enthusiasts. Even though the control group sample is of low sample quality and size, it gives an indication that there is a difference in how invested into the smart home ecosystem one are and their security awareness level. Enthusiasts with many smart home devices tends to follow best practices better than casual users, which is a good thing and certainly necessary since the more invested one are, the larger the attack surface becomes.

When it comes to use of devices, most of the respondents have a good grasp on how to use the smart home devices securely, although their use of network segmentation could be much better. Regarding the respondents management of credentials they do know that it is important to change the default password, but the use of password managers are not widespread enough and password reuse happens more than what is recommended. My results also suggests that older people usually prefer wireless connections to the internet, which can carry additional risks. Overall, the respondents reported that they were knowledgeable about security aspects such as risks of buying used devices, data flow between their devices and internet, and the security systems they use.

When it comes to pitfalls the users might fall into, my results suggests that not segmenting their home network, so that smart home devices and personal devices

are not in direct contact, are one of the major pitfalls. Password reuse is also a major issue for both the primary sample and the control group. Furthermore, while many responded that they do update their devices, waiting a while can result in devices staying unsecured for long enough that it might be an issue.

Regarding risk perception, the results imply that the highest security risks, according to the respondents, are loss of login credentials, unauthorised access to personal information, and infection by malware. It is interesting to note that unauthorised controlling of ones devices to attack others are perceived to be second to last according to my results, although this question could have easily been misunderstood.

7.1 Future work

For future work, it could be interesting to focus more on sampling of so called casual smart home users in Norway who only have a couple of smart devices, as well as passive users that are not the smart home administrators of the household. This thesis mostly focused on smart home enthusiasts and people with many integrated smart home devices, so it could be rewarding to take another approach. Another possible aspect that could be explored is the security culture of households with smart homes, and how that affects their security awareness.

Bibliography

- [1] Wikipedia contributors, *2016 dyn cyberattack* — *Wikipedia, the free encyclopedia*, [Online; accessed 15-December-2019], 2019. [Online]. Available: https://en.wikipedia.org/w/index.php?title=2016_Dyn_cyberattack&oldid=923850977.
- [2] M. Rouse. (). Smart home or building (home automation or domotics), [Online]. Available: <https://web.archive.org/web/20200521150950/https://internetofthingsagenda.techtarget.com/definition/smart-home-or-building>. (accessed: 25.05.2020).
- [3] ENISA, ‘Security and resilience of smart home environments good practices and recommendations’, 2015.
- [4] S. Mennicken and E. Huang, ‘Hacking the natural habitat: An in-the-wild study of smart homes, their development, and the people who live in them’, vol. 7319, Jun. 2012, pp. 143–160. DOI: 10.1007/978-3-642-31205-2_10.
- [5] G. Assenza, A. Chittaro, M. Maggio, M. Mastrapasqua and R. Setola, ‘A review of methods for evaluating security awareness initiatives’, *European Journal for Security Research*, Sep. 2019. DOI: 10.1007/s41125-019-00052-x.
- [6] R. Shaw, C. C. Chen, A. L. Harris and H.-J. Huang, ‘The impact of information richness on information security awareness training effectiveness’, *Computers Education*, vol. 52, no. 1, pp. 92–100, 2009, ISSN: 0360-1315. DOI: <https://doi.org/10.1016/j.compedu.2008.06.011>. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0360131508001012>.
- [7] R. Kang, L. Dabbish, N. Fruchter and S. 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)*, Ottawa: USENIX Association, Jul. 2015, pp. 39–52, ISBN: 978-1-931971-249. [Online]. Available: <https://www.usenix.org/conference/soups2015/proceedings/presentation/kang>.
- [8] L. Drevin, H. Kruger and T. Steyn, ‘Value-focused assessment of ict security awareness in an academic environment’, *Computers & Security*, vol. 26, pp. 36–43, Feb. 2007. DOI: 10.1016/j.cose.2006.10.006.

- [9] E. McReynolds, S. Hubbard, T. Lau, A. Saraf, M. Cakmak and F. Roesner, 'Toys that listen: A study of parents, children, and internet-connected toys', in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ser. CHI '17, Denver, Colorado, USA: ACM, 2017, pp. 5197–5207, ISBN: 978-1-4503-4655-9. DOI: 10.1145/3025453.3025735. [Online]. Available: <http://doi.acm.org/10.1145/3025453.3025735>.
- [10] N. Gerber, B. Reinheimer and M. Volkamer, 'Home sweet home? investigating users' awareness of smart home privacy threats', Aug. 2018.
- [11] H. Gunleifsen, 'Cyber security awareness and culture in rural norway', eng, Tech. Rep., 2018. [Online]. Available: <http://hdl.handle.net/11250/2592269>.
- [12] M. Ghiglieri, M. Volkamer and K. Renaud, 'Exploring consumers' attitudes of smart tv related privacy risks', May 2017, pp. 656–674, ISBN: 978-3-319-58459-1. DOI: 10.1007/978-3-319-58460-7_45.
- [13] C. D. McDermott, J. P. Isaacs and A. V. Petrovski, 'Evaluating awareness and perception of botnet activity within consumer internet-of-things (iot) networks', Feb. 2019.
- [14] B. Ali and A. Awad, 'Cyber and physical security vulnerability assessment for iot-based smart homes', *Sensors*, vol. 18, p. 817, Mar. 2018. DOI: 10.3390/s18030817.
- [15] T. Denning, T. Kohno and H. M. Levy, 'Computer security and the modern home', *Commun. ACM*, vol. 56, no. 1, pp. 94–103, Jan. 2013, ISSN: 0001-0782. DOI: 10.1145/2398356.2398377. [Online]. Available: <http://doi.acm.org/10.1145/2398356.2398377>.
- [16] L. Cavaglione, J.-F. Lalande, W. Mazurczyk and S. Wendzel, 'Analysis of human awareness of security and privacy threats in smart environments', Aug. 2015. DOI: 10.1007/978-3-319-20376-8_15.
- [17] P. Schaik, 'Risk perceptions of cyber-security and precautionary behaviour', *Computers in Human Behavior*, May 2017.
- [18] G. Conti and E. Sobiesk, 'An honest man has nothing to fear: User perceptions on web-based information disclosure', Jul. 2007, pp. 112–121.
- [19] D. Solove, 'i've got nothing to hide' and other misunderstandings of privacy', vol. 44, Jul. 2007.
- [20] E. Zeng, S. Mare and F. Roesner, 'End user security & privacy concerns with smart homes', in *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security*, ser. SOUPS '17, Santa Clara, CA, USA: USENIX Association, 2017, pp. 65–80, ISBN: 978-1-931971-39-3. [Online]. Available: <http://dl.acm.org/citation.cfm?id=3235924.3235931>.

- [21] B. Ur, J. Jung and S. Schechter, 'Intruders versus intrusiveness: Teens' and parents' perspectives on home-entryway surveillance', in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, ser. UbiComp '14, Seattle, Washington: ACM, 2014, pp. 129–139, ISBN: 978-1-4503-2968-2. DOI: 10.1145/2632048.2632107. [Online]. Available: <http://doi.acm.org/10.1145/2632048.2632107>.
- [22] L. A. Tangstad, F. Bentzen and P. N. Schjem, 'Risikoer ved smarthus', 2017.
- [23] A. Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu and C. Dixon, 'Home automation in the wild: Challenges and opportunities', May 2011, pp. 2115–2124. DOI: 10.1145/1978942.1979249.
- [24] M. Asplund and S. Nadjm-Tehrani, 'Attitudes and perceptions of iot security in critical societal services', *IEEE Access*, vol. 4, pp. 2130–2138, 2016.
- [25] N. Gerber, B. Reinheimer and M. Volkamer, 'Investigating people's privacy risk perception', *Proceedings on Privacy Enhancing Technologies*, vol. 2019, pp. 267–288, Jul. 2019. DOI: 10.2478/popets-2019-0047.
- [26] N. Rahim, S. Hamid, M. L. Mat Kiah, S. Shamshirband and S. Furnell, 'A systematic review of approaches to assessing cybersecurity awareness', *Kybernetes*, May 2015. DOI: 10.1108/K-12-2014-0283.
- [27] P. D. Leedy and J. E. Ormrod, *Practical Research: Planning and Design*. Pearson, 2015.
- [28] G. Norman, 'Likert scales, levels of measurement and the "laws" of statistics', *Advances in Health Sciences Education*, vol. 15, no. 5, pp. 625–632, 2010, ISSN: 1573-1677. DOI: <https://doi.org/10.1007/s10459-010-9222-y>. [Online]. Available: <https://link.springer.com/article/10.1007/s10459-010-9222-y>.
- [29] S. .-. S. Sentralbyrå. (). 07459: Alders- og kjønnsfordeling i kommuner, fylker og hele landets befolkning (k) 1986 - 2020, [Online]. Available: <https://www.ssb.no/statbank/table/07459>. (accessed: 10.06.2020).
- [30] S. .-. S. Sentralbyrå. (). Befolkningens utdanningsnivå, [Online]. Available: <https://www.ssb.no/utniv/>. (accessed: 10.06.2020).
- [31] J. Ehrlinger, K. Johnson, M. Banner, D. Dunning and J. Kruger, 'Why the unskilled are unaware: Further explorations of (absent) self-insight among the incompetent', *Organizational behavior and human decision processes*, 2008. DOI: <https://doi.org/10.1016/j.obhdp.2007.05.002>.
- [32] I. A. McCormick, F. H. Walkey and D. E. Green, 'Comparative perceptions of driver ability— a confirmation and expansion', *Accident Analysis Prevention*, vol. 18, no. 3, pp. 205–208, 1986, ISSN: 0001-4575. DOI: [https://doi.org/10.1016/0001-4575\(86\)90004-7](https://doi.org/10.1016/0001-4575(86)90004-7). [Online]. Available: <http://www.sciencedirect.com/science/article/pii/0001457586900047>.

- [33] H. Carlsen and D. V. Krekling. (). Frykter at smarthøytaleren sladrer om privatlivet ditt, [Online]. Available: <https://www.nrk.no/norge/frykter-at-smarthoyttaleren-sladrer-om-privatlivet-ditt-1.14429863>. (accessed: 04.06.2020).
- [34] NRK. (). Avslørt av mobilen, [Online]. Available: <https://www.nrk.no/norge/xl/avslort-av-mobilen-1.14911685>. (accessed: 04.06.2020).
- [35] V. Gkioulos, G. B. Wangen, S. Katsikas, G. Kavallieratos and P. Kotzanikolaou, 'Security awareness of the digital natives', *Information (Switzerland)*, vol. 8, Apr. 2017. DOI: 10.3390/info8020042.
- [36] M. Nicholas. (). How hackers steal your reused passwords: Credential stuffing, [Online]. Available: <https://blog.dashlane.com/hackers-steal-your-reused-passwords-using-credential-stuffing/>. (accessed: 14.06.2020).
- [37] LastPass. (). Psychology of passwords: The online behavior that's putting you at risk, [Online]. Available: <https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LastPass-B2C-Assets-Ebook.pdf>. (accessed: 14.06.2020).
- [38] P. Stancik. (). At least 15% of home routers are unsecured, [Online]. Available: <https://web.archive.org/web/20191230070532/https://www.welivesecurity.com/2016/10/19/least-15-home-routers-unsecure/>. (accessed: 01.06.2020).

Appendix A

Main questionnaire form

This appendix will include the questionnaire form I used to collect data from my main sample. This questionnaire is written in Norwegian and can be viewed starting from the next page.

Sikkerhetsbevissthet ved bruk av smarthus

Side 1

Formålet med denne undersøkelsen er å kartlegge sikkerhetsbevisstheten til personer som bor i smarthus. Undersøkelsen er en del av et masterprosjekt på NTNU og vil ta deg gjennom spørsmål om blant annet dine daglige bruksvaner, risikovurderinger, og kjennskap til ulike områder som er relevant til smarthus.

Undersøkelsen er fullstendig anonym og det vil ikke behandles personopplysninger som kan knyttes til deg.

Spørreskjemaet vil ta ca 5 minutter å gjennomføre. Takk for at du tar deg tiden!

- Fredrik Løvaas Theien, Masterstudent ved NTNU



Side 2

Hva er din alder? *

- Yngre enn 20
- 20-29
- 30-39
- 40-49
- 50-59
- Eldre enn 60
- Ønsker ikke oppgi

Hva er ditt kjønn? *

- Mann
- Kvinne
- Ønsker ikke oppgi

Hva er ditt høyeste fullførte utdanningsnivå? *

- Ingen
- Grunnskolenivå
- Videregående skolenivå
- Fagskolenivå
- Universitets- og høyskolenivå, til og med 4 år

- Universitets- og høgskolenivå, lengre enn 4 år
- Ønsker ikke oppgi

Hvilket fylke er du bosatt i? *

- Oslo
- Viken
- Innlandet
- Vestfold og Telemark
- Agder
- Rogaland
- Vestland
- Møre og Romsdal
- Trøndelag
- Nordland
- Troms og Finnmark
- Ønsker ikke oppgi



Side 3


Hvilke typer smartenheter har du i boligen din? *

(Kryss av for alle som gjelder)

- Stemmeassistent
- Høytaler
- Støvsuger
- Smarthub
- SmartTV
- Smart skjerm
- Ruter
- Dørlås
- Lyspærer

- Smart dimmer
- Smart bryter
- Kjøkkenutstyr
- Overvåkning
- Alarmer
- Bevegelsessensor
- Termostat
- Andre, vennligst spesifiser under
- Ingen

Hvilke andre smartenheter har du?

-  Dette elementet vises kun dersom alternativet «Andre, vennligst spesifiser under» er valgt i spørsmålet «Hvilke typer smartenheter har du i boligen din?»

Er du husholdningens smarthus administrator? *

- Ja
- Nei
- Vet ikke

Har du en profesjonell og/eller hobbybasert bakgrunn i IT eller teknologi? *

- Ja
- Nei
- Vet ikke

Hvor kjent er du med følgende områder?

Teknologi *

- Lite kjent

- Litt kjent
 - Kjent
 - Godt kjent
-

Datasikkerhet *

- Lite kjent
 - Litt kjent
 - Kjent
 - Godt kjent
-

Smarthus *

- Lite kjent
- Litt kjent
- Kjent
- Godt kjent



Side 4

Oppdaterer du, eller andre i husholdningen, smartenhetene når oppdateringer blir tilgjengelige? *

- Ja, stort sett alltid med en gang
- Ja, men det hender jeg venter en stund
- Nei, tenker ikke så veldig mye på det
- Vet ikke

Bytter du, eller andre i husholdningen, standard passord på smartenheter etter de er kjøpt? *

- Ja
- Ja, men bare hvis enheten ikke kommer med et unikt passord når den er kjøpt
- Nei
- Vet ikke

Bruker du en passord manager for å holde styr på passordene dine? *

- Ja
- Nei
- Kjenner ikke til passord managere

Bruker du samme passord på flere smartenheter/tjenester? *

- Ja, bruker alltid samme passord
- Ja, men bare på noen få enheter og tjenester
- Nei, men bruker små variasjoner av samme passord
- Nei, bruker aldri samme passord

Når du bruker en smartenhet, pleier du å skru av tjenester og funksjoner du ikke benytter deg av? *

- Ja
- Nei
- Vet ikke

Er smartenhetene dine koblet på et adskilt segment av hjemmenettverket ditt der det er mulig? *

Med adskilt segment mener jeg segmentering av hjemmenettverket slik at smarte enheter ikke har direkte kontakt med dine personlige enheter, som for eksempel mobil, PC, og nettbrett.

- Ja
- Nei
- Vet ikke

Endrer du vanligvis personvern og sikkerhetsinnstillingene på smartenhetene dine? *

- Ja
- Nei
- Vet ikke

For å koble smartenhetene dine til Internett, foretrekker du kabel eller trådløs? *

- Foretrekker kabel der det er mulig
- Foretrekker trådløst der det er mulig
- Ikke viktig
- Annet

Hvilke andre tanker har du rundt dette?

- Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «For å koble smartenhetene dine til Internett, foretrekker du kabel eller trådløs?»



Side 5

På en skala fra 1-6, hvor høy risiko tenker du følgende scenarier utgjør?

(1 tilsvarer lav risiko, og 6 tilsvarer høy risiko)

En eller flere av smartenhetene dine blir infisert av skadelig programvare *

- 1
- 2
- 3
- 4
- 5
- 6

En uautorisert person får tilgang til innloggingsdetaljer til en eller flere smartenheter

- 1
- 2
- 3
- 4
- 5
- 6

En uautorisert person bryter seg inn i huset og stjeler smartenhetene dine *

- 1
- 2
- 3
- 4
- 5
- 6

En uautorisert person tar kontroll over dine smartenheter og bruker de i angrep mot andre *

- 1
- 2
- 3
- 4
- 5

Appendix B

Control group questionnaire form

This appendix will include the questionnaire form I used to collect data from my control group sample. This questionnaire is written in Norwegian and can be viewed starting from the next page.

Sikkerhetsbevissthet ved bruk av smarthus - kontrollgruppe

Side 1

Formålet med denne undersøkelsen er å kartlegge en kontrollgruppe for å undersøke og sammenligne sikkerhetsbevisstheten til personer som bor i smarthus med resten av befolkningen. Undersøkelsen er en del av et masterprosjekt på NTNU og vil ta deg gjennom spørsmål om blant annet dine daglige bruksvaner, risikovurderinger, og kjennskap til ulike områder relatert til datasikkerhet og smartenheter. Du trenger ikke eie smartenheter for å delta i denne undersøkelsen.

Når du er ferdig med spørreundersøkelsen kan du be om kvittering som gir deg muligheten til rette på eller slette ditt svar. All data i denne undersøkelsen vil bli behandlet anonymt.

Spørreskjemaet vil ta ca 5 minutter å gjennomføre. Takk for at du tar deg tiden!

- Fredrik Løvaas Theien, Masterstudent ved NTNU



Side 2

Hva er din alder? *

- Yngre enn 20
- 20-29
- 30-39
- 40-49
- 50-59
- Eldre enn 60
- Ønsker ikke oppgi

Hva er ditt kjønn? *

- Mann
- Kvinne
- Ønsker ikke oppgi

Hva er ditt høyeste fullførte utdanningsnivå? *

- Ingen
- Grunnskolenivå
- Videregående skolenivå
- Fagskolenivå

- Universitets- og høghskolenivå, til og med 4 år
- Universitets- og høghskolenivå, lengre enn 4 år
- Ønsker ikke oppgi

Hvilket fylke er du bosatt i? *

- Oslo
- Viken
- Innlandet
- Vestfold og Telemark
- Agder
- Rogaland
- Vestland
- Møre og Romsdal
- Trøndelag
- Nordland
- Troms og Finnmark
- Ønsker ikke oppgi




Side 3

Eier du en eller flere smartenheter? *

En smartenhet er en elektronisk enhet som vanligvis er koblet til andre enheter eller nettverk gjennom ulike trådløse protokoller, og som til en viss grad kan fungere interaktivt og selvstendig.

- Ja
- Nei
- Vet ikke

Hvilke typer smartenheter har du i boligen din? *

-  Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Eier du en eller flere smartenheter?»

(Kryss av for alle som gjelder)

- Stemmeassistent
- Høytaler
- Støvsuger
- Smarthub
- SmartTV
- Smart skjerm
- Ruter
- Dørlås
- Lyspærer
- Smart dimmer
- Smart bryter
- Kjøkkenutstyr
- Overvåkning
- Alarmer
- Bevegelsessensor
- Termostat
- Andre, vennligst spesifiser under

Hvilke andre smartenheter har du?

- i Dette elementet vises kun dersom alternativet «Andre, vennligst spesifiser under» er valgt i spørsmålet «Hvilke typer smartenheter har du i boligen din?»

Er du husholdningens smarthus administrator?

- i Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Eier du en eller flere smartenheter?»

Et smarthus er et hus utstyrt med smartenheter som ofte kan fjernkontrolleres.

- Ja
- Nei
- Vet ikke

Har du en profesjonell og/eller hobbybasert bakgrunn i IT eller teknologi? *

- Ja
- Nei
- Vet ikke

Hvor kjent er du med følgende områder?

Teknologi *

- Lite kjent
- Litt kjent
- Kjent
- Godt kjent

Datasikkerhet *

- Lite kjent
- Litt kjent
- Kjent
- Godt kjent

Smarthus *

- Lite kjent
- Litt kjent
- Kjent



Godt kjent



Sideskift

Side 4

Oppdaterer du, eller andre i husholdningen, dine elektroniske enheter når oppdateringer blir tilgjengelige? *

- Ja, stort sett alltid med en gang
- Ja, men det hender jeg venter en stund
- Nei, tenker ikke så veldig mye på det
- Vet ikke

Bytter du, eller andre i husholdningen, standard passord på smartenheter etter de er kjøpt? *

- Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Eier du en eller flere smartenheter?»
- Ja
- Ja, men bare hvis enheten ikke kommer med et unikt passord når den er kjøpt
- Nei
- Vet ikke

Bruker du en passord manager for å holde styr på passordene dine? *

- Ja
- Nei
- Kjenner ikke til passord managere

Bruker du samme passord på flere enheter/tjenester? *

- Ja, bruker alltid samme passord
- Ja, men bare på noen få enheter og tjenester
- Nei, men bruker små variasjoner av samme passord
- Nei, bruker aldri samme passord

Når du bruker et elektronisk produkt, pleier du å skru av tjenester og funksjoner du ikke benytter deg av? *

- Ja
- Nei
- Vet ikke

Er smartenhetene dine koblet på et adskilt segment av hjemmenettverket ditt der det er mulig? *

- Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Eier du en eller flere smartenheter?»

Med adskilt segment mener jeg oppdeling av hjemmenettverket slik at smarte enheter ikke har direkte kontakt med dine personlige enheter, som for eksempel mobil, PC, og nettbrett.

- Ja
- Nei
- Vet ikke

Endrer du vanligvis personvern- og sikkerhetsinnstillinger på enheter og tjenester du benytter deg av? *

- Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Eier du en eller flere smartenheter?»

- Ja
- Nei
- Vet ikke

For å koble smartenhetene dine til Internett, foretrekker du kabel eller trådløs? *

- Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Eier du en eller flere smartenheter?»

- Foretrekker kabel der det er mulig
- Foretrekker trådløst der det er mulig
- Ikke viktig
- Annet

Hvilke andre tanker har du rundt dette?

- i** Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «For å koble smartenhetene dine til Internett, foretrekker du kabel eller trådløs?»

 Sideskift

Side 5

På en skala fra 1-6, hvor høy risiko tenker du følgende scenarioer utgjør?

1 tilsvarer lav risiko, og 6 tilsvarer høy risiko.

Risiko regnes som forholdet mellom sannsynligheten for at en hendelse kan inntreffe, og konsekvensen av hendelsen dersom den inntreffer.

En eller flere av smartenhetene dine blir infisert av skadelig programvare *

- 1
- 2
- 3
- 4
- 5
- 6

En uautorisert person får tilgang til innloggingsdetaljer til en eller flere smartenheter *

- 1
- 2
- 3
- 4
- 5

6

En uautorisert person bryter seg inn i huset og stjeler smartenhetene dine *

 1 2 3 4 5 6

En uautorisert person tar kontroll over dine smartenheter og bruker de i angrep mot andre *

 1 2 3 4 5 6

En uautorisert person avlytter nettverks-trafikken til smartenhetene dine *

 1 2 3 4

Appendix C

Bivariate analysis of age differences

		Descriptives							
		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
To connect your smart devices to the Internet, do you prefer cable or wireless?	20-29	33	1.61	0.827	0.144	1.31	1.90	1	3
	30-39	102	1.34	0.637	0.063	1.22	1.47	1	4
	40-49	56	1.63	0.885	0.118	1.39	1.86	1	4
	Older than 50	30	1.90	0.845	0.154	1.58	2.22	1	4
	Total	221	1.53	0.784	0.053	1.43	1.63	1	4
Knowledge of the security of the smart devices you utilise?	20-29	33	2.67	0.890	0.155	2.35	2.98	1	4
	30-39	102	2.75	0.814	0.081	2.60	2.91	1	4
	40-49	56	2.79	0.847	0.113	2.56	3.01	1	4
	Older than 50	30	3.20	0.610	0.111	2.97	3.43	2	4
	Total	221	2.81	0.820	0.055	2.70	2.92	1	4
Knowledge of risks you expose yourself to by buying used smart devices?	20-29	33	2.88	0.992	0.173	2.53	3.23	1	4
	30-39	102	2.88	0.882	0.087	2.71	3.06	1	4
	40-49	56	2.98	0.820	0.110	2.76	3.20	1	4
	Older than 50	30	3.47	0.681	0.124	3.21	3.72	2	4
	Total	221	2.99	0.876	0.059	2.87	3.10	1	4

Figure C.1: Descriptive statistics of age up against other variables

Multiple Comparisons

Tukey HSD

Dependent Variable			Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval		
						Lower Bound	Upper Bound	
To connect your smart devices to the Internet, do you prefer cable or wireless?	20-29	30-39	0.263	0.153	0.317	-0.13	0.66	
		40-49	-0.019	0.168	0.999	-0.45	0.42	
		Older than 50	-0.294	0.193	0.424	-0.79	0.21	
	30-39	20-29	-0.263	0.153	0.317	-0.66	0.13	
		40-49	-0.282	0.127	0.122	-0.61	0.05	
		Older than 50	-.557*	0.159	0.003	-0.97	-0.15	
	40-49	20-29	0.019	0.168	0.999	-0.42	0.45	
		30-39	0.282	0.127	0.122	-0.05	0.61	
		Older than 50	-0.275	0.173	0.386	-0.72	0.17	
	Older than 50	20-29	0.294	0.193	0.424	-0.21	0.79	
		30-39	.557*	0.159	0.003	0.15	0.97	
		40-49	0.275	0.173	0.386	-0.17	0.72	
	Knowledge of the security of the smart devices you utilise?	20-29	30-39	-0.088	0.162	0.948	-0.51	0.33
			40-49	-0.119	0.178	0.908	-0.58	0.34
			Older than 50	-.533*	0.204	0.047	-1.06	0.00
30-39		20-29	0.088	0.162	0.948	-0.33	0.51	
		40-49	-0.031	0.135	0.996	-0.38	0.32	
		Older than 50	-.445*	0.168	0.043	-0.88	-0.01	
40-49		20-29	0.119	0.178	0.908	-0.34	0.58	
		30-39	0.031	0.135	0.996	-0.32	0.38	
		Older than 50	-0.414	0.183	0.111	-0.89	0.06	
Older than 50		20-29	.533*	0.204	0.047	0.00	1.06	
		30-39	.445*	0.168	0.043	0.01	0.88	
		40-49	0.414	0.183	0.111	-0.06	0.89	
Knowledge of risks you expose yourself to by buying used smart devices?		20-29	30-39	-0.004	0.172	1.000	-0.45	0.44
			40-49	-0.103	0.189	0.947	-0.59	0.39
			Older than 50	-.588*	0.217	0.036	-1.15	-0.03
	30-39	20-29	0.004	0.172	1.000	-0.44	0.45	
		40-49	-0.100	0.143	0.898	-0.47	0.27	
		Older than 50	-.584*	0.179	0.007	-1.05	-0.12	
	40-49	20-29	0.103	0.189	0.947	-0.39	0.59	
		30-39	0.100	0.143	0.898	-0.27	0.47	
		Older than 50	-0.485	0.195	0.064	-0.99	0.02	
	Older than 50	20-29	.588*	0.217	0.036	0.03	1.15	
		30-39	.584*	0.179	0.007	0.12	1.05	
		40-49	0.485	0.195	0.064	-0.02	0.99	

*. The mean difference is significant at the 0.05 level.

Figure C.2: Post-hoc tukey of age categories up against other variables

Appendix D

Bivariate analysis of education differences

Descriptives

Are you using a password manager to store your passwords?

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
High school level	48	1.65	0.565	0.081	1.48	1.81	1	3
Vocational college level	55	1.62	0.527	0.071	1.48	1.76	1	3
University- and college level, up to and including 4 years	76	1.41	0.521	0.060	1.29	1.53	1	3
University- and college level, longer than 4 years	42	1.43	0.501	0.077	1.27	1.58	1	2
Total	221	1.52	0.536	0.036	1.44	1.59	1	3

Figure D.1: Descriptive statistics of education up against the use of password managers

Multiple Comparisons

Dependent Variable: Are you using a password manager to store your passwords?
Tukey HSD

(I) What is your highest completed education level?		Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
		J)			Lower Bound	Upper Bound
High school level	Vocational college level	0.028	0.104	0.993	-0.24	0.30
	University- and college level, up to and including 4 years	0.238	0.097	0.072	-0.01	0.49
	University- and college level, longer than 4 years	0.217	0.112	0.212	-0.07	0.51
Vocational college level	High school level	-0.028	0.104	0.993	-0.30	0.24
	University- and college level, up to and including 4 years	0.210	0.094	0.114	-0.03	0.45
	University- and college level, longer than 4 years	0.190	0.108	0.300	-0.09	0.47
University- and college level, up to and including 4 years	High school level	-0.238	0.097	0.072	-0.49	0.01
	Vocational college level	-0.210	0.094	0.114	-0.45	0.03
	University- and college level, longer than 4 years	-0.021	0.102	0.997	-0.28	0.24
University- and college level, longer than 4 years	High school level	-0.217	0.112	0.212	-0.51	0.07
	Vocational college level	-0.190	0.108	0.300	-0.47	0.09
	University- and college level, up to and including 4 years	0.021	0.102	0.997	-0.24	0.28

Figure D.2: Post-hoc tukey of education categories up against the use of password managers

Appendix E

Analysis of changing settings and knowing data flow

Descriptives

Knowledge of the data flow between your smart devices and the Internet?

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Yes	125	3.06	0.878	0.078	2.91	3.22	1	4
No	86	2.55	0.916	0.099	2.35	2.74	1	4
I don't know	11	2.36	0.674	0.203	1.91	2.82	1	3
Total	222	2.83	0.921	0.062	2.71	2.95	1	4

Figure E.1: Descriptive statistics of changing privacy and security settings and knowledge of data flow

Multiple Comparisons

Dependent Variable: Knowledge of the data flow between your smart devices and the Internet?
Tukey HSD

(I) Do you usually change the privacy and security settings of your smart devices?	J	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Yes	No	.517 [*]	0.124	0.000	0.23	0.81
	I don't know	.700 [*]	0.278	0.033	0.04	1.36
No	Yes	-.517 [*]	0.124	0.000	-0.81	-0.23
	I don't know	0.183	0.283	0.795	-0.49	0.85
I don't know	Yes	-.700 [*]	0.278	0.033	-1.36	-0.04
	No	-0.183	0.283	0.795	-0.85	0.49

*. The mean difference is significant at the 0.05 level.

Figure E.2: Post-hoc tukey of changing privacy and security settings and knowledge of data flow

Appendix F

Control group analysis

Descriptive Statistics of Perceived Risk					
	N	Min	Max	Mean	Std. Dev.
1. One or more of your smart devices gets infected by malicious software	35	1	6	3.11	1.278
2. An unauthorized person gets access to login details for one or more smart devices	35	1	6	3.14	1.240
3. An unauthorized person breaks into the house and steals your smart devices	35	1	6	2.23	1.114
4. An unauthorized person takes control of your smart devices and uses them to attack others	35	1	6	2.60	1.288
5. An unauthorized person intercepts the network traffic to your smart devices	35	1	6	2.86	1.375
6. One or more smart devices are accidentally rendered unusable	35	1	6	2.94	1.349
7. An unauthorized person gets remote access to one or more of your smart devices	35	1	6	2.69	1.157
8. An unauthorized person accesses personal information through your smart devices	35	1	6	3.23	1.516

Table F.1: Descriptive statistics of perceived risk from my control group based on 8 risk scenarios

Do you, or others in the household, update your electronic devices when updates are available?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes, pretty much always right away	20	46.5	46.5	46.5
	Yes, but I sometimes wait a while	18	41.9	41.9	88.4
	No, don't think about that very much	3	7.0	7.0	95.3
	I don't know	2	4.7	4.7	100.0
	Total	43	100.0	100.0	

Table E2: Frequencies of the control groups routines towards updating their electronic devices

When using an electronic device, do you tend to turn off services and features you do not use?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	26	60.5	60.5	60.5
	No	14	32.6	32.6	93.0
	I don't know	3	7.0	7.0	100.0
	Total	43	100.0	100.0	

Table E3: Frequencies of the control groups routines towards turning off features and services they do not use

Do you usually change the privacy and security settings of your smart devices?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	16	37.2	45.7	45.7
	No	17	39.5	48.6	94.3
	I don't know	2	4.7	5.7	100.0
	Total	35	81.4	100.0	
Missing	System	8	18.6		
Total		43	100.0		

Table E4: Frequencies of the control groups routines towards changing the privacy and security settings of their smart devices

Are you using a password manager to store your passwords?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	16	37.2	37.2	37.2
	No	23	53.5	53.5	90.7
	I don't know about password managers	4	9.3	9.3	100.0
	Total	43	100.0	100.0	

Table E5: Frequencies of the control groups routines towards using password managers

Do you use the same password on multiple devices/services?		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes, I always use the same password	3	7.0	7.0	7.0
	Yes, but only on a few devices and services	28	65.1	65.1	72.1
	No, but I use small variations of the same password	4	9.3	9.3	81.4
	No, I never use the same password	8	18.6	18.6	100.0
	Total	43	100.0	100.0	

Table E6: Frequencies of the control groups routines towards using the same password on multiple devices/services

