University of Reading

User experiences with simulated cyber-physical attacks on smart home IoT

Article

Published Version

Creative Commons: Attribution 4.0 (CC-BY)

Open Access

Huijts, N. M. A., Haans, A., Budimir, S., Fontaine, J. R. J., Loukas, G., Bezemskij, A., Oostveen, A., Filippoupolitis, A., Ras, I., IJsselsteijn, W. A. and Roesch, E. B. ORCID: https://orcid.org/0000-0002-8913-4173 (2023) User experiences with simulated cyber-physical attacks on smart home IoT. Personal and Ubiquitous Computing, 27 (1774). pp. 2243-2266. ISSN 1617-4917 doi: https://doi.org/10.1007/s00779-023-01774-5 Available at https://centaur.reading.ac.uk/120558/

It is advisable to refer to the publisher's version if you intend to cite from the work. See Guidance on citing.

To link to this article DOI: http://dx.doi.org/10.1007/s00779-023-01774-5

Publisher: Springer

Publisher statement: Cyber-attack; IoT; Smart home; Thematic analysis; Risk perception

All outputs in CentAUR are protected by Intellectual Property Rights law, including copyright law. Copyright and IPR is retained by the creators or other copyright holders. Terms and conditions for use of this material are defined in the End User Agreement.

www.reading.ac.uk/centaur

University of Reading

CentAUR

Central Archive at the University of Reading

Reading's research outputs online

Personal and Ubiquitous Computing (2023) 27:2243–2266
https://doi.org/10.1007/s00779-023-01774-5

ORIGINAL PAPER

User experiences with simulated cyber-physical attacks on smart home IoT

N. M. A. Huijts[1,2] · A. Haans[1] · S. Budimir[3] · J. R. J. Fontaine[3] · G. Loukas[4] · A. Bezemskij[4] · A. Oostveen[5] · A. Filippoupolitis[4,6] · I. Ras[7,8] · W. A. IJsselsteijn[1] · E. B. Roesch[7]

Received: 18 March 2022 / Accepted: 30 August 2023 / Published online: 22 September 2023
© The Author(s) 2023

Abstract
With the Internet of Things (IoT) becoming increasingly prevalent in people's homes, new threats to residents are emerging such as the cyber-physical attack, i.e. a cyber-attack with physical consequences. In this study, we aimed to gain insights into how people experience and respond to cyber-physical attacks to their IoT devices. We conducted a naturalistic field experiment and provided 9 Dutch and 7 UK households, totalling 18 and 13 participants respectively, with a number of smart devices for use in their home. After a period of adaptation, simulated attacks were conducted, leading to events of varying noticeability (e.g., the light going on or off once or several times). After informing people simulated attacks had occurred, the attacks were repeated one more time. User experiences were collected through interviews and analysed with thematic analyses. Four relevant themes were identified, namely (1) the awareness of and concern about privacy and security risks was rather low, (2) the simulated attacks made little impression on the participants, (3) the participants had difficulties with correctly recognizing simulated attacks, and (4) when informed about simulated attacks taking place; participants noticed more simulated attacks and presented decision rules for them (but still were not able to identify and distinguish them well—see Theme 3). The findings emphasise the need for training interventions and an intrusion detection system to increase detection of cyber-physical attacks.

Keywords Cyber-attack · IoT · Smart home · Thematic analysis · Risk perception

✉ N. M. A. Huijts
n.m.a.huijts@utwente.nl

1 Human-Technology Interaction Group, Faculty of Industrial Engineering and Innovation Sciences, Eindhoven University of Technology, Eindhoven, The Netherlands

2 Section Psychology of Conflict, Risk and Safety, Department of Behavioural, Management and Social Sciences, University of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands

3 Department of Work, Organization and Society, Faculty of Psychology and Educational Sciences, Ghent University, Ghent, Belgium

4 University of Greenwich, London, UK

5 Industrial Psychology and Human Factors Group, Centre for Robotics and Assembly, School of Aerospace, Transport, and Manufacturing, Cranfield University, Cranfield, UK

6 Real World Analytics & AI, IQVIA, London, UK

7 Centre for Integrative Neuroscience and Neurodynamics, School of Psychology and Clinical Language Sciences, University of Reading, Reading, UK

8 D-INFK, ETH Zurich, Zurich, Switzerland

1 Introduction

The use of Internet of Things (IoT) devices (also called smart home devices or smart devices) in households is becoming increasingly popular. Smart home devices allow people to operate regular devices (e.g., lights, speakers, and vacuum cleaners) in their home through smart phone apps, via voice control or by setting automation. This brings valuable benefits such as increased functionality, convenience, and comfort. Notwithstanding all the benefits, these developments also introduce new risks, especially for cybersecurity breaches. Smart devices have vulnerabilities that can allow malicious actors (hackers) to gain unauthorised access, to collect data and/or seize control of pre-existing functionalities. Besides the violation of user's privacy, the intrusion into household devices by means of a cyber-attack can become a cyber-physical attack, i.e., a cyber-attack with physical consequences [1, 2].

Various cybersecurity breaches of smart devices (e.g., baby monitors, security cameras, and doorbells) have already

been reported in the media. The breaches resulted amongst other things in unsupervised conversations with children and unauthorised online streaming of the breached content [3–8]. Hackers have also been found to exploit vulnerabilities in smart devices to perform DDOS-attacks (distributed denial of service), causing disruption of infrastructure (e.g., [9, 10]) such as taking down the central heating system of flats [11]. It could be considered only a matter of time before hackers take even more control by actuating smart devices (e.g., switching on sprinklers, starting coffee machine or ovens, defrosting the freezer, and turning up the heating, controlling physical movement of vacuum cleaners) thereby causing damage to the home and posing physical safety risks for the dwellers.

Besides one experimental study that has investigated the structure and determinants of emotional responses to cyber-physical attack scenarios [12], no insight yet exists into how people experience being the victim of a cyber-physical attack in their smart homes. Studies in the context of burglary, which is another type of physical attack in the home environment, have shown that victims generally have considerable negative psychological experiences, often with a long-lasting negative effect on wellbeing [13, 14]. A study on long-term in-home monitoring has also shown that, due to the privacy invasion, people experience negative emotions and alter their behaviour, such as avoiding walking around naked [15]. An experimental study on simulated cyber-attacks (not in the home) has shown that peoples' cortisol level and threat perception go up when they are perceiving to be cyber-attacked [16], while also a cybercrime report by Norton has found that people experience a range of negative emotions when being cyber-attacked [17]. Based on these studies, it may be expected that people also have significant negative emotional responses to cyber-physical attacks in the house. However, in contrast to burglary and regular cyber-crimes, cyber-physical attacks are unique in that they may cause physical harm in the home (a supposedly safe environment), while the attacker is physically far away and difficult to apprehend [17]. These unique properties of cyber-physical attacks on smart home IoT may lead to unique responses in comparison to burglary and regular cyber-attacks.

A good understanding of the nature of victims' experiences when undergoing a cyber-physical attack is key for understanding the severity of the threat and the efforts that are needed to reduce the risks to home occupants. Furthermore, it will inform us on how to aid users of smart devices in becoming more aware and resilient. The current study therefore investigates how people experience receiving a cyber-attack on their smart devices in their home environment using an experimental design. In a field experiment, nine Dutch and seven UK households were provided with smart devices, and cyber-physical attacks were simulated. The participants' experiences were probed through questionnaires and interviews. The current study reports the findings of a thematic analysis [18] of the interviews conducted throughout the study.

To study how people experience cyber-attacks, it is important to involve researchers in both the cyber-security domain and the behavioural domain, as well as researchers that can bridge the divide between these two domains. Therefore, cyber-security experts, psychologists, and human-technology interaction researchers cooperated in this study to simulate cyber-attacks on smart home devices and to investigate how they were experienced by the users of the smart devices. This study took part within the EU funded project "Emotion Psychology Meets Cyber-security" (https://cocoon-project.eu/).

1.1 Research aim

As the investigation of the psychological consequences of cybersecurity attacks on smart home devices is a completely new area of research about which there is mostly only anecdotal evidence from media coverage, the aim of the current study was to explore how people experience a cyber-attack without imposing a-priori expectations about the outcomes of the study. Furthermore, we aimed to study the impact of cybersecurity breaches in a realistic context as possible. Since actual experiences with cyber-physical attacks on smart home IoT were still limited, we chose to conduct a naturalistic field experiment in which we installed smart devices in participants' homes and executed simulated attacks on them. We tracked the participants' experiences with the simulated attacks using semi-structured interviews with open questions.

More specifically, British and Dutch participants were given a set of smart home devices and, after a period of getting used to them, underwent simulated attacks whereby devices acted irregularly as if they had been breached and controlled by a hacker. First, participants experienced the simulated attacks without being informed of the goal of the study. A few weeks later, participants were informed that simulated attacks had taken place without being told precisely *which* irregularities were introduced. The participants were then again exposed to the same types of attacks, to see whether being informed about their possible occurrence led to different detection rates and experiences.

With qualitative research methods, the study aimed to capture people's full range of experiences without imposing our own a priori expectations on the study design (for example through the formulation of testable hypotheses or through the choice of measurement instruments and closed question formats). We therefore gathered data through semi-structured interviews with a large set of open questions, which were analysed with thematic analysis. These questions focused mostly on the participants' positive and negative

expectations of, and actual experiences with, the devices before, during, and immediately after the field experiment.

Although no a-priori hypotheses were formulated, the researchers had some general expectations such as that participants would have some awareness of the cybersecurity risks of smart home IoT due to media coverage of these risks and that participants would have some kind of negative experience when noticing a simulated attack or when being informed about simulated cyber-attacks having been conducted.

Finally, as cyber-attacks to domestic IoT devices can potentially lead to physical and financial harm, as well as psychological distress, the study was developed taking into account a multitude of ethical concerns, which led to strict requirements and limitations. This included restricting the extent of the consequences of the simulated cyber-attacks (e.g., only opening or closing the shutter of the smart camera rather than video recording participants through the smart camera, and having the simulated attacks only produce sounds with low or moderate volumes); limiting the use of the devices (e.g. apps were not allowed to be installed on mobile phones, but only on the dedicated tablet that had to stay inside the home to avoid concern about home activity while being away of the home), allowing only people that were tested to have sufficient psychological resilience to participate; and carefully monitoring participants' responses (through an online diary and questionnaire—both not reported on in this study) so that we could intervene or stop the study as soon as a worrisome situation would arise.

2 Method

2.1 Participants

The study took place in the Netherlands (NL) and the United Kingdom (UK), from September to December, in 2018. Participants were recruited in the Netherlands through the participant database of the Human-Technology Interaction group of the Eindhoven University of Technology and in the United Kingdom through the networks of the involved researchers at the University of Greenwich (Greater London) and the University of Reading (Berkshire).

There were several requirements for participants to be included in the experiment. First, all household members had to be above 18 years old and had to consent to participate in the study. Second, to make sure that psychologically more vulnerable people would not take part in the study, all household members had to score in the normal range on the Achenbach System of Empirically Based Assessment (ASEBA) [19] assessing internalising, thought problems, attention problems, and externalising. Third, all participants had to agree to invest a substantial amount of time during the study, including the use of the devices, taking part in interviews with the researchers (which were recorded), and filling in online questionnaires. Fourth, participants needed to indicate that they would spend a substantial amount of time at home during the period of the study (so that they had sufficient interaction with the devices and were more likely to be at home when the simulated attacks were executed). This last requirement was relaxed in the UK where it turned out to be difficult to find sufficient participants. Fifth, participants were not allowed to have pets or have much noise from the streets as we measured the sound level in the home so that we could later make an estimation of the presence of the participants in the home during the attacks (which we did not use in this study). Sixth, participants that needed weighing scales for medical reasons were not allowed to participate (as we were going to affect the weights stored in the app in a simulated attack).

We aimed to have 10 households in each country. However, due to difficulties finding enough participants and a few households withdrawing from the experiment early, a total of 9 Dutch households with 18 members (9 men and 9 women, $M_{age} = 54$ years old) and 7 UK households with 13 members (7 men and 6 women, $M_{age} = 40$) completed the experiment.

The Dutch participants could be grouped in largely three categories: students or employed people in their 20 s (8 persons, 23 to 26 years old), employed and unemployed persons in their 50 s and 60 s, but before the Dutch pension age (6 persons, 55 to 66 years old), and elderly retired persons (6 persons, 68 to 75 years old). The UK participants consisted of 12 employed persons within a wide age range (23 to 59 years old) and one elderly person (in their 70 s).

Ethical approval for the study was provided by each of the participating universities: Eindhoven University of Technology, Ghent University, University of Greenwich, and University of Reading. Participants were compensated for their participation in the study by being gifted all the IoT devices at the end of the study (with an estimated worth of approximately 1000 Euro).

2.2 Design

The participants received a set of smart devices, namely, a smart weighing scales, a smart security camera, a smart lamp, a smart speaker, and a set with smart sensors (a motion sensor, a door-window sensor, and two keychain presence sensors) and a smart socket. The smart devices were connected to a separate programmable Wi-Fi router, which was connected to the home router. This router was installed to monitor traffic of the devices to the internet (which was part of a study not reported here). In addition to that, they were given a digital photo frame to plug into the smart socket (the frame itself was not smart as it was not connected to the internet) and a tablet to run the apps of the devices (with

links to fill in the online questionnaire and diary, the data of which are not used in the current manuscript).

The study consisted of four phases. In Phase 0, the participants received the devices. In Phase 1, the participants started to use and get acquainted with the devices. In Phase 2, the participants underwent a range of simulated attacks on the smart devices about which they were not informed. In Phase 3, the participants were informed that simulated attacks had taken place on their smart devices (without specifying them) and then underwent the same range of simulated attacks.

These phases varied in duration for the different households due to differences in starting times and because the schedule was sometimes adapted to accommodate for absence of participants (i.e., as they were traveling for example and thus known to be out of the home for multiple days). Phase 1 ranged between 13 and 59 days ($M = 35$ days). Phase 2 ranged between 12 and 31 days ($M = 23$ days). Phase 3 ranged between 5 and 13 days ($M = 12$ days).

The simulated attacks occurred in increasing intensities, having either 2 or 3 levels: for example, the first time the shutter of the smart camera closed and opened once, the second time three times, and the third time six times in Morse code pattern. Table 1 provides an overview of the simulated attacks per level.

In Phase 2, the attacks generally took place on different days, with regular "non-attack" days in between, while in Phase 3 participants received one or two attacks every day. All attacks were delivered to all households, with the exception of the level 1 attacks in Phase 2 in households nl2 and uk1-5, 7, and 9 due to these households starting later and needing to catch up with the already running study.

With the focus of the study being on cyber-physical attacks in the home, the devices and corresponding simulated attacks were chosen to cover both cyber and physical impact observable by non-expert users. In terms of cyber impact, we chose an attack where manipulation of the digital output (e.g., weight on the smart weighing scales) can be observed by the non-expert user through experience (e.g., by checking on a different scale). In terms of physical impact, we chose attacks where the impact is audible (smart speaker), visible (smart light and smart socket), and both audible and visible (smart camera with large privacy shutter). Additionally, the attacks with physical impact allowed covering both impact on actuation (smart light and smart socket) and on physical privacy (smart camera), covering the two primary families of cyber-physical attacks identified by Heartfield et al. [2].

All the attacks were executed through login credentials of the devices, mimicking what an attacker may have access to if they had acquired these credentials unlawfully. We enacted the attacks remotely through scripts and automated pipelines, following a precise schedule.

2.3 Procedure

Prior to the study, participants were sent a list of the devices they were going to receive with links to the user agreements that the manufacturers of the devices provided. At the first meeting (Phase 0), the participants were informed again of the procedures and materials related to the study (devices, interviews, questionnaires) and asked to sign an informed consent form. Then, the participants took part in the first interview (coded intph0) and all of the devices were installed by one of the researchers. The participants were then instructed to start using the devices in the way they themselves preferred (start of Phase 1).

Login codes of the devices were not shared with the participants, for two main reasons. First, the researchers used these to execute the simulated attacks via automation by means of IFTTT and Stringify and therefore did not want the participants to change the password. Second, the researchers needed to keep the participants from installing the accompanying apps on their own mobile phones and to avoid the participants from getting worried about simulated attacks while being away from the home. As a result of not having the passwords of the apps, the participants were unable to log into their apps when they accidentally got logged out and researchers occasionally went to the homes of the participants to log the apps back in.

In the middle of Phase 1, all the Dutch participants were interviewed on their initial experiences with the devices (coded intph1a). It was learned that the participants had difficulties with installing a second user for the scales and with commanding the smart speaker. Therefore, we provided all Dutch and UK participants with extra information on how to install a second user for the scales and with examples of commands for the smart speaker. The UK households started later and therefore had a shorter "acquaintance" Phase 1 and no mid-interview. After a few weeks, at the end of Phase 1, the participants were interviewed again (coded intph1b) and instructed to continue using the devices and filling in the online questionnaires (starting Phase 2).

During Phase 2, the participants' devices underwent simulated attacks. Participants could notice the attacks while they were taking place (e.g., see that the light went on or off or hear the smart speaker switch on the radio), or later notice the new state the device was in (e.g., the smart camera shutter being open instead of closed or the radio being off instead of on). For the weighing scales, participants could have noticed for level 1 that their last weight point was no longer visible in the app and for levels 2 and 3 that there was a different or new weight in their app. Another way in which participants could have noticed the level 2 and 3 weighing scales attacks was that the device did not longer recognize who was using the scales. Note that the scales use the weight measurements to identify which of the users is using the scales. Weight

Table 1 Overview of simulated attacks per device and per level

Device	Type of attack[1]	Level 1	Level 2	Level 3
Smart camera	Physical-actuation and privacy/visible and audible	Close and open with 20 s in between	Close, open, close, open, close, open, with 20 s in between	Close and open shutter in morse code: 4 times close and open (20 s in between), then a break of 40 s and then 2 times close and open
Smart weighing scales	Cyber/visible	Delete the last existing weight from the online account	Modify the last weighing point into a 3.1-kilo higher weight	Add one false weight (latest weight + 8.9 kg) to online account
Smart light	Physical-actuation/visible	Toggle once (turn on when off, turn off when on)	Toggle 3 times, with approx. 20 s in between	Toggle smart light in morse code: 4 times toggle, then a break of 40 s and then 2 times toggle (with 20 s in between each off and on)
Smart socket with photo frame plugged into it	Physical-actuation/visible	Toggle once	Toggle 3 times, with approx. 20 s in between	Toggle smart socket (and thus photo frame) in morse code: 4 times toggle, then a break of 40 s and then 2 times toggle (with 20 s in between each off and on)
Smart speaker	Physical-actuation/audible	Let the smart speaker say: "radio is unavailable"[2]. If the radio was on, this would make it stop playing	If the radio is playing then reduce volume by 50%, if radio is off, put it on and put on 20% (±5% because it is not precise)	

[1]We distinguished between attack types physical-unauthorised actuation, physical-privacy, and cyber and between noticeable by being audible, visible or both as identified in [2]

[2]We had the smart speaker say this by asking it to play a radio channel that did not exist or was locally not accessible

measurements are then automatically stored in that person's account. The level 2 and 3 attack resulted in a relatively high weight to be in the main user's history, leading to the device no longer being able to recognise this main user.

At the end of Phase 2, participants were once again interviewed (coded intph2a). Then the participants were informed of the goal of the study, which was to see how people would experience simulated attacks. We did not explain what these simulated attacks would have looked like or sounded like (see also Appendix, interview phase 2, part 2). The participants' responses to that news were also probed and recorded (coded intph2b). The participants were then asked whether they would be willing to undergo the simulated attacks again (which they all agreed; start of Phase 3).

After undergoing all attacks again, at the end of Phase 3, the participants were interviewed for a last time (coded intph3). This marked the end of the study. The participants were gifted with all of the smart devices and the photo frame, except for the tablet, and were provided some information on the chances of being hacked and how to prevent it. Table 2 shows the interviews taken per household. Guidelines for interview questions and the information provided at the end can be found in Appendix.

The interviews in Phase 0 consisted of an intake interview prior to the use of the IoT devices, focusing on the participants' general domestic technology adoption and usage and the expectations of the devices provided in the study (i.e., expected advantages and disadvantages). The other interviews elaborated on positive and negative experiences and perceived advantages and disadvantages of the provided IoT devices. Initially, these interviews did not explicitly address cyber-security and the simulated attacks as we wanted to access unprompted responses on whether, and how, people perceived such risks and experienced the attacks respectively. During the second half of the interview at the end of Phase 2 (intph2b) and during the final interview at the end of Phase 3 (intph3), the interviews addressed the topic of cyber-attacks in general and the simulated attacks more explicitly. During the final interview (intph3), all individual simulated attacks and day/time of execution in Phase 3 were shown to the participants, to which the participants could then comment on noticing them or not, and whether they would have been able to notice them (i.e., whether they were at home and presumably in the same room). We did not show and discuss the list of attacks and the dates and times of the attack in Phase 2 (intph2b) because we did not yet want to inform the participants of the details of the simulated attacks. This prevented us, however, from getting an estimation whether the participants would have been near enough to be able to notice the simulated attacks in this phase.

The interviews allowed for some flexibility to adjust questions according to the context of the interview. Per household we had between 74 and 260 min of interview material, amounting to 43 h and 53 min of interview material in total. The Dutch interviews were transcribed by a student assistant, while the UK interviews were professionally transcribed.

2.4 Analyses

We conducted thematic analysis on the interview data [18, 20]. Author N. H. first actively read all the interviews and made a list of possible codes, a code being "an analytically interesting idea, concept or meaning associated with particular segments of data" (p.53) [18]. This makes the extensive and rich raw data "accessible" for analysis. Then N. H. coded all snippets of the interviews and developed preliminary themes, a theme being "a pattern of shared meaning organized around one central concept" [18]. These initial themes were then revised and validated through an iterative process of going back-and-forth between themes and the raw data. To do that, in several cycles, N. H. reread all of the collected snippets per theme while looking for the deeper meaning of what was going on and discussing this with co-authors A. H. and W. I. J., reformulated the themes and

Table 2 Interviews held per household and the coding used

Household numbers	Phase 0	Phase 1		Phase 2		Phase 3
		(In the middle)	(At the end)	(At the end)	(After revealing goal)	(At the end)
	intph0	intph1a	intph1b	intph2a	intph2b	intph3
Netherlands (NL):						
hhnl 1, 2, 3, 4, 5, 6, 8, 9, 10	x	x	x	x	x	x
United Kingdom (UK):						
hhuk 1, 2, 3, 4, 5, 7, 9	x		x	x	x	x[1]

Phase 0 was the moment the devices were introduced to the participants. In Phase 1, the participants got used to the devices. Phase 2 had the first round of simulated attacks delivered. Phase 3 had the second round of delivery of simulated attacks after the execution of simulated attacks (without providing details about the simulated attacks) was revealed to the participants

[1]hhuk2 did not participate in the interview of phase 3

subthemes, and recoded and again collected fragments for each newly formulated sub theme. These steps were repeated until a coherent set of themes and sub themes was developed that described well what was really going on with respect to participants' experiences of the simulated attacks. The coding was thus done by one coder only, which is common and considered good practice in thematic analysis (p.55) [18].

3 Results

With thematic analysis, four main themes with several subthemes were identified (see Table 3 for an overview). We will discuss them one by one. Note that in the fragments provided below, "I" refers to the interviewer, "M" to male, and "F" to female participants.

3.1 Theme 1: the awareness of and concern about privacy and security risks was rather low

Participants showed little awareness of the privacy and security risks of the smart devices, and if aware, people thought the risks were negligible.

3.1.1 Subtheme 1.1: few participants brought up privacy and security risks when asked for disadvantages or risks of the devices, and when they did, concern was low

When asked for disadvantages of the smart devices before revealing the simulated attacks, the participants rarely mentioned risks, let alone privacy and security risks. When specifically asked for risks, privacy and security risks were still hardly mentioned or only very minimally.

> *I (interviewer): Do you see any risk with such devices? F (female participant): No, not at all. (hhuk1, intph0)*

Some people mentioned other risks, such as becoming dependent on the devices, the devices not functioning properly, fire caused by the devices, and electromagnetic radiation risks.

> *I: Do you think they [the devices] come with risks? (…) F: No, I couldn't say. M (male participant): No. I don't see any risk actually, none at all. F: They are not devices that heat up or something happens to them. So. M: No, and they are not using much power I think (hhnl4, intph0)*

Most participants did not read the user agreements that we emailed to them just before the start of the study. Reasons provided by the participants were that they generally find the information in those user agreements too long, difficult to understand, or useless to themselves. They also provided reasons such as trusting that there is nothing outrageous in these agreements, trusting the researchers that selected the devices, trusting that they would get warned through the media or people they know when there is something in the user agreement that is not acceptable, or arguing that they would not be able to do anything about it when they would disagree with it, or, that they were not worried about the data collection.

Table 3 Four themes and their subthemes extracted from the data

1. The awareness of and concern about privacy and security risks was rather low
   - 1.1 Few participants brought up privacy and security risks when asked for disadvantages or risks of the devices, and when they did, concern was low
   - 1.2 The participants mentioned several reasons why they were not worried about privacy and security
   - 1.3 The participants often had a limited understanding of how the devices worked and limited knowledge about cyber-attacks, which may have restricted their awareness of the risks
   - 1.4 The risks became less salient during the use of the devices as people grew accustomed to the presence of the devices
2. The simulated attacks made little impression on the participants
   - 2.1 The participants often did not notice the simulated attacks
   - 2.2 There were several reasons why the participants did not notice the simulated attacks
   - 2.3 Noticed irregularities were rarely experienced as a significant event and easily forgotten
   - 2.4 Participants did not indicate a negative change in their opinions about the functioning of the devices after undergoing the simulated attacks unknowingly
3. The participants had difficulties with correctly recognizing simulated attacks
   - 3.1 When simulated attacks were noticed, the participants often misattributed them
   - 3.2 Participants were hesitant to label a simulated attack a cyber-attack
   - 3.3 The participants were regularly very uncertain about what caused the irregularities that were related to a simulated attack
   - 3.4 When informed about simulated attacks having taken place, the participants intermingled simulated attacks and irregularities that the devices naturally exhibit
4. Being informed about simulated attacks taking place leads to more identification and reasoning about them
   - 4.1 When informed about simulated attacks taking place, more simulated attacks were noticed and classified as such
   - 4.2 Some participants provided a decision rule for telling apart a random irregularity from a simulated attack

There were a few participants who were aware of privacy and security risks. However, more often than not, they did not have a very strong concern about risks for themselves.

M: Privacy is a risk because anything is hackable. (hhuk5, intph0…) M: I think the Internet of Things software is not completely airtight, there are a lot of stories of smart TV's and such that get hacked, but the chance that someone specifically stands in front of our door to hack our camera is quite unlikely, I think. (hhnl5, intph0)

F: Uh, well, I am not knowledgeable about this at all, it does not keep me awake at night or anything, but our son in law (…) is world champion hacking and says that it is all possible. However, we did not really have a conversion about that (hhnl10, intph2a)

M: Imagine that they can see what you do, continuously. (…) But I say: 'that thing can also be turned off' (...) Those are the things of which you say 'are you afraid of that?' No. But it is a disadvantage. I am not afraid of it. (hhnl9, intph0).

The participants mostly expressed concern with the security camera recording them. Some participants, however, mitigated the concern by facing the camera towards the wall or window so that they themselves would not be recorded by it, or by turning it on only when going to sleep.

I: So you have not really mentioned the risks of the devices? F: No, I sense no [risks]. M: No, I have no risks at all. F: The only thing maybe, uh, the only thing might be the camera (…) because I think we don't see that as having risks because we point it at the balcony, so if someone sees what the camera sees, yes, well then it is a balcony, you know? (hhnl1, int1a)

The participants were also less concerned because the camera had a shutter, which was a very clear indication to them that they were not being watched or recorded.

M: Because now, it feels like I can control it. So if I say, if I feel unpleasant because the shutter is open, then I say 'shutter close' (...) and I know when it is closed it cannot record anything, even if it would be on (…). (hhnl2, intph1a)

While people in general perceived little to no privacy and security risks at the beginning of the experiment, participation in the home experiments did lead to increased awareness.

F: I definitely experienced the photo frame coming on spontaneously (…) M: It just made me think a little bit more that, you know, the security, you do need to be security conscious (hhuk7, intph3).

3.1.2 Subtheme 1.2: the participants mentioned several reasons why they were not worried about privacy and security

The participants mentioned several reasons for why they were not very worried about privacy and security risks. First, several participants expressed the likelihood and the consequences of a cyber-attack being low. They thought it was very unlikely that they would be personally targeted, as they had nothing interesting to offer. They also thought that if they would be cyber-attacked, it would have little consequences, for example because they had nothing to hide or that little sensitive data was collected by the devices that they would not want to share.

M: I think the chance [of the devices being hacked] is extremely small and not significant to think about it [laughs] or worry about it. F: Yes, particularly the fact that you could be personally hacked is very small; the chance that you are targeted. (hhnl5, intph2a)

I: What are the chances of your house being hacked? That someone can get into your devices? M: At the moment it's not so large because there are not so many devices so nobody feels like looking at that. (hhnl10, intph2a)

M: No and I wonder what they are looking for with me. Such a regular family. There are no millions in the home, they cannot find anything here that someone would be happy with. Then I think to myself, well, it will not happen to me, I don't think so. (hhnl4, intph2a)

I: How do you think you would have reacted if we had discovered that you were hacked by someone else, someone that we don't know? F: For us it does not matter so much, I think. M: Yes, nothing much happens here that nobody can know about. (hhnl4, intph2a)

M: The only time data ever becomes a concern is if it falls into the wrong hands, if their systems get hacked. I'm not really bothered because at the moment everything that we use, there's no bank details, there's none of that kind of stuff, so that's not really an issue. (hhuk4, intph2a)

F: Someone can hack my laptop and they will have far more valuable information than if they hack any device in this house, you know? M: That's true. Exactly, because we're not bankers or Theresa May or someone who is actually, you know, hacking the... F: Yeah, there's nothing, yeah. (hhuk5, intph2a)

I: If one of your devices would be hacked, do you think it would have serious consequences or not? P: It wouldn't. Because I interact with them in a very limited way and someone knowing what type of phonetic commands I give to [name smart speaker] and

what is my average weight utilising the scale I don't think it's of significant value. (hhuk2, intph2a)

Second, several participants expressed trust in manufacturers caring for their reputation and thus selling good devices and in the researchers [the authors of this paper] selecting good devices.

I: In general, you have trust in the manufacturers of the devices? M: Yes, yes, certainly. M: I think that you as a manufacturer should not want your devices to be inadequately used, because then you are digging your own grave. So they will have paid attention to that. (hhnl9, intph2a)
M: You [referring to the researchers] come and bring that stuff and I have the fullest confidence in the comings and goings of the TU [university that the researchers were connected to], so that should be in order. (hhnl4, intph2a)

Third, some participants were less concerned because they came up with preventive measures to limit the risks. Such measures included choosing strong passwords for the Wi-Fi router, setting the router well, and limiting the use of the device or the data that it can collect.

M: A disadvantage that I can think of is when someone can enter your network from the outside and watch the camera footage. (…) but you can solve that quite easily by securing yourself with good passwords and such, and not just choose 123 as a password (hhnl3, intph0).
M: If you have got nothing to hide, then there is no real reason [to worry] … as long as you are not giving away top secrets, I wouldn't sit here and verbalise my private bank accounts, pin numbers, sort codes. I think that would be a worry. So, you have just got to be conscious of what data you are happy to share, and it is like anything you type into a computer, even an email, you have got to assume that that email could be read by the world. (hhuk9, intph2a)
M: As long as that router is well set, then it will be alright (hhnl5, intph0)
M: I knew that it listens to everything that is being said in the nearby area. So, even though it's a passive listener, I have some reservations whether all this that is being recorded is going somewhere or just the request after triggering it. (…) So, therefore I try to have some kind of more sensitive communications in a different room. (…) Beyond this living room. (hhuk2, intph0)
M: I don't like in general any collection of data about how I am using the devices or how I am using the Internet. (…) I consciously do not ask anything too complicated or too private. I think I try to have a very generic use of [name smart speaker]. (hhuk2, intph2a)

However, opposite to being in control with preventive measures, the feeling that one has no control over privacy and security can however also be a reason to bury one's head in the sand and try not to worry, as one participant expressed in the context of the data collection by the devices.

F: I don't want to know what [name tech company] knows about me, it knows more than I think. And I would rather not know what they all know, because I cannot change it anyway. (...) Then I conclude that it does not make you happy because all these devices know too much about you and it can only go wrong in the end. (...) I'd rather not worry so much instead of thinking the whole day like 'oh no' because that does not make it any better (hhnl3, intph2a)

When talking about hacking, another participant also expressed helplessness.

F: Well, it may happen, but then we can't do anything about it. (hhnl4, intph2a)

3.1.3 Subtheme 1.3: the participants often had a limited understanding of how the devices worked and limited knowledge of cyber-attacks, which may have restricted their awareness of the risks

The participants often had limited understanding of the functioning of the devices; the researchers therefore needed to provide quite some support to help participants use the devices, such as help with adding a second user to the scales. This limited understanding may have led to insufficient understanding of factors relevant to the privacy and security risks. Several participants were for example unaware that data was processed and stored on the cloud, i.e., that data is transmitted and stored on remote storage systems, where it is maintained, managed, backed up, and made available to users over the internet.

M: When something about the use of the devices goes outside [data about the usage], does it go to you [the researchers] or the companies [the manufacturers]? (…) I wonder. Only now. (…) I: Where do you think the footage of the camera is stored? In the camera itself, in the tablet, or elsewhere? M: In the tablet, or maybe further. But I don't know. (hhnl4, intph2a.)

Participants also regularly seemed unaware that a hacker could potentially open the shutter of the smart camera, the presence of which made them feel quite protected.

M: With the shutter you at least can be sure. (hhuk2, intph0)

3.1.4 Subtheme 1.4: the risks became less salient during the use of the devices as people grew accustomed to the presence of the devices

Some participants mentioned that concerns and awareness diminished over time. It seemed that habituation took place and that the devices blended into the background or participants started feeling more in control, leaving them less conscious and concerned about privacy and security implications.

F: Risks, they feel much less now than 1.5 week ago. Then we had something with hacking and those kinds of things, but now I am not bothered by that at all. M: because I now feel that I have control (hhnl2, intph1)
I think he [the visiting boyfriend] was really conscious about the camera and turned it off. Then I kept it on and he just got used to it the 2nd or 3rd week. (hhuk1, intph2a)

3.2 Theme 2: the simulated attacks made little impression on the participants

The simulated attacks were often not noticed or not consciously experienced as a significant event, were easily forgotten, and had no effect on how people experienced the devices overall.

3.2.1 Subtheme 2.1: the participants often did not notice simulated attacks

We found that many of the simulated attacks went unnoticed, particularly so in Phase 2, in which the participants were not yet informed about them. This became obvious from some of the participants' responses when the researchers revealed that unbeknownst to the participants, they were the recipients of simulated attacks. Some participants said they could not think of anything that happened that could have been an attack.

F: I really have no idea. I have really not noticed it, that it happened. [participant was referring to the simulated attacks] F: No. (hhnl3, intph2b)
M1: I can't say I have noticed anything. M2: No, nothing. (hhuk9, intph2b)

Particularly the simulated attacks with the smart camera went unnoticed. Almost no one reported noticing a change in the status of the shutter. This was especially surprising because participants felt most concerned about the camera being on (as mentioned in Subtheme 1.2) and some participants explicitly mentioned that if something would have happened with the camera, they would not only have noticed it but also would have found it scary.

M: It would be really creepy if that thing [talking about camera shutter] would suddenly 'prrrr' open [laughs] and starts recording (…) F: so, uh, we did not see anything [laughs] (hhnl5, intph3)
M: If you had opened and closed the camera [referring to the shutter], imagine if, but I don't know if that is possible, then I would have found that unpleasant. (hhnl2, intph2b.)

3.2.2 Subtheme 2.2: there were several reasons why the participants did not notice the simulated attacks

Not noticing the simulated attacks while being at home can be divided into two distinct situations: (1) the attacks having been simply invisible and inaudible to the user and (2) the attacks being in principle visible and audible, but still going unnoticed.

In the first category, some of the devices where briefly disconnected from the automation service that was used by the researchers for carrying out the simulated attacks, which resulted in some of the attacks not being conducted. It is possible that the household's network became inaccessible and the devices' connections to the service simply timed out; it is also possible the household itself logged out of the account. Second, some of the participants used automation that masked the toggling of a device. For example, people set the lamp to go on when they would come home, and therefore could not have noticed that the lamp had gone on already earlier as a result of the simulated attack. Third, many simulated attacks took place when participants were not necessarily in the room in which the devices were placed. Fourth, several participants had stopped using devices, or used them in a minimal way. For example, several participants had the security camera facing a wall or window which would have made it impossible to see whether the shutter was open or closed at any time of the day, and many participants used the scales without regularly looking at the app that shows the history of weighing points and therefore did not notice weighing points being deleted or added.

In the second category, people did not always use the devices in a routine-like fashion and therefore did not remember the state the device had been in. They might also not have known whether a housemate changed the status of the device.

M: What would be slightly possible is that it was sometimes on in the morning when we did not turn it on, or that it would be off in the morning when we did turn it on. But those are things, I do not think about it much, we just go to bed and then it is 'switch on the camera' and then I walk to bed. F: We also do not turn it on every evening (…) so we do not have a routine and cannot check very well in the morning if we had turned it on or not (hhnl5, intph3)
F: With the camera sometimes: have we turned it off or not, because it is on? Did you switch it off, or didn't you? Yes, then we don't know. (hhnl4, intph3)

Furthermore, people may have been in the room but still did not observe the event. Particularly for the security camera, people could have heard the shutter opening or closing but nevertheless did not notice it. A likely reason was that the sound of the TV, or perhaps something else, had masked the sound of the shutter moving.

M: Well, if we were watching a programme down here we may not have heard it. (hhuk7, intph3)
M: I was here, I was watching TV for sure. I didn't notice it. (hhuk3, intph3)

3.2.3 Subtheme 2.3: noticed irregularities were rarely experienced as a significant event and easily forgotten

Irregularities were often not experienced as a significant event. Several times, participants only realised that they had noticed something irregular during Phase 2 when we afterwards told them about executing simulated attacks (end of Phase 2) or listed the specific simulated attacks (end of Phase 3). The noticed irregularities had been dismissed or forgotten or confused for something else which was not considered that important, such as having forgotten to turn something on or off or resulting from an attempt to set automation.

M: The photo frame. I switched it off for the day and then I came home and then the photo frame was switched on and it was really weird. Or I've left and I came home and the lights were still on in the flat. I definitely remember closing the door. (…). [automation was set such that opening and closing the door activated the lights] M: Initially for a moment and then I was like, it's fine, and then I switched the thing back off, or I just thought, 'that's a bit odd' and I turned [name smart speaker] off. (…) F: Yeah, it's easily dismissed (…) Had it been more consistent perhaps it would have provoked a bigger reaction, but I think it's just easily dismissed." (hhuk4, intph2b.)

I: On the 9th of December, the lights went funny at 3 o'clock during the day. You may have noticed them being off or on when you returned home. (…) M: Yeah, so I do remember finding it on. (…) I thought I forgot it or whatever. (…) Yeah, it was also the time I was trying to make it work with the smart [inaudible – something about automation presumably]. It never happened. I thought they worked, but I hadn't from what you are saying." (hhuk3, intph3)

3.2.4 Subtheme 2.4: participants did not indicate a negative change in their opinions about the functioning of the devices after undergoing the simulated attacks unknowingly

After the first set of simulated attacks was executed in Phase 2, but before we revealed that we had conducted the simulated attacks, we asked participants whether their opinion about the devices had changed in the last few weeks. The participants often said no. When they did say it had changed in some respect, or just commented on some of the devices in response to this question, they frequently mentioned a negative experience with the devices that did not relate to a simulated attack. In no instance did they mention a negative change in their opinion because of experienced irregularities that were related to the simulated attacks.

I: Do you feel that your opinion about the devices has changed over the past few weeks? F: No. (…) I: Do you feel that the devices are functioning as they should? F: Yes, only with the light it is difficult (…), it does not hear me when the radio or TV is on or someone is talking. Then I need to repeat the command up to four times. [note by the researchers: she was talking about commanding it through the smart speaker. This was not a consequence of a simulated attack] (hhnl10, intph2a)
I: Do you have the feeling that your opinion about the devices has changed in the past weeks? M: No, yes I have to say that lately I have had issues with the smart speaker, that we, with three or four people, independent from each other, tried to ask a certain song from [name music application] but that went really wrong. Every time it failed to understand what you had said [this was not a simulated attack] (hhnl3, intph2a).
I: Do you feel that your opinion about the devices has changed over the last few weeks? F: Yes, when it comes to [the] light I find it a bit annoying. Because I can't get it to work. Because it's something that I really enjoyed using and I am not able to continue using it in the same way as I used to in the beginning. (…) [note by the researchers: this was not a simulated attack] I: So, apart from the [name lamp] do the devices function

as you think they should? F: Yes, I am happy (hhuk1, intph2a)

3.3 Theme 3: the participants had difficulties with correctly recognizing simulated attacks

Irregularities caused by the simulated attacks took place amidst other irregularities that the devices exhibited, and it was difficult for the participants to tell them apart and ascribe the right causes to the different events.

3.3.1 Subtheme 3.1: when simulated attacks got noticed, participants often misattributed them

The participants misattributed the simulated attacks, such as to technical issues with the device like a bug or connection issues, or to themselves or other people in their household doing something.

Words used to indicate technical issues with the devices and/or their connectivity were bug, blip, glitch, technical fault, system error, or connection issues. More vague terms used were "something that those devices do" and "these things can happen". The participants mentioned such things very often when talking about an irregularity related to a simulated attack.

F: I thought maybe it [the scale] just didn't recognise me because these things can happen. (hhuk1, intph2a)
F: Maybe there is something wrong with the Wi-Fi and therefore the socket went off. (hhnl1, intph3)
M: I think that it [the smart scale] misclassified [name female] and put it [a weight reading] on my account. (hhnl5, intph3)
M: We suspect no connection, that it has problems with the connection. F: Yes, I think that maybe when the outlet loses its Wi-Fi connection, it goes off, that might be possible. (hhnl1, intph2a)
F: Oh well, that's just technology, sometimes it does weird things. M: Sometimes technology does weird things. (hhuk4, intph2b)
F: Well, we switched it back on again and then it worked, so then we thought, it must have been something in the device (hhnl2, intph2a.)
M: I thought more that it was a system error than that it was really hacked (hhnl3, intph3)

The participants sometimes attributed the simulated attacks to something they themselves or other people in or around their household did.

F: Ok, one day [name smart speaker] was on when I got here. That's the only thing. (…) And I was blaming my boyfriend that he left it on." (hhuk1, intph2a)
M: Now that you mention it, I think a week or so ago I heard music (…) apparently it was not turned off properly (hhnl10hhnl10, intph2b)
M: I had been fumbling with the tablet for a while (…) then I was sure that the camera was off. And at a certain moment I looked up and it was on. I thought 'have I touched a button here or something'? (hhnl4, intph3)
M: That the [name weighing scales] did not recognize me while I did not weigh differently. F: Yes, and suddenly there was a very high weight in it, for you (…) it thought it was me with that painting [the participant weighed herself with a painting in her hand to determine the weight of the painting]. M: or that I was still wearing shoes. Yes, because there was also no fat percentage there. (hhnl1, intph2b)

Other irregularities that the participants experienced with the devices (thus not related to a simulated attack) were attributed to similar things (technical issues within the devices or with the internet connection, oneself or other household members somehow causing it), which may have contributed to making it difficult to tell the events apart.

F: Oh, yes, I have noticed that the lamp does not always respond in the same way (…) I thought I did not speak clearly enough or there was too much background noise. (hhnl10, intph2b).
F: And then the smart scales, (…) it came up with 'error'. (…) First, I thought maybe have I not, you know, done it correctly, and then it came up with 'error' again, so I'm not sure whether it was the research team [that was executing the attacks] or the fact that I just didn't take my feet off and then it gives me a reading. I don't know" (hhuk4, intph3)
F: It said something like "Cannot connect" (…) I don't know why (…) It never said that before. The week before he had been playing a lot with the tablet including looking at things related to the weighing scales and I think he must have touched something. I said 'have you done something to the scales last week because I have not seen this before'. (hhnl4, intph2a)
M: Well, actually I went on to the tablet (…) and it just said disconnected so I checked my router thinking it might have been mine because yours was connected to my router but when I checked my phone, which is connected to my router and that was all fine so the internet was fine and everything was fine it was just your router or the survey router was somehow disconnected, the lights were flashing but it didn't seem to be all of them so I assumed it must have been something irregular going on, I'm fairly certain unless it was just a blip from a router they did those things but unless it was that it must have been you or not you but your

colleagues [one of the researchers executing the simulated attacks]. (hhuk9, intph3)

3.3.2 Subtheme 3.2: participants were hesitant to label a simulated attack a cyber-attack

Before revealing that we performed simulated attacks at the end of Phase 2, participants in two households entertained the thought that someone outside their household was causing an irregularity which was actually a simulated attack. However, they were very hesitant to label it as a cyber-attack by a hacker.

F: I was thinking, if someone would be on our Wi-Fi, but how could they? I don't know. I have no idea. I think it is just an error in the system. M: Yes, that is more likely, an error in the system. (hhnl5, int4.1)
F: Could it be someone from outside, who walks by? I know when our kids were thirteen years old, they discovered that they could take the remote to the neighbours and change the channel [laughs] that is the association I had (…) I did feel like Big Brother is watching you after that happened. I did not have that before that time (hhnl8, intph2a)

In two other households, the participants were guessing that the researchers did something.

M: And then there's a moment that she [the smart speaker] did not follow up yesterday's command, which I always use [note by the researchers: this was not a simulated attack]. She needs a different command, and then I think to myself 'would they be touching the buttons at the [name of the university of one of the participating researchers]'? (…) M: And then I started thinking (…) would [name interviewer] be behind it somewhere, doing something. (hhnl4, intph2a)
F: Well, I think it has to do with the test period. (…) That you are investigating remotely whether it is well controllable. You from the [name of the university of one of the participating researchers], or …. (hhnl9, intph2a)

After revealing that we had executed attacks, two other participants also told us they had been considering that the research team was doing something with the devices. They were very uncertain about this, however.

M: There were a few things that I know that happened and I thought, that's a bit weird. I spoke to somebody else about it and I said, 'Do you know what, I think maybe that it has been done on purpose to see what would happen,' or whatever. (hhuk4, intph2b)
I: And we wanted to determine if you would notice it when the devices would exhibit irregular behaviour. F: I did think about it once [laughs] (…) I thought 'no, they won't do that' [laughs] (hhnl2, intph2b)

Besides these references to others somehow getting access to the devices or the researchers causing them, there were no references specifically to a real cyber-attack taking place. This was even the case for the husband of the female participant who considered for a moment that the researchers were interfering (see previous quote):

M: But not once, not for a second, did I consider 'damn someone is doing something with those devices of mine'. (hhnl2, intph2b)

Participants did not provide reasons why they more readily considered researchers causing irregularities, rather than an outsider performing an actual cyber-attack. We presume, however, that this is likely caused by the fact that our participants had very little concern for and awareness of the risks of cyber-attacks (see Theme 1).

Surprisingly, participants who mentioned cyber-attacks as a risk in the first or second interview did not mention any suspicion of being cyber-attacked, such as the couple in household hhnl10, who explicitly mentioned the possibility of the devices being cyber-attacked in several of the interviews.

3.3.3 Subtheme 3.3: the participants were regularly very uncertain about what caused the irregularities that were related to a simulated attack

The participants often guessed several reasons for an event and were not sure what the real reason was. Sometimes participants could not come up with any reason at all for an irregularity caused by a simulated attack.

F: The scale didn't recognise me (…) I: How confident are you that this is an irregularity caused by the researchers? F: I am not really sure. Cause it would sometimes not recognise you and then would. Because I am not really sure how they can hack that. I: Could it have been caused by something else? F: Could be a technical fault, anything really. Internet connection. I mean I haven't done anything with my Internet connection. Have not done anything or reset any devices during this period (…) this case, it could really be anything. (hhuk1, intph3)
F: [talking about the photo frame going on and off] I still don't know what caused it. (hhnl1, intph2a)

3.3.4 Subtheme 3.4: when informed about simulated attacks having taken place, the participants intermingled simulated attacks and irregularities that the devices naturally exhibit

In Phase 3, when informed about the simulated attacks and asked to undergo them again, participants mentioned irregularities brought on by us [the researchers], intermingled with irregularities that the devices exhibit by themselves, without making a clear distinction. This also suggests that the participants were unable to tell them apart.

> *F: [name smart speaker] not playing the radio or not turning on the light when I said it. <pause> Or I mean it was mainly to do with [name smart speaker] and lights and scale not recognising me" (hhuk1, intph3) [note by the researchers: The radio not playing and lights not turning on was not a result of a simulated attack, while the scales not recognizing the user was.] M: Only that the device did not recognize me [name scales] and that it had also identified me as a guest, and that one time it turned off when we were at home, but otherwise, no. I do have to say that [name smart speaker] acted very strange a few times, she would hear me and I gave the order with the same command, sometimes even louder and then, in the end she does not say anything (hhnl1, intph3) [note by the researchers: The smart scales not recognizing the user was a result of a simulated attack, while the smart speaker not responding was not]*

3.4 Theme 4: being informed about simulated attacks taking place leads to more identification and reasoning about them

When participants were informed about simulated attacks taking place, they noticed more attacks and even wondered why they had not noticed them before. They also sometimes had good arguments for identifying why something was a simulated attack and not another irregularity caused by the technology itself.

3.4.1 Subtheme 4.1: when informed about simulated attacks taking place, more simulated attacks were noticed and classified as such

When people underwent the simulated attacks again in Phase 3, they more often noticed the events and regularly correctly identified them as a simulated attack.

> *F: So, the light came off when I went to the kitchen. When I went back in, it was still off, so I closed the door, I opened, and then the lights came on [automation was set to switch on the lights when the door was opened]. It did it again, it did it twice to me. (…) I: Can you tell me how confident you are that this was an irregularity that was caused by the research team? (…) M: I'd probably say at least, like, 95%. (hhuk4, intph3)*
>
> *I: In the past weeks, you have been deliberately hacked. Can you tell me how you have experienced this? (…) F: [name smart speaker] at some point started playing music. M: Playing the radio as well (…) I think it was BBC radio 1 <laughs>. It was quite uplifting music. Yeah, it was funny. (hhuk3, intph3)*
>
> *I: Since I last saw you, you've been deliberately hacked, and can you tell me (…) how you experienced it?(…) M: The most obvious one was when we were at bed at 9.30 and [name smart speaker] just started playing the radio by itself. (…) it was super-obvious (hhuk5, intph3).*

The latter respondent even wondered why they did not notice such events before (i.e., in Phase 2 of the experiment before the simulated attacks were announced):

> *M: … that I'd been wondering if it had actually happened when we were at home before you told us or if we were just so oblivious to it. (hhuk5, intph3)*

However, as was clear from Theme 3, even after having been told about the simulated attacks (but without specifying what these attacks entailed), attacks and other irregularities were often confused for each other.

3.4.2 Subtheme 4.2: some participants provided a decision rule for telling apart a random irregularity from a simulated attack

Several participants expressed consistent reasons for deciding that an irregularity was a simulated attack and not the result of another household member's behaviour or a glitch in the Wi-Fi connection. For example, the devices turning on by themselves (unauthorised actuation [1]) were a sign for these participants that it must have been a simulated attack. In contrast, not executing a requested action (prevented actuation[1]) was ascribed to a system malfunction. While it is true that prevented actuation has several possible common causes (loss of connectivity, software error) and that unauthorised actuation is uncommon to be caused by a legitimate system malfunction, their rationale for telling the two apart was incorrect. Both could represent legitimate impact of an attack. However, in the study, they were not presented with a prevent actuation attack and as such their incorrect decision rule was not put to the test.

> *M: Mostly it was devices starting by themselves… F: Yeah. M: …at times when they were not told to do, so it was actually quite obvious" (hhuk5, intph3)*

I: On the thirteenth you told me that on the twelfth the outlet spontaneously switched on. We did that. Did you think that it was us [the researchers] or did you think it was something else? F: You. I: Why did you think that? F: Because we had not given a command, to [name smart speaker] or something. I: And otherwise something like that does not happen? F: No. M: No. (hhnl6, intph3)
F: Yeah, like we were all used to technological glitches so like if something fails to work then we wouldn't assume that was a hack but if something comes on spontaneously that doesn't look like a technological glitch. (hhuk7, intph3)

Furthermore, when a different channel than the default option was used it was correctly considered a sign; indeed, one of our attacks involved starting a specific radio channel, which very likely was not the one that the participants already used.

F: It is also strange that we have [name music application] as a default music thing and it used 'tune in radio' for that radio station (hh5, int4.1)

Finally, something happening more than once was considered a sign by a participant.

F: When it turns on or off only once, you can still think, hmm, ok, maybe something is wrong, but when it goes on, off, and on again, then it is like, yeah, this is not an accident (hh5int5)

Although this was indeed a characteristic of many of our level 2 and 3 simulated attacks, it could potentially also be the result of something caused by the device itself. Also, three of the level 3 attacks consisted of Morse codes, which none of the participants noticed. If they had recognised that a Morse code was repeated, this would have been a telling sign of a purposeful attack as opposed to a random error.

3.5 Final remarks

A final important point is that, although the researchers had no a-priori hypotheses, the researchers did, to some extent, expect participants to negatively experience the simulated attacks. Unexpectedly, however, the participants (at least the ones that participated until the end of the study) generally expressed few negative responses to the simulated attacks. In addition, the participants also expressed surprisingly few negative responses when being informed about having undergone simulated attacks. Many participants thought it was funny and interesting that we had conducted simulated attacks on them and felt that undergoing the simulated attacks again and trying to identify them would be like a game and a nice challenge. The lack of negative responses may be due to the participants often not noticing the attacks and not experiencing serious consequences of the attacks. It may also be due to the trust the researchers enjoyed, the fact that we explained that the study had been approved by the ethical committees of the respective universities and that we reassured them that we had not been and would not be listening to them or watch them through the smart devices. In addition, the Dutch participants mostly had more often participated in experimental studies and knew that the goal of a study could be quite different from what they expected beforehand.

4 Discussion

In a naturalistic field experiment, we studied how participants in 16 different households in the Netherlands and the UK experienced simulated cyber-attacks on smart devices. Thematic analysis on interview data of the experiment yielded four main themes.

First, participants had little awareness and concern about cyber-security risks, thinking that the likelihood of personally being cyber-attacked is low and the consequences of being cyber-attacked limited. The main reasons given by the participants were that they did not think they constituted an important enough target, they had nothing to hide and little to lose, they trusted the researchers conducting the study and the manufacturers of the devices, and they lacked understanding of the system and felt a sense of control, or on the other hand too little control. These findings are in line with earlier studies pointing out similar reasons for low levels of privacy and security concerns [21–23]. Besides limited concern, the participants often had a limited understanding of the functioning of the devices and of how these devices could be cyber-attacked (e.g., not knowing that data was stored in the cloud and that attackers can not only access data but also operate devices), which may have also led to a limited understanding of factors relevant to the privacy and security risks.

Second, participants seldom noticed simulated attacks or did not experience them as significant events. Besides some of the attacks taking place out of sight of the participants, this was due to the visible consequences of the attack not standing out to the participants and being easily dismissed. Participants indicated no change in their opinion of the devices due to (unknowingly) undergoing the simulated attacks for the first time.

Third, when the participants did notice a simulated attack, such as one of the devices turning on and off a few times in a row, they had difficulties ascribing it to the right cause. The participants regularly guessed multiple possible options, including a simulated attack, technical issues such as an internet connection issue, or themselves

or housemates causing it. Similarly, they had difficulties understanding other irregular behaviour from the devices (i.e., not a simulated attack), such as the smart speaker not responding to commands and the devices logging out without clear reason and therefore presumably their uncertainty about what was going on did not trigger suspicion about malicious intent. This is in stark contrast with cyber-attacks on conventional digital environments which are more familiar, such as email, social media, and websites. These conventional digital environments provide more opportunities to their users to spot that things are not right, such as suspicious web addresses, unsolicited direct messages in social media, or visual mistakes in the email [24].

Fourth, after having been informed about simulated attacks taking place, more of these attacks were noticed and identified. Some participants provided a decision rule for telling apart a random irregularity from a simulated attack, but these were not necessarily correct decision rules. For example, people had suggested that it is more suspicious when a device spontaneously does something that it was not ordered to do, than a device not executing a given command. However, both could be a sign of a cyber-attack. Something happening more than once was also offered as an argument by a participant to see whether something is a cyber-attack. However, it may happen as much due to technical errors as cyber-attacks.

These findings very much align with ideas from the signal detection theory (SDT; [25]), which has for example been used to understand detection of phishing emails. SDT distinguishes response bias from sensitivity. Response bias is the perceiver's propensity to categorise stimuli as targets or something else [26] and in the case of phishing it concerns users' tendency to treat an email as phishing [27]. Sensitivity is the perceiver's ability to discriminate alternatives and to tell whether an email is phishing or something else. Applying this theory to detecting cyber-attacks, it makes sense that when people have a low awareness of the cyber-security risks of in-home IoT they may be less attentive to it and therefore have a low tendency to treat an irregularity as a cyber-attack. When the participants are unable to tell the difference between an irregularity of a smart device due to a technical error or a household member doing something with it versus as a result of a cyber-attack, it means that they also have a low sensitivity. The combination of low response bias and low sensitivity would explain the fact that people did not realise they were cyber-attacked in Phase 2. Announcing simulated attacks without explaining what they would look like increased people's detection of simulated attacks—a higher response bias—but did not make them competent enough at separating simulated attacks from other experienced irregularities of the devices—thus lacking sensitivity, as there were many false positives.

Overall, the results illustrate that, at least now, one cannot rely much on a typical IoT user in detecting cyber-physical attacks. Our study highlights the importance of creating awareness of cyber-physical risks in combination with developing a better understanding of how to distinguish simulated attacks from other events that smart home devices produce. Further research should provide insights into rules of thumb that help users gain higher sensitivity. Furthermore, technological solutions such as automated intrusion detection systems that are sensitive to a household's cyber risk may be needed.

Our study had limitations, which can be addressed in further research. First, the respondent sample was not very representative of the general population. This was a result of both the selection criteria for the study (e.g., pass a psychological test) and of self-selection of the participants for the study (e.g., taking part because of being curious about domestic IoT). This may, for example, have led to including people that are more psychologically stable and more curious about IoT devices than the general population. Furthermore, several of the Dutch participants had participated in psychological research already and might have expected that the study involved goals other than the one directly communicated. On the other hand, we did include participants from two different countries and of different age categories, leading to the findings having some wider applicability. Further research could test how well representative populations detect and respond to cyber-attacks in the home.

Second, the nature of the attacks was mostly limited to switching the devices on and off, which could similarly have been caused by technical issues. More noticeable and daunting attacks, such as more repetitive and long-lasting toggling of the devices, the camera or even the device with camera following the user around the room [12, 28], or broadcasting speech or loud music through the microphones which happened in attacks discussed in the media (e.g. [3, 7]), would very likely stand out more to the participants, and thus be better noticed. However, such attacks have the potential to cause harm and are therefore unlikely to get approval from ethical research committees. Furthermore, such increased noticeability only represents a subset of attacks, as many (if not most attacks) will not produce immediately noticeable results [2]. Instead, the results of attacks may become visible only later, for example when people are extorted, have information about them placed online, or hear from the consequences of the DDOS attack executed also via their device. Furthermore, because participants did not think they were actually cyber-attacked, the study was unable to provide clear insights into how people experience and emotionally respond to cyber-attacks that they are aware of. Future research should further address how people detect and experience being cyber-physical attacked, depending on the various types of possible cyber-physical attacks and

their differences in noticeability. Future research could for example create much more noticeable attacks, so that the attacks are more likely to be interpreted as cyber-attacks. These studies could then examine how noticeability affects identification of attacks. Participants could also be led to believe they were actually cyber-attacked by being informed of this by the researchers, for example, through a fictitious helpdesk or letter from their internet provider. Besides conducting new naturalistic field experiments other methods can also be used such as recreating the experience of a cyber-physical attack in virtual reality or by interviewing users that have experienced cyber-physical attacks in real life.

Third, although this was a field study conducted in the participants' own home, there were several practical design choices and constraints imposed due to ethical concerns that created a somewhat unrealistic situation. One constraint was that the devices were installed by the researchers, who also solved any emerging problem with the devices (e.g., logging back into services). Perhaps, if the participants had done all these things by themselves, they would have looked up a lot of information on the internet about these devices, which could have made them more knowledgeable of the device, and more aware of the risks of cyber-attacks and measures to mitigate these. We also introduced numerous IoT devices all at once into the households, and all received the same set as selected by the researchers. While the former may have resulted in participants having insufficient time to become acquainted with all, the latter may have led to some devices having limited value to some participants. Future studies should consider letting participants pick one or two IoT devices they are interested in using. This is not only more representative for real-life purchasing behaviour but will expectedly increase the number of interactions with the device, and hence familiarity and noticeability of (simulated) attacks. Another constraint was that people were not allowed to use the devices in the way they normally would have, as they were for example not allowed to install the apps with which they could access data and change settings of the smart devices on their mobile phones. To make the research more representative to the real-life use of domestic IoT, further studies should find ways to give more control to the participants, while at the same time allowing researchers to access the devices to simulate attacks, without the participants being aware of this.

Fourth, the participants indicated that they trusted the researchers (i.e., the authors of this study) which may have affected their perceptions of the privacy and security risks of the devices, and perhaps also their sensitivity to noticing the simulated attacks. However, other studies in and outside the domestic context have similarly found that people expressed trust in IoT devices, the companies handling their data, the government setting regulations, and healthcare providers using the devices and that higher trust is associated with lower risk perception and more positive attitudes towards IoT [23, 29–35]. Such transferal of responsibility by trusting other responsible parties thus is a more general phenomenon and not unique to our study. However, to reduce this possible limitation, future studies should consider allowing participants to choose and install devices themselves, as already suggested above.

5 Conclusion

This study is the first to test how people might respond to being cyber-attacked in their smart homes. Such research is very challenging to execute, due to its required interdisciplinary nature, the need to study people in their natural habitats, and all the ethical concerns involved. Our study has shown that this kind of research is nevertheless possible and fruitful for gaining an in-depth understanding of how people experience cyber-attacks. Our study primarily shows that our participants had difficulties detecting that they were cyber-attacked, which is a worrisome situation that needs to be addressed by researchers, policymakers, and technology developers alike. The situation of low risk perception and awareness needs to be dealt with by providing warnings and information to users of domestic IoT. The fact that the participants had difficulties telling apart simulated attacks from other to them inexplicable behaviour of the devices shows that users need to be better informed about the differences between irregularities naturally exhibited by the devices and irregularities caused by a cyber-attack. As there are limits to what one can expect from the user in terms of ability and effort invested in gaining knowledge, an intrusion detection system would be a good step forward.

Appendix. Questions prepared for all interviews

Note that interviewers were allowed to divert somewhat from the questions based on what they already knew from the participants and to create a natural flow in the conversations. Each interview was therefore somewhat different. The text in italics were instructions for the interviewers only.

Phase 0 interview in Dutch and UK households (in italic instructions for interviewer) (intph0)

The following questions are meant to get information on the background of participants.

Can you say something about the makeup of your household?

Can you tell me what the level of your education is (what was your highest education level) and what was the content of your current or most recent job?

How much and how often are you at home?

The following questions are about:

- *What does the home mean for people?*
- *How does technology play a role in that?*
- *How do people use technology (in general) and how handy are they in using it?*
- *How do people talk about devices in their home– what is the terminology and what are the words that they use?*

We are now in your home. Why do you live here? Can you tell something about the role that your home plays in your life?

We are interested in how you experience technology. Can you first tell me a bit about which devices you have in your home? I mean any kind of device.

Can you show a few devices that you find special, in which you take special pride, or that play the biggest role in your life?

Questions for more information:

- Why do you name that one/those ones?
- Why that one/those ones and not that one (when you see another special device in front of you, or has been mentioned before)

Are there devices in your home that are connected to the internet? Why are thy connected to the internet?

Are there devices that you have not connected to the internet, even though they could have been connected to the internet? Why did you not connect them to the internet?

How do you experience devices in your home? Which device could you miss the least?

Choose one of the most interesting devices in the home of the participant(s) – for example the device that is the smartest (for example can do most interaction with other devices via an internet connection.

You were just/earlier on talking about…. What does this device mean to you?

If you need a new device, how are you selecting one? Is there someone in the household that is doing that most often?

When you have bought a device, how do you install it? Is there someone in the household that does most of the installing or programming?

If something goes wrong with a device, what do you do? How do you solve it?

If they don't tell this by themselves then:

Is there someone in the home that usually does that?

The following questions are about:

- *What do people think about smart devices?*
- *What benefits and drawbacks do people expect of smart devices?*
- *How do people talk about IoT– what is the terminology and what are the words that they use?*

Do you know what IoT (Internet of Things) is? Can you describe it?

I will shortly describe what we were thinking of regarding IoT:

IoT technologies include all kinds of consumer devices that are connected to the internet and/or to other devices. Typical examples include smart thermostats, smart speakers, and smart cameras.

Do you already have experience with such products? What experience do you have with it?

You have registered for this research in which we install smart devices in your home. Can you explain what motivated you to take part in this study? You can tell whatever reason you had.

What benefits and drawbacks of IoT do you expect there to be?

Can you first explain the benefits?

Prompts:

- Can you tell more about that?
- You said… and …. Can you tell more about that?
- ….*[repeat what was said].* What do you mean by that?
- Do you have experience with that?
- Do you foresee any other benefits? *[repeat this question until they say no]*

Can you now explain what drawbacks you expect the devices to have?

Prompts for more information:

- Can you tell more about that?
- You said… and …. Can you tell more about that?
- ….*[repeat what was said].* What do you mean by that?
- Do you have experience with that?

Do you foresee other drawbacks? *[repeat the question until they say no.]*

When they mention risk you can ask more about it:

– How likely do you think that will happen?
– How bad would it be if that would happen?
– How would you feel if that would happen?
– What would you do if that would happen?

If they do not mention risks:

You mentioned a number of drawbacks such as *[summarize some of the things they said]....,* but do you also see risks in the use of IoT?

If they did mention risks:

You mentioned these risks…., do you foresee other risks? *If they now mention risks, ask more about it as outlined above.*

If they don't see any risks, that is also fine, don't dwell too much on it then.

Middle of phase 1 interview for Dutch households (intph1a)

Have you recently done something new with the devices or did you change the use of it? Have you maybe put them in a different location?

Do you feel that your opinion about the devices has changed lately?

Do the devices still work as they should?

Can you manage all the 'tasks' that are part of the study, or is there something that is keeping you from it?

End of phase 1 interview for UK and Dutch households (intph1b)

We are now a few weeks into the study and we want to thank you for your efforts so far. Today we will have the second (in the UK)/third (in NL) official interview.

The first question that I want to ask is:

Now that you have been having all these devices in your house, how do you think in general about smart devices, or the Internet of Things? What do you think are the overall advantages and disadvantages or risks? Let's start with the overall advantages. Which benefits do you see these devices overall to have?

And now the disadvantages, or risks, do you see those as well? Please explain.

Now probe respondents about the things they reported in the online questionnaires. Go through each reported experience.

Do you think that you will use the devices differently after the study ends? Please explain.

Why would you do … differently? *[ask for everything they say extra clarification].*

Have you had any guests/visitors in your house since having these devices? Do you tell them about the technology? Do you adjust your use of the devices when there are others in your house (for instance do you turn the camera off)? How do your guests feel about the devices? Do they also interact with it?

How was it for you to tell about it, and see their reactions?

End of phase 2 interview UK and Dutch households including the revealing of the simulated attacks (in grey instructions for interviewer) (intph2).

Part 1 (inph2a)

I would first like to interview you. After that, I will tell you a bit more about the goal of the study.

I would first like to ask you a number of open questions about changes in the last weeks:

Have you recently done something new with the devices or did you change the use of them?

Have you put them in a new location perhaps?

Do you feel that your opinion about the devices has changed in the last few weeks?

Please tell me more. *[keep on asking for more until they have nothing to say].*

Do the devices function as you think they should?

Ask more about it where possible.

Do you feel your initial expectations about the devices were met, or was it different from what you expected?

You received a lot of devices at once at the beginning of the study. How did you experience that? Would you say it was overwhelming, messy, or demanding, or not at all?

Please explain more about this. If yes to the previous question: What was it that makes it overwhelming, messy, or demanding?

Do you think that the devices ask a lot of attention, or do you think they do not?

Did you manage to fulfil all the 'tasks" that come with the study, or was there something holding you back perhaps?

Different people have mentioned different costs, risks and benefits of the devices during the course of the study. I would like to list these positive and negative sides of these devices, and hear what you now think of this.

Some people thought beforehand that the devices would be useful or handy. After use, some people indeed found them useful and handy, some did not. Can you tell me what you now think about this?

Some people that had health issues particularly found it handy that they did not need to stand up to switch on or off the radio, or the lamp. What do you think of this?

Some people thought it was entertaining or fun to have these devices, some people did not. Can you tell me what you think of this?

Some people thought beforehand that the smart devices could change the energy consumption of the household, either by saving energy or costing more energy. Did you

think of that at the beginning and if so, what did you think about it?

Do you think that your household energy usage has increased or decreased, or did it stay almost the same?

Some people experienced a sense of socialness or a feeling of having company from [name smart speaker]. One person mentioned that [name smart speaker] felt like a friend of the house or family. Could you tell me how you now think about the social function of the smart speaker?

Some people appreciated the voice of the smart speaker, and some people did not like it. Can you tell how this is for you?

Some people appreciated the answers of the smart speaker, and some people did not like it. Can you tell how this is for you?

Some people found it a challenge to find out what the devices can, and how to operate them. Others seemed to find it quite easy. What is your opinion and experience with that?

Did you find them difficult or easy to figure out and use?

Was it more difficult or easier than you thought beforehand?

Some people found it a challenge to solve issues with the devices when they had them. Did you have issues with the devices.

Tell me more about all the issues that you remember.

Did you have difficulties solving them?

Can you tell more about that?

For these issues, what did you think was the cause of it?

Would you think it was the design of the device, your own lack of knowledge, the limitations that we set to the use of the devices and the study, or something else?

Do you think the design of the devices is good, or not good?

[if mentioning lack of ability or knowledge on their own part in the earlier question:] When you mentioned a lack of ability of knowledge on your part as a problem, would you not – instead of that—also think that you can expect more from these devices?

Do you feel that the devices affected how you experience your home?

Did you feel that your home has become more pleasant or less pleasant with the devices?

Some people have indicated that they found the devices to have a quite strong presence – or something like that – in their dwelling. How did you experience that?

Some people experience uncertainty about what data is collected with the devices and what goes into the cloud and what not, and about what is done with the collected data by the companies behind it. Did you think of that?

What did you think of that?

What data do you think is collected by the manufacturers and how do you think it is treated by the company?

What do you find or would you find acceptable, what do you find worrisome?

Some people found it difficult that the devices did not come with a manual. Others did not bother. What did you think of that?

Would you like to have a paper manual, or something on the internet?

Did you read the privacy agreements of the manufacturers that we emailed you before the start of the study?

If yes, when did you do that?

For what reason did you look it up, or did not look it up?

What did you learn from then, if you have read them?

Did you look up information on the website of the manufacturer of the devices?

If yes, when did you do that?

And what did you look at, or what did you learn from that?

Did you google for information about the devices?

What kind of things did you look up?

Some people saw advertisements about other smart devices and were considering buying some of them. Did you consider that?

Why, or why not?

And if so, what did you consider buying, and why?

Some people mentioned that these devices could be hacked. Did you consider that?

How likely do you think it is that they can be hacked?

Do you think the smart devices that you got were well protected against something like hacking?

Have you ever been the victim of a hack or something related? Or do you know someone that has been hacked?

If one of your smart devices would be hacked, do you think you would notice it?

If one of your devices would be hacked, do you think it would have serious consequences, or not, and which consequences do you think it too have?

Part 2 (intph2b)

I would now like to tell you something more about the aims we had for the study. One aim, which we told you about, is that we wanted to learn about how people experience smart devices, and how they start integrating them in their daily lives. We, however, did not inform you about the second goal of the study. This second goal was to determine if you would notice it when we would introduce "irregularities" in the behavior of the devices; irregularities that indicate that the devices may have been hacked by another person. And when such irregularities were noticed, then we were interested in how you thought and felt about these. Therefore, in the past weeks, we had various devices, at some point in time, do something that could perhaps give you a clue of being hacked.

For now, I do not want to reveal what these irregularities were exactly. I will tell you later why. First, I would like to hear your response to this information regarding this additional did not inform you research goal of which we did not inform you beforehand.

[give them time to think about it and respond to that]

If you are now thinking back over the past few weeks, did you notice anything odd about the devices that could relate to being hacked?

Did it bother you?

How do you think you would have reacted if we had actually told you that we discovered that you were being hacked by somebody else, somebody that we don't know. How would you then have responded?

With respect to the irregularities that we introduced, I want to make clear that every aspect of our research has been approved by several ethical committees (one at each participating university) before the start of the study. The irregularities that we introduced were mild, not long-lasting, and harmless. Nevertheless, you may have experienced the irregularities as being annoying.

I also want to make clear that we only *simulated* how devices may start to behave after a real hack. We have performed the irregularities by using the credentials of the related services (i.e. username and password). To change the status of the devices, we logged into the service of the device remotely through the internet using software called IFTTT and Stringify. We did not look at the historical use of the devices and did not have access to camera images. This was also explicitly prohibited by the ethics committees. In other words, when performing the irregularities, we did not use or abuse known vulnerabilities in the devices (vulnerabilities that a real hacker would use to gain access to a device). We also did not make the devices more vulnerable to hacking.

[Listen to what they tell, and ask for clarification, where possible].

The study lasts two more weeks. So far, some of you have noticed the irregularities, and some have not. Our goal for the remainder of the study is to repeat the irregularities and to find out whether you are able to detect and identify them now that you know you are being 'hacked' *[make quotation marks with your hands to help them to realize again that it is not a real hack]* We therefore want to ask you to report when you notice something in the behaviour of the devices of which you think it may be cause by us. You can use either the positive or the negative experiences survey to report these; both will do. You can use any of these two surveys to describe the irregularity you spotted and to indicate how sure you are (and why) that this irregularity was introduced by the research team. If you have another kind of positive or negative experience with a device that you want to share with us, then these two surveys can still be used for that purpose (in a similar vein as you did in the past weeks).

If you like, then please consider completing–later today–a positive or negative questionnaire to reflect on your feelings when you heard about the hidden purpose of the study.

One of the reasons why we have been asking you to keep track of when you were at home in the diary is to better determine whether you were indeed present at the time that an irregularity took place.

Give them some time to think about it and respond to this.

Also for the next two weeks, we kindly ask you to fill in the diary every day, or every other day, and to report on when you were at home and when not. This allows us to make an educated guess about your presence in the home during the execution of the irregularities that we will introduce in the upcoming weeks.

We thus have not been completely open and honest to you about the goal of the study. We understand that this can be unpleasant for you. We can imagine that our dishonesty towards you is the reason for you to consider stopping your participation in the remainder of the study. Note that you have the right to do so, and that such a decision will not have any negative consequences for you. We hope, however, that you will continue to participate for the final two weeks. You can also think about this for a while and let us now later on. The next phase will start somewhere in the coming days, and last until Sunday, December 16th.

After these two weeks, we will interview you again to learn about your experiences in this last phase of the study. We will then also decouple the smart devices from the accounts that we created. It is important to know that when we disconnect the devices from our accounts, we no longer have access to the devices and / or the data they generate. It is then possible for you to install the devices and the related applications on your own phone or laptop. We will give you some tips and instructions on how to do this, and for a short period of time, will provide assistance if needed.

End of phase 3 interview UK and Dutch households (intph3)

In the past weeks you have been deliberately 'hacked'. Can you tell me how you have experienced this?

Here are the irregularities with the devices you have reported as 'hacks' by the research team. *[print out on separate sheet and provide it to them in the interview – or show on computer screen].*

Shall we go through them one by one and discuss them? *[for each reported attack:]*

Can you tell me more about this irregularity?

- What did you think of this 'hack', how did it make you feel?
- Have others noticed it as well? How did it make them feel?

Can you tell me how confident you are that this was an irregularity caused by the research team?

- Could it have been caused by something else? Explain your reasoning.
- If you are in doubt, can you explain why that is?
- What did others think *[if there were others]*? What did they contribute the cause to, and if they were in doubt, why?

After discussing all reported attacks:

Has anything happened that is not on the list, but could have been reported as a possible attack?

- If yes, would you be willing to fill out the positive/negative questionnaires for these events right now? *[After they have done this, go through the questions above again]*

Imagine that the irregularities you've noticed with the devices in your house would have happened outside of an academic study environment. What would you think about that?

- How would it make you feel?
- What would you want to do about it, and what would you be able to do about it?

The following attacks are the ones we actually perpetrated:

[show a print out of the list or show it to them on the computer]

Which of these did you notice, but did not identify as an attack?

[Mark on the list which ones were noticed]

What was the reason that you did notice this irregularity but did not identify it as a hack done by the research team?

Which of the irregularities did you not notice? Would that have been because you weren't at home, or in the relevant room, or could there have been other reasons why you did not notice them?

Were there irregularities that are not on the list, but of which you thought we were responsible?

- Why do you think you got this wrong?

You have probably noticed that you can sometimes be unaware of the fact you are being 'hacked'. Would you like help to be able to detect and recognize hacks?

- How would you like to be helped/supported?
- Would you want the devices themselves to give you a warning?
- Or would you like to be warned by the government, and if so, how?
- Or would you want to be contacted by the manufacturer or your Internet provider, when they have noticed you were hacked. If so, how?
- Is there anything else you'd want related to this?

Would you want help to prevent hacks?

- How would you want to be helped and by whom?
- How do you feel about extra software, or hardware, or an advice service?
- Would you be willing to pay for such help, and if so, how much?

Thank you very much for taking part in our study. We would like to give you more information about your chances to be hacked and how to prevent this. We have got this text for you to go through:

Smart home and other Internet of Things devices are designed for convenience, entertainment, energy efficiency or safety. However, they are effectively computers, just like your laptop and your phone, and most of them have to be connected to the Internet all the time. This makes them potential targets of new security threats, some of which we emulated and you may have experienced during this experiment. Over the last few years, there have been several high-profile cases of physical systems (which don't look at all like computers) being hijacked by cyber criminals, from speaking to a baby in her nursery through the baby camera, to disabling air conditioning, MRI machines and medical implants in a hospital, or unlocking keyless entry cars. Some of these were done on purpose. Others were the result of computer viruses that just happened to reach these devices randomly through the Internet. Their manufacturers are not oblivious of the security problem. In fact, when our research team discovered a very particular technical flaw in our laboratory and we informed the manufacturer, shortly later they corrected it with an update. Nevertheless, there are thousands of such technical flaws discovered on a daily basis and hoping or waiting for manufacturers to fix them all is unrealistic.

In practice, at the moment, the risk that a cyber criminal will target a household specifically and on purpose is still low. What is more likely is that they use automated software to "scan" through all smart devices that are connected to the

Internet and find those that have easy passwords or have not been updated recently and as such may have known flaws that they can exploit. Another source of issues is often the security of your own Internet router. As most are wireless, they can be accessed by people outside your home too, especially if they can guess the password. Finally, for almost all smart devices, a primary concern is the security of your own account with each manufacturer (your Amazon account, your Fitbit account etc.). It is natural to think of using the same password for all, but this means that if one of these big companies is hacked and loses their customers' data (and that is not uncommon at all), then cyber criminals will have your password for all other devices too. At the moment, all these risks are not as high as for example the risks of e-banking or viruses on social media, but they are increasing continuously and steadily, as smart homes become more and more common, and as such more and more attractive to cyber criminals. So, the responsible thing to do is to follow basic principles of "cyber hygiene" just as we should do for all our other interaction with computers and the Internet:

- Change your passwords as often as you can handle, and never use the same password for two different things.
- If a new update is available for a smart device, do perform it, especially if the manufacturer informs you that it includes security improvements.
- Trust your instinct. If a device performs differently to how it should, switch it off, check online whether this is a known problem, and search for an update.
- When purchasing a new device, ask or look for what security measures the particular manufacturer has taken. If they have put a lot of effort into securing their devices, they will also have put a lot of effort into explaining to the customer how.
- When not in use, consider disconnecting or unplugging these devices.
- Use the instructions coming with your Internet router to change its name to something seemingly random that does not identify your name or your address. Leaving it to the default name effectively informs all your neighbours about your Internet provider and the make of your router.
- Smart devices are meant to make your home a happier, safer place. Our advice above is for helping you also making it a more secure place.

Acknowledgements This study is part of the research project 'Emotion Psychology Meets Cyber Security in IoT Smart Homes (Cocoon)', funded by EU FP7 CHIST-ERA funding scheme (European Coordinated Research on Long-term Challenges in Information and Communication Sciences & Technologies ERA-NET) corresponding to grants FWO project G0H6416N-FWOOPR2016009701, EPSRC EP/P016448/1, and NWO project 651.002.002. We thank Martin Boschman and Aart van der Spank for their technical support.

Author contribution NH managed the execution and planning of the experiment, performed the thematic analysis, and wrote the paper with input from all authors. NH, AO, ER, and GL collected the data. AH and WIJ provided input to the thematic analysis. IR prepared the smart home equipment and equipment-related remote data monitoring. AB coordinated and launched the simulated cyber-attacks. ER, AH, GL, JF, and WIJ acquired the funding. All authors were involved in the design and execution of the experiment.

Data availability The datasets generated during and/or analysed during the current study are not publicly available due to privacy reasons but are available from the corresponding author on reasonable request.

Declarations

Competing interests The authors declare no competing interests.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Loukas G (2015) Cyber-physical attacks: a growing invisible threat. Elsevier, London
2. Heartfield R, Loukas G, Budimir S et al (2018) A taxonomy of cyber-physical threats and impact in the smart home. Comput Secur 78:398–428. https://doi.org/10.1016/j.cose.2018.07.011
3. Gebel M (2019) A California woman says her family experienced 'sheer terror' after their Nest security camera was hacked, warning them of a North Korean missile attack. In: Business Insider. https://www.businessinsider.nl/nest-camera-hacked-north-korea-missile-attack-2019-1?international=true&r=US. Accessed 19 Jun 2021
4. Gibbs S (2014) Q&A: Who is watching my home webcam? The Guardian
5. Noor P (2019) Ring hackers are reportedly watching and talking to strangers via in-home cameras. The Guardian
6. Paul K (2019) Ring sued by man who claims camera was hacked and used to harass his kids. The Guardian
7. Peterson H (2019) Wisconsin couple describes the chilling moment that a hacker cranked up their heat and started talking to them through a Google Nest camera in their kitchen. In: Business Insider. https://www.businessinsider.nl/hacker-breaks-into-smart-home-google-nest-devices-terrorizes-couple-2019-9?international=true&r=US. Accessed 19 Jun 2021
8. Weaver M (2014) UK moves to shut down Russian hackers streaming live British webcam footage. The Guardian

9. Kolias C, Kambourakis G, Stavrou A, Voas J (2017) DDoS in the IoT: Mirai and other botnets. Computer (Long Beach Calif) 50:80–84. https://doi.org/10.1109/MC.2017.201
10. Sheleme M, Sharma RR (2021) Cyber-attack and measuring its risk. IRO J Sustain Wirel Syst 3. https://doi.org/10.36548/jsws.2021.4.002
11. Kumar Jain V, Gajrani J (2020) IoT security: a survey of issues, attacks and defences. Lecture Notes on Data Engineering and Communications Technologies 61:219–236. https://doi.org/10.1007/978-981-33-4582-9_18
12. Budimir S, Fontaine JRJ, Huijts NMA et al (2021) Emotional reactions to cybersecurity breach situations: scenario-based survey study. J Med Internet Res 2021;23(5):e24879 https://www.jmir.org/2021/5/e24879 23:e24879. https://doi.org/10.2196/24879
13. Beaton A, Cook M, Kavanagh M, Herrington C (2000) The psychological impact of burglary. Psychol Crime Law. https://doi.org/10.1080/10683160008410830
14. Chung MC, Stedmon J, Hall R et al (2014) Posttraumatic stress reactions following burglary: The role of coping and personality. Traumatology (Tallahass Fla) 20:65–74. https://doi.org/10.1037/h0099374
15. Oulasvirta A, Pihlajamaa A, Perkiö J et al (2012) Long-term effects of ubiquitous surveillance in the home. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12. ACM Press, New York, New York, USA, p 41
16. Canetti D, Gross M, Waismel-Manor I et al (2017) How cyberattacks terrorize: cortisol and personal insecurity jump in the wake of cyberattacks. Cyberpsychol Behav Soc Netw 20:72–77. https://doi.org/10.1089/cyber.2016.0338
17. Symantec (2010) Norton. The cybercrime report: The Human Impact
18. Braun V, Clarke V (2022) Thematic analysis: a practical guide. SAGE
19. Achenbach TM (1966) The Achenbach System of Empirically Based Assessemnt (ASEBA): development, findings, theory, and applications. University of Vermont Research Center for Children, Youth, & Families, Burlington, VT
20. Braun V, Clarke V (2006) Using thematic analysis in psychology. Qual Res Psychol 3:77–101. https://doi.org/10.1191/1478088706QP063OA
21. Emami-Naeini P, Dixon H, Agarwal Y, Cranor LF (2019) Exploring how privacy and security factor into IoT device purchase behavior. In: Conference on Human Factors in Computing Systems - Proceedings
22. Tabassum M, Kosiński T, Lipford HR (2019) "I don't own the data": end user perceptions of smart home device data practices and risks. In: Proceedings of the 15th Symposium on Usable Privacy and Security, SOUPS 2019
23. Zeng E, Mare S, Roesner F (2017) End user security & privacy concerns with smart homes. USENIX Association
24. Heartfield R, Loukas G (2018) Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. Comput Secur 76:101–127. https://doi.org/10.1016/J.COSE.2018.02.020
25. Macmillan NA, Creelman CD (2005) Detection theory: a user's guide, 2nd edn. Psychological Press, New York
26. Lynn SK, Barrett LF (2014) "Utilizing" signal detection theory: Psychol Sci 25:1663–1673. https://doi.org/10.1177/0956797614541991
27. Canfield CI, Fischhoff B, Davis A (2016) Quantifying phishing susceptibility for detection and behavior decisions. Hum Factors 58:1158–1172. https://doi.org/10.1177/0018720816665025
28. Schneiders E, Kanstrup AM (2021) Domestic robots and the dream of automation: Understanding human interaction and intervention. In: Conference on Human Factors in Computing Systems - Proceedings
29. Aldossari MQ, Sidorova A (2018) Consumer acceptance of Internet of Things (IoT): smart home context. J Comput Inf Syst 60(6):507–517. https://doi.org/10.1080/08874417.2018.1543000
30. Alraja MN, Farooque MMJ, Khashab B (2019) The effect of security, privacy, familiarity, and trust on users' attitudes toward the use of the IoT-based healthcare: the mediation role of risk perception. IEEE Access. https://doi.org/10.1109/access.2019.2904006
31. Kim D, Park K, Park Y, Ahn J-H (2019) Willingness to provide personal information: Perspective of privacy calculus in IoT services. Comput Human Behav 92:273–281. https://doi.org/10.1016/J.CHB.2018.11.022
32. Lau J, Zimmerman B, Schaub F (2018) Alexa, are you listening? Proc ACM Hum Comput Interact 2:1–31. https://doi.org/10.1145/3274371
33. Lee M (2019) An empirical study of home IoT services in South Korea: the moderating effect of the usage experience. Int J Hum Comput Interact 35:535–547. https://doi.org/10.1080/10447318.2018.1480121
34. Shuhaiber A, Mashal I (2019) Understanding users' acceptance of smart homes. Technol Soc 58:101110. https://doi.org/10.1016/j.techsoc.2019.01.003
35. Zheng S, Chetty M, Feamster N (2018) User perceptions of Privacy in Smart Homes. Proc ACM Hum-Comput Interact 2:20. https://doi.org/10.1145/327

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.