"Secure settings are quick and easy!" – Motivating End-Users to Choose Secure Smart Home Configurations

Sarah Prange*
sarah.prange@unibw.de
University of the Bundeswehr Munich
Germany

Niklas Thiem
niklas.thiem@outlook.de
LMU Munich
Germany

Michael Fröhlich†
froehlich@cdtm.de
Center for Digital Technology and Management
Germany

Florian Alt
florian.alt@unibw.de
University of the Bundeswehr Munich
Germany

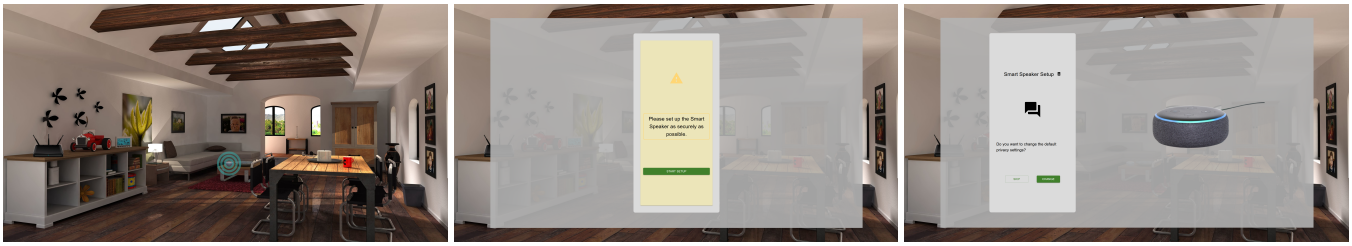


Figure 1: In a randomized online experiment ($N = 210$), we simulated a smart home setup procedure (left) to investigate nudges (center) with the aim of fostering secure smart home configurations. For a set of standard smart home devices (e.g., smart speaker, right), users were prompted with both, security-enhancing options and options with no security impact. We found that nudges providing a detailed description of threats and countermeasures led users to choose more secure options.

ABSTRACT

While offering many useful features, novel smart home devices also provide an attack surface to users' allegedly secure place: their homes. Thus, it is essential to employ effective threat mitigation strategies, such as securely configuring devices. We investigate how users can be motivated to do so. To foster secure actions, we designed two types of *nudges* based on the Protection Motivation Theory (PMT): one with low and one with high level of detail. As such, our nudges particularly target users' threat appraisal (including perceived severity and likelihood of threats) and self-efficacy to take action. In a randomized online experiment ($N = 210$), we simulated a smart home setup procedure. Participants chose significantly more secure configurations when being provided with detailed nudges, and indicated higher perceived threat and coping appraisal (i.e., higher protection motivation) after the experiment. Based on our results, we discuss the design and deployment of nudges for (future) smart home setup procedures. Our work can help to a) increase users' threat awareness in general, and b) motivate users to take actions such as securely configuring their devices.

CCS CONCEPTS

• **Security and privacy** → **Usability in security and privacy**; • **Human-centered computing** → *Ubiquitous and mobile devices.*

KEYWORDS

Smart Home, Usable Security, Protection Motivation Theory

ACM Reference Format:
Sarah Prange, Niklas Thiem, Michael Fröhlich, and Florian Alt. 2022. "Secure settings are quick and easy!" – Motivating End-Users to Choose Secure Smart Home Configurations. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces (AVI 2022), June 6–10, 2022, Frascati, Rome, Italy.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3531073.3531089

1 INTRODUCTION

Smart home devices are on the rise with a continuous market growth since 2016[1]. Such devices serve a rich variety of purposes including, but not limited to, home automation or sustainable energy consumption [31]. At the same time, such devices are prone to

*Also with LMU Munich.
†Also with LMU Munich, University of the Bundeswehr Munich.

AVI 2022, June 6–10, 2022, Frascati, Rome, Italy

ACM ISBN 978-1-4503-9719-3/22/06…$15.00
https://doi.org/10.1145/3531073.3531089

[1]https://www.statista.com/statistics/682204/global-smart-home-market-size/, last accessed January 17, 2022

novel attacks and threats [4, 46], both from within and outside the home [21]. For example, attackers might be able to inject malicious code on devices not properly configured and, hence, get access to the smart home's data and/or make it unusable [3]. Moreover, the potential for "cyber-physical" attacks is a growing concern: attackers might not only get access to digital, but also physical assets [22]. For instance, burglars could identify absence of owners based on presence sensor data [3].

Key to mitigating attacks is the proper configuration of smart home devices. The setup and configuration of smart home devices is commonly done by end users rather than by security experts. Yet, lay users might either not be aware of security and privacy issues or not consider themselves knowledgeable enough to configure their devices securely and, hence, not be *motivated* to invest time in the secure setup of new devices. This is particularly worrisome, as even a single vulnerable device can substantially increase the attack surface on users' home network. With one's home generally considered to be a "secure place", helping users configure their devices securely can help reclaiming parts of this notion.

To address the aforementioned challenges, it is essential to generate awareness and *motivate users to employ secure configurations* as a means for threat prevention. To this end, we use the Protection Motivation Theory (PMT) [37] as theoretical framework. According to this theory, users' protection motivation is impacted by two major factors: 1) their awareness for threats, including individual consequences (*threat appraisal*), and 2) their confidence to cope with threats and apply adequate countermeasures (*coping appraisal*). These factors can efficiently inform the design of *nudges*, that ultimately lead to more secure decisions in security and privacy contexts [40, 41, 47].

We investigate the question *"How can end-users' motivation to configure their smart home devices (more) securely be increased?"* Based on the PMT, we built two types of nudges for the context of smart home configurations, differing in their levels of detail (see Table 1): low (with basic information) and high (with detailed information on threats and countermeasures). In a randomized online experiment ($N = 210$), participants were asked to complete a simulated smart home setup procedure with three typical smart home devices — a router, a light bulb, and a smart speaker – while being exposed to either type of nudge or a control message (Figure 1). Users could configure each of the devices by choosing several *secure actions* (e.g., changing the router's default password or updating the light bulb's firmware).

We found that participants exposed to nudges chose significantly more secure actions compared to a control group with simple instructions. While high detail nudges result in the largest change of user behavior, we found that already low detail nudges lead to improved behavior. In line with the PMT, we also found that exposure to either type of nudge increased participants' protection motivation along several dimensions. These results show that increasing users' motivation can help them to protect their home by employing secure configurations.

We conclude with a discussion around the design and deployment of PMT-inspired nudges in the context of smart home configurations. We hope our work to inform future nudge designs and mechanisms to ultimately support users securing their homes.

2 BACKGROUND & RELATED WORK

In this section, we highlight the need for secure configurations of smart home devices (cf. security and privacy in smart homes, 2.1), introduce the Protection Motivation Theory (2.2), and illustrate prior work applying nudges in usable security research (2.3) .

2.1 Smart Home Security & Privacy

Smart home devices provide great benefits to users for various application cases [31]. However, privacy and security concerns are growing. Smart devices collect and access potentially sensitive user data (e.g., [13]) to serve their rich functionalities. At the same time, devices are also prone to threats [46]. Potential attacks can originate from outside, but also from within the home [21].

Consequences of attacks towards the home are severe. Attackers with physical access to a smart home device could get access to personal data and credentials stored on (unsecured) devices. Attackers who gain remote access to presence data collected by a smart home could identify chances for physical burglary [3]. Furthermore, attackers could manipulate devices or automation routines [39], and, ultimately take over control of the smart home system and make it unusable [3]. As both, physical and digital attacks are blending, such attacks are commonly referred to as *cyber-physical* [3, 22].

Mitigation & Countermeasures. To preserve privacy and security in the sensitive context of smart homes, employing appropriate measures is essential [3, 5, 7, 22, 46]. This not only includes increasing users' awareness [34], but also changing default configurations and employing secure authentication or access control mechanisms [3, 21, 22, 46]. However, the design of such mechanisms is challenging [21, 33, 35]. Current privacy and security interfaces are oftentimes of limited usability [8, 39] or are poorly integrated in devices and thus rarely used [26]. Another challenge is that manufacturers as well as end-users tend to focus on functionality and convenience rather than security in the first place [46]. It is, thus, essential to *motivate* users to actively take action [39].

2.2 Protection Motivation Theory (PMT)

First introduced in 1975, Rogers' Protection Motivation Theory (PMT) describes the impact of fear appeals on human behavior [36, 37]. At the core of the PMT are two cognitive processes, influencing people's protection motivation: *Threat Appraisal* and *Coping Appraisal*. The higher individuals perceive these components, the higher their motivation to take action and protect themselves [37]). The threat appraisal comprises users' perceived threat severity and vulnerability, which should outweigh the perceived maladaptive rewards (i.e., perceived benefits of not changing the own behavior) [15, 36]. For the coping appraisal, users' perceived self- and response efficacy need to outweigh the perceived response cost to increase motivation [11, 15, 36].

PMT in the Smart Home Context. The PMT factors can serve as predictors for consumer behavior related to smart home devices. In particular, users are willing to engage in privacy protection as long as they consider themselves able to (efficacy) and the response cost is not too high [11]. Moreover, users who secure their home networks are significantly impacted by their perceived severity, response efficacy, self-efficacy, and response cost [45].

Table 1: Example Nudge Texts for the Smart Speaker: Nudge content for both PMT components, threat and coping appraisal, in the low and high detail version, respectively.

	Threat Appraisal	Coping Appraisal
Low Detail	**Smart Speakers are risk-prone:** Poorly configured smart speakers are very likely to be hacked. Potential risks are leakage of personal data and/or financial damage.	**You can easily minimize the risk yourself:** Best practices include e.g. changing the manufacturer's default configurations.
High Detail	**Smart Speakers are risk-prone:** Poorly configured smart speaker devices are likely to be hacked. Potential consequences can be severe for the end-users. Read here what happened to other users: [web links] **But users are active:** Over 77 percent of smart home device owners in your area are actively protecting themselves with proper configuration of their smart speaker.	**You can easily minimize the risks yourself:** Best practices for smart speakers are: • connect to a secure network • review and adjust privacy configurations • change the default wake word **Effort for a secure setup:** The additional time needed for a secure configuration is appr. three minutes.

2.3 Nudging in Privacy and Security Contexts

Thaler and Sunstein introduced *nudging* as a means to predictably alter users' behavior by subtly changing the "choice architecture" [28]. In privacy and security contexts, nudging can help users to act according to their preferences and needs [40]. In particular, nudges with clear information can support privacy and security decisions [2, 23] (e.g., creating secure passwords or choosing secure cloud services [47]), and ultimately lead to more secure behaviors. In the context of smart homes, nudges displayed in a smartphone interface can influence users' energy-saving behavior [25]. We consider smart homes as a security and privacy critical context, and aim to nudge users to more secure and privacy-protecting decisions.

PMT-Inspired Nudges. Prior research designed *nudges* inspired by the PMT constructs to evoke users' protection motivation. Nudges inspired by the PMT have been used in prior work to resolve misconceptions towards privacy tools [41], and to foster the adoption of security-enhancing technologies (e.g., mobile payment) [40].

2.4 Summary

Prior research designed *nudges* to evoke users' protection motivation and, ultimately, lead to more secure and privacy-protecting decisions [23, 40, 41, 47]. In the particularly sensitive context of smart homes, secure behavior (i.e., device setup) is crucial to be protected against *cyber-physical* attacks [3, 22]. However, many users are unaware of potential threats to their smart home and/or lack the efficacy to take action. Hence, it is crucial to *motivate* users to actively take appropriate countermeasures [39].

We focus on increasing smart home users' motivation to actively protect their homes against threats. Using the Protection Motivation Theory (PMT), we designed nudges to motivate them and help them take more secure decisions during a smart home setup procedure. We derive the following research questions for our work:

RQ1: How do PMT-inspired nudges impact users' *configuration choices* in the smart home context?

RQ2: How do PMT-inspired nudges impact users' *protection motivation* in the smart home context?

3 PMT-INSPIRED NUDGES FOR SECURE SMART HOME CONFIGURATIONS

To target users' protection motivation in the context of smart homes, we created two types of text-based nudges, with LOW and HIGH level of detail. Table 1 shows an example.

Nudges targeting the PMT constructs can be an efficient means to foster secure behavior and the adoption of security-enhancing technologies [40, 41]. Moreover, previous work found the combination of both, threat and coping appraisal, to be more effective than targeting just one dimension [36, 42, 43]. Hence, we designed both nudge versions to particularly target users' perceived threat severity and vulnerability (by, e.g., providing concrete examples of risks and consequences), as well as perceived efficacy and response cost (by, e.g., describing necessary steps to employ appropriate countermeasures and estimated time).

For three sample devices, we created LOW DETAIL nudges providing a short and general message, and HIGH DETAIL nudges with longer descriptions. The LOW DETAIL versions are closely adapted from related work [42, 43].

Prior work showed that abstract risks (as shown in the LOW DETAIL version) are often perceived likely, but only moderately severe [18]. At the same time, raising users' risk perception can increase their protection motivation in the context of smart homes [10]. Combining nudges with educational information about *why* users are being nudged can foster active decision making in cyber security [47]. These findings motivate our HIGH DETAIL nudge version. Following Story et al.'s suggestion that nudges should be designed in such a way that they can help users protect from *well-defined* threats [41], we added concrete real-world examples to the HIGH DETAIL versions. We also emphasize the efficacy of the proposed countermeasure [41] by showing concrete steps and estimated time.

In summary, our nudges address the components of the PMT as follows (cf. Table 1):

Low Detail Nudge To target users' *threat appraisal*, this nudge illustrates potential threats (*severity*) and their high likelihood (*vulnerability*) for poorly configured devices. As for the *coping appraisal*, this nudge provides basic instructions to mitigate threats (*self-* and *response efficacy*).

High Detail Nudge In addition to the information from the low detail version, this nudge provides the following details: For *threat appraisal*, it comprises concrete examples for threats (*severity*) and consequences (*vulnerability*) using web articles on cyber attacks towards the respective device. Additionally, we used information about social expectations ("norm nudging" [6]) to indicate the desired behavior and minimize *maladaptive rewards*. For *coping appraisal*, it provides detailed instructions for appropriate countermeasures (*self-* and *response efficacy*) and estimated time (*response cost*).

4 METHOD

In a randomized online experiment ($N = 210$), we tested the effects of our nudge designs (LOW DETAIL VS HIGH DETAIL) on participants' smart home protection motivation. This study was approved by an IRB at LMU Munich, under EK-MIS-2021-076.

4.1 Apparatus

To test our hypotheses and measure the impact of nudges on user behavior, we developed a web-based smart home setup simulation using Directus[2], React[3], and Material Design[4] (Figure 1). The simulation replicated the standard procedures of smart home setup processes and implemented a storyline covering three common smart home devices and a total of 15 different configuration options. The setup procedures comprised both, security-enhancing configuration options (*Secure Actions*), and options with no direct security impact (*Additional Actions*[5]). Table 2 shows an overview. Three smart home devices were simulated in the experiment – a WiFi router, a smart speaker, and a smart light bulb. The devices were selected considering popularity, vulnerability to risks, and options for security measures. The respective setup procedures were derived from real devices. During the simulation, a smartphone app guided participants through several setup steps (Figure 2).

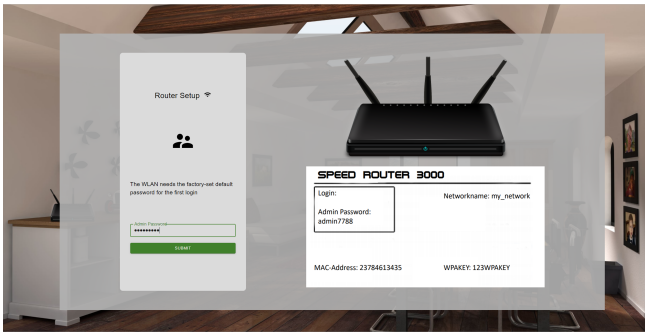


Figure 2: Smart Home Configuration Simulation: The web-based application showed a simulated smartphone app (left) and the device under configuration (here: router).

4.1.1 Collected Data. During the simulation, we collected multiple data points. We recorded which *secure actions* were taken, the *password strength* chosen, the *time spent* configuring devices, and a pre-/ post-experiment assessment of participants' smart home protection motivation using a questionnaire.

Secure Actions. Participants could perform several configuration steps for every smart device. To assess their motivation to secure their smart home devices, we recorded how many *Secure Actions* participants performed during the simulation. Table 2 provides an overview of the possible configuration options.

[2]https://directus.io/, last accessed June 01, 2021
[3]https://reactjs.org/, last accessed June 01, 2021
[4]https://material.io/design, last accessed June 01, 2021
[5]Note: some of the *Additional Actions* might have an indirect impact on security that we did not consider in our analysis.

Table 2: Configuration Options: Overview of the configuration options for each smart home device in the simulation including both, *Secure Actions* and *Additional Actions*.

	Secure Actions	Additional Actions
router	change default password create guest network refresh WPA key	change network name change connection type change timezone
smart speaker	adjust privacy settings select segmented WiFi change wake word	register/ login adjust language change timezone
smart bulb	update firmware select segmented WiFi	change device name change timezone

Password Strength. The configuration of the smart speaker required the creation of a user account. Reflecting participants' motivation to secure their account, we tracked the strength of the selected password. Note that both nudge designs hinted to changing default configurations (including passwords), however we did not include explicit guidelines for secure passwords. Using a popular npm package[6], we assigned passwords numerical categorical values (0 = Too weak, 1 = Weak, 2 = Medium, 3 = Strong). The algorithm considers diversity (lowercase, uppercase, numbers, symbols) as well as length. The strength was calculated locally in participants' browsers and only the final scores were stored.

Time. We tracked participants' time spent in the simulation as an indicator for motivation. Since different types of nudges were of different length, the time spent reading nudges was excluded, i.e. we recorded the time between "Start Setup" and "Finish Setup".

Smart Home Protection Motivation. Grounding our experiment in the Protection-Motivation-Theory (PMT), we hypothesize that nudges would affect participants' motivation to secure their smart devices. To understand how the different PMT constructs would be influenced, we adapted a survey instrument by MacDonell et al. to the smart home context [30]. Answers were collected on a 7-point Likert scale ranging from "completely disagree" to "completely agree", with one item per PMT construct (see Table 3).

Table 3: PMT-Questionnaire: Questions to assess users' smart home protection motivation pre- and post-experiment.

Question	PMT construct
If my smart home devices was hacked, it would have severe consequences for me.	Severity
There is a high chance that my smart home devices are targets of cyber attacks.	Vulnerability
Leaving the default settings on my smart home devices saves me time and energy.	Maladaptive Intrinsic Rewards
It is common to leave the standard settings set by the manufacturer.	Maladaptive Extrinsic Rewards
I know how to configure my smart home devices securely.	Self-efficacy
Secure configurations of my smart home devices are good protection against cyber attacks.	Response Efficacy
Secure configurations of smart home devices are a great effort for me.	Response Cost

[6]https://.npmjs.com/package/check-password-strength, last accessed June 01, 2021

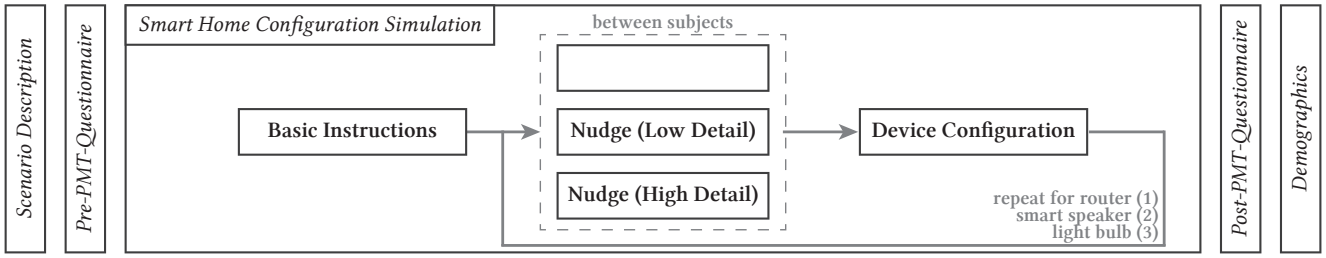


Figure 3: Experiment Procedure: Participants (1) were introduced to the scenario, (2) filled the PMT-questionnaire, (3) completed the simulation, (4) filled the PMT-questionnaire, and (5) provided demographics and prior smart home experience.

4.2 Experimental Design

To investigate the influence of nudges on users' configuration behavior, we implemented a between-subjects design [27] with one independent variable (*type of nudge*) which could take one of three forms: NO nudge (control group), LOW DETAIL nudge, and HIGH DETAIL nudge. Participants were exposed to only one type of nudge throughout the study. Thus, we designed six nudges: one LOW DETAIL and one HIGH DETAIL nudge for each of the three smart home devices (router, smart speaker, smart light bulb). The control group was shown no nudge. Participants were randomly assigned to one of the groups prior to the start of the simulation.

As *dependent variable* we measured the total number of *Secure Actions* participants applied during the simulation, the *time* participants spent for the configuration, and the *password strength* for the smart speaker's account.

4.3 Procedure

The experiment was administered online and could be accessed through a web browser using a desktop computer. All data was collected anonymously. The detailed procedure was as follows (Fig. 3):

1) *Scenario Description.* To immerse participants in the scenario, we provided a textual description. They should imagine that they just bought a couple of smart home devices and their task was to now set them up in their home.
2) *Pre-PMT-Questionnaire.* Participants then filled in the PMT-questionnaire (see Table 3) to assess their protection motivation.
3) *Smart Home Configuration Simulation.* The setup simulation comprised the configuration of three devices, namely (1) router, (2) smart speaker, and (3) smart light bulb, in this exact order. We assumed this order to align with real-world setup procedures. Before participants could start setting up each device, they were exposed to the treatment of our experiment – they were shown a nudge on the simulated smartphone screen.
4) *Post-PMT-Questionnaire.* We again collected participants' protection motivation using the PMT-questionnaire (Table 3).
5) *Demographics.* We additionally collected demographic information and data on past smart home and cyber attack experiences.

Participants were randomly assigned to one group (control, LOW DETAIL, HIGH DETAIL) and exposed to the same type of nudge throughout the complete configuration simulation. The order of the PMT-questions was randomized to avoid order effects bias.

4.4 Participants

We recruited our sample via Prolific[7], an online service specialized on providing a subject pool for research [32]. Participants were required to have a desktop computer and be fluent in English. Our final sample consisted of 210 participants, out of which 115 (55%) were female, 89 (42%) were male, two indicated "other" and four participants preferred not to say. The average age was 25.3 years (MIN18, MAX69, SD11.9). A total of 117 participants stated to own at least one smart home device and 11 participants reported having experienced cyber attacks. Attacks mainly targeted their social media ($N = 6$), gaming ($N = 1$), or banking ($N = 1$) accounts. Two participants reported attacks towards their devices (one computer, one smartphone), and one reported a phishing attack.

4.5 Limitations

Our sample is rather young (mean age 25.3) and based in western countries. Hence, our results may not apply to the general public and to other cultures. We conducted the study online using a simulation. Thus, we can only make limited assumptions about actual behavior as privacy and security preferences may differ from actual behavior (cf. the "privacy paradox" [17]). However, online studies have been shown to be an effective means in HCI research [44].

5 RESULTS

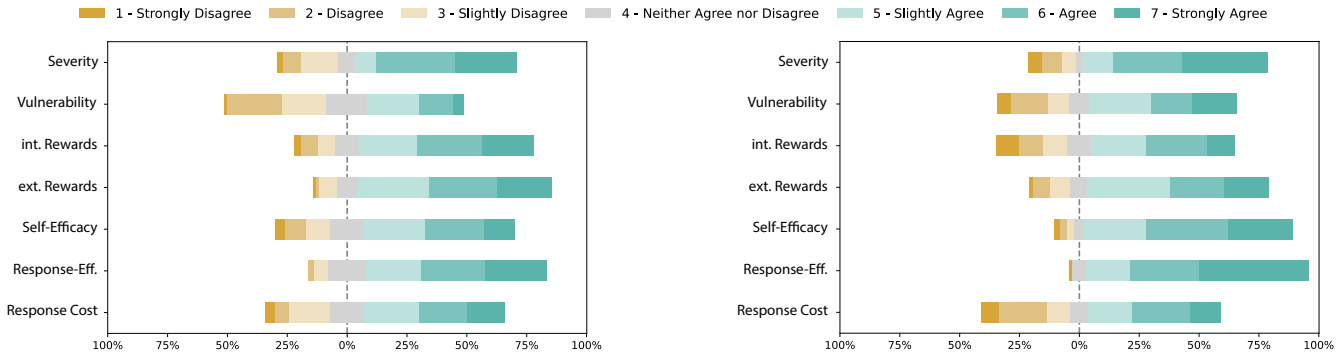
Given the between-group design, our sample can be divided into three groups: (1) control group, which saw NO nudge ($N = 70$), (2) LOW DETAIL group, which saw the low detail versions of the nudges ($N = 70$), and (3) HIGH DETAIL group, which saw the high detail versions of the nudges ($N = 70$). All statistical tests are conducted with $\alpha = 0.05$ as threshold for statistical significance. Moreover, with a sufficiently large sample size per group (>30), the central limit theorem allows us to assume a normal distribution for all statistical tests in the following [1].

5.1 RQ1: Configuration Choices

Addressing **RQ1**, we look into users' configuration choices during our simulation. In particular, we analyzed the number of *secure actions*, *time* spent for the configuration, and *password strength*.

5.1.1 Secure Actions. Participants' number of performed secure actions during the simulated setup procedure differs between the three groups (cf. Table 4). In particular, participants in the control

[7] https://prolific.co/, last accessed September 01, 2021



(a) Pre-PMT Questionnaire

(b) Post-PMT Questionnaire

Figure 4: Participants' smart home protection motivation in the high detail group before and after the experiment.

group performed on average the fewest number of secure actions (mean 2.51), followed by participants in the low detail group (mean 2.93). Participants in the high detail group performed on average the most secure actions (mean 3.79). A Levene's-Test [29] showed significant difference in variance between the groups ($F(2, 207) = 13.019, p < 0.001$), violating the homogeneous variance assumption required to use ANOVA [9, 14]. Hence, we used Welch's ANOVA, which relaxes the homogeneity of variance assumption [9].

Table 4: The number of *Secure Actions* per treatment group.

Group	Mean	SD	Median	Min	Max
control	2.51	1.45	2	0	6
low detail	2.93	1.62	3	0	7
high detail	3.79	2.21	4	0	7

Testing with Welch's ANOVA showed that the number of secure actions taken differed significantly between the groups ($F(2, 134.62) = 8.0468, p < 0.001$). Since Welch's ANOVA only states the existence of a difference, we conducted an additional pair-wise post-hoc analysis between the groups. We used a Games-Howell post-hoc test as it is suited for comparing groups with unequal variances [16, 38]. The analysis revealed a significant difference between the number of secure actions between the High Detail and the control group ($p < 0.001$) and between the High Detail and Low Detail group ($p = 0.027$). The difference between the control group and the Low Detail group was not statistically significant ($p = 0.252$).

5.1.2 Time. Participants in the high detail group spent on average the most time on device configurations ($mean = 3.12mins$, $SD = 1.36$, $MIN = 0.43mins$, $MAX = 7.19mins$), while participants in the low detail group spent less time on average ($mean = 2.90mins$, $SD = 1.07$, $MIN = 0.99mins$, $MAX = 5.88mins$). Participants in the control group spent on average the least time ($mean = 2.73mins$, $SD = 1.06$, $MIN = 0.28mins$, $MAX = 5.20mins$). A Levene's-Test [29] showed no significant difference in variance between the groups ($F(2, 207) = 1.2341, p = 0.293$). An ANOVA showed no statistical differences between the groups ($F(2, 207) = 4.71, p < 0.056$).

5.1.3 Password Strength. Looking at the average password strength, the descriptive results are less clear. The control group shows the lowest average password strength with a score of 1.32 ($SD = 0.92$, $MIN = 0$, $MAX = 3$), followed by the high detail group with a mean of 1.37 ($SD = 0.98$, $MIN = 0$, $MAX = 3$). The most secure passwords were entered by participants from the low detail group achieving an average strength of 1.53 ($SD = 0.94$, $MIN = 0$, $MAX = 3$). A Levene's-Test [29] showed no significant difference in variance between the groups ($F(2, 207) = 0.0292, p = 0.971$). We therefore used ANOVA. The results showed no statistical differences between the groups ($F(2, 207) = 0.083, p = 0.774$).

5.2 RQ2: Protection Motivation

In addition to participants' configuration choices, we collected participants' smart home protection motivation with a survey in a pre-/ post-experiment assessment. After a visual inspection, we conducted a more detailed analysis for each PMT construct. We compared the answers to each item before and after exposure to the treatment during the experiment. We used the Wilcoxon-Signed-Rank-Test to test for statistical significant differences for each treatment group. The results are described in Table 5. In the control group, no statistically significant difference was found in any dimension. For the low detail group, the Wilcoxon-Signed-Rank-Test showed a significant change in perceived intrinsic (-0.58, p=0.0013) and extrinsic maladaptive rewards (-0.31, p=0.0041), as well as self-efficacy (+0.34, p=0.0299) and response efficacy (+0.31 , p=0.0172). In simple words, after being exposed to the experiment, participants of the low detail group felt less intrinsic and extrinsic rewards from not changing their behavior. They felt more able to configure their smart home devices securely, and believed that configuring devices would be an effective response.

For the high detail group, the Wilcoxon-Signed-Rank-Test showed a significant change along the following dimensions: vulnerability (+0.55, p=0.0024) increased, intrinsic maladaptive rewards decreased (-0.24, p=0.0052), self-efficacy increased (+0.86, p<0.001), response efficacy increased (+0.68, p<0.001), and response cost decreased (-0.35, p<0.0281). In simple words, after being exposed to the experiment, participants of the high detail group felt it was more likely their devices could be targets of cyber attacks and perceived less intrinsic rewards from not changing their behavior. They felt more able to configure their smart home devices securely, believed that configuring devices would be an effective response, and were less inclined to think that doing so would be a great effort for them. Figure 4 shows an overview of participants' answers pre- and post-treatment for the high detail group.

Table 5: Comparison of the Pre-/Post-PMT-Questionnaire per Group. The results are as follows: 1) no statistically significant differences in the control group (NO nudge); 2) significant differences for the intrinsic and extrinsic maladaptive rewards, self-efficacy, and response efficacy dimensions in the LOW DETAIL group; 3) significant differences for vulnerability, intrinsic maladaptive rewards, self-efficacy, response efficacy, and response cost in the HIGH DETAIL group.

	1) NO nudge					2) LOW DETAIL nudge					3) HIGH DETAIL nudge				
	pre-treatment		post-treatment			pre-treatment		post-treatment			pre-treatment		post-treatment		
	mean	**median**	**mean**	**median**	**p-value**	**mean**	**median**	**mean**	**median**	**p-value**	**mean**	**median**	**mean**	**median**	**p-value**
Severity	5.07	5.50	5.11	5.50	0.7115	5.16	5.00	5.17	5.00	0.8616	5.13	5.00	5.37	6.00	0.1400
Vulnerability	3.76	4.00	3.93	4.00	0.1421	3.96	4.00	4.13	4.50	0.3624	3.94	4.00	4.59	5.00	**0.0024***
Intr. Reward	4.51	5.00	4.50	5.00	0.9597	4.87	5.00	4.29	5.00	**0.0013***	5.13	5.00	4.49	5.00	**0.0052***
Extr. Reward	5.79	5.00	4.83	5.00	0.9762	5.11	5.00	4.80	5.00	**0.0041***	5.41	6.00	5.09	5.00	0.0658
Self-Efficacy	4.79	5.00	4.84	5.00	0.7939	4.99	5.00	5.33	6.00	**0.0299***	4.73	5.00	5.59	6.00	**0.0000***
Resp. Efficacy	5.43	6.00	5.57	6.00	0.4402	5.73	6.00	6.04	6.0	**0.0172***	5.43	6.00	6.09	6.00	**0.0000***
Resp. Cost	5.00	5.00	4.81	5.00	0.5192	4.43	4.00	4.30	5.00	0.5508	4.69	5.00	4.34	5.00	**0.0281***

6 DISCUSSION

We found that both types of nudges resulted in desirable behavior change compared to the control group, with statistically significant changes in the HIGH DETAIL group. In the following, we summarize and discuss these results, including potential future designs and deployments of nudges for the smart home context.

6.1 Overview

In line with related work [40, 41], we found that PMT-inspired nudges can increase users' protection motivation: the pre- and post-assessment of protection motivation shows changes along all dimensions for participants in the LOW DETAIL as well as the HIGH DETAIL group. In particular, negative components (e.g., response cost) were perceived lower, while positive components (e.g., self-efficacy) were perceived higher after exposure to the nudges.

Looking at our specific context, i.e. configuration of a smart home setup, the descriptive statistics showed increased means in the desired direction along all observed categories in both groups with nudges (low and high detail): more secure actions, longer configuration time, stronger passwords (see Table 6). While longer configuration time might seem undesirable, related work showed that such delays are acceptable for users as long as the threat is clear to them [12]. As such, our HIGH DETAIL nudges (including specific risks [18] and educational content [47]) led to statistically significant improvement of the number of secure actions. We speculate that the more concrete descriptions in the high detail version helped participants relate the potential security threats back to themselves, by increasing their perceived vulnerability and severity according to the PMT.

To summarise, our results show that designing PMT-inspired nudges resulted in a) changes in user behavior – i.e., more secure configuration actions taken during the setup procedures, and b) change in users' perception of both, threat and coping appraisal, in the context of smart homes. In the following, we discuss practical implications and map out paths for future research.

6.2 Designing Nudges for Smart Homes

In line with related work [36, 40–43], our results indicate that nudge designs targeting the PMT components (threat and coping appraisal) can be effective in increasing users' protection motivation. Moreover, we found that high detail nudge designs including specific risks [18] and educational content [47] were highly effective in provoking secure actions and decisions. In particular, our high detail nudge version provided graspable details on possible consequences and concrete suggestions for countermeasures, while still being concise with low reading effort. In contrast, the low detail nudge design with rather abstract content was not as effective.

Table 6: Summary of Results: Both, user behavior (secure actions, time spent, password strength) and the pre/post change rate of PMT items (measured smart home protection motivation), moved in the desired direction.

	control	**low detail**	**high detail**
Secure Actions	2.51	2.93	3.79
Time Spent	2.73 mins	2.90 mins	3.12 mins
Password Strength	1.32	1.53	1.37
Severity	+0.04	+0.01	+0.24
Vulnerability	+0.17	+0.17	**+0.55***
Intr. Reward	-0.01	**-0.58***	**-0.24***
Extr. Reward	-0.04	**-0.31***	-0.32
Self-Efficacy	+0.05	**+0.34***	**+0.86***
Resp. Efficacy	+0.14	**+0.31***	**+0.68***
Resp. Cost	-0.19	-0.13	**-0.35***

Hence, we argue that future nudge designs should address both, threat and coping appraisal, in sufficiently high detail to achieve high protection motivation. Also, providing concrete examples of possible consequences can help to increase awareness, perceived severity, and vulnerability. By providing a simple estimate of required time and detailing required steps, users' perceived response cost, self- and response-efficacy can be addressed (i.e., increase efficacy while decreasing perceived response cost).

In our web-based simulation, we tested text-based nudge content enhanced with web-links. Future nudge designs could explore other visual designs, as these can enhance users' understanding of privacy- and security-related aspects [24]. Audio-based content could be employed in cases a display is not necessarily available, e.g. for the configuration of smart speakers or door locks. Other nudge designs could use personalized examples [19] or adapt to users' characteristics [20]. For instance, nudges could adapt to users' general protection motivation: for users with low default motivation, higher effort would need to be taken to convince them to adapt secure behaviors. For users who are highly motivated per se, nudges can help them to act according to their privacy and security needs.

Finally, such nudges can be designed for various contexts. Threats are increasingly ubiquitous with advances in technology, and effective threat prevention is required in many contexts. For instance, in private environments such as the home, nudges can help lay users to employ effective threat prevention in their own environment. Nudges could also be employed to help users who visit foreign

public or private environments, to increase their awareness and motivation to counteract threats. In office environments, where usually dedicated persons are in charge of employing threat prevention, nudges can help them to protect others.

6.3 Deploying Nudges for Smart Homes

In our study, users were exposed to the nudges in a web-based simulation of a stringent smart home setup with a fixed order: router, smart speaker, light bulb. While we assumed this to be in line with a natural smart home configuration storyline, we cannot assume that users employ these devices in that exact order in a similarly short time frame. Rather users might start with one device and only step by step add more. This raises the question as to *when* and *where* to deploy such nudges to be effective.

6.3.1 Timing. Timing needs to be considered for nudges to be effective [2]. Information that is presented in a clear way and in-time (i.e., when users actually make a decision), can foster privacy-protecting behavior [23].

In the smart home context, nudges might be employed during a device's *setup procedure* (one time). Another opportunity is to employ nudges on a regular basis, e.g., every time users *interact with a device*. In these cases, users could be nudged to adjust security and privacy settings or perform new secure actions such as updating the firmware. Lastly, nudges could support users recovering from threats. Supposing the smart home system could recognize threats automatically, nudges could come up to help eliminate the cause as far as possible (e.g., updating firmware, changing passwords).

6.3.2 Modality. Another essential question is where to employ the nudges, and who is responsible to do so. First and foremost, nudges can be employed with the actual device or respective companion application, and, hence, be directly included in the device's setup procedure. However, this relies on the cooperation of manufacturers' and/or legal regulations. In case this is not available, nudges can still be employed by third parties in the form of, e.g., mobile applications [2]. For instance, our nudges could be employed on users' personal devices (e.g., smartphones) as a helper application, that users could consult when needed. Such an application could, however, also act proactively. For instance, it could detect new devices in the ecosystem, and provide help for the configuration. A more sophisticated version of such an application could detect moments in which users would be free to take time for their device configurations (e.g., if a smartphone or smartwatch would detect users being idle). As another modality, nudges could be displayed in augmented reality glasses to provide in-situ information and guidance, or on devices within the home that provide displays.

7 CONCLUSION

In this paper, we present nudges as a means to increase users' motivation to employ effective threat prevention (i.e., secure configurations) in smart homes. In particular, we present two nudge designs, with low and high level of detail, targeting the components of the Protection Motivation Theory (PMT). Our online experiment, which simulated a smart home setup procedure, showed that participants employed significantly more secure configurations when being provided with detailed nudges. In particular, with nudge content targeting the threat as well as the coping appraisal, we could confirm prior work and successfully applied the PMT in the sensitive context of smart homes. While our work can help to increase threat awareness in general, it can also support the design of means to increase users' motivation to actively take countermeasures. In particular, we suggest including concrete and concise details on vulnerability and consequences, as well as required steps to employ countermeasures to successfully increase users' protection motivation in smart homes.

ACKNOWLEDGMENTS

We thank all participants for their time conducting our simulation. This research was funded by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr [Voice of Wisdom].

REFERENCES

[1] 2008. Central Limit Theorem. In *The Concise Encyclopedia of Statistics*. Springer New York, New York, NY, 66–68. https://doi.org/10.1007/978-0-387-32833-1_50

[2] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Comput. Surv.* 50, 3, Article 44 (aug 2017), 41 pages. https://doi.org/10.1145/3054926

[3] Bako Ali and Ali Ismail Awad. 2018. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors* 18, 3 (2018). https://doi.org/10.3390/s18030817

[4] Florian Alt and Emanuel von Zezschwitz. 2019. Emerging Trends in Usable Security and Privacy. *i-com* 18, 3 (2019), 189–195. https://doi.org/10.1515/icom-2019-0019

[5] Malik Nadeem Anwar, Mohammad Nazir, and Khurram Mustafa. 2017. Security threats taxonomy: Smart-home perspective. In *2017 3rd International Conference on Advances in Computing,Communication Automation (ICACCA) (Fall)*. 1–4. https://doi.org/10.1109/ICACCAF.2017.8344666

[6] Cristina Bicchieri and Eugen Dimant. 2019. Nudging with care: The risks and benefits of social information. *Public choice* (2019), 1–22.

[7] Bernardo Breve, Giuseppe Desolda, Vincenzo Deufemia, Francesco Greco, and Maristella Matera. 2021. An End-User Development Approach to Secure Smart Environments. In *End-User Development*, Daniela Fogli, Daniel Tetteroo, Barbara Rita Barricelli, Simone Borsci, Panos Markopoulos, and George A. Papadopoulos (Eds.). Springer International Publishing, Cham, 36–52.

[8] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. "It Did Not Give Me an Option to Decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 555, 16 pages. https://doi.org/10.1145/3411764.3445691

[9] Marie Delacre, Christophe Leys, Youri L Mora, and Daniël Lakens. 2019. Taking parametric assumptions seriously: Arguments for the use of Welch's F-test instead of the classical F-test in one-way ANOVA. *International Review of Social Psychology* 32, 1 (2019).

[10] Reyhan Duezguen, Peter Mayer, Benjamin Berens, Christopher Beckmann, Lukas Aldag, Mattia Mossano, Melanie Volkamer, and Thorsten Strufe. 2021. How to Increase Smart Home Security and Privacy Risk Perception. In *20th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 18 - 20 Augus 2021, Shenyang, China*. 46.23.01; LK 01.

[11] M. Dupuis and Mercy Ebenezer. 2018. Help Wanted: Consumer Privacy Behavior and Smart Home Internet of Things (IoT) Devices. In *Proceedings of the 19th Annual SIG Conference on Information Technology Education*.

[12] Serge Egelman, David Molnar, Nicolas Christin, Alessandro Acquisti, Cormac Herley, and Shriram Krishnamurthi. 2010. Please Continue to Hold: An Empirical Study on User Tolerance of Security Delays. In *9th Annual Workshop on the Economics of Information Security, WEIS 2010, Harvard University, Cambridge, MA, USA, June 7-8, 2010*. http://weis2010.econinfosec.org/papers/session3/weis2010_egelman.pdf

[13] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '17)*. USENIX Association, Berkeley, CA, USA, 399–412.

[14] Julian James Faraway. 2002. *Practical regression and ANOVA using R*. Vol. 168. University of Bath.

[15] D. L. Floyd, S. Prentice-Dunn, and R. W. Rogers. 2000. A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology* 30 (2000), 407–429.

[16] Paul A Games and John F Howell. 1976. Pairwise multiple comparison procedures with unequal n's and/or variances: a Monte Carlo study. *Journal of Educational Statistics* 1, 2 (1976), 113–125.

[17] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security* 77 (2018), 226 – 261. https://doi.org/10.1016/j.cose.2018.04.002

[18] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. 2019. Investigating People's Privacy Risk Perception. *Proceedings on privacy enhancing technologies* 2019, 3 (2019), 267–288. https://doi.org/10.2478/popets-2019-0047

[19] Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. 2014. Using Personal Examples to Improve Risk Communication for Security & Privacy Decisions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 2647–2656. https://doi.org/10.1145/2556288.2556978

[20] Katrin Hartwig and Christian Reuter. 2021. Nudge or Restraint: How Do People Assess Nudging in Cybersecurity - A Representative Study in Germany. In *European Symposium on Usable Security 2021* (Karlsruhe, Germany) *(EuroUSEC '21)*. Association for Computing Machinery, New York, NY, USA, 141–150. https://doi.org/10.1145/3481357.3481514

[21] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 255–272. https://www.usenix.org/conference/usenixsecurity18/presentation/he

[22] Ryan Heartfield, George Loukas, Sanja Budimir, Anatolij Bezemskij, Johnny R.J. Fontaine, Avgoustinos Filippoupolitis, and Etienne Roesch. 2018. A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security* 78 (2018), 398–428. https://doi.org/10.1016/j.cose.2018.07.011

[23] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as Part of the App Decision-Making Process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 3393–3402. https://doi.org/10.1145/2470654.2466466

[24] Agnieszka Kitkowska, Mark Warner, Yefim Shulman, Erik Wästlund, and Leonardo A. Martucci. 2020. Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affect. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, 437–456. https://www.usenix.org/conference/soups2020/presentation/kitkowska

[25] Tobias Kroll, Ute Paukstadt, Kseniya Kreidermann, and Milad Mirbabaie. 2019. Nudging People to Save Energy in Smart Homes with Social Norms and Self-Commitment. In *Proceedings of the 27th European Conference on Information System*.

[26] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 102 (Nov. 2018), 31 pages. https://doi.org/10.1145/3274371

[27] Jonathan Lazar. 2017. *Research methods in human computer interaction* (2nd edition ed.). Elsevier, Cambridge, MA.

[28] Thomas C Leonard. 2008. Richard H. Thaler, Cass R. Sunstein, Nudge: Improving decisions about health, wealth, and happiness.

[29] Howard Levene. 1961. Robust tests for equality of variances. *Contributions to probability and statistics. Essays in honor of Harold Hotelling* (1961), 279–292.

[30] Karen MacDonell, Xinguang Chen, Yaqiong Yan, Fang Li, Jie Gong, Huiling Sun, Xiaoming Li, and Bonita Stanton. 2013. A Protection Motivation Theory-Based Scale for Tobacco Research among Chinese Youth. *Journal of addiction research & therapy* 4 (2013), 154.

[31] Davit Marikyan, Savvas Papagiannidis, and Eleftherios Alamanos. 2019. A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change* 138 (2019), 139 – 154. https://doi.org/10.1016/j.techfore.2018.08.015

[32] Stefan Palan and Christian Schitter. 2018. Prolific.ac — A subject pool for online experiments. *Journal of Behavioral and Experimental Finance* 17 (2018), 22–27.

[33] Sarah Prange, Ceenu George, and Florian Alt. 2021. Design Considerations for Usable Authentication in Smart Homes. In *Mensch Und Computer 2021* (Ingolstadt, Germany) *(MuC '21)*. Association for Computing Machinery, New York, NY, USA, 311–324. https://doi.org/10.1145/3473856.3473878

[34] Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. PriView– Exploring Visualisations to Support Users' Privacy Awareness. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 69, 18 pages. https://doi.org/10.1145/3411764.3445067

[35] S. Prange, E. von Zezschwitz, and F. Alt. 2019. Vision: Exploring Challenges and Opportunities for Usable Authentication in the Smart Home. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. 154–158. https://doi.org/10.1109/EuroSPW.2019.00024

[36] R Rogers, John Cacioppo, and Richard Petty. 1983. *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation*. 153–177.

[37] Ronald W. Rogers. 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology* 91, 1 (1975), 93–114. https://doi.org/10.1080/00223980.1975.9915803 PMID: 28136248.

[38] Graeme D Ruxton and Guy Beauchamp. 2008. Time for some a priori thinking about post hoc testing. *Behavioral ecology* 19, 3 (2008), 690–693.

[39] Joseph Shams, N. A. Arachchilage, and J. Such. 2020. Vision: Why Johnny Can't Configure Smart Home? A Behavioural Framework for Smart Home Privacy Configuration. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (2020), 184–189.

[40] Peter Story, Daniel Smullen, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. From Intent to Action: Nudging Users Towards Secure Mobile Payments. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, 379–415. https://www.usenix.org/conference/soups2020/presentation/story

[41] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2021. Awareness, Adoption, and Misconceptions of Web Privacy Tools. *Proceedings on Privacy Enhancing Technologies* 2021, 3 (2021), 308–333. https://doi.org/doi:10.2478/popets-2021-0049

[42] R. Van Bavel and N. Rodriguez Priego. 2016. Nudging Online Security Behaviour with Warning Messages: Results from an online experiment. *Publications Office of the European Union*, (2016). https://doi.org/10.2791/2476

[43] René Van Bavel, Nuria Rodríguez-Priego, José Vila, and Pam Briggs. 2019. Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies* 123 (2019), 29–39.

[44] Alexandra Voit, Sven Mayer, Valentin Schwind, and Niels Henze. 2019. *Online, VR, AR, Lab, and In-Situ: Comparison of Research Methods to Evaluate Smart Artifacts*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300737

[45] Irene Woon, Gek-Woo Tan, and R Low. 2005. A protection motivation theory approach to home wireless security. (2005).

[46] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu. 2019. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal* 6, 2 (2019), 1606–1616. https://doi.org/10.1109/JIOT.2018.2847733

[47] Verena Zimmermann and Karen Renaud. 2021. The Nudge Puzzle: Matching Nudge Interventions to Cybersecurity Decisions. *ACM Trans. Comput.-Hum. Interact.* 28, 1, Article 7 (Jan. 2021), 45 pages. https://doi.org/10.1145/3429888