Nudge or Restraint: How do People Assess Nudging in Cybersecurity - A Representative Study in Germany

Katrin Hartwig
Christian Reuter
hartwig@peasec.tu-darmstadt.de
reuter@peasec.tu-darmstadt.de
Science and Technology for Peace and Security (PEASEC), Technische Universität Darmstadt
Darmstadt, Germany

ABSTRACT

While nudging is a long-established instrument in many contexts, it has more recently emerged to be relevant in cybersecurity as well. For instance, existing research suggests nudges for stronger passwords or safe WiFi connections. However, those nudges are often not as effective as desired. To improve their effectiveness, it is crucial to understand how people assess nudges in cybersecurity, to address potential fears and resulting reactance and to facilitate voluntary compliance. In other contexts, such as the health sector, studies have already thoroughly explored the attitude towards nudging. To address that matter in cybersecurity, we conducted a representative study in Germany ($N = 1,012$), asking people about their attitude towards nudging in that specific context. Our findings reveal that 64% rated nudging in cybersecurity as helpful, however several participants expected risks such as intentional misguidance, manipulation and data exposure as well.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**.

KEYWORDS

nudging, cybersecurity, usable security

ACM Reference Format:
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 (EuroUSEC '21), October 11–12, 2021, Karlsruhe, Germany.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3481357.3481514

1 INTRODUCTION

The concept of nudging has evolved to be widely applied in many contexts and for many years to change people‘s behavior for the better. A nudge is *"any aspect of the choice architecture that alters people‘s behavior in a predictable way without forbidding any options or significantly changing their economic incentives"* [40]. While forcing people‘s decisions towards the desired outcome tends to create reactance, nudging aims to be perceived as less paternalistic, maintaining the freedom of choice. There are many ways in which nudges can be utilized, both harmfully and favorably. While the advertising industry nudges consumers to buy their products, nudges are also widely applied in the health sector to encourage healthy eating habits, or to prevent smoking (e.g., [13, 30]. In the context of privacy and security, nudging has recently become a growing research field (e.g. [2, 38]). For usable security, it is crucial to address user-centered approaches during the design process [4, 22, 36]. Recent works have started to investigate how bad security and privacy decisions of users can be nudged towards more beneficial decisions [2]. However, these studies are mostly based on one-size-fits-all nudges, while not being as effective as desired [9, 19]. Several studies therefore suggest personalized nudges, e.g. considering character traits (e.g. [9, 15, 20, 28, 41]). To facilitate personalization, it is crucial to understand how specific people assess nudges in specific contexts. To make nudges effective, people need to willingly endorse them and have positive attitudes towards specific nudges [29].

Until now, there are several studies on the attitude towards nudging, which compare nudges in different contexts (e.g. [12, 17, 32, 39]) in one or several countries. While the health context has already been addressed on a larger scale and there are initial investigations for the context of privacy [8, 18], studies investigating the attitude towards nudging in cybersecurity are largely missing. To address that gap, this article presents an initial investigation on how people assess nudging in the context of cybersecurity. Hence, our research questions are:
RQ1: How do people assess nudging in cybersecurity?
In order to answer this question, we want to address the following sub-questions: *RQ1.1 Do they see risks of nudging in cybersecurity? RQ1.2: Does the attitude differ concerning different scenarios? RQ1.3: Do user characteristics or priming conditions affect the attitude?* Based on these answers we like to derive implications for design, answering our second question:
RQ2: What are design implications for nudging in cybersecurity?
To answer our research questions, we conducted a representative survey in Germany ($N = 1,012$ after data cleansing), including priming with nudges for password strength and two standardized psychometric scales. The article is organized as follows: Section 2

EuroUSEC'21, October 11–12, 2021,

ACM ISBN 978-1-4503-8423-0/21/10…$15.00
https://doi.org/10.1145/3481357.3481514

presents related work on the attitude towards nudging in multiple-context studies and context-specific studies, highlighting the research gap. In section 3 we present our survey design, the characteristics of our survey participants, and the method of analysis. In section 4 we present the empirical results before discussing (section 5) and concluding (section 6) our contributions and limitations.

2 RELATED WORK & RESEARCH GAP

Within the research area of attitudes towards nudging, two distinct groups can be identified: First, some studies investigate the attitude concerning nudges in multiple contexts. They often present descriptions of several nudges for different contexts so that the participants can assess them in comparison or give a more general statement [e.g. [12, 17]]. Second, some studies focus on one context to evaluate how the participants perceive nudging concerning that specific matter [e.g., [18, 18]].

2.1 Attitude Towards Nudging in Multiple-Context Studies

The majority of studies do not focus on a specific context but on general attitudes. Hagman et al. [12]] explored how American and Swedish citizens perceived different nudge-policies regarding organ donation and climate compensation among others. To explore individual differences, they conducted the Rational-Experiential Inventory scale (REI) and the Cultural Cognition Worldview Group scale. In an online survey they found that while the overall support for nudges was high in both countries, the general acceptance was higher in Sweden compared to the United States. Concerning influencing factors, they found that preferences in analytical thinking were not significant [12], while participants that scored high on the REI-rational scale perceived nudges as more intrusive. In a multi-country study, Reisch et al. [32] explored the attitude of Europeans towards nudges from different contexts on a larger scale. They focused on nudges in the contexts of healthy eating and organ donation among others. Analyzing cross-country differences, they found that nudges that have been adopted in democratic nations were supported in all listed countries. More recently, Peer et al. [29] investigated the attitude towards nudging of two distinct minority groups in Israel (Israeli Arabs and Ultra-Orthodox Jews). Similar to other studies, they focused on the contexts of healthy eating, organ donation, privacy settings on social networks, and smoking among others. They stress the importance of attitudes of minorities or other groups within a country towards nudging, which are largely overlooked by national and cross-national studies. They found that nudges were less supported when they were not consistent with a minority group's social norms [29].

2.2 Attitude Towards Nudging in Context-Specific Studies

Several studies have explored people's attitudes towards nudges for a healthier lifestyle. For instance, conducting in-depth semi-structured interviews in the UK, Junghans et al. [18], investigated how consumers approve of specific nudges, whether they believed in their effectiveness and whether who designed those nudges mattered. The authors found that in the context of health, most consumers approved of nudging, when they were beneficial to individuals and society and the targeted behavior was transparent [18]. Diepeveen et al. [7] conducted a systematic literature review on studies exploring the attitude in Europe, North America, Australia and New Zealand towards interventions to change tobacco and alcohol use, diet, and physical activity. They found that the public acceptability of interventions in the health sector is greatest for the least intrusive nudges [7]. Evers et al. [10] investigated whether citizens from different European countries approved of nudges for healthy eating. Despite cross-country differences, they further explored if characteristics such as gender, age or Body Mass Index and the level of intrusiveness of the nudges were influencing factors on the attitude. They found that women were more likely than men to approve of nudges in eating behavior. Again, less intrusive nudges had generally higher approval rates than intrusive nudges.

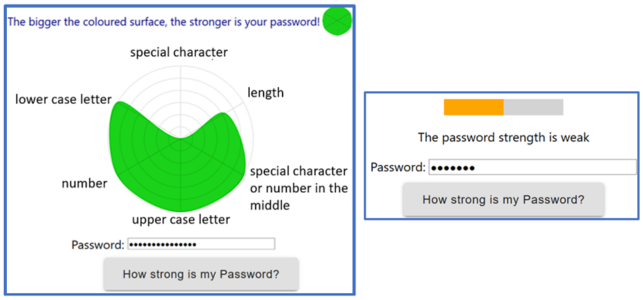
2.3 Research Gap

While there is an upcoming trend of nudges in privacy and security, little has been explored about the public attitude. Dogruel et al. [8] compared the attitude towards policy interventions in information privacy between the United States and Germany. They found that privacy nudges were generally supported and nudges for education and information were preferred [8]. Although nudges in the context of cybersecurity are a growing research field [2], to the best of our knowledge there is no study that explicitly explores the attitude towards nudging within that context. Several studies have designed nudges for privacy and evaluated their effectiveness (e.g. [1, 3, 6, 16, 21, 23, 25]). Other studies have explored the effectiveness of nudges in cybersecurity (e.g. [5, 14, 24, 26, 28, 31, 42, 43]). For instance, Zimmermann and Renaud [44] evaluated nudges and hybrid nudges including information provision for different contexts in cybersecurity (e.g., password creation and choice of public WiFi). They found that for some contexts hybrid nudges were even more effective than a simple nudge, complementing a previous study on hybrid nudges [35]. However in other cases, nudges in cybersecurity are often not as effective as desired, because they are mostly designed for the average user, showing one-size-fits-all nudges [9, 19] and neglecting public attitude towards nudging in the design process, even though nudging *"strongly relies on voluntary compliance [and] public attitude towards specific nudges"* [29].

Personalization is an upcoming trend (e.g. [5, 9, 20, 28, 33, 41]) which can be facilitated by exploring the attitude of people towards nudging in specific contexts. While people's attitude have already been addressed in other contexts on a wider scale (e.g. [8, 10, 12, 17, 18, 32, 39]), to the best of our knowledge, studies investigating the attitude towards nudging in cybersecurity are largely missing. We suggest that it remains important to expand knowledge on this matter, identifying both a general trend on people's attitude for that specific context, and differences between people's characteristics. We focused on the attitude of a representative sample from Germany to provide an opportunity for cross-country comparability in future studies.

3 APPROACH

To give an overview of the attitudes of the German population towards nudging in cybersecurity, we conducted a representative


The bigger the coloured surface, the stronger is your password!

Password: •••••••••••••••

The password strength is weak

Password: •••••••
special character
lower case letter
length
number
special character or number in the middle
upper case letter
How strong is my Password?
How strong is my Password?

Figure 1: Radar chart (left) and password meter (right) as priming conditions. (own figure)

survey in Germany and investigated a general tendency as well as differences between demographic subgroups and the effect of different priming scenarios.

3.1 Survey Design

We conducted a representative online survey with 1,012 participants (after data cleansing) from the German adult population (18 to 74 years) in July 2019, using the panel provider *Respondi*. Each participant was paid a small allowance (€1). To ensure good quality answers, we included multiple attention check questions (e.g. *"Please select answer option number three."*) and excluded 92 participants that did not answer them correctly. In this work, we particularly investigate four survey questions. The first question aims at gaining insights into who had already consciously noticed nudges online (*yes, no, no answer*). In the second question, we asked in five items how helpful, dangerous, necessary, patronizing or superfluous our participants assessed nudging in cybersecurity on a Likert scale from 1 to 5. To get more specific information, we further asked in question three on a five-step Likert scale how useful nudging in cybersecurity was assessed in eight concrete contexts (see section 4.2). Since some participants might not have enough knowledge of specific contexts to answer the question reasonably, answering those items was optional. To gain deeper inductive information, with question four we included an optional free-text question, asking more openly about the attitude towards nudging in cybersecurity and potential risks.

To investigate potential influencing factors, we included two psychometric scales: the *General Decision Making Style scale* (GDMS) with two subscales: *rational* (making decisions in a logical and systematic way) and *dependent* (rarely making important decisions without consulting other people) and the *Rational-Experiential Inventory* (REI) with two subscales: *REI-RA: rational ability* (ability to think logically and analytically) and REI-RE: *rational engagement* (reliance on and enjoyment of thinking in an analytical, logical manner) [27, 37]. Both psychometric scales are measured on a scale from 1 to 5. While the GDMS scale measures how individuals make decisions, the REI measures preferences for information-processing. Particularly the REI was already successfully used by Peer et al. [29] to personalize nudges and by Hagman et al. [12] to identify influencing factors on the attitudes towards nudges. We intend to investigate if they also influence attitudes towards nudging in the specific cybersecurity context.

While all participants were presented with identical definition and descriptive examples of nudging before asking our survey questions (see A.3), there were three distinct settings of additional priming (see Figure 1). One-third of our participants had interacted with a common password meter as a nudge for password strength before answering the survey questions, another third had interacted with a radar chart visualization of password strength as a nudge [15] and the last third was not presented with any interactive nudge beforehand. Hence, in our evaluation we further investigated if those varied primings had an effect on the attitude towards nudging in cybersecurity. The sample sizes between our three groups slightly differ as participants were excluded that did not pass the quality check questions.

While we used password nudges that encourage complexity, it is important to acknowledge that recommending complex passwords has been ruled out due to usability conflicts [11]. However, state-of-the-art password nudges still use disaggregated information on what to do to strengthen a password [42] using complexity recommendations and some studies argue that focusing on password length alone does not always result in better results as many users still tend to prefer shorter passwords [15]. Hence, for our evaluation we decided to include a nudge that encourages complexity as well.

3.2 Characteristics of Survey Participants

After data cleansing, 1,012 participants out of 1,104 were included for the analysis of the single and multiple-choice questions. For the free-text question, we performed an additional data cleansing and included a total of 489 participants. Our survey on the attitude of German citizens towards nudging in cybersecurity is representative for the German population in all groups regarding gender, age from 18 to 74, education and income. To analyze potential group differences, we formed clusters for age (18-29; 30-39; 40-49; 50-59; 60-74 years) and income (<€2,000; €2,000-€4,000; >€4,000). We also asked participants to select their highest level of education from three groups (without a school diploma; certificate of secondary education ("Hauptschulabschluss"), general certificate of secondary education ("mittlere Reife"), qualification for university entrance ("Abitur"); university degree). Regarding geographical spread, our sample is widely and approximately proportionally distributed across all 16 German federal states.

3.3 Analysis

We used *SPSS* and *R* for data preparation and statistical analysis and *Tableau* to create data figures. In a first step, we calculated the basic frequencies, including all demographic information. To verify the representativeness of our sample, we determined significant differences in gender, age, education, income, and federal states applying the χ^2-test of independence. For our survey questions that were answered on a Likert-scale, we determined main effects of group differences performing a multivariate analysis of variance (*MANOVA*). As dependent variables we included the five items on general attitudes as well as the eight items on context-specific attitudes.

We were interested in the following independent variables: priming condition (interaction with nudge), age, gender, education as well as decision-making and information-processing styles. Before performing the *MANOVA*, we tested for homogeneity of variance as necessary condition, using the *Levene's test.* As the test was significant for some dependent variables, we adjusted the respective data with a *Box-Cox Power-transformation.* To identify which mean values were responsible for significant *MANOVA* results, we subsequently performed post-hoc tests. Therefore, we used the *Tukey's HSD*-test. We set the significance level to $\alpha = 0.05$. To counteract the problem of multiple comparisons we applied a Bonferroni-correction of the p-values.

While there were 1,012 valid answers to the Likert scale questions, we excluded 523 participants from the optional free-text question that decided not to answer it or explicitly stated to be too undecided to give a specific input. The remaining 489 textual answers to our open question were evaluated in detail performing a qualitative content analysis. Hence, we deductively assigned each answer to a cluster (rating nudges as useful, undecided and thoroughly evaluated answers, rating nudges as inappropriate, comments on potential risks) by thoroughly analyzing the answers while looking for keywords (e.g. "dangerous"). Clusters were assigned in a two-step approach where answers were first grouped roughly into unambiguously positive or negative contents as well as contents that needed a more intensive reflection before decision. Afterwards, the answers were assigned to one of the four final clusters while especially reflecting on the initially ambiguous contents. Clustering was conducted independently by two people with *RQDA* and the inter-coder reliability was calculated, resulting in a substantial level (Cohen's kappa coefficient of $\kappa = 0.76$). On the basis of the assigned clusters, we later determined significant differences regarding specific participant characteristics such as demographics.

4 EMPIRICAL RESULTS

We present the findings of our representative online survey, by starting with the general attitude towards nudging in cybersecurity. Afterwards, we suggest our results regarding people's attitudes in more specific scenarios within the context of cybersecurity. Further, we will give an overview of effects of priming and user characteristics on the attitude in subsection 4.3.

4.1 General Attitude Towards Nudging in Cybersecurity

Aiming to contextualize our findings, we first asked our participants if they ever noticed nudges online. We found that the majority (72%) stated to not have noticed them, while 21% noticed nudges online and 7% did not make a statement.

We further asked if it was important to our participants to realize when someone tried to nudge them online. 69% agreed it was important to them. To get a better understanding of the general attitude, we first asked our participants on a Likert scale from 1 to 5, how helpful, dangerous, necessary, patronizing, or superfluous they perceived nudging in cybersecurity. You can see an overview of the results in Figure 2. Further we need to consider that two-third of the participants were assigned to a priming condition before answering the survey questions which slightly influenced the general attitude towards nudging for the better, unconditionally whether the participants interacted with the password meter or the radar chart. For instance, they were slightly less likely to agree with nudging in cybersecurity being dangerous ($M_{nudge} = 2.24, SD_{nudge} = 1.0, M_{none} = 2.73, SD_{none} = 1.1; F(1, 769) = 48.41, p < .0005; d = 0.25$).

We found that many participants assessed nudging in cybersecurity in a positive way. For instance, 64% (priming: 68%) agreed that it was a helpful instrument. Further, 38% (priming: 42%) stated to agree that nudging in cybersecurity was necessary. However, many (42%) were undecided concerning this matter and 20% disagreed (priming: 41%, 17%). Correspondingly, 57% (priming: 62%) disagreed with nudging in cybersecurity being superfluous. To gain a general insight into the perception of possible risks, we asked our participants how dangerous they assessed nudging in cybersecurity. 57% stated to not rate it as a dangerous instrument while 14% assessed it as dangerous (priming: 64%, 10%). As avoiding reactance is an important aim of nudging, we asked how patronizing our participants rated nudging in cybersecurity. 48% stated to disagree with it being patronizing while 30% were undecided and 21% agreed with nudging in cybersecurity being patronizing (priming: 52%, 31%, 17%).

While our Likert scale questions aimed at gaining a quantitative insight into the general attitude towards nudging in cybersecurity, we decided to include an optional question in free-text format for deeper inductive information. Hence, we more openly asked our participants if they considered nudges to be a sensible way to steer online behavior in a secure direction or if they saw any risks. In a deductive approach, two researchers independently assigned each answer to one of four clusters using RQDA. As the reliability was sufficient, we report the mean values.

Rating Nudges as Useful. We found that 56% explicitly made a positive statement on nudging in cybersecurity. Among the most frequently mentioned benefits were paying more attention to online security, support for unaware users, protection from certain risks and preservation of freedom of choice. For instance, one participant stated: *"I see it as a useful method. The freedom of choice remains, as the hint can be ignored"* (P253). Another participant wrote: *"Yes, a bit of Internet education does not hurt as long as you can decide for yourself"* (P309). Further, P301 stated: *"Yes because many are very careless with their data and information. A hint in the right direction would be just right".* Others only stated they found nudging in cybersecurity a sensible instrument without giving any reasons (e.g. P293: *"Yes, it is useful"*).

Undecided and Thoroughly Evaluated Answers. 15% intensively evaluated benefits and risks but were undecided whether nudging in cybersecurity was a sensible instrument or not. Several participants highlighted that they assessed nudging in cybersecurity as a useful instrument as long as nudges were not followed blindly (e.g. P113: *"Yes, I see risks, namely that the users rely blindly on the programs written by humans [...] without having to think about it themselves"*). Moreover, our participants highlighted the importance of nudges being transparent (e.g. P180: *"[...] The way*

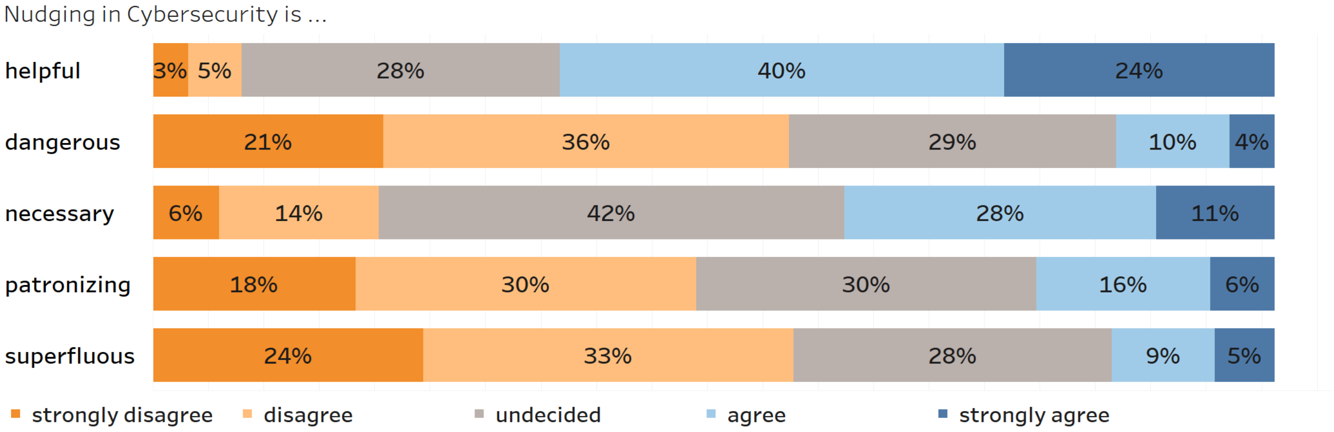


Figure 2: Attitudes towards nudging in cybersecurity without priming.

the nudges work and make their decisions must be completely transparent"). Further, several participants stated it was important that nudges came from a trustworthy source (e.g. P437: *"As long as the creator of the nudges is morally sound, I see it as a useful method [...]"*). Some participants stated that nudges should appear only occasionally to prevent feeling annoyed (e.g. P439: *"As long as it happens occasionally, it's okay and helpful. But I believe that the benefits quickly turn into the opposite and people feel that things are just annoying and [nudges are] overlooked"*). Hence, when looking deeper into the answers, we identified four main aspects that were mentioned as crucial for making nudges in cybersecurity a sensible instrument: Not following blindly, transparency of benefits and intentions, trustworthy sources, and only occasional appearance of nudges.

Rating Nudges as Inappropriate. Some participants (11%) explicitly disagreed with nudging being useful in that specific context. For instance, one participant stated: *"Actually, I do not find it useful. I find it patronizing"* (P15). Another participant stated: *"No, not really. I find it annoying at a certain point"* (P72). Similarly, P122 stated: *"No real risk, but annoying. I do not like, for example, to be told how to choose my password. I know how to generate an (allegedly) strong password but I think that it is weaker than a simple one that I can remember without writing it down. That's why I find nudging more harmful"*. More critically, P11 wrote: *"In the end, it only serves to spy on personal data. No normally, rationally thinking person needs that"*. Furthermore, P20 wrote: *"It is a deliberate and intended manipulation of the Internet user, which I consider very dangerous. A subconscious control of the user takes place"*. Others simply claimed they did not find nudging in cybersecurity useful without specifying a reason (e.g. P70: *"No, I do not think it is useful"*). When analyzing all answers in cluster C, we found that the most frequently given reasons for rating nudges in cybersecurity as inappropriate were: Being superfluous, being annoying and being manipulative. We discuss explicitly mentioned risks more precisely in the following cluster.

Comments on Potential Risks. Others (17%) only named potential risks while not answering if they assessed nudging in cybersecurity as a useful instrument or not. When looking deeper into the given answers, we found that the most frequently named risks were *intentional misguidance / manipulation*, followed by *data exposure / data collection*. One participant wrote: *"I am not sure how far such nudges can be used to intercept data"* (P463). Four participants brought up the term "fake nudges" as a potential risk, which was used as a matching part to the commonly discussed term "fake news" (e.g. P217: *"I only see a risk in fake nudges"*). Further mentioned risks were hackers, paternalism, people are unlearning thinking, lack of independent control and fear of censorship. For instance, P113 stated: *"Yes, I see risks. Namely that the users rely blindly on the programs written by humans. They only serve the purpose of increasing their security without having to think about it themselves"*.

4.2 Context-Specific Attitude Towards Nudging in Cybersecurity

After gaining general insight into the attitude, we asked more specifically on a five-step Likert scale about how useful our participants assessed nudging in eight concrete contexts of cybersecurity that are not exhaustive but exemplary. Scenarios were chosen by looking for commonly implemented nudges in cybersecurity in scientific literature (e.g. [42] for password creation) and adding other, partly more generic scenarios for user-related cyber incidents (e.g. loss of data). Although we set the question as optional, for all items a minimum of 835 participants felt capable of answering. We included the following contexts and scenarios: (1) password creation for important accounts, (2) password creation for unimportant accounts, (3) management of cryptocurrencies, (4) reminders of backups regarding important data, (5) protection from loss of money, (6) protection from loss of data, (7) prevention from sharing private data with strangers and (8) prevention from risky behavior on the Internet.

For all investigated contexts, many participants assessed nudging as a useful instrument. The interaction with one of the nudges had a priming effect only for password creation ($M_{nudge} = 4.21, SD_{nudge} = 1.0, M_{none} = 3.85, SD_{none} = 1.2; F(1,769) = 22.83, p < .0005; d = 0.17$). In the context of *password creation*, 73% agreed with nudging being useful regarding important accounts while 19% were undecided and 8% disagreed (N=976; priming: 76%, 16%, 5%). For unimportant accounts, still 41% (priming: 44%) rated nudges as

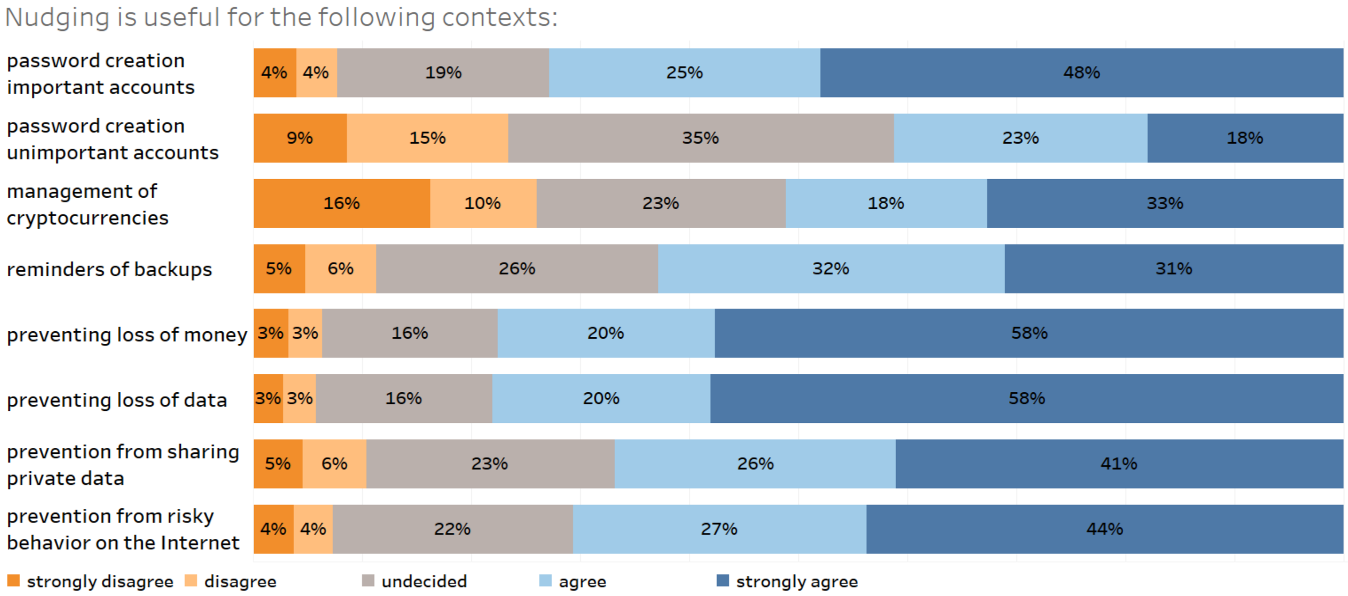


Figure 3: Context-specific attitudes towards nudging in cybersecurity.

useful (N=978). Furthermore, in the context of *cryptocurrencies*, 51% agreed with nudging being useful (N=835). For *reminders of backups* regarding important data, a total of 63% agreed with nudges being useful (N=959). Moreover, we asked our participants if they assessed nudges as useful when they were protecting against loss of money or loss of data. For *loss of money*, 78% agreed with nudges being a useful instrument (N=950). Similarly, concerning *loss of data*, 78% agreed (N=949). Regarding the *prevention from sharing private data with strangers*, a total of 67% agreed with nudges being a useful instrument while 23% were undecided and 10% disagreed (N=960). More generally, we asked about nudges to *prevent from risky behavior on the Internet*. Here, 71% rated nudges as useful, 22% were undecided and 8% rated nudges as not useful (N=971). A visualization of the results is presented in Figure 3.

4.3 Effects of User Characteristics on Attitudes

We investigated if the attitude towards nudging was influenced by specific user characteristics. Hence, in the following, we will suggest our findings regarding effects of demographics and decision-making as well as information-processing styles. We tested for statistical significance applying a *MANOVA*. The overall model was significant for all tested dependent variables. Main effects of the investigated independent variables were mostly low to medium.

Demographics. To investigate if the attitude towards nudges in cybersecurity differed regarding demographic characteristics of our participants, we included demographic groups in the *MANOVA* as well. Concerning gender and education, we found no significant difference both for general attitudes and scenario-specific attitudes. Regarding age, there were no significant differences in general attitudes towards nudging in cybersecurity. However, the scenario-specific assessment of usefulness slightly differed for management of cryptocurrencies (F(4,769) = 3.24, p=.012; d=0.13) between the age groups. More specifically, the post-hoc tests reveal that younger participants tend to rate nudging in those contexts as more helpful than older participants.

Decision-Making and Information-Processing Styles. Similar to the work of Hagman et al. [12], we further investigated if individual differences in rational thinking and decision-making styles were an influencing factor on the attitude towards nudging in cybersecurity by conducting two subscales each of the *Rational-Experiential Inventory scale* (REI) and the *General Decision Making Style scale* (GDMS) [12, 27, 37]. We found no significant differences regarding general and scenario-specific attitudes towards nudges in cybersecurity between participants with a high score (from 3.0 to 5) and participants with a low score (from 1 to 2.9) on the rational ability subscale (REI-RA: ability to think logically and analytically). However, when comparing the results of the rational engagement subscale (REI-RE: reliance on and enjoyment of thinking in an analytical, logical manner), we found that participants with a low score rated nudging in cybersecurity slightly but significantly less necessary ($M_{high} = 3.42, SD_{high} = 1.1, M_{low} = 3.17, SD_{low} = 1.0; F(1,769) = 9.20, p = .003; d = 0.11$) than participants with a high score. When examining the results of the GDMS-subscales, we found that for both the general and the scenario-specific attitudes it made no significant difference if participants were scoring low (from 1 to 2.4) or high (from 2.5 to 5) on the rational-subscale (making decisions in a logical and systematic way). For the dependent-subscale (rarely making important decisions without consulting other people) however, we found slight differences regarding the attitudes. Participants with a high score rated nudging in cybersecurity as slightly more necessary than those with a low score ($M_{high} = 23.30, SD_{high} = 1.0, M_{low} = 3.02, SD_{low} = 1.1; F(1,769) = 12.21, p = .001; d = 0.13$).

5 DISCUSSION

Nudging has emerged to be a relevant research field in the context of cybersecurity to steer people's behavior in a more secure direction. While several works have already developed and evaluated different types of nudges for cybersecurity, they are often not as effective as desired. To gain deeper insights on requirements for successful nudging in cybersecurity, Peer et al. [29] suggest including knowledge about the public attitude in the design process for the specific context. As personalization is an emerging trend to make nudges more effective, exploring people's attitudes for a specific context and identifying differences between people's characteristics can facilitate that idea. In other contexts, such as health and privacy, attitudes towards nudging have already been investigated. Furthermore, multiple-context studies have explored general attitudes towards nudging for several scenarios. However, the context of cybersecurity has largely been excluded from those investigations. Hence, our scientific contribution is an initial exploration of general and scenario-specific attitudes towards nudging in cybersecurity through a representative survey in Germany while identifying differences for user characteristics and priming conditions.

To answer our first research question (*RQ1: How do people assess nudging in cybersecurity?*), our findings suggest a partially positive attitude of the German population. Similar to studies on the health and privacy contexts, *(1)* many agreed that nudging was a helpful instrument in cybersecurity. However *(2)*, many were also undecided if it was a necessary tool. When asking free-text questions, we had the opportunity to gain deeper insights into the participants' assessments. For instance, 52% made an explicitly positive statement on nudging in cybersecurity, while *(3)* frequently revealing benefits such as *paying more attention to online security, support for unaware users, protection from certain risks and preservation of freedom of choice. (4)* Interestingly, 69% agreed that it was important to them to realize when someone tried to nudge them online. We gained insights into requirements, both concerning end-users and designers, that make nudges a useful instrument in cybersecurity: *(5) not following blindly, transparency of benefits and intentions, trustworthy sources, and only occasional appearance of nudges.* The highlighted relevance of transparency corresponds to the ethical guidelines for nudging by Renaud et al. [34] who suggest that nudges should be transparent to the nudgees and *"should only be deployed when the benefit is clear"*. **Thus, we suggest focusing on transparent nudges for the context of cybersecurity where benefits are evident.**

Diving deeper into peoples' assessments, we evaluated sub-question *RQ1.1 (Do people see risks of nudging in cybersecurity?).* We found that *(6)* generally around half of the participants did not assess nudging in cybersecurity as dangerous, while however 21% agreed with nudging in cybersecurity being patronizing. Again, we gained deeper inductive insights by evaluating free-text formats. Our qualitative content analysis revealed that *(7)* 12% explicitly rated nudging in cybersecurity as inappropriate while most frequently giving reasons such as *being superfluous, being annoying, and being manipulative.* When asking more specific about potential risks *(8), intentional misguidance / manipulation, data exposure / data collection, hackers, paternalism, unlearning thinking, lack of independent control, and fear of censorship* were further mentioned. Interestingly, four participants brought up the term "fake nudges" in that context as a potential risk. **We suggest to exhaustively evaluate the potential risks when designing nudges in cybersecurity, aiming to address the concerns of end-users.**

We further investigated sub-question *RQ1.2. (Does the attitude differ concerning different scenarios?).* Here we found a widely consistent attitude across most addressed scenarios. For all investigated scenarios *(9)*, many assessed nudging as a useful instrument while revealing the largest approval for nudges to protect against loss of data. **We suggest to further extend the design of nudges to other scenarios in cybersecurity, such as protection against loss of data and money.**

For further insights we evaluated sub-question *RQ1.3. (Do user characteristics or priming conditions affect the attitude?).* We investigated if interacting with an exemplary nudge for stronger passwords affected the attitudes. We found that indeed *(10)* participants that beforehand interacted with an exemplary nudge were less likely to agree with nudging in cybersecurity being dangerous, patronizing or superfluous. While demographic characteristics had almost no effect on the attitudes, we found *(11)* that decision-making and information-processing styles were slightly affecting attitudes, too. People that do not rely on and do not enjoy thinking in an analytical way, assessed nudging in cybersecurity as slightly less necessary. Hence, consistently with the work of Hagman et al. [12], differences in the REI score did slightly affect attitudes towards nudging in cybersecurity. Furthermore, participants that tend to make important decisions consulting other people rated nudging in cybersecurity as slightly more necessary than participants. Hence, our findings suggest that decision-making as well as information processing styles make small but significant differences for attitudes towards nudging in cybersecurity. **To facilitate personalization, we suggest considering user characteristics for the design of nudges in cybersecurity where sensible. We however suggest to identify other psychometric scales that have a greater impact on attitudes.**

Our findings on *RQ1* reveal a partially positive attitude towards nudging in cybersecurity. However, we further found that people perceive a number of potential risks as well. Although the majority stated to have never noticed nudges for cybersecurity, it was striking that many were able to thoroughly think about potential benefits and risks which can partly be addressed by recommendations retrieved from our findings. As Peer et al. [28] have stated, the effectiveness of nudges *"strongly relies on voluntary compliance"* [and] *public attitude towards specific nudges can play an important role"'* [28].

Summarizing our previously demonstrated main findings on *RQ1*, we make several suggestions to address challenges and make nudges in that specific context more effective and to facilitate the emerging trend of personalization (see Table 1), answering our second research question *(RQ2: What are design implications for nudging in cybersecurity?).* Given the concern that users might rely blindly on the feedback of nudges when moving through the digital space (challenge 1), we consider it crucial to design nudges for cybersecurity that encourage individual users to keep thinking for themselves while being assisted by nudges. Similarly, we found that making transparent that final decisions are up to the end-user may be an important step to avoid reactance and feelings of paternalism (challenge 2). Further, to design effective nudges, our findings reveal that considering users requirements and concerns is essential. We found that this applies to making benefits of nudges salient (challenge 3), taking fear of potential risks serious (challenge 4), and enabling users to understand if a nudge comes from a trustworthy source (challenge 5). While we have identified several design implications for nudges in cybersecurity, it is still important to not overuse nudges, even when designed adequately, and to implement nudges that do not significantly delay the respective process. Our findings reveal that users tend to feel annoyed when nudges are used when not necessary (challenge 6).

6 CONCLUSION & LIMITATIONS

Nudging in cybersecurity is perceived as helpful by many German citizens, however they see potential risks as well. We suggest to address the perceived concerns and to extend research on how far those fears pose a realistic threat. The majority states to have never consciously noticed nudges for cybersecurity. Interestingly, many participants were still able to evaluate possible benefits and disadvantages. However, our survey questions were based on a priming description of nudges that highlighted specific application scenarios (especially password creation) more than others. Hence, we suggest gaining richer insights into the attitudes based on different scenarios to enhance a vivid imagination of benefits and risks, preferably in realistic field study. We propose that a comprehensive knowledge on people's attitudes is a first step to enhance effectiveness of nudges in cybersecurity as it facilitates personalization and helps to address concerns adequately.

While our work is an initial contribution, it also has its limitations: (1) The results were acquired using a survey, which is a method prone to social desirability biases and relies on self report. While it is a challenge to measure attitudes indirectly, we suggest utilizing complementing techniques of data collection (e.g., thinking-aloud studies) to find more reliable results. (2) Also, it is important to consider that we used a selection of priming conditions as exemplary password nudges for comparison with a control group without a nudge, other than an exhausting selection of nudges of all inquired contexts. Of course, different types of nudges (e.g., fear appeals) and priming nudges for other contexts than password creation may result in different context-related attitudes. Also, our experiment was conducted using a web browser on a PC and may differ when displaying the selected nudges e.g. on a smartphone or with different size, timing and frequency. Hence, we suggest taking a thorough look at a more exhaustive selection of priming conditions in future studies. (3) Although the sample was representative concerning several characteristics, the method implies the risk of participants being more technophile than the average internet user. (4) Our survey questions were not based on a standardized test; hence, other methods need to confirm that we measured attitudes in an adequate way. (5) Furthermore, many differences cannot be considered strong. Thus, they reveal existing tendencies other than game-changing influences. Our work provides an opportunity for cross-country comparability in future studies which may contribute to a more accurate understanding of the perception of nudging as an instrument in cybersecurity.

ACKNOWLEDGMENTS

This research work has been funded by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE and by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – SFB 1119 (CROSSING) – 236615297.

REFERENCES

[1] Alessandro Acquisti. 2009. Nudging privacy: The behavioral economics of personal information. *IEEE security & privacy* 7, 6 (2009), 82–85.

[2] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. 2017. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)* 50, 3 (2017), 1–41.

[3] Rebecca Balebako and Lorrie Cranor. 2014. Improving app privacy: Nudging app developers to protect user privacy. *IEEE Security & Privacy* 12, 4 (2014), 55–58.

[4] Tom Biselli and Christian Reuter. 2021. On the Relationship between IT Privacy and Security Behavior : A Survey among German Private Users. *16th International Conference on Wirtschaftsinformatik* March (2021), 1–17.

[5] Debora Briggs, Lynne Jeske, Pam Coventry, and Aad van Moorsel. 2014. Nudging whom how: IT proficiency, impulse control and secure behaviour. *Networks* 49 (2014), 18.

[6] Eun Kyoung Choe, Jaeyeon Jung, Bongshin Lee, and Kristie Fisher. 2013. Nudging people away from privacy-invasive mobile apps through visual framing. In *IFIP Conference on Human-Computer Interaction*. Springer, 74–91.

[7] Stephanie Diepeveen, Tom Ling, Marc Suhrcke, Martin Roland, and Theresa M Marteau. 2013. Public acceptability of government intervention to change health-related behaviours: a systematic review and narrative synthesis. *BMC public health* 13, 1 (2013), 756.

[8] Leyla Dogruel. 2019. Privacy nudges as policy interventions: comparing US and German media users' evaluation of information privacy nudges. *Information, Communication & Society* 22, 8 (2019), 1080–1095.

[9] Serge Egelman and Eyal Peer. 2015. The myth of the average user: Improving privacy and security systems through individualization. In *Proceedings of the 2015 New Security Paradigms Workshop*. 16–28.

[10] Catharine Evers, David Marchiori, Astrid Junghans, J. Cremers, and Denise De Ridder. 2018. Citizen approval of nudging interventions promoting healthy eating: the role of intrusiveness and trustworthiness. *BMC public health* 18, 1 (2018), 1–10.

[11] Paul A. Grassi, James L. Fenton, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, Justin P. Richer, Naomi B. Lefkovitz, Jamie M. Danker, Yee-Yin Choong, Kristen K Greene Theofanos, and Mary F. 2017. *NIST Special Publication 800-63B, Digital Identity Guidelines*. Technical Report. NIST. https://pages.nist.gov/800-63-3/sp800-63b.html

[12] William Hagman, David Andersson, Daniel Västfjäll, and Gustav Tinghög. 2015. Public views on policies involving nudges. *Review of philosophy and psychology* 6, 3 (2015), 439–453.

[13] Andrew S. Hanks, David R. Just, Laura E. Smith, and Brian Wansink. 2012. Healthy convenience: Nudging students toward healthier choices in the lunchroom. *Journal of Public Health (United Kingdom)* 34, 3 (2012), 370–376. https://doi.org/10.1093/pubmed/fds003 https://academic.oup.com/jpubhealth/article/34/3/370/1559501.

[14] Katrin Hartwig, Atlas Englisch, Jan Pelle Thomson, and Christian Reuter. 2021. Finding Secret Treasure? Improving Memorized Secrets Through Gamification. In *The 2021 European Symposium on Usable Security (EuroUSEC)*. 2021.

[15] Katrin Hartwig and Christian Reuter. 2021. Nudging Users Towards Better Security Decisions in Password Creation Using Whitebox-based Multidimensional Visualizations. *Behaviour & Information Technology (BIT)* (2021). https://doi.org/10.1080/0144929X.2021.1876167

[16] Corey Brian Jackson and Yang Wang. 2018. Addressing the Privacy Paradox through personalized privacy notifications. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies* 2, 2 (2018), 1–25.

[17] Janice Y. Jung and Barbara A. Mellers. 2016. American attitudes toward nudges. *Judgment & Decision Making* 11, 1 (2016).

[18] Astrid Junghans, Tracy Cheung, and Denise De Ridder. 2015. Under consumers' scrutiny-an investigation into consumers' attitudes and concerns about nudging in the realm of health behavior. *BMC public health* 15, 1 (2015), 336.

[19] Shipi Kankane, Carlina DiRusso, and Christen Buckley. 2018. Can We Nudge Users Toward Better Password Management? An Initial Study. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–6.

[20] Bart P. Knijnenburg. 2017. Privacy? I can't even! Making a case for user-tailored privacy. *IEEE Security & Privacy* 15, 4 (2017), 62–67.

Table 1: Design implications for nudging in cybersecurity.

Challenges	*Design Implication*
Challenge 1: Unlearning thinking	Enabling and encouraging the individual user to keep thinking for himself while being assisted by the nudge instead of relying blindly.
Challenge 2: Reactance	Make transparent that the final decisions are up to the end-user to avoid feeling patronized.
Challenge 3: Benefits are not clear	Enabling the user to understand the benefits that result from a specific nudge.
Challenge 4: Fear of potential risks	Make transparent to the nudgee how a nudge works at any time. Address concerns in the nudge design e.g. by transparently showing what data is being used. Evaluate potential risks iteratively during nudge design.
Challenge 5: Trust	Enable users to understand if a nudge comes from a trustworthy source.
Challenge 6: Annoyance	Nudge only when necessary and without delaying the respective process to prevent users from feeling annoyed.

[21] Hye-Chung Kum, Eric D. Ragan, Gurudev Ilangovan, Mahin Ramezani, Qinbo Li, and Cason Schmit. 2019. Enhancing privacy through an interactive on-demand incremental information disclosure interface: applying privacy-by-design to record linkage. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*.

[22] Ulrike Lechner. 2019. Future security: Processes or properties?—Research directions in cybersecurity. In *Models, Mindsets, Meta: The What, the How, and the Why Not?* Springer, 235–246.

[23] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun Aerin Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. 2016. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. 27–41.

[24] Nathan Malkin. 2013. Waiting Makes the Heart Grow Fonder and the Password Grow Stronger. In *Symposium on Usable Privacy and Security (SOUPS)-Posters. USENIX Association, Newcastle, UK*. 1–2.

[25] Nicholas Micallef, Mike Just, Lynne Baillie, and Maher Alharby. 2017. Stop annoying me! an empirical investigation of the usability of app privacy notifications. In *Proceedings of the 29th Australian Conference on Computer-Human Interaction*. 371–375.

[26] James Nicholson, Lynne Coventry, and Pam Briggs. 2017. Can we fight social engineering attacks by social means? Assessing social salience as a means to improve phish detection. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 285–298.

[27] Rosemary Pacini and Seymour Epstein. 1999. The relation of rational and experiential information processing styles to personality, basic beliefs, and the ratio-bias phenomenon. *Journal of personality and social psychology* 76, 6 (1999), 972.

[28] Eyal Peer, Serge Egelman, Marian Harbach, Nathan Malkin, Arunesh Mathur, and Alisa Frik. 2019. Nudge me right: Personalizing online nudges to people's decision-making styles. *Available at SSRN 3324907* (2019).

[29] Eyal Pe'er, Yuval Feldman, Eyal Gamliel, Limor Sahar, Ariel Tikotsky, Nurit Hod, and Hilla Schupak. 2019. Do minorities like nudges? The role of group norms in attitudes towards behavioral policy. *Judgment and Decision Making* 14, 1 (2019), 40.

[30] Muireann Quigley. 2013. Nudging for health: On public policy and designing choice architecture. *Medical Law Review* 21, 4 (2013), 588–621. https://doi.org/10.1093/medlaw/fwt022

[31] George Raptis, Christina Katsini, Andrew Jian-Lan Cen, Nalin Asanka Gamagedara Arachchilage, and Lennart Nacke. 2021. Better, Funner, Stronger: A Gameful Approach to Nudge People into Making Less Predictable Graphical Password Choices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–17.

[32] Lucia A. Reisch and Cass R. Sunstein. 2016. Do Europeans like nudges? *Judgment and Decision making* 11, 4 (2016), 310–325.

[33] Karen Renaud, Verena Zimmerman, Joseph Maguire, and Steve Draper. 2017. Lessons learned from evaluating eight password nudges in the wild. In *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2017)*. 25–37.

[34] Karen Renaud and Verena Zimmermann. 2018. Ethical guidelines for nudging in information security & privacy. *International Journal of Human-Computer Studies* 120 (2018), 22–35.

[35] Karen Renaud and Verena Zimmermann. 2019. Nudging folks towards stronger password choices: providing certainty is the key. *Behavioural Public Policy* 3, 2 (2019), 228–258.

[36] M. Angela Sasse and Ivan Flechais. 2005. Usable security: Why do we need it? How do we get it? O'Reilly.

[37] Susanne G Scott and Reginald A Bruce. 1995. Decision-making style: The development and assessment of a new measure. *Educational and psychological measurement* 55, 5 (1995), 818–831.

[38] 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)*. 379–415.

[39] Cass R. Sunstein, Lucia A. Reisch, and Julius Rauber. 2017. Behavioral insights all over the world? Public attitudes toward nudging in a multi-country study. *Public Attitudes Toward Nudging in a Multi-Country Study (February 21, 2017)* (2017).

[40] Richard H. Thaler and Cass R. Sunstein. [n.d.]. Nudge: Improving decisions about health, wealth, and happiness.

[41] Iis Tussyadiah, Shujun Li, and Graham Miller. 2019. Privacy protection in tourism: Where we are and where we should be heading for. In *Information and Communication Technologies in Tourism 2019*. Springer, 278–290.

[42] Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, et al. 2017. Design and evaluation of a data-driven password meter. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 3775–3786.

[43] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, et al. 2012. How does your password measure up? the effect of strength meters on password creation. In *Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)*. 65–80.

[44] Verena Zimmermann and Karen Renaud. 2021. The nudge puzzle: matching nudge interventions to cybersecurity decisions. *ACM Transactions on Computer-Human Interaction (TOCHI)* 28, 1 (2021), 1–45.

A APPENDIX

A.1 Demographic Items

- What gender do you identify with?
  - female
  - male
  - other
- What is your age (in years)?
  - younger than 18
  - 18 - 29
  - 30 - 39
  - 40 - 49
  - 50 - 59
  - 60 or older
- In which federal state do you currently live? [choose from list of all German federal states]
- Please indicate your highest level of education.

  - without a school diploma / certificate of secondary education
  - general certificate of secondary education
  - qualification for university entrance / university degree
- What is your monthly household income?
  - under 2,000
  - €2,000 to €4,000
  - above €4,000
- I regularly interact with IT systems in my everyday life. [Likert scale from 1 (strongly disagree) to 5 (strongly agree)]

A.2 Psychometric Tests

- General Decision Making Style (subscales R = *rational* and D = *dependent*) [37] [scoring: 1 (strongly disagree) to 5 (strongly agree)]
  - I rarely make important decisions without consulting other people. (D)
  - I double-check my information sources to be sure I have the right facts before making decisions. (R)
  - I use the advice of other people in making my important decisions. (D)
  - I make decisions in a logical and systematic way. (R)
  - I like to have someone to steer me in the right direction when I am faced with important decisions. (D)
  - My decision making requires careful thought. (R)
  - When making a decision, I consider various options in terms of a specific goal. (R)
  - I often need the assistance of other people when making important decision. (D)
  - If I have the support of others, it is easier for me to make important decisions. (D)
  - I make decisions in a logical and systematic way. (R)
- Rational-Experiential Inventory (subscales RA = *rational ability* and RE = *rational engagement* [27] [scoring: 1 (strongly disagree) to 5 (strongly agree)])
  - I try to avoid situations that require thinking in a depth about something. (RE)
  - I'm not that good at figuring out complicated problems. (RA)
  - I enjoy intellectual challenges. (RE)
  - I am not very good at solving problems that require careful logical analysis. (RA)
  - I don't like to have to do a lot of thinking. (RE)
  - I enjoy solving problems that require hard thinking. (RE)
  - Thinking is not my idea of an enjoyable activity. (RE)
  - I am not a very analytical thinker. (RA)
  - Reasoning things out carefully is not one of my strong points. (RA)
  - I prefer complex problems to simple problems. (RE)
  - Thinking hard and for a long time about something gives me little satisfaction. (RE)
  - I don't reason well under pressure. (RA)
  - I am much better at figuring things out logically than most people. (RA)
  - I have a logical mind. (RA)
  - I enjoy thinking in abstract terms. (RE)
  - I have no problem thinking things through carefully. (RA)
  - Using logic usually works well for me in figuring out problems in my life. (RA)
  - Knowing the answer without having to understand the reasoning behind it is good enough for me. (RE)
  - I usually have clear, explainable reasons for my decisions. (RA)
  - Learning new ways to think would be very appealing to me. (RE)

A.3 Items on Attitudes

A nudge is an instrument to alter people's behavior. The individual is gently steered in a specific direction without forbidding any alternative options. In the context of health, an exemplary nudge can be arranging fruits and vegetables in the school cafeteria at eye level. Thus, the students are animated to choose healthier food.

Also, in the context of cybersecurity nudges can be applied to steer people's behavior in a more secure direction. Nudges can, for instance, remind of backups of important data, warn against phishing mails or indicate when a password is not strong enough. That can, for example, take place using images, slogans or colors among other.

Please indicate to what extent you agree with the following statements. There is no right or wrong, we are only interested in your opinion.

- Nudging in cybersecurity is ... [scoring: 1 (strongly disagree) to 5 (strongly agree)]
  - helpful
  - dangerous
  - necessary
  - patronizing
  - superfluous
- It is important to me to understand how the assessment of the strength of my password was calculated online. [scoring: 1 (strongly disagree) to 5 (strongly agree)]
- It is important to me to realize when someone tries to nudge me online. [scoring: 1 (strongly disagree) to 5 (strongly agree)]
- Nudging is useful for the following contexts: [scoring: 1 (strongly disagree) to 5 (strongly agree), no answer]
  - password creation for important accounts
  - password creation for unimportant accounts
  - management of cryptocurrencies
  - reminders of backups regarding important data
  - protection from loss of money
  - protection from loss of data
  - prevention from sharing private data with strangers
  - prevention from risky behavior on the Internet
- Do you consider nudges to be a sensible way to steer online behavior in a secure direction or do you see any risks? [free-text format]
- Have you ever noticed nudges online? [yes, no, no answer]