Counteracting manipulative cookie designs – The effect of nudges on website users' tendencies to share private online data.

Fabienne Großart
Department of Conflict, Risk and Safety
University of Twente

Dr. I. van Sintemaartensdijk (1st Supervisor)
Dr. S.J. Watson (2nd Supervisor)

29th of June 2022

Table of Contents

Abstract

To our best knowledge, this study is the first to experimentally examine the effect of nudges on cookie acceptance behaviour. In particular, the present study uses type 2 nudges, which trigger reflective thinking and conscious cognitive processing. By identifying underlying human factors influencing cookie message decisions, this study aims to better protect users' data privacy. In total, 100 participants were randomly assigned to either a transparent or a non-transparent type 2 nudge and performed a specific task on two self-created websites. Afterwards, respondents answered questionnaires regarding their personality, security behaviour intentions, risk-taking and self-efficacy. Two main findings were observed in relation to the use of nudges. The use of nudges leads to a decrease in users' cookie acceptance rates, while the level of transparency of the nudge had no effect on cookie acceptance behaviour. In terms of individual characteristics, the study found that a) the personality trait openness supported safer cookie acceptance behaviour, b) security behaviour intentions had a positive influence on cookie acceptance behaviour, and c) the control measures risk-taking and self-efficacy showed no influence. Findings from this study show that type 2 nudges are an effective tool in promoting safer cookie acceptance behaviour. While the degree of transparency showed no influence, this research encourages the importance of investigating other design choices in more detail. Furthermore, the present study highlights the importance of individual characteristics underlying users' cookie acceptance behaviour. Extended insights into individual characteristics and their influence would enhance our understanding of cookie acceptance decisions as well as enable choice architects to identify both facilitating and inhibiting factors to make nudging interventions more effective.

Introduction

Relevance of present study

As digital technologies become increasingly integrated into people's daily lives, the issue of cybersecurity is a central topic of public debate. In particular, the COVID-19 pandemic and its associated restrictions, such as social contact and distance limitations, caused a significant increase in cybercrime as the online environment became crucial for human communication (Zimmermann & Renaud, 2021). Although the rapid development of digital technologies offers many favourable opportunities, such as immense connectivity and economic growth, it also fosters the progress of cybercrime. Phishing, malicious codes, viruses and malware are among the most frequent forms of cybercrime. However new attack types, tools and techniques are constantly evolving (Bendovschi, 2015). In the past, research mainly investigated cybercrime from a technology-centric perspective, however recently it has become clear that human factors are a crucial element in preventing cybercrime (Pollini et al., 2021; Gerber et al., 2018). As a result, researchers have recently started to adopt a more holistic approach to cybercrime by considering technological factors as well as the cognitive and behavioural processes of users (Pollini et al., 2021; Back & LaPrade, 2019).

Due to the rise in internet usage, users make an increasing amount of personal data available online. This high availability of user data in the online environment greatly benefits companies and marketers, while users face an increasing risk of cybercrime (Bauer et al., 2021). In this regard, the European Union's General Data Protection Regulation (GDPR) came into effect in 2018, to protect users' private data (Coventry et al., 2016). The GDPR requires websites to explicitly ask for users' content via cookie banners before storing, processing or using personal user data (Bauer et al., 2021). A cookie is a small bit of data sent by a website, which is stored in a user's browser. The cookie stores limited information from a web browsing session that is transmitted back to the website each time the user returns in the future (Pollini et al., 2021). Although cookies are intended to help improve users' experiences, they raise several privacy concerns. Cookies themselves are not harmful, the privacy threat lies in several attributes of cookies, such as the ability to track users, their use by third-party websites, the concealment of cookies and their expiry date, which often reach long after the computers' expiry date (Acquisti et al., 2017). Particularly problematic is the fact that, apart from a few ground rules, there are no explicit regulations for the design of such cookie banners. As a result, websites choose cookie designs that stimulate high cookie acceptance rates (Bauer et al., 2021). Such designs rely on the manipulation of user decisions and exploit our human vulnerabilities by targeting specific heuristics and biases (Moustafa et al., 2021; Miyazaki, 2008). Bauer et al.

(2021) show that manipulations of cookie banners, such as inequalities in salience, size and framing of the accept and decline button, can even lead to an 85% increase in acceptance rates. Considering such high consent rates stemming from manipulative cookie designs, it is necessary to explore the reciprocal relationship between the disclosure of cookies and users' privacy behaviour becomes apparent (Acquisti et al., 2017). To better protect users' data privacy, an encompassing understanding of the human factors underlying this relationship is essential.

Human factors in cybersecurity and cookie acceptance

Previous research on human factors in cybersecurity has shown that humans themselves are often the biggest vulnerability in cybersecurity. The study conducted by Moustafa et al. (2021) predicts that about 95% of cyberattacks are due to human errors (Acquisti et al., 2017). Such high estimates highlight the importance of using cognitive psychology and behavioural science in cybersecurity research, especially its insights into human biases and heuristics. In particular, human biases cause an individual to take irrational actions or decisions, while heuristics are mental shortcuts that an individual uses to quickly reach a conclusion (McAlaney & Benson, 2020). While many companies already exploit such biases and heuristics for their advantage, security and software developers aiming to promote users' data privacy are lagging behind (Xu & Warkentin, 2020).

One phenomenon that psychological and behavioural based research often mentions, is the common discrepancy between people's intentions and their actual behaviour regarding cybersecurity (Moustafa et al., 2021). This discrepancy is called the privacy paradox and states that even though humans report high privacy concerns, they repeatedly behave in ways that clearly contradict their intentions (Furnell & Clarke, 2012). Connecting this to privacy related cookie banners, the privacy paradox illustrates a potential explanation for the phenomenon that people show high cookie acceptance rates, despite reporting immense privacy concerns. The Elaboration Likelihood Model (ELM) provides further insights into why people make contradictory decisions regarding online cookies (Cacioppo & Petty, 2020). Generally, two different routes of information processing are suggested by the ELM, namely the central route and the peripheral route. These two routes differ in the amount of cognitive effort applied and influence an individual's attitude as well as behaviour in distinct ways (Choi et al., 2018). While the central route is slow, deliberate and conscious, the peripheral route is fast, automatic and unconscious. According to Becker et al. (2019), the peripheral route of processing plays a major role regarding the privacy paradox in the online environment. Regarding cookie acceptance decisions, peripheral processing is characterized by simple heuristics, automatic intuition and less cognitive deliberation and can be considered to cause less secure cookie behaviour (Bauer et al., 2021). As a result, users develop privacy impeding mechanisms such as consent fatigue, causing them to simply accept cookies without reflecting upon them (Bauer et al., 2021). Hence, it can be argued that designing cookies in a way that appeals to the central route of elaboration could consequently promote more secure behaviour among users.

To activate the central route of processing, the various factors underlying the peripheral processing of a person's daily cookie acceptance choices need to be elaborated further. First of all, Miyazaki (2008) points out that humans display a decreased response to repeated stimulation, which is defined as habituation. Thus, considering the constant exposure to cookie messages and their similar design, it becomes apparent that individuals show less attentive behaviour towards this visual information and its meaning (Miyazaki, 2008). As a result, users are more likely to accept cookies immediately rather than consider them carefully. In this regard, choosing a more attention capturing and distinctive design for cookie messages illustrates one way to promote safer cookie acceptance behaviour (Bauer et al., 2021).

Furthermore, considering that security and privacy decisions are often complex and uncertain, a large number of cognitive resources are needed to process them (Xu & Warkentin, 2020). However, as individuals have only a limited number of cognitive resources available, this scarcity often impedes the extensive evaluation of all possible options and consequences of their cybersecurity behaviour. This psychological phenomenon is also called bounded rationality (Acquisti et al., 2017). In the face of bounded rationality, individuals tend to rely on their peripheral processing, using heuristics to simplify the decision-making process of complex privacy issues (Xu & Warkentin, 2020). According to Acquisti et al. (2017), two heuristics are particularly important in cybersecurity decisions. First, the representativeness heuristic leads an individual to estimate the likelihood of privacy invasions as low, since such invasions are not directly observable. Second, the availability heuristic alters an individual’s risk perceptions based on the recall of past risk experiences (Ting, n.d.). Consequently, individuals who have not experienced a cyberattack in the past are likely to show lower privacy concerns. Given that cookie induced cybersecurity threats are rather invisible than overt, people tend to accept cookies because their risk perception is altered by heuristics at play.

Concludingly, peripheral processing and its various underlying heuristics and biases better explain why people make contradictory security decisions in the online environment, especially regarding cookie decisions. Taking into account these often unconscious influences on an individual’s decision making, the necessity for interventions that promote safer user behaviour becomes apparent. Specifically, interventions are needed that make the decision-making process more conscious, for example by activating reflective thinking via the central route of processing. Thereby, manipulative elements, such as manipulative cookie banners, can be effectively counteracted and users' data privacy can be better protected.

With regards to such interventions, it is crucial to also take individual characteristics into account. In addition to the underlying cognitive processes, personality traits, attitudes and intentions also play a crucial role in an individual's decision-making process. According to Halevi et al. (2013), personality traits have a major impact on an individual's online behaviour, such as security awareness. While some personality traits, such as conscientiousness, have been shown to promote safer behaviour in the online environment, others, such as neuroticism, tend to impede safer behaviour (Coventry et al., 2016). One personality trait of particular interest is openness, as it is surrounded by generally mixed research findings (Gratian et al., 2018; Halevi et al., 2013). To better comprehend an individual's cybersecurity decision making, such as cookie acceptance decisions, it is crucial to gain clarity on the facilitating and inhibiting influence of an individual's personality. This will help to better promote user privacy and tailor interventions to specific personality traits.

Nudging

One form of intervention that has been shown to positively influence a wide range of cybersecurity behaviours is nudges. According to Tagliabue et al. (2019), nudges are behaviour modification tools that alter an individual's behaviour, by providing contextual features. More specifically, nudges are designed based on specific choice architectures, such as specific wording, that trigger automatic cognitive processes. This way, nudges aim to bridge the discrepancy between intention and behaviour that is often present in an individual's decision-making process (Moustafa et al., 2021). Essentially, nudges can be divided into two main types that trigger different cognitive processes: type 1 and type 2 nudges. Connecting to the ELM, type 1 nudges trigger the fast and automatic cognitive processes executed by the peripheral route, while type 2 nudges trigger the controlled and slow cognitive processes of the central route (Choi et al., 2018; Zimmermann & Renaud, 2021). In the last years, several studies investigated the influence of nudges on our cognitive processes active in cybersecurity related decisions. While some studies report a positive influence of nudges on users' privacy behaviour, others show insignificant or ineffective results (Acquisti et al., 2017; Caraban et al., 2019). However, several factors such as the privacy decision context, influences of individual differences and choice architectures have not yet been sufficiently researched, illustrating a potential cause for the mixed results regarding the effectiveness of nudges (Zimmermann & Renaud, 2021).

Despite the mixed results, many companies are already effectively using type 1 nudges to influence users' decision making in the company's interest (Xu & Warkentin, 2020). One example is the intended differences between the accept and decline button of cookie banners. While the accept button is often outstanding and attention capturing, the decline button is rather hidden and unobtrusive. Thereby, companies influence users' peripheral processing with the aim to achieve high cookie acceptance rates (Bauer et al., 2021). While companies benefit from these manipulations, users' data privacy is put at an increased risk. However, research shows that nudges can be likewise used to promote users' data privacy (Vaan Bavel et al., 2019). Here, the use of type 2 nudges is especially effective to counteract type 1 nudge manipulations. In particular, the use of type 2 nudges activates an individual's automatic cognitive processes that are influenced by type 1 nudges, and target reflective attention and thinking (Zimmermann & Renaud, 2021). The colourful feedback bar tested by Hansen and Jespersen (2013) illustrates only one example of the effective use of type 2 nudges in cybersecurity decisions. Based on the user's actual input, the feedback bar provides coloured feedback ranging from red, indicating a weak password, to green, representing a strong password, to nudge the user to choose a stronger password (Zimmermann & Renaud, 2021).

In addition to categorising nudges according to the way they are processed, they can also be differentiated according to their degree of transparency. Specifically, there are transparent and non-transparent nudges, which differ in the disclosure of their intentions. While a transparent nudge is implemented in such a way that both the intention and the intended behavioural change behind it can be recognised and expected, a non-transparent nudge is implemented in such a way that a person cannot see either the intention or the intended behaviour changes behind it (Hansen & Jespersen, 2013). While the typology of nudges has already received attention in research, the differences in transparency have not yet been sufficiently investigated. Although previous research reported concerns regarding the effectiveness of transparent nudges, the study conducted by Paunov et al. (2018) showed that full transparency can actually increase effectiveness (Wachner et al., 2020; Hansen & Jespersen, 2013). Specifically, Paunov et al. (2019) found that individuals showed increased policy compliance when exposed to a transparent nudge. Park and Blenkinsopp (2011) argue that this increase in compliance is due to the fact that individuals associate transparency with trustworthiness, which leads to more satisfaction and willingness to comply. Following Park and Blenkinsopp's (2011) reasoning, it can be argued that especially in the online environment, which is often characterized by opacity, a transparent nudge would be particularly effective as it would increase users' trustworthiness, leading to higher compliance with safe cybersecurity behaviour. Considering that cybersecurity threats caused by cookies are rather invisible than overt, the impact of a transparent nudge would be particularly strong. Therefore, research should follow the call for transparency in nudging interventions and further investigate the role of design choices, such as transparency, in cookie acceptance decisions.

Present study

Given the increasing threats to data privacy in the online context, this study aims to further examine the effectiveness of type 2 nudges in cookie acceptance behaviour. Generally, the present study has two main goals. The first goal is to establish the effect of nudges on users' cookie acceptance rate. Investigating this relationship benefits our understanding of how to promote safer cookie acceptance behaviour among users. This leads to the following hypothesis, *H_1: Website users exposed to a nudge will show a lower cookie acceptance rate compared to website users not exposed to a nudge.*

Besides testing the general influence of nudges on cookie acceptance behaviours, this research uses type 2 nudges, specifically one transparent and one non-transparent. Connecting this to the first assumption, it is hypothesised that *H_2: Website users exposed to a transparent nudge will show a lower cookie acceptance rate compared to users exposed to a non-transparent nudge.*

The second aim of this study is to examine the influence of individual differences on cookie acceptance behaviour. In particular, this study focuses on the personality trait openness to clarify the inconsistent line of research on whether openness promotes or inhibits safe behaviour in the online environment. Clarifying this relationship contributes to our understanding of how personality can promote or impede secure cookie acceptance behaviour. This leads to the third hypothesis, *H_3: Users reporting a higher score on openness will show a higher cookie acceptance rate compared to users reporting a low score on openness.*

Methods

Research design

An experimental between-within design was used for this research study. More specifically, a within-subject design was used, as all respondents were first exposed to a manipulative cookie message only and then to a manipulative cookie message in combination with a nudge. In addition, participants' a) security behaviour intention and b) actual security behaviour was measured both, before and after receiving a nudge as treatment. In addition, participants were assigned to one of the two nudge conditions using a between-subjects design. They received either a transparent nudge or a non-transparent nudge.

Participants

This research used convenience sampling and snowball sampling for recruitment. Participants were reached via social media platforms such as Instagram and Facebook, as well as via an internal university system called SONA. While some respondents took part in the study voluntarily, others received mandatory study points via the SONA system. Potential participants were identified based on two main inclusion criteria, namely a minimum age of 18 and having adequate English language skills. The exclusion criteria were straight-lining behaviour and not passing the attention check. This resulted in a final sample consisting of 100 participants. Regarding the socio-demographic characteristics, the sample consisted of 54 females and 46 males, aged from 18 to 56 with a mean age of 24 (*SD* = 7.5). Regarding participants' nationality, 78 were from Germany, 18 were from the Netherlands, and 4 indicated to have other nationalities. While 70 participants had a high school degree, 20 had a bachelor's degree and ten a master' degree. With regards to the employment status, 85 participants were students, twelve were employed full-time and three were employed part-time. All selected respondents were randomly assigned to one out of the two nudge conditions, they either received a transparent nudge or a non-transparent nudge. This left 54 participants for the transparent nudge condition and 46 participants for the non-transparent nudge condition. Regarding the main variables of interest, participants had a mean score of 3.6 (*SD* = .06) on openness, a mean score of 3.2 (*SD* = .05) for security behaviour intentions, a mean score of 3.4 (*SD* = .08) for risk-taking and a mean score of 3.4 (*SD* = .08) for general self-efficacy.

Materials

Websites

To measure the cookie acceptance behaviour of participants, two artificial websites were created with the online website builder "Wix" (*Log in | Wix*, n.d.). For both websites, an identical theme as well as structure was chosen, which allowed for later comparisons. As a general theme, both websites represented an online shop, selling educational and creative products, such as journals, notebooks, and desk accessories (Appendix A). Regarding the structure of the two websites, participants were able to navigate on the homepage, investigate the online shop including all products, and receive more information under the sections "About" and "Contact". In addition, a cookie message was displayed right at the beginning when entering the websites. The design of the cookie message was based on GDPR guidelines and additional manipulative aspects commonly used by real website operators (Appendix B; General Data Protection Regulation (GDPR) Compliance Guidelines, n.d.).

Nudges

In addition to the cookie message itself, a nudge was displayed on the second website parallelly with the cookie message. More specifically, this research used two different kinds of nudges, one transparent nudge design and one non-transparent nudge design (Appendix C). The design choices of the used nudges were mainly based on the stepwise approach conducted in the research by Meske and Amojo (2020). First of all, users were analysed and understood. In this step, it was found that users generally want to protect their privacy, but that different heuristics and biases often lead to contradictory behaviour. Second, the goal of digital nudging in this research was identified, namely to protect users' privacy by promoting safer cookie acceptance behaviour. Finally, the design of the digital nudges used in this research was identified.

More specifically, both nudges used in this research were so-called type 2 nudges, characterised by their influence on humans' reflective thinking. More specifically, the first nudge illustrated a transparent type 2 nudge, while the second illustrated a non-transparent type 2 nudge. In line with Meske's and Amojo's (2020) ethical guidelines for the construction of digital nudges, the transparent type 2 nudge was a) transparent, b) easy to resist and c) non-controlling (see Appendix C). The non-transparent type 2 nudge was a) consistent with the researcher's goal of protecting users' privacy and promoting safer cookie acceptance behaviour and b) does not entail any negative consequences for the users themselves (see Appendix C). In terms of their specific design, both nudges had similarities in shape, size and positioning. More specifically, both nudges were displayed as a red circle that rotated to attract users' attention. The nudges statement was displayed in black font in the middle of the red circle. In terms of positioning, both nudges were placed in the upper left corner of the cookie message. The main difference between the two nudges was their individual message. While the non-transparent nudge only stated, "Navigate safely", the transparent nudge stated, "Navigate safely. Your personal cybersecurity and privacy is at increased risk. You can easily minimise the risk by declining the use of cookies".

Questionnaires

HEXACO Personality Inventory – Revised (HEXACO-PI-R).

The HEXACO-PI-R was used to measure participants' personality traits (de Vries, 2013). Based on 24 items the scale assesses six personality dimensions, namely (a) Honesty-Humility (b)

Emotionality (c) Extraversion (d) Agreeableness (e) Conscientiousness and (f) Openness to Experience. Respondents have to answer questions such as “I have a lot of imagination.” and “I often do things without really thinking.”. Responses are reported on a 5-point Likert scale ranging from (1) Strongly disagree to (5) Strongly agree. This study mainly focuses on the openness subscale of the HEXACO-PI-R (*M* = 3.7, *SD* = 0.6, *a* = 0.51).

Security Behaviour Intention Scale (SeBIS).

The SeBIS was used to measure participants’ computer security attitudes (Egelman & Peer, 2015). Based on 16 items, the scale assesses end-users’ security attitudes regarding four different security domains (a) Device Securement (b) Password Generation (c) Proactive Awareness and (d) Updating. Items such as “I use a password/passcode to unlock my mobile phone.” and “I submit information to websites without first verifying that it will be sent securely.” are answered on a 5-point Likert scale ranging from (1) Never to (5) Always (*M* = 3.10, *SD* = 0.44, *a* = 0.78).

Domain-Specific Risk-Taking (DOSPERT) scale.

The DOSPERT scale was used to measure participants’ behavioural intentions of engaging in risky behaviours regarding five domains, namely ethical, financial, health/safety, and social and recreational risks (Blais & Weber, 2006). Respondents have to indicate the likelihood of engaging in certain activities or behaviours described in 30 different items, including statements like “Going camping in the wildness.” and “Driving a car without wearing a seat belt.”. Responses are reported on a 7-point Likert scale, ranging from (1) Extremely unlikely to (7) Extremely likely (*M* = 3.41, *SD* = 0.86, *a* = 0.89).

General Self-Efficacy Scale (GSE).

The GSE was used to measure participants’ self-efficacy based on ten items, such as “I can always manage to solve difficult problems if I try hard enough.” (Schwarzer, 2012). Responses are reported on a 4-point Likert scale ranging from (1) Not at all true to (4) Exactly true (*M* = 3.2, *SD* = 0.57, *a* = 0.92).

Trustworthiness questionnaire.

In order to measure participants' perceived trustworthiness regarding the two presented websites, four trustworthiness items were created. A sample item was “I would safe my payment details on this website.” (Appendix D). Responses were reported on a 7-point Likert scale, ranging from (1) Strongly Disagree to (7) Strongly Agree. Additionally, to test participants' conscientiousness, they had to indicate which website they saw out of two possible choices (Appendix D). Thereby, the reliability and value of participants' responses were determined.

Cookie questionnaire.

A cookie questionnaire was created to investigate participants' actual cookie acceptance behaviour on the two presented websites. In addition, the questionnaire included questions regarding the amount of attention participants paid to the cookie message as well as their memory. Thus, first participants' conscientiousness was tested by asking them which cookie message they saw, providing one correct and one false option (Appendix E). Furthermore, based on a yes/no option participants were asked whether they remembered well if they accepted or declined the cookie message. Regarding the second website, an additional question was asked to examine participants' conscientiousness regarding the displayed nudge (Appendix E). Two different nudges were displayed, and participants had to indicate which display they saw.

Actual security behaviour question.

Actual security behaviour was measured with the question "Did you accepted the cookie message?". By answering this question, participants had to indicate whether they accepted or rejected the cookie messages displayed on the experiment websites. Participants had to answer with either yes or no.

Procedure

At the beginning of the online experiment, participants gave their informed consent (Appendix F). Afterwards, they were informed about the purpose of the study. The genuine purpose of this study was to use nudges to counteract manipulative cookie messages in order to better protect the privacy of users. However, this research used deception regarding the actual purpose of the study, as pre-existing knowledge could have potentially influenced participants' natural cookie acceptance behaviour. Therefore, participants were told that the purpose of the study was to investigate users' perceived trustworthiness of websites in order to improve user privacy. The only aspect that the used deception changed for participants was that they had to fill out ten additional trustworthiness questions. Thus, the deception used in this research entailed no harm for participants, as the main goal of protecting users' data privacy remained the same.

Next, important moderators of the target behaviour were measured, namely participants' security behaviour intention, personality, domain specific risk-taking and self-efficacy. Afterwards, participants started with the main task of the experiment, which required them to navigate themselves around two websites that had been created for the purpose of this research. More specifically, participants were instructed to put a specific item found on the website into their shopping bag. The first website displayed a manipulative cookie message only, while the second website displayed a manipulative cookie message in combination with a nudge. As this research used a transparent and a non-transparent nudge, participants were randomly assigned to one of the two conditions. After each website, participants had to complete questions about the trustworthiness of the website and the cookie message displayed. Once participants had completed the two tasks, their security behaviour intentions were measured again. At the end of the experiment, participants were given a comprehensive debriefing about the actual purpose of the study and had to give their informed consent once again.

Statistical analysis

The data was analysed using the IBM SPSS 26 software. In order to test the hypotheses, a significance level of 5% was chosen. In the preliminary analysis, the final data set was determined by omitting participants who did not finish the questionnaire, showed straight-lining behaviour such as only responding with “Strongly agree”, or did not pass the attention check. Descriptive statistics were used to identify prior differences in demographic variables. Lastly, before examining the main hypotheses descriptive statistics were used to explore variables of interest.

With regards to the main analyses, the Chi-Square test of independence was used to examine the relation between cookie acceptance behaviour when being exposed to a nudge and cookie acceptance behaviour when not being exposed to a nudge. For further analyses, binary logistic regression was used to examine a) the difference in cookie acceptance behaviour when facing a transparent nudge versus facing a non-transparent nudge and b) examining the relationship between the personality trait openness and cookie acceptance behaviour without facing a nudge. Beforehand, the assumption of multicollinearity was checked, using a tolerance value of above 0.1 as the cut-off score (Senaviratna & A. Cooray, 2019)

Lastly, an auxiliary analysis was performed. With regards to the main analysis, we were interested in examining whether openness illustrates a moderator for the relationship between nudges and cookie acceptance behaviour. Therefore, a moderation analysis was conducted using the PROCESS Macro: Model 4 in SPSS, including the Hayes’ bootstrapping method (Hayes, 2017). Besides, the following control measures were investigated. First, a repeated measures ANOVA was used to compare participants' security behaviour intentions before and after the experiment. Second, a binary logistic regression was chosen to examine the relationship between a) security behaviour intention and cookie acceptance behaviour without a nudge b) risk-taking and cookie acceptance behaviour without a nudge and c) general self-efficacy and cookie acceptance behaviour without a nudge. Lastly, although trustworthiness was originally used for deception purposes, we were interested in whether the exposure to a nudge affects the perceived trustworthiness of a website. Therefore, a Wilcoxon Signed Rank Test was conducted.

Results

Preliminary analysis

Cleaning the data set according to the specified exclusion criteria lead to an overall sample size of 100. The preliminary assumption analysis of the first logistic regression suggested that the assumption of multicollinearity was met (tolerance = 1.0). An inspection of the standardised residual values revealed that there were no outliers. Likewise, the assumption of multicollinearity was met for the second logistic regression (tolerance = 1.0) and no outliers were found. In addition, multicollinearity was met for the auxiliary moderation analysis (tolerance = .99).

Main analysis

Cookie acceptance behaviour

The Chi-Square test of independence revealed a significant difference between cookie acceptance behaviour without a nudge and cookie acceptance behaviour with a nudge, X^2 (1, N = 100) = 20.89, p < .001 (Table 1). Thus, participants showed a lower cookie acceptance rate when exposed to a nudge (total $_{\text{acceptance}}$ = 24), than when not exposed to a nudge (total $_{\text{acceptance}}$ = 51). As can be seen in table 1, respondents who declined the cookie message on the first website, no nudge, were more likely to also decline on the second website, including a nudge, while participants who accepted the cookie message on the first website were also more likely to decline on the second website. In general, the results show that overall participants had a rather safe cookie acceptance behaviour, as cookie messages were rejected a total of 125 times and accepted only 75 times.

Table 1

Chi-Square test of independence for hypothesis 1

			Cookie acceptance **with** a nudge		
			decline	accept	Total
Cookie acceptance **without** a nudge	decline	Count	47	2	49
		Expected count	37.2	11.8	49.0
	accept	Count	29	22	51

	Expected count	38.8	12.2	51.0
Total	Count	76	24	100
	Expected count	76.0	24.0	100.0

Transparent nudge versus non-transparent nudge

Contrary to expectations, binary logistic regression revealed a statistically non-significant effect of degree of transparency on cookie acceptancy behaviour, X^2 (1, *N* = 100) = 1.93, *p* = .16. Thus, no difference in cookie acceptance behaviour was found when exposed to a transparent and a non-transparent nudge, *B* = 0.65, *SE* = 0.47, *p* = .16.

Openness

Binary logistic regression showed a statistically significant relation between openness and cookie acceptance behaviour, X^2 (1, *N* = 100) = 7.88, *p* = .005. However, against expectations the analysis revealed that people who report a high score on openness are less likely to accept a cookie message, *B* = -1.01, *SE* = 0.38, *p* = .009.

Auxiliary analyses

Openness as moderator

The moderation analysis revealed that the personality trait openness is no significant moderator of the relationship between nudges and cookie acceptance behaviour (*B* = -0.51, z = -0.61, *p* = .54). Thus, the relationship between nudges and cookie acceptance behaviour does not depend on an individual's score on openness and openness does not interact with the specific type of nudge.

Security behaviour intentions

The repeated measures ANOVA showed a statistically significant relation between security behaviour intention and cookie acceptance behaviour, X^2(1, *N* = 100), *p* < .001. In other words, individuals with high security behaviour intentions were less likely to accept a cookie message (*B* = -.15, *SE* = 0.04, *p* < .001). In addition, the repeated measures ANOVA revealed a statistically significant difference in means, *F*(1, 98) = 15.46, *p* < .001. Consistent with our predictions, participants reported higher security behaviour intentions after the experiment (*B* = 3.35, *SE* = 0.05, *p* < .001) than before the experiment (*B* = 3.22, *SE* = 0.05, *p* < .001).

Risk-taking

Binary logistic regression showed a non-significant effect for risk-taking on cookie acceptance behaviour, X^2 *(1, N* = 100) = 0.41, *p* = .52. Contrary to our expectations, there was no difference in cookie acceptance between participants with high and low risk-taking (*B* = 0.14, *SE* = 0.23, *p* = .52).

Self-efficacy

Against our expectations, binary logistic regression showed a non-significant effect for self-efficacy on cookie acceptance behaviour, X^2 (1, *N* = 100) = 0.42, *p* = .51. In other words, there was no difference in cookie acceptance behaviour between participants with high and low self-efficacy (*B* = 0.23, *SE* = 0.35, *p* = .51).

Trustworthiness

A Wilcoxon signed rank test showed that there is no significant difference in trustworthiness when exposed to a nudge (*Md* = 4.25) compared to when not exposed to a nudge (*Md* = 4.5), *z* = -1.87, *p* = .06. Thus, participants perceived both websites as equally trustworthy, regardless of whether they had been exposed to a nudge or not.

Discussion

To our best knowledge, this study is the first to experimentally examine whether the use of nudges can support more secure user behaviour regarding cookie acceptance. While current research reports the effective use of nudges in a variety of privacy and security domains, the area of cookie acceptance is relatively poorly understood (Acquisti et al., 2017; Caraban et al., 2019). To bridge the gap of missing research, this study aimed to identify the impact of type 2 nudges on cookie acceptance decisions. It was predicted that cookie acceptance rates will decrease when a nudge is presented. In addition, it was hypothesized, that this positive effect is stronger for transparent than for non-transparent nudges. Following the research conducted by Halevi et al. (2013), this study also investigated the influence of personality on cookie acceptance decisions. It was precited, that a high score on openness is related to less secure cookie acceptance behaviour. In addition, individuals' security behaviour intentions, risk-taking as well as self-efficacy were investigated to broaden the understanding of cookie acceptance behaviour. First, we found support for the positive effect of type 2 nudges on cookie acceptance behaviour. However, against expectations, the degree of transparency does not have an influence. Furthermore, the influence of the personality trait openness was contrary to our expectations, as a high score on openness was shown to be associated with lower cookie acceptance rates. In addition, while the control measures risk-taking and self-efficacy had no effect on cookie acceptance behaviour, security behaviour intention did. Findings showed that high security behaviour intentions were associated with a lower cookie acceptance rate.

The impact of nudges on cookie acceptance behaviour

Participants were predicted to show a lower cookie acceptance rate when exposed to a nudge compared to when not exposed to a nudge. We found support for this first hypothesis, as participants were less likely to accept a cookie message when exposed to a nudge. This finding is in line with the study conducted by Coventry et al. (2016), illustrating a positive behaviour change in the face of a nudge. Although research reports mixed results regarding the general effectiveness of nudges, the present study illustrates another example of the positive relation. According to Caraban et al. (2019), mixed results are no sign of a general ineffectiveness of nudges, but rather signify that nudges are not a one-size-fits-all approach. The decrease in cookie acceptance rate in this study is an example of how effective nudges can be when adjusted to the context. Based on the ELM, the difference in cookie acceptance rates could be due to the differences in cognitive effort applied. It can be argued that cookie acceptance was higher for the cookie message without a nudge because participants used their peripheral route of processing. Given that peripheral processing is characterized by underlying biases and heuristics, privacy impeding mechanisms, such as habituation, potentially explain why participants were more likely to accept the cookie message without a nudge (Bauer et al., 2021). This reasoning is in line with the study conducted by Becker et al. (2019), arguing that the mental shortcuts which individuals use when facing a privacy related decision are causing less secure behaviour.

Contrarily, it can be argued that cookie acceptance was lower for the cookie message with a nudge because here participants used their central route of processing. This difference in cognitive effort applied, can be explained by the use of type 2 nudges (Zimmermann & Renaud, 2021). More specifically, as participants were exposed to a type 2 nudge in combination with the cookie message, their peripheral processing got activated. This activation targeted more reflective attention and thinking. Through this change in processing, participants used their conscious and slow processing instead of relying on biases and heuristics. As a result, it can be argued that the privacy decision became more salient, its consequences more outstanding and therefore participants were less likely to accept the cookie message (Bauer et al., 2021). This supports the results of Zimmermann and Renaud (2021), who found that nudges can make security and privacy decisions more salient, consequently leading to more secure behaviour. Thus, present findings suggest that nudging interventions for safer cookie acceptance behaviour must ensure that targeted individuals use their central route of processing.

To ensure that website users make use of their central route of processing, a closer look needs to be taken at the design of type 2 nudges. One specific design aspect was the degree of transparency. It was hypothesised that users exposed to a transparent nudge will show a lower cookie acceptance rate compared to users exposed to a non-transparent nudge. Contrary to our expectations, the present study found no support for the second hypothesis, as there was no difference in cookie acceptance rates between the transparent and the non-transparent nudge. In other words, individuals were just as likely to accept the cookie message with a transparent nudge as with a non-transparent nudge. This result contradicts the research conducted by Grüne-Yanoff (2012), who reports that non-transparency increases the effectiveness of a nudge. In general, however, current research still reports mixed results on the difference in effectiveness regarding transparency (Weijers et al., 2020). By examining the two nudges used in this study, it can be argued that the lack of support for hypothesis two may be due to the design similarities between the two nudges. In particular, the transparent and non-transparent nudges were very similar in terms of shape, colour, size and position on the cookie message. The only significant difference between the two nudges was their message. The transparent nudge stated, "Navigate safely. Your personal cybersecurity and privacy is at increased risk. You can easily minimise the risk by declining the use of cookies", while the non-transparent nudge only stated, "Navigate safely". Although the non-transparent nudge’s statement is more generally worded and less transparent about the intention behind it, the similarities with the transparent nudge likely outweighed this difference.

Despite the potential influence of similarities in the nudge designs, we also have to consider the possibility that the degree of transparency actually does not matter for the effectiveness of a nudge. Based on the present findings, it can be argued that the mere presence of a type 2 nudge is crucial, regardless of its transparency. One explanation for this could be the fact that the transparent, as well as the non-transparent nudge, were type 2 nudges. Since type 2 nudges generally target reflective thinking, it seems plausible that the degree of transparency does not make a big difference. In particular, as both nudges were designed to appeal to the central route of processing, it is likely that they caused greater privacy concerns and consequently a lower likelihood to accept the cookie message, regardless of their degree of transparency. Therefore, it can be questioned whether the application of different transparency degrees is necessary for type 2 nudges. It can be argued that different transparency degrees are rather a matter of type 1 nudges only. Assuming that the degree of transparency of type 2 nudges does not affect their effectiveness, new questions arise regarding which design aspects architects of choice should focus on. Different types of framing, the use of different theoretical foundations as well as more outward characteristics such as colour and size of wording are focal points for consideration in further research on nudging interventions.

Individual differences in cookie acceptance behaviour

Regarding the impact of individual characteristics, it was hypothesised that users reporting a high score on openness will show a higher cookie acceptance rate compared to users reporting a low score on openness. Surprisingly, the relationship between openness and cookie acceptance rate was exactly the opposite of what we expected. In other words, people who had a high openness score were less likely to accept a cookie message. Although this study did not find support for the third hypothesis, it helps to clarify the inconsistent research around the personality trait openness (Gratian et al., 2018; Halevi et al., 2013; Pattinson et al., 2012). Based on the findings of van de Weijer and Leukfeldt (2017), one might assume that openness makes people more likely to follow manipulative traits, leading to less safe behaviour. However, looking at Junglas et al.'s (2008) research, it becomes plausible that the influence of openness might be the other way around. According to Junglas et al. (2008), individuals with a high openness score are less likely to stick to habitual behaviours and are more likely to be open to new behaviours. Thus, it can be inferred that individuals with a high openness score are less prone to biases and heuristics, such as habituation. Consequently, it can be argued that individuals with a high openness score are more likely to change their behaviour regarding cookie acceptance. Furthermore, individuals with a high score on openness have a deeper awareness due to their various learning experiences in life. As a result, Junglas et al. (2008) argue that individuals with a high score on openness are both more aware and more sensitive to threatening life situations. Thus, it can be inferred that individuals scoring high on openness perceive a cookie message as more threatening than individuals scoring low on openness. Consequently, they are less likely to accept a cookie message. In light of the prior argumentation and present findings, it can be concluded that a high score on openness is in general associated with more secure behaviour, including a lower likelihood to accept a cookie message.

Findings shed an interesting light on the role of personality traits in cookie acceptance decisions and highlight the importance of considering individual differences in the design of privacy promoting nudging interventions. In particular, if we want to promote safer behaviour by effectively nudging people to their central route of processing, we perhaps need to target them according to their personality. Openness is only one example where, despite the general interpretation of related characteristics, openness actually illustrates a supportive factor for safer behaviour. Hence, it is important that other personality traits and their role in cookie acceptance decisions are investigated more in depth. Thereby choice architects are able to make use of and strengthen promoting personality factors while inhibiting personality factors can be counteracted or balanced.

In addition to personality, this study examined the following three control measures: risk-taking, self-efficacy and security behaviour intentions. Past research showed that risk-taking and self-efficacy are two predictors of cookie acceptance behaviour. First, Coventry et al. (2016) found that individuals high in risk-taking are more likely to accept a cookie message. However, the current study found no support for this finding, as there was no difference in cookie acceptance between individuals high in risk-taking compared to individuals low in risk-taking. Second, this study investigated the concept of self-efficacy and its influence of cookie acceptance behaviour. According to Bandura (1994), individuals with a high self-efficacy are better able to approach difficult tasks. Connecting this to cookie acceptance, it was argued that individuals with a high self-efficacy are better able to decline a cookie message because they are less likely to avoid the threat illustrated by the cookie message. However, the current study found no support for this, as there was no difference in cookie acceptance behaviour between individuals with high and low self-efficacy.

While no support was found for the first two concepts, the present study found support for security behaviour intention being a significant predictor of cookie acceptance behaviour. Particularly, this study showed that individuals with high security behaviour intention are less likely to accept a cookie message. This finding supports the study conducted by Egelman et al. (2016), who found that high security behaviour intentions translate well into safer behaviour. However, Egelman et al. (2016) note that this mostly counts for security behaviours that are included in the SeBIS scale, used in this study. In light of the present findings, it can be argued that support was found as cookie acceptance behaviour belongs to the SeBIS subscale of “proactive awareness”. Thus, generalizability to security behaviours outside the SeBIS scale is limited and needs further investigation. Despite the limited generalizability, the gained insights into security behaviour intentions can help to promote more secure user behaviour regarding cookie acceptance decisions. Specifically, increasing an individual’s security behaviour intentions could promote in turn safer user behaviour and should be considered when designing nudging interventions.

In addition, the present study aimed to fill the gap of research on the durability of nudges. Therefore, changes in security behaviour intentions with and without a nudge were examined, as an individual's intention can be considered a potential predictor of future behaviour (Pollini et al., 2021). Findings revealed that exposure to a nudge leads to an increase in security behaviour intentions. This implies that the use of nudges likely leads to more secure behaviour in the future. Based on the research conducted by Zimmermann and Renaud (2021), it can be argued that security behaviour intention increased as the nudge made the security decision more salient. Thereby the perceived threat of a cookie message increased as well. Present findings indicate that this increase in threat, caused by the nudge, potentially lasts in the long term. Concludingly, the results of this study suggest that nudges are likely to have high durability, as they have the potential to not only influence current safety behaviours but also future safety behaviours.

Strengths and limitations

To our best knowledge, the present study is the first to investigate the influence of nudges on cookie acceptance behaviour and thus contributes to the literature on general data privacy and cybersecurity. Although current research reports mixed results regarding the effectiveness of nudges in the field of cybersecurity, the present findings confirm the general effectiveness of nudges. In particular, the current study draws attention to the relatively under researched field of cookie banners and filled the gap in the literature on nudges' role in cookie acceptance decisions. The experimental design of this study illustrates one of its main strengths. The fact that we created real websites, which participants visited and interacted on, significantly strengthens the current findings, as the whole experiment had a very realistic character. Moreover, given that participants conducted the study in their home environment, we were able to observe how individuals actually behave in everyday life, wherefore our results probably contain very natural behaviour. Furthermore, the examination of the personality trait openness brought more clarity to the mixed results of current research. In fact, high openness illustrates a supporting factor for more secure decision-making. This finding broadens the understanding of the various factors underlying an individual’s cookie acceptance behaviour and can be further used for the development of nudges.

Some limitations must be considered as well. First, this study used a relatively homogenous sample, consisting of individuals who were mostly German and students in their twenties. In addition, many participants were recruited from the University of Twente. This homogeneity could have potentially impacted the results of the current study. Consequently, the generalizability of the findings is limited. Furthermore, given the scarce room for lengthy personality instruments, this study used the short HEXACO PI R 24-items scale, which reports relatively low alpha reliability. However, according to de Vries (2013), the scale validity remains adequate. Another limitation relates to the design of the used nudges. The noticed similarities between the transparent and non-transparent nudge likely influenced the results. Lastly, the current study used behavioural intention to predict the long-term effect of nudges.

Although an individual’s intention is a good predictor of actual behaviour, measuring actual behaviour would yield more meaningful results.

Future directions

Given the increasing number of cybersecurity threats, the need for further research on how to promote safer user behaviour becomes apparent. To the best of our knowledge, this study is the first to investigate the impact of type 2 nudges in the context of cookie acceptance behaviour. As there are a number of privacy concerns associated with cookies, more research attention should be paid to this area. This study found support for the effective use of type 2 nudges to promote safer cookie acceptance behaviour. While a relatively homogenous sample was used in this research, future research should consider different samples in similar study designs. In addition, methods such as mouse movements or eye tracking would be powerful tools to study the effectiveness of nudges in a more controlled way. However, it must be taken into account that a person's behaviour in a controlled environment is likely to be less natural than in the home environment.

The research conducted by Coventry et al. (2016) already suggests that cookie acceptance behaviour is strongly influenced by several factors. To promote safe cookie acceptance behaviour, a more accurate picture of the external influences as well as the individual differences underlying cookie message decisions is needed. The present study highlights the importance of individual characteristics underlying users’ cookie acceptance behaviour. Current findings call for further replication with other samples, a broader focus on all Big Five personality traits as well as the use of an expanded version of the HEXACO PI R. In addition, to better understand the influence of personality, related sub-facets of the Big Five should be investigated in more detail. This way, both facilitating and inhibiting factors can be identified and nudging interventions can be made more effective.

Regarding the design of type 2 nudges, the present study found no influence of transparency on cookie acceptance behaviour. However, as transparency is only one of several design aspects, future research should investigate other aspects. Clarifying the role of different design aspects will help choice architects to design nudge interventions more effectively. This will help to promote safer cookie acceptance behaviour among users. Regarding the durability of nudges, this study used behavioural intention as an indicator, showing that nudges have the potential to have a long-term effect. Further studies should replicate these findings using actual behaviour. Longitudinal studies for example would provide more powerful insights into the durability of nudges.

Conclusion

A popular topic in cybersecurity research is the use of nudges to promote safer user behaviour and decision-making. While companies already use nudges extensively for their own benefit, security and software developers lag behind when it comes to using nudges to promote user privacy. This study is the first to examine the impact of type 2 nudges on cookie acceptance behaviour. Results of this study show that type 2 nudges are an effective approach to promote safer cookie acceptance behaviour, by nudging users towards their central route of processing. Since companies primarily use type 1 nudges that trigger peripheral processing, users' central route of processing is our only chance to counteract companies' privacy impeding manipulations. Here, the design of nudges plays a crucial role. An important question is the durability of nudges, how often do we need to nudge against cookie banners? In addition, it is important to ensure that type 2 nudges do not become trivial and trigger central processing even after months of exposure. Therefore, we need to consider that type 2 nudges might require design changes from time to time, such as differences in placement and framing. This is where insights into human factors can help to better understand users' decision-making processes around cookie messages and can be used to design nudges more effective and personalised. It is now time to pay more attention to this line of research, as companies have exploited users' peripheral processing through nudges long enough.

References

Acquisti, A., Sleeper, M., Wang, Y., Wilson, S., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., & Schaub, F. (2017). Nudges for Privacy and Security. *ACM Computing Surveys*, *50*(3), 1–41. https://doi.org/10.1145/3054926

Bandura, A. (1994). Encyclopedia of mental health. *Self-Efficacy*, *4*, 71–81. http://happyheartfamilies.citymax.com/f/Self_Efficacy.pdf

Bauer, J. M., Bergstrom, R., & Foss-Madsen, R. (2021). Are you sure, you want a cookie? – The effects of choice architecture on users' decisions about sharing private online data. *Computers in Human Behavior*, *120*, 106729. https://doi.org/10.1016/j.chb.2021.106729

Becker, M., Klausing, S., & Hess, T. (2019). Uncovering the privacy paradox: the influence of distraction on data disclosure decisions. *Researchgate*, 1–13. https://www.researchgate.net/profile/Thomas-Hess-6/publication/340492606_Uncovering_the_Privacy_Paradox_The_Influence_of_Distraction_on_Data_Disclosure_Decisions/links/5e8ce8bb299bf1307985d0eb/Uncovering-the-Privacy-Paradox-The-Influence-of-Distraction-on-Data-Disclosure-Decisions.pdf

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

Blais, A.-R., & Weber, E. U. (2006). Domain-Specific Risk-Taking Scale. *PsycTESTS Dataset*, *1*. https://doi.org/10.1037/t13084-000

Cacioppo, J. T., & Petty, R. E. (2020). The Elaboration Likelihood Model of Persuasion. *ACR North American Advances*, *NA-11*. https://www.acrwebsite.org/volumes/6329/volumes/v11/NA%20-%2011

Caraban, A., Karapanos, E., Gonçalves, D., & Campos, P. (2019). 23 Ways to Nudge. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, *503*. https://doi.org/10.1145/3290605.3300733

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Coventry, L. M., Jeske, D., Blythe, J. M., Turland, J., & Briggs, P. (2016). Personality and Social Framing in Privacy Decision-Making: A Study on Cookie Acceptance. *Frontiers in Psychology*, *7*. https://doi.org/10.3389/fpsyg.2016.01341 de Vries, R. E. (2013). The 24-item Brief HEXACO Inventory (BHI). *Journal of Research in Personality*, *47*(6), 871–880. https://doi.org/10.1016/j.jrp.2013.09.003

Egelman, S., Harbach, M., & Peer, E. (2016). Behavior Ever Follows Intention? *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/2858036.2858265

Egelman, S., & Peer, E. (2015). Scaling the Security Wall. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*. https://doi.org/10.1145/2702123.2702249

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983–988. https://doi.org/10.1016/j.cose.2012.08.004

General Data Protection Regulation (GDPR) Compliance Guidelines. (n.d.). GDPR.eu. https://gdpr.eu

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

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behaviour intentions. *ScienceDirect*, *73*, 345–358. ScienceDirect. https://doi.org/https://doi.org/10.1016/j.cose.2017.11.015

Grüne-Yanoff, T. (2012). Old wine in new casks: libertarian paternalism still violates liberal principles. *Social Choice and Welfare*, *38*(4), 635–645. https://doi.org/10.1007/s00355-011-0636-0

Grüne-Yanoff, T., & Hansson, S. O. (2009). *Preference Change* (T. Grüne-Yanoff & S. O. Hansson, Eds.; Vol. 42, pp. 207–219). Springer Netherlands. https://doi.org/10.1007/978-90-481-2593-7

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. *Proceedings of the 22nd International Conference on World Wide Web - WWW '13 Companion*. https://doi.org/10.1145/2487788.2488034

Hansen, P. G., & Jespersen, A. M. (2013). Nudge and the Manipulation of Choice. *European Journal of Risk Regulation*, *4*(1), 3–28. https://doi.org/10.1017/s1867299x00002762

Hayes, A. F. (2017). Introduction to Mediation, Moderation, and Conditional Process Analysis, Second Edition: A Regression-Based Approach. In *Google Books*. Guilford Publications.

https://books.google.nl/books?hl=en&lr=&id=6uk7DwAAQBAJ&oi=fnd&pg=PP1&dq=Introduction+to+Mediation

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, *17*(4), 387–402. https://doi.org/10.1057/ejis.2008.29

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Log In | Wix. (n.d.). Users.wix.com. https://manage.wix.com/account/sites

McAlaney, J., & Benson, V. (2020). Shibboleth Authentication Request. *ScienceDirect*, 1–8. https://doi.org/https://doi.org/10.1016/B978-0-12-819204-7.00001-4

Meske, C., & Amojo, I. (2020). *Ethical Guidelines for the Construction of Digital Nudges*. https://arxiv.org/pdf/2003.05249.pdf

Miyazaki, A. D. (2008). Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage. *Journal of Public Policy & Marketing*, *27*(1), 19–33. https://doi.org/10.1509/jppm.27.1.19

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Psychology*, *12*. https://doi.org/10.3389/fpsyg.2021.561011

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024

Ortloff, A.-M., Zimmerman, S., Elsweiler, D., & Henze, N. (2021). The Effect of Nudges and Boosts on Browsing Privacy in a Naturalistic Environment. *Proceedings of the 2021 Conference on Human Information Interaction and Retrieval*. https://doi.org/10.1145/3406522.3446014

Park, H., & Blenkinsopp, J. (2011). The roles of transparency and trust in the relationship between corruption and citizen satisfaction. *International Review of Administrative Sciences*, *77*(2), 254–274. https://doi.org/10.1177/0020852311399230

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Digital.library.adelaide.edu.au*, *20*(1). https://doi.org/10.1108/09685221211219173

Paunov, Y., Wänke, M., & Vogel, T. (2018). Transparency effects on policy compliance: disclosing how defaults work can enhance their effectiveness. *Behavioural Public Policy*, *3*(02), 187–208. https://doi.org/10.1017/bpp.2018.40

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*. https://doi.org/10.1007/s10111-021-00683-y

Schwarzer, R. (2012). *(PDF) The General Self-Efficacy Scale (GSE)*. ResearchGate. https://www.researchgate.net/publication/298348466_The_General_Self-Efficacy_Scale_GSE

Senaviratna, N. A. M. R., & A. Cooray, T. M. J. (2019). Diagnosing multicollinearity of logistic regression model. *Asian Journal of Probability and Statistics*, *5*(2), 1–9. https://doi.org/10.9734/ajpas/2019/v5i230132

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177–191. https://doi.org/10.1016/j.cose.2015.01.002

Tagliabue, M., Squatrito, V., & Presti, G. (2019). Models of Cognition and Their Applications in Behavioral Economics: A Conceptual Framework for Nudging Derived From Behavior Analysis and Relational Frame Theory. *Frontiers in Psychology*, *10*. https://doi.org/10.3389/fpsyg.2019.02418

Ting, D. (n.d.). *Why Cognitive Biases and Heuristics Lead to an Under-investment in Cybersecurity*. Retrieved February 21, 2022, from https://www.cs.tufts.edu/comp/116/archive/fall2019/dting.pdf

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big Five Personality Traits of Cybercrime Victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407–412. https://doi.org/10.1089/cyber.2017.0028

Wachner, J., Adriaanse, M., & De Ridder, D. (2020). The influence of nudge transparency on the experience of autonomy. *Comprehensive Results in Social Psychology*, 1–15. https://doi.org/10.1080/23743603.2020.1808782

Weijers, R. J., de Koning, B. B., & Paas, F. (2020). Nudging in education: from theory towards guidelines for successful implementation. *European Journal of Psychology of Education*, *36*, 883–902. https://doi.org/10.1007/s10212-020-00495-0

Xu, F., & Warkentin, M. (2020). Integrating Elaboration Likelihood Model and Herd Theory in Information Security Message Persuasiveness. *Computers & Security*, *98*, 102009. https://doi.org/10.1016/j.cose.2020.102009

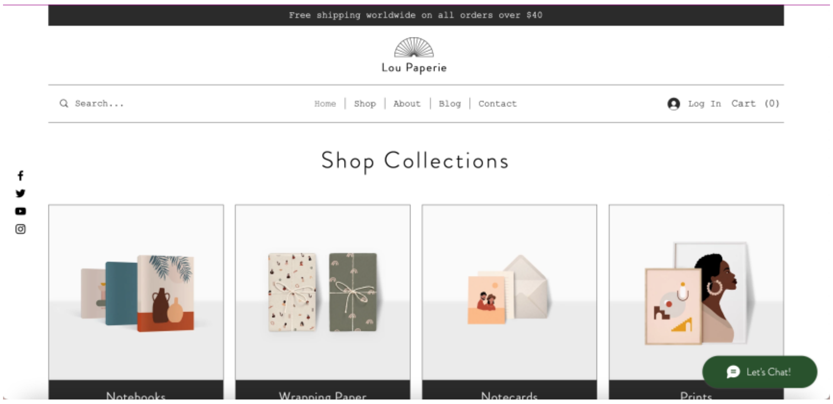
Zimmermann, V., & Renaud, K. (2021). y *ACM Transactions on Computer-Human Interaction*, *28*(1), 1–45. https://doi.org/10.1145/3429888

Appendix

Appendix A

Figure A1

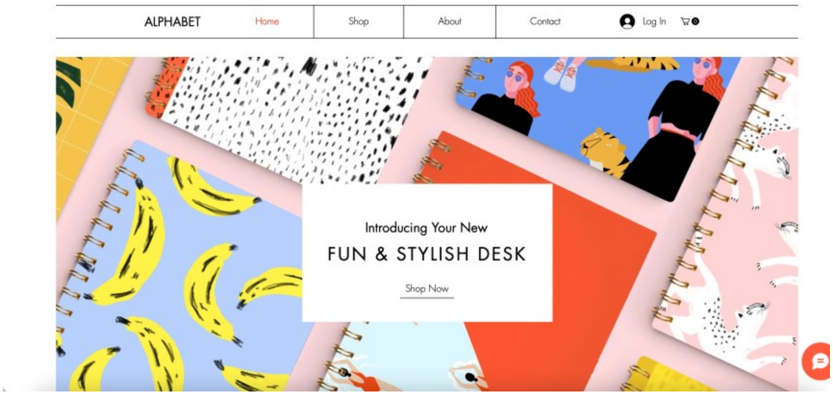
First website



Free shipping worldwide on all orders over $40

Figure A2

Second website

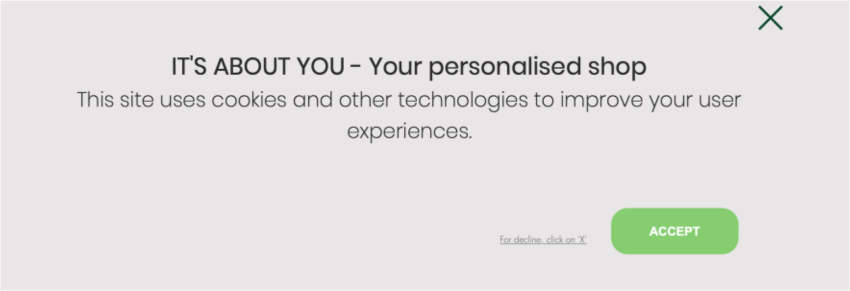


Introducing Your New FUN & STYLISH DESK

Appendix B

Figure B1

Cookie message design



IT'S ABOUT YOU - Your personalised shop

This site uses cookies and other technologies to improve your user experiences.

Appendix C

Figure C1

Transparent nudge

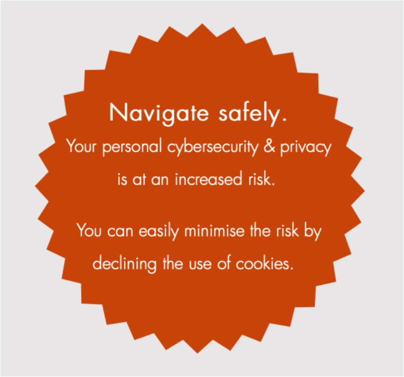
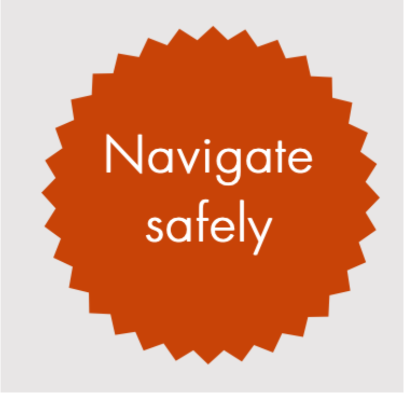

Navigate safely.
Your personal cybersecurity & privacy is at an increased risk.
You can easily minimise the risk by declining the use of cookies.

Figure C2

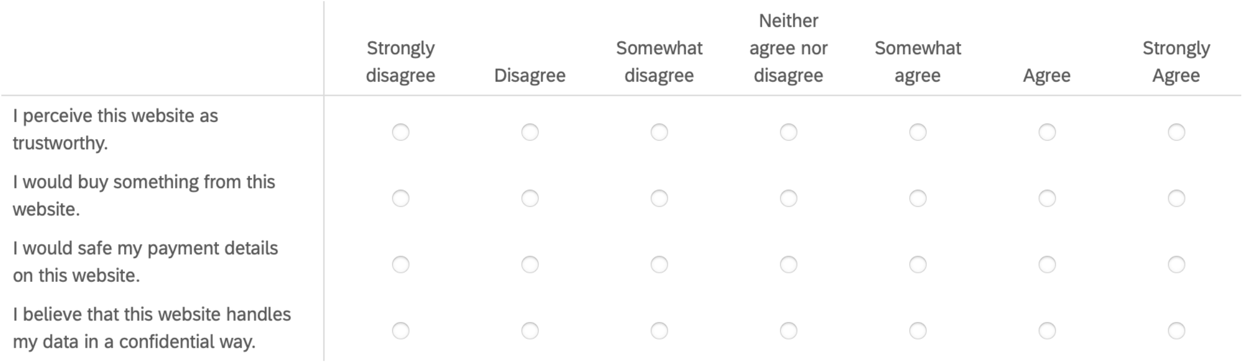
Non-transparent nudge



Appendix D

Figure D1

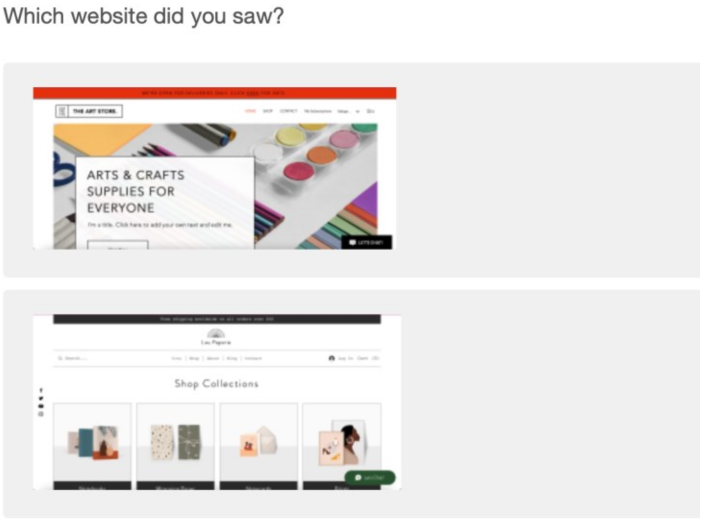
Trustworthiness questions



	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly Agree
I perceive this website as trustworthy.	○	○	○	○	○	○	○
I would buy something from this website.	○	○	○	○	○	○	○
I would safe my payment details on this website.	○	○	○	○	○	○	○
I believe that this website handles my data in a confidential way.	○	○	○	○	○	○	○

Figure D2

Conscientiousness question

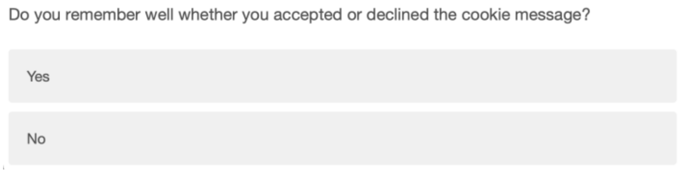


Which website did you saw?

Appendix E

Figure E1

Cookie questions



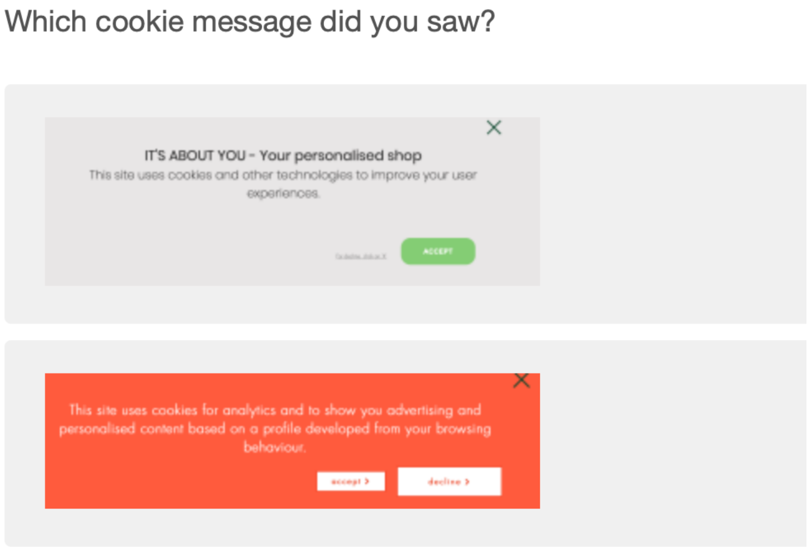
Do you remember well whether you accepted or declined the cookie message?

Yes

No

Figure E2

Conscientiousness question



Which cookie message did you saw?

IT'S ABOUT YOU - Your personalised shop

This site uses cookies and other technologies to improve your user experiences.

This site uses cookies for analytics and to show you advertising and personalised content based on a profile developed from your browsing behaviour.

Appendix F

Informed consent

Welcome to this research study!

Dear participant,

You are being invited to participate in the research study titled **"Examining users' perceived trustworthiness in the online environment."** More specifically, I am examining users' perceived trustworthiness regarding different websites, with the aim to better protect users' data privacy. In this study, you are presented with two different websites, where you have to navigate on and fulfill a specific task. Based on this, you will be given a questionnaire which I would like to ask you to fill in. The whole experiment will take approximately 20 minutes to complete. Your participation in this study is completely voluntary and you are allowed to withdraw your participation at every moment in time, without giving any reason. Furthermore, anonymity will be ensured, and your data will not be used for any other purpose than this research. Your answers in this study will remain confidential as well.

This research is approved by the **Ethics Committee of the Behavioural, Management and Social Sciences (BMS) Faculty of the University of Twente**. Furthermore, there are no risks associated with participating this research study.

If you have any further questions, feel free to contact me via the following email address: **f.grosart@student.utwente.nl**