Adopting Protective Behaviours against Hypernudging: The Role of Awareness and Protection Motivation Theory

Loes Elfrink (s2857170)

Department of Psychology, University of Twente

202000384 - BSc Thesis PSY

prof. dr. J.H. Kerstholt & dr. ir. P.W. de Vries

July 4, 2025

Abstract

There is an increasing prevalence of hypernudging, which refers to the use of algorithms to create highly personalised and dynamic choice architectures that subtly and continuously influence individual decision-making in digital environments. This cross-sectional study investigated to what extent awareness and Protection Motivation Theory (PMT) factors predicted adopting protective behaviours against hypernudging. A sample of 108 participants completed a survey measuring protective behaviour and its predictors: awareness, perceived vulnerability, perceived severity, perceived benefits, response efficacy, self-efficacy, and perceived costs. Then, multiple linear regression analysis was conducted, in which a significant positive relationship was found between perceived severity and protective behaviour, response efficacy and protective behaviour, as well as a significant negative relationship between perceived costs and protective behaviour. No significant relationships were found between the other predictors and protective behaviour. Some limitations should be acknowledged, including a predominantly Dutch sample with potential language comprehension issues, the use of self-report data, the benefits construct that was reverse-worded, and the relatively low reliability of the protective behaviour measure. Despite these limitations, the study found that perceived severity, response efficacy, and perceived costs predicted protective behaviour against hypernudging, while awareness and other PMT factors did not. The results stress the importance of focusing on perceived severity, response efficacy, and perceived costs, rather than awareness to increase protective behaviour.

Keywords: hypernudging, algorithms, protective behaviours, awareness, protection motivation theory

Adopting Protective Behaviours against Hypernudging: The Role of Awareness and Protection Motivation Theory

Every day, millions of people make choices online—what to read, what to buy, and even what to believe—without realising that data-driven algorithms are subtly influencing their decisions. This is a process known as hypernudging, which can be defined as the use of Big Data analytics and algorithms to create highly personalised and dynamic choice architectures that subtly and continuously influence individual decision-making in digital environments (Yeung, 2017). Unlike traditional nudging, which involves static interventions, hypernudging continuously collects and analyses large amounts of personal data to adjust the informational context in real time, thereby steering user behaviour in a pervasive manner (Yeung, 2017). As digitalisation accelerates, the implementation of hypernudging techniques has become increasingly prevalent, which may raise concerns about user autonomy and privacy (Lanzing, 2019). Despite these concerns, little is known about how individuals perceive the influence of hypernudging or what motivates them to resist it. Understanding the underlying mechanisms behind adopting protective behaviours is important to increase digital autonomy and privacy. Therefore, this study focuses on what psychological mechanisms trigger people to adopt protective behaviours against hypernudging.

Building on this, hypernudging operates through continuous feedback loops that are often difficult to notice for users. These loops work by continuously collecting personal data (Yeung, 2017). Sherman (2021) adds that this is primarily done by data brokers, which are entities that gather and analyse personal information from various sources (e.g., online interactions, browsing history, online purchases, or Internet of Things (IoT) devices). They aggregate data to develop personalised user profiles, which can then be sold to third parties. Algorithmic analysis enables

predictions to be made about future online behaviours based on these profiles, allowing content and recommendations to be tailored to steer users toward specific actions (Yeung, 2017). Commercial motives primarily drive this process, as companies and websites seek to maximise user engagement and increase revenue through personalised content, dynamic pricing, and creating a sense of urgency (e.g., “only few products are left in stock”) (Lanzing, 2019). Moreover, organisations can implement hypernudging strategies that can be updated based on concurrently obtained data (Yeung, 2017). Consistent with these findings, Lanzing (2019) highlights that hypernudges can undermine user autonomy by breaching informational and decisional privacy. To conclude, hypernudging happens subtly, which makes it challenging for users to detect its influence with awareness.

However, certain online protective behaviours may reduce the influence of hypernudging. Protective behaviours refer to intentional actions individuals perform to protect their privacy, autonomy, and decision-making processes in digital environments. These include, for example, adjusting privacy settings, using privacy-enhancing tools such as ad blockers or VPNs, managing cookies and permissions, checking one’s default settings, and critically evaluating online content (Kozyreva et al., 2020). Performing these online behaviours limits the data available for hypernudging strategies and their influence (Habib et al., 2022). Protective actions are important because many user interface designs are intentionally crafted in a confusing manner to manipulate people into actions they might not take otherwise, also known as dark patterns. There are many types of dark For example, the provider can make the process of choosing for a privacy protective option time-consuming. Another example of a dark pattern is framing, which entails that a userdesign focuses on the positive aspects of a choice, while downplaying the negative aspects (Mathur et al., 2021). These patterns are often beneficial for the provider but not for the

consumer, as dark patterns can exploit cognitive biases and lead to unintended financial commitments, privacy invasions, or other adverse consequences (Luguri & Strahilevitz, 2020). Therefore, adopting protective behaviours is important to reduce the influence of hypernudging and preserve users' privacy, autonomy, and decision-making processes.

Awareness

To understand what drives individuals to adopt protective behaviours, a distinction is made between awareness and Protection Motivation Theory (PMT) factors. While awareness can influence how people perceive digital threats by knowing about hypernudging and its risks, PMT focuses more deeply on how individuals evaluate and respond to those threats through processes such as threat and coping appraisal (Rogers, 1975). In this study, awareness is treated as a distinct construct to examine whether simply being aware of hypernudging is enough to motivate individuals to adopt protective behaviour.

Interestingly, research suggests that many individuals do not fully understand that their online behaviour contributes to data collection and personalised algorithmic interventions (Morozovaite, 2022), which stresses a lack of digital awareness in users. Ferré et al. (2021) conceptualise digital awareness as an individual's consciousness of the opportunities and risks associated with information and communication technologies, including aspects like online identity, digital footprint, and data protection rights. Without this awareness, individuals may fail to recognise the effect of digital choice architectures on their decisions. This can make them susceptible to manipulation through hypernudging strategies. Thus, awareness may be an important underlying factor in adopting protective behaviours.

Supporting this, Zwilling et al. (2020) found that individuals with higher levels of cybersecurity awareness were more likely to engage in protective behaviours such as using strong passwords and antivirus software. Therefore, awareness seems to be a prerequisite for adopting protective behaviour in a broader digital context. However, it remains unclear whether these findings can be applied to the context of hypernudging, which involves more subtle manipulations.

Protection Motivation Theory

Another way to understand what motivates people to adopt protective behaviours in the context of hypernudging is Protection Motivation Theory (PMT), which may provide valuable insights (Rogers, 1975). According to PMT, individuals respond to threats through two processes: threat appraisal and coping appraisal. Threat appraisal involves assessing the severity of and vulnerability to a threat. Additionally, potential intrinsic and extrinsic rewards of not engaging in protective behaviour are taken into account. In other words, if the perceived threat is high and the rewards of inaction are low, individuals are more likely to adopt protective behaviours. Coping appraisal involves assessing one's ability to deal with a threat, a process comprising multiple components. First, response efficacy refers to the belief about the extent to which the protective behaviour will have the desired outcome. Additionally, self-efficacy refers to an individual's perceived ability to implement protective behaviours successfully. Last, response costs address the perceived disadvantages or barriers associated with adopting protective behaviours (Rogers, 1983).

In the context of hypernudging, the question remains to what extent protective behaviours are influenced by individuals' threat and coping appraisal to reduce its influence. For example,

when individuals recognise the potential risks of hypernudging and feel capable of managing their digital interactions, they are more likely to adopt protective behaviours (Liang & Xue, 2010). However, when users perceive hypernudging as inevitable or too complex to address, they may adopt a passive approach, which makes them more vulnerable to manipulation (Acquisti et al., 2015). To conclude, understanding how individuals evaluate PMT elements related to hypernudging may provide valuable insights into underlying mechanisms contributing to adopting protective behaviours.

Present Study

Despite its relevance, hypernudging remains understudied according to Morozovaite (2022). While previous studies have explored PMT and awareness in the context of cybersecurity and online privacy (Anderson & Agarwal, 2010; Ifinedo, 2012; Johnston & Warkentin, 2010), little is known about how PMT elements (e.g., perceived vulnerability, perceived severity, perceived benefits, response efficacy, self-efficacy, and perceived costs) and awareness shape protective behaviours against hypernudging. Therefore, the question of this research states: "To what extent do Protection Motivation Theory factors (e.g., perceived vulnerability, perceived severity, perceived benefits, response efficacy, self-efficacy, and perceived costs) and awareness predict adopting protective behaviour against hypernudging?"

This report first discusses the methods used to conduct the research, including participants, materials, design and procedure, and data analysis. Subsequently, the results are presented. Then, there is a discussion in which results are interpreted, conclusions are drawn, reflections are presented, and recommendations are given.

Methods

Participants

Initially, 177 participants were recruited via convenience, snowball, and voluntary response sampling. Inclusion criteria were that participants had to be above the age of 18 and sufficiently proficient in English. Exclusion criteria included participants who had not given informed consent or did not complete the survey as intended. This resulted in a final sample of 108 participants: 2 participants were excluded because they indicated that their English proficiency was poor; 46 participants were excluded because they did not finish the survey; 7 participants were excluded because they finished the survey in less than five minutes; 9 participants were excluded because they skipped questions, and 5 participants were excluded because their z-scores exceeded 3.

The final sample was (46.3% female, 51.9% male, and 1.9% other) aged between 18 and 75 years old ($M = 29.7$, $SD = 13.3$). Additionally, 97 participants were Dutch, 9 participants were German, and 2 participants had another nationality. 88 participants stated their English proficiency was good, and 20 participants stated it was sufficient. Prior to conducting the research, ethical approval was obtained from the BMS Ethics Committee on March 25, 2025 (number 250517).

Materials

The primary instrument for data collection was a self-report online survey (see Appendix B), which was administered via Qualtrics XM (https://www.qualtrics.com). The survey consisted of items adapted from previously validated questionnaires to fit the context of hypernudging. The questionnaire included eight scales: protective behaviours, awareness, perceived vulnerability,

perceived severity, perceived benefits, response efficacy, perceived costs, and self-efficacy. Items were averaged to obtain one score per construct.

Protective behaviour was initially measured by nine Likert-scale items (1 = never, 7 = once every hour) ($\alpha = 0.73$). These items included online protective behaviours to keep users' information safe (adapted from Boerman et al., 2018) and protective behaviours regarding consciously avoiding activities that enable hypernudging (Litowsky, 2023). The items were based on the following protective behaviours: (a) using an ad blocker, (b) deleting cookies and/or browser history, (c) refusing cookies when requested by websites, (d) using private mode in a browser, (e) activating the "Do Not Track" function in a browser, (f) using opt-out websites (such as www.youronlinechoices.com) to configure whether ads are based on your personal online behaviour, (g) choosing not to use services or devices that require personal data to be helpful (such as current location for Google Maps), (h) refraining from using services that rely on recommending personalised content (such as Netflix, YouTube, and Instagram), and (i) limiting the algorithm's ability to learn more about you by, for example, not hitting the like button on posts. However, item f showed extremely low variability ($M = 1.22$, $SD = 0.75$), suggesting it did not differentiate between respondents. Therefore, this item was removed from the construct ($\alpha = 0.70$). Subsequently, this item was removed from two other constructs (e.g., response efficacy and self-efficacy) to maintain cohesiveness.

Awareness was measured by six Likert-scale items (1 = strongly disagree, 7 = strongly agree), developed based on the existing literature on hypernudging by Mills (2022) and Morozovaite (2023) ($\alpha = 0.88$). An example item was: "When websites and apps ask my permission to collect personal data (e.g., cookies), I know that this can be used to influence my behaviour".

Perceived vulnerability was measured by five Likert-scale items (1 = strongly disagree, 7 = strongly agree), adapted from Liang and Xue (2010) (α = 0.89). An example was: "I believe that algorithms can easily affect my online decisions or choices".

Perceived severity was measured by seven Likert-scale items (1 = harmless, 7 = extremely devastating) and created by adapting items from Liang and Xue (2010) (α = 0.94). An example was: "Personalised content could invade my autonomy by influencing what I see or do online".

Perceived benefits was measured by three Likert-scale items (1 = strongly disagree, 7 = strongly agree) and created by adapting items from Dodge et al. (2023) (α = 0.86). An example was: "Not following privacy recommendations (e.g., using privacy tools or adjusting settings) prevents me from feeling confused or overwhelmed".

Response efficacy was initially measured by nine Likert-scale items (1 = not at all, 7 = extremely useful) based on the protective behaviours items (α = 0.83). Participants were asked to rate the degree to which they perceived the behaviours as helpful in protecting them from being influenced by hypernudging, such as: "using an ad blocker" and "limiting the algorithm's ability to learn more about you by, for example, not hitting the like button on posts". As mentioned, one item was removed to maintain parallelism (α = 0.77).

Self-efficacy was initially measured by nine Likert-scale items (1 = not at all confident, 7 = extremely confident) (α = 0.82). The items were paralleled to those of response efficacy, such as: "I feel confident that I can successfully install an ad blocker" and "I feel confident that I can limit the algorithm's ability to learn more about me by, for example, not hitting the like button on posts". As mentioned, one item was removed to maintain parallelism (α = 0.79).

Perceived costs was measured by three Likert-scale items (1 = strongly disagree, 7 = strongly agree) and created by adapting items from Liang and Xue (2010) ($\alpha = 0.84$). An example was: "Setting up and configuring privacy tools seems too complicated or time-consuming".

Design and Procedure

In this correlational study, a cross-sectional design was employed to investigate the extent to which awareness and PMT factors predict adopting protective behaviours against hypernudging, where awareness and PMT factors are the independent variables and protective behaviours the dependent variable.

The survey was distributed via a link to participants. Participants could access the survey on any internet-enabled device. The survey took approximately 15 to 20 minutes to complete. Upon clicking the survey link, participants were first presented with an informed consent form that explained the purpose of the study and that participation was voluntary and confidential (see Appendix C). After giving their informed consent, they proceeded to the survey questions.

First, demographic questions were asked about participants' gender, age, nationality, and English proficiency. Subsequently, the survey items were presented fixedly, as shown in the materials section. After completing the survey, participants were thanked.

Data Analysis

After the data was collected in the Qualtrics environment, it was prepared for further analysis. This entailed deleting irrelevant columns, outliers, and responses from participants who skipped question(s) or finished the survey in less than five minutes. All statistical analyses were

conducted using Rstudio version 4.4.0 (see Appendix D for the R script). The internal consistency was assessed by calculating Cronbach's alpha.

First, descriptive statistics were calculated to gain insight into demographic characteristics of the participants. Percentages were reported for categorical variables, including gender (male, female, other), nationality (Dutch, German, other), and English proficiency (sufficient, good). For age, the mean, standard deviation, and range were calculated to summarise participant distribution. Additionally, descriptive statistics, including means, standard deviations, and correlations, were calculated for each variable.

Then, parametric assumptions of the model were tested (see Appendix E). These included linearity, normality of residuals, homoscedasticity, absence of multicollinearity, and independence of errors. Linearity was assessed through scatterplots between each independent variable and dependent variable. Normality was checked using Q-Q plots and the Shapiro-Wilk test with a p-value greater than .05 indicating that normality is met (Shapiro & Wilk, 1965). Homoscedasticity was checked by residuals versus fitted values plots and a Breusch-Pagan test (Breusch & Pagan, 1979). Multicollinearity was tested using variance inflation factors (VIF), with values below five indicating acceptable levels. Independence was checked using a Durbin-Watson test (Durbin & Watson, 1950).

Last, multiple linear regression analysis was conducted to investigate the extent to which independent variables (e.g., awareness, perceived vulnerability, perceived severity, perceived benefits, response efficacy, self-efficacy, and perceived costs) predicted adopting protective behaviours against hypernudging. All independent variables were integrated into the regression simultaneously. Regression coefficients (β), significance levels (p-values), and 95% confidence

intervals (CIs) were calculated to assess the strength, direction, and precision of each variable's effect.

Results

Descriptive Statistics

First, descriptive statistics were performed. Interestingly, the mean of awareness was 6.35 (*SD* = .69) among participants indicating generally high levels of awareness of hypernudging. A visual representation of the distribution (see Appendix E, Figure 1) revealed a ceiling effect for the awareness construct (e.g., 7 = strongly agree), resulting in limited variability. However, the participants only scored 3.11 on protective behaviour (*SD* = .99).

Additionally, statistically significant correlations were found between protective behaviour and some predictor variables. Namely, between protective behaviour and perceived severity ($r(106) = .34$, $p < .01$), between protective behaviour and response efficacy ($r(106) = .31$, $p < .05$), and between protective behaviour perceived costs ($r(106) = -.39$, $p < .01$). However, no significant correlation was found between protective behaviour and awareness. An overview of all descriptive statistics is presented in Table 1.

Table 1

Descriptive Statistics per Variable

Variables	*M*	*SD*	2	3	4	5	6	7	8
1. Protective behaviour	3.11	.99	.28	.02	.34**	-.17	.31*	.20	-.34**
2. Awareness	6.35	.69	-	.20*	.36**	.02	.25	.19	-.23
3. Perceived vulnerability	4.33	1.23	-	-	.33**	.28**	.13	-.15	.17
4. Perceived severity	5.19	.94	-	-	-	.07	.41***	.15	-.10
5. Perceived benefits	4.31	1.27	-	-	-	-	-.18	-.23	.41***
6. Response efficacy	5.13	.81	-	-	-	-	-	.40***	-.00
7. Self-efficacy	4.94	.98	-	-	-	-	-	-	-.27*
8. Perceived costs	3.75	1.40	-	-	-	-	-	-	-

Note. $N = 108$ for all variables. *M* and *SD* represent mean and standard deviation. α = Cronbach's alpha.

* represents significance < .05.

** represents significance < .01.

*** represents significance < .001.

The Antecedents of Protective Behaviours

A multiple linear regression analysis was conducted to examine the extent to which awareness, perceived vulnerability, perceived severity, perceived benefits, response efficacy, self-efficacy, and perceived costs predicted adopting protective behaviour against hypernudging (see Table 2). The overall model was statistically significant ($F(7, 100) = 4.98$, $p < .001$) and explained approximately 26% of the variance in protective behaviour ($R^2 = .26$, adjusted $R^2 = .21$).

Among the predictors, perceived severity, response efficacy, and perceived costs were significant predictors. Specifically, perceived severity and response efficacy predicted an

increase in adopting protective behaviour. On the other hand, perceived costs predicted a decrease in adopting protective behaviour. However, awareness was not found to be a statistically significant predictor, which suggests that awareness does not influence adopting protective behaviour. Moreover, other predictors were not statistically significant either.

Table 2

Regression Coefficients for Predicting Protective Behaviour

Predictor	*B*	*SE*	*β*	*t*	*p*	95% CI
(Intercept)	.80	1.02	-	.79	.43	[-1.22, 2.82]
Awareness	.14	.14	.10	1.03	.31	[-0.13, 0.42]
Perceived vulnerability	-.03	.08	-.04	-.44	.66	[-0.19, 0.12]
Perceived severity	.23	.11	.22	2.12	-.04*	[0.02, 0.45]
Perceived benefits	-.02	.08	-.03	-.30	.77	[-0.18, 0.14]
Response efficacy	.23	.13	.19	1.78	.05*	[0.01, 0.49]
Self-efficacy	-.01	.10	-.01	-.06	.96	[-0.20, 0.19]
Perceived costs	-.19	.07	-.28	-2.68	.01**	[-0.34, -0.05]

Note. $N = 108$. All parametric assumptions for multiple linear regression were checked. Some assumptions (e.g., linearity and normality) were violated (see Appendix E). Therefore, results must be interpreted with caution.

* represents significance < .05.

** represents significance < .01.

Discussion

This study aimed to investigate the extent to which awareness and Protection Motivation Theory (PMT) factors predict adopting protective behaviours against hypernudging. The multiple linear regression model showed that perceived severity, response efficacy, and perceived

costs predicted adopting protective behaviours. Namely, individuals who were more inclined to adopt protective behaviours against hypernudging perceived it as a severe phenomenon, expected positive effects of performing protective actions, and considered the costs of doing so low. However, awareness, perceived vulnerability, perceived benefits, and self-efficacy did not predict the adoption of protective behaviour.

These findings suggest that individuals who perceive hypernudging as a severe threat and perceive performing protective behaviours to be effective are more likely to adopt protective behaviours against hypernudging. Conversely, individuals who score high on perceived costs are less inclined to adopt protective behaviours. Interestingly, awareness did not predict adopting protective behaviour. Moreover, a ceiling effect was observed on the awareness construct (see Appendix E, Figure 1), suggesting that participants generally reported high awareness of hypernudging and its potential influence on behaviour, leaving little variability in this construct to predict differences in protective behaviour. In other words, most individuals appear to be highly aware of hypernudging, but this awareness alone seems insufficient to prompt protective behaviours. Additionally, perceived vulnerability, perceived benefits, and self-efficacy alone are also insufficient to motivate individuals to adopt protective behaviours.

In relation to existing literature, these results align with research on PMT, suggesting that perceived severity and response efficacy are of importance for adopting protective behaviours in the cybersecurity context (Liang & Xue, 2010). Furthermore, the finding that scoring high on perceived costs is related to adopting less protective behaviours further supports previous findings that stress how perceived barriers lead to a decrease in protective behaviours (Acquisti et al., 2015). However, the findings regarding awareness suggesting it does not influence protective behaviour contrasts with some prior research, which suggests that awareness increases

adopting protective behaviour in online environments (Zwilling et al., 2020). While Zwilling et al. (2020) focus on rather tangible cybersecurity practices, hypernudging is a newer phenomenon in which manipulations occur subtly. Therefore, the relation between awareness and protective behaviour may not translate to the context of hypernudging. Interestingly, Morozovaite (2022) suggests that many individuals lack awareness of how their online behaviour contributes to data collection and personalised algorithmic interventions. However, the present study found a ceiling effect on the awareness construct. Nevertheless, the current findings align with the privacy paradox, which posits that individuals are concerned about their digital privacy and claim to be aware of online risks, yet do not engage in behaviours that align with these concerns (Barth & de Jong, 2017). Thus, high awareness may not translate into action, especially if individuals perceive protective behaviours as too demanding or if the threat lacks tangible consequences. This may also be the case for the other predictors that were found to have no influence.

Despite these insights, some limitations are also worth noting. First, the sample consisted predominantly of Dutch individuals. Although participants claimed their English proficiency was sufficient or good, some provided feedback that they found the questions difficult to understand. Thus, a Dutch questionnaire might have been more suitable. Second, the benefits construct was reverse-worded, which could have been confusing for some participants in hindsight. Additionally, the study relied on self-report data, which can introduce biases. This does not necessarily pose a threat to the interpretability of the findings, as the relative associations between the variables still hold. However, the absolute scores on the constructs may be over- or underestimated. Fourth, the internal consistency of protective behaviour was relatively low (Cronbach's $\alpha = .70$). Although this meets the threshold of reliability, the measure may not fully capture the protective behaviour construct. Therefore, its relation with the predictor variables

might be underestimated. Last, multiple linear regression was performed despite some parametric assumptions being violated. Subsequently, the findings of the model should be interpreted with caution.

Future research could take these limitations into account to improve reliability of the data. Additionally, this study found that the model used explained approximately a quarter of adopting protective behaviour against hypernudging. In other words, predictors other than PMT and awareness may also play a crucial role. Thus, conducting qualitative research could offer valuable insights into other underlying predictors.

These findings contribute to the research on hypernudging. Moreover, simply raising awareness about hypernudging does not translate into adopting protective behaviours against it. This insight is valuable when considering interventions aimed at protecting oneself against hypernudging, as the findings implicate that it would be more effective if the focus does not lie on raising awareness, but rather on perceived severity, response efficacy, and perceived costs. For example, privacy tools and protective measures could be made more accessible and user-friendly to reduce perceived costs.

In conclusion, this study found that perceived severity, response efficacy, and perceived costs significantly predict whether individuals adopt protective behaviours against hypernudging, whereas awareness, perceived vulnerability, perceived benefits, and self-efficacy do not. These results indicate that perceiving hypernudging as a serious threat, believing in the effectiveness of protective behaviour, and perceiving few barriers when adopting protective behaviour are crucial aspects of combating hypernudging. Although participants reported high awareness, this alone does not translate into action. Thus, addressing perceived severity, response efficacy, and

perceived costs—rather than just knowledge—is of importance when encouraging protective behaviour.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613–643. https://doi.org/10.2307/25750694

Barth, S., & De Jong, M. D. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Breusch, T. S., & Pagan, A. R. (1979). A simple test for heteroscedasticity and random coefficient variation. *Econometrica, 47*(5), 1287. https://doi.org/10.2307/1911963

Dodge, C. E., Fisk, N., Burruss, G. W., Moule, R. K., & Jaynes, C. M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy*, *22*(4), 849–868. https://doi.org/10.1111/1745-9133.12641

Durbin, J., & Watson, G. S. (1950). Testing for serial correlation in least squares regression: I. *Biometrika, 37*(3/4), 409. https://doi.org/10.2307/2332391

Ferré, R. V., Segura, J. Á. A., Pastor, C. C., Ferré, M. T. F., Villegas, E. G., & Gomez, J. M. Y. (2021). Creating digital awareness. *XV Jornadas De Ingeniería Telemática*, 105–111. https://upcommons.upc.edu/bitstream/2117/355753/1/Article_JITEL21-ENTEL-EETAC-UPC.pdf

Habib, H., Li, M., Young, E., & Cranor, L. (2022). “Okay, whatever”: An Evaluation of Cookie Consent Interfaces. *CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3491102.3501985

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549–566. https://doi.org/10.2307/25750691

Kozyreva, A., Lewandowsky, S., & Hertwig, R. (2020). Citizens versus the Internet: Confronting digital challenges with Cognitive tools. *Psychological Science in the Public Interest*, *21*(3), 103–156. https://doi.org/10.1177/1529100620946707

Lanzing, M. (2019). “Strongly recommended” Revisiting decisional privacy to judge hypernudging in Self-Tracking technologies. *Philosophy & Technology*, *32*(3), 549–568. https://doi.org/10.1007/s13347-018-0316-4

LaRose, R., Rifon, N. J., & Enbody, R. (2008). User control and information privacy: A longitudinal study of user intentions to use privacy-protective web services. Computers in Human Behavior, 24(6), 2770-2784. https://doi.org/10.1177/14614448221142799

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394–413. https://doi.org/10.17705/1jais.00232

Litowsky, Y. C. (2023). Hypernudging and Protection Motivation Theory: Investigating Awareness, Previous Protective Behaviour, and Protection Motivation [Unpublished master’s thesis]. *Universiteit Utrecht*

Luguri, J., & Strahilevitz, L. J. (2020). Shining a light on dark patterns. *The Journal of Legal Analysis*, *13*(1), 43–109. https://doi.org/10.1093/jla/laaa006

Mathur, A., Kshirsagar, M., & Mayer, J. (2021). What Makes a Dark Pattern. . . Dark? Design Attributes, Normative Considerations, and Measurement Method. *Association for Computing Machinery*, 1–18. https://doi.org/10.1145/3411764.3445610

Mills, S. (2022). Finding the 'nudge' in hypernudge. *Technology in Society*, *71*, 102-117. https://doi.org/10.1016/j.techsoc.2022.102117

Morozovaite, V. (2022). Hypernudging in the changing European regulatory landscape for digital markets. *Policy & Internet*, *15*(1), 78–99. https://doi.org/10.1002/poi3.329

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude change. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social Psychophysiology: A Sourcebook*, 153–176.

Shapiro, S. S., & Wilk, M. B. (1965). An analysis of variance test for normality (complete samples). *Biometrika, 52*(3–4), 591–611. https://doi.org/10.1093/biomet/52.3-4.591

Sherman, J. (2021). Data brokers and sensitive data on US individuals. *Duke University Technology Policy Lab.* https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf

Yeung, K. (2017). 'Hypernudge': Big Data as a mode of regulation by design. *Information Communication & Society*, *20*(1), 118–136. https://doi.org/10.1080/1369118x.2016.1186713

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Appendix A

AI Statement

During the preparation of this work, I used ChatGPT 4.0 to restructure some parts of the text and to help with coding in Rstudio. Additionally, I used Scribbr to help with generating some references. After using these tools, I thoroughly reviewed and edited the content as needed, taking full responsibility for the final outcome.

Appendix B

Survey

Thank you for taking part in our survey! Before we start, we would like to ask you a few demographic questions.

Demographics

1. What is your gender?
    a. Male
    b. Female
    c. Other
    d. Prefer not to answer
2. How old are you?
3. What is your nationality
    a. Dutch
    b. German
    c. Other
4. How proficient are you in English?
    a. Poor
    b. Sufficient
    c. Good

Now, we will move on to questions about your online behaviour and how you interact with algorithms.

Protective Behaviour

How often do you (1 = never, 2 = less than once a month, 3 = one to two times a month, 4 = once a week, 5 = several times a day, 6 = once a day, 7 = every hour):

5. Use an ad blocker?

6. Delete cookies and/or browser history?

7. Refuse cookies when requested by websites?

8. Use private mode in a browser?

9. Activate the "Do Not Track" function in a browser?

10. Use opt‑out websites (such as www.youronlinechoices.com) to configure whether ads are based on your personal online behaviour?*

11. Abstain from using services or devices that require personal data to be helpful (such as current location for Google Maps)?

12. Refrain from using services that rely on recommending personalised content (such as Netflix, YouTube, and Instagram)?

13. Limit the algorithm's ability to learn more about you by, for example, not hitting the like button on posts?

Awareness

Please indicate the extent to which you agree or disagree with the following statements (1 = strongly disagree, 7 = strongly agree).

14. I know that AI algorithms analyse my online behaviour (e.g., searches, clicks, views) to build a personal profile of me.

15. I know that every user of websites and apps such as Facebook, Netflix or Google sees different information and search results.

16. I know that the information I see on websites and apps such as Facebook, Netflix or Google has been selected specifically for me, based on information that has been collected about me (such as my age, location, online behaviour, posts liked, browsing and purchase history).

17. I know that websites and apps try to influence my online choices and behaviour with the information they offer me.

18. I know that the information I see online is constantly being adapted to the choices I make online.

19. When websites and apps ask my permission to collect personal data (e.g., cookies), I know that this can be used to influence my behaviour.

Perceived Vulnerability

Please indicate the extent to which you agree or disagree with the following statements (1 = strongly disagree, 7 = strongly agree).

20. I feel that I am at risk of being influenced by personalised content or ads online.

21. I believe that algorithms can easily affect my online decisions or choices.

22. I feel that I am often exposed to content or advertisements that are tailored to my interests, which might influence my behaviour.

23. I worry that the recommendations I see online (e.g., products, videos, news) are designed to influence my decisions without my full awareness.

24. I am susceptible to being steered by algorithmic influence into making decisions based on what they predict I will like or want.

Perceived Severity

Please indicate how harmful or serious you think the consequences of the following statements would be (1 = harmless, 7 = extremely devastating).

25. Algorithmic recommendations could manipulate my personal preferences without my knowledge.

26. Personalised content could invade my autonomy by influencing what I see or do online.

27. Personal data collected by algorithms could be misused to influence my decisions or behaviours.

28. Algorithms could track my online activities and send targeted recommendations or content to influence my actions.

29. Personal information collected by algorithms could be used in ways that I am unaware of.

30. Information gathered by algorithms could be shared with third parties to influence my online decisions.

31. Algorithms might interfere with my decision-making process by continuously presenting options that suit their agenda rather than my own.

Perceived Benefits

Please indicate the extent to which you agree or disagree with the following statements (1 = strongly disagree, 7 = strongly agree).

32. Not following privacy recommendations (e.g., using privacy tools or adjusting settings) saves me time.

33. Not following privacy recommendations (e.g., using privacy tools or adjusting settings) requires less effort and is more convenient.

34. Not following privacy recommendations (e.g., using privacy tools or adjusting settings) prevents me from feeling confused or overwhelmed.

Response Efficacy

Please indicate to what extent you think these measures are useful in protecting you from being influenced by algorithms (1 = not at all, 7 = extremely useful).

35. Using an ad blocker.

36. Deleting cookies and/or browser history.

37. Refusing cookies when requested by websites.

38. Using private mode in a browser.

39. Activating the "Do Not Track" function in a browser.

40. Using opt‑out websites (such as www.youronlinechoices.com) to configure whether ads are based on your personal online behaviour.*

41. Abstaining from using services or devices that required personal data to be helpful (such as current location for Google Maps).

42. Refraining from using services that rely on recommending personalised content (such as Netflix, YouTube, and Instagram).

43. Limiting the algorithm's ability to learn more about you by, for example, not hitting the like button on posts.

Perceived Costs

Please indicate the extent to which you agree or disagree with the following statements (1 = strongly disagree, 7 = strongly agree). 'I do not use privacy-enhancing tools (e.g., ad blockers, VPNs) because:

44. I feel that using privacy-enhancing tools would reduce the convenience or ease of my online experience.'

45. I worry that these tools might interfere with my other online activities or programs.'

46. Setting up and configuring privacy tools seems too complicated or time-consuming.

Self-Efficacy

Please indicate how confident you feel at successfully performing the following actions (1 = not at all confident, 7 = extremely confident).

47. Using an ad blocker.

48. Deleting cookies and/or browser history.

49. Refusing cookies when requested by websites.

50. Using private mode in a browser.

51. Activating the "Do Not Track" function in a browser.

52. Using opt‑out websites (such as www.youronlinechoices.com) to configure whether ads are based on your personal online behaviour.*

53. Abstaining from using services or devices that required personal data to be helpful (such as current location for Google Maps).

54. Refraining from using services that rely on recommending personalised content (such as Netflix, YouTube, and Instagram).

55. Limiting the algorithm's ability to learn more about you by, for example, not hitting the like button on posts.

We thank you for your time spent taking this survey. Your response has been recorded.

* These items were removed during the data analyses.

Appendix C

Informed Consent Form

Dear participant,

Thank you for your participation in this study! Before you give your informed consent, we ask you to read and understand the following information.

The aim of this study is to explore the role of Protection Motivation Theory (PMT) and Awareness in explaining why individuals engage in protective behaviours to safeguard their online privacy, autonomy, and decision-making against algorithmic influence. Your participation will help us understand the factors that influence individuals' protective behaviours against algorithmic influence in online environments.

If you decide to participate, you will be asked to complete an online survey. The survey will take approximately 15 to 20 minutes to complete. It will include questions about your demographic information (e.g., age, gender, nationality) as well as questions related to your online behaviours and attitudes towards privacy and algorithms.

Participation in this study is completely voluntary, and you can withdraw at any time without negative consequences or need to explain. All data collected will remain anonymous, securely stored, used solely for the purpose of this study, and will be deleted once the study is completed.

There are no significant risks associated with participation in this study. However, you may feel uncomfortable answering certain questions about your online behaviour. While there may be no direct benefit to you from participating, your participation will contribute to a greater understanding of which factors motivate people to adopt protective behaviours against algorithmic influence.

This study is conducted by Loes Elfrink, currently undergoing their Bachelor's thesis in Conflict, Risk, and Safety Psychology in the faculty of Behavioural, Management, and Social Sciences (BMS) at the University of Twente under the supervision of José Kerstholt and Peter de Vries. The research has been reviewed and approved by the BMS Ethics Committee.

If you have any questions or concerns about your rights as a research participant, or wish to discuss any aspect of this study, please contact the Secretary of the Ethics Committee of the Faculty of Behavioural, Management, and Social Sciences at the University of Twente via ethics committee-bms@utwente.nl. For further information or any questions, please feel free to reach out to Loes Elfrink at l.l.t.elfrink@student.utwente.nl.

Thank you for helping us with research!

Informed Consent

□I hereby confirm that I am at least 18 years old and have read and understood the information.My participation in this study is voluntary.

□I do not consent and will not participate in the study.

Appendix D

R Script

```
install.packages("readxl")
library(readxl)
library(tidyverse)

###Data Analysis
setwd("/Users/loes/Downloads")
data <- read_xlsx("Column.xlsx")
View(data)
numeric_col <- as.numeric(data[["1"]])
sd(data[["1"]], na.rm = TRUE)
mean(data[["1"]], na.rm = TRUE)

data <- read_xlsx("FDS.xlsx")
View(data)

#Make Numeric
data[ , 1:47] <- lapply(data[ , 1:47], function(x) as.numeric(as.character(x)))

#Constructs
data <- data %>%
  mutate(
    protective_behaviour = rowMeans(select(., starts_with("protective_behaviour")), na.rm =
TRUE),
    awareness = rowMeans(select(., starts_with("awareness")), na.rm = TRUE),
    vulnerability = rowMeans(select(., starts_with("vulnerability")), na.rm = TRUE),
    severity = rowMeans(select(., starts_with("severity")), na.rm = TRUE),
    benefits = rowMeans(select(., starts_with("benefits")), na.rm = TRUE),
    response_efficacy = rowMeans(select(., starts_with("response_efficacy")), na.rm = TRUE),
    self_efficacy = rowMeans(select(., starts_with("self_efficacy")), na.rm = TRUE),
    costs = rowMeans(select(., starts_with("costs")), na.rm = TRUE)
  )

#Outliers
variables <- c("protective_behaviour", "awareness", "vulnerability",
               "severity", "benefits", "response_efficacy",
               "self_efficacy", "costs")
z_scores <- scale(data[ , variables])
outlier_rows <- apply(abs(z_scores), 1, function(row) any(row > 3))
which(outlier_rows)

standardized_resid <- rstandard(model)
which(abs(standardized_resid) > 3)
```

```
data <- data %>%
  slice(-c(44, 54, 61, 65, 106))

###Descriptive Statistics
install.packages("psych")
library(psych)

#Means, Standard Deviations, Correlations
descriptive_stats <- data %>%
  select(protective_behaviour, awareness, vulnerability, severity, benefits, response_efficacy,
self_efficacy, costs) %>%
  psych::describe()

correlations <- corr.test(data[, variables])
print(correlations$r)
print(correlations$p)

#View
print(descriptive_stats)

#Cronbach's Alpha
alpha(select(data, starts_with("awareness")))
alpha(select(data, starts_with("vulnerability")))
alpha(select(data, starts_with("severity")))
alpha(select(data, starts_with("benefits")))
alpha(select(data, starts_with("response_efficacy")))
alpha(select(data, starts_with("self_efficacy")))
alpha(select(data, starts_with("costs")))
alpha(select(data, starts_with("protective_behaviour")))

###Parametric Assumptions
##Linearity
install.packages("ggplot2")
library(ggplot2)

#Scatterplots
predictors <- c("awareness", "vulnerability", "severity", "benefits",
                "response_efficacy", "self_efficacy", "costs")

for (var in predictors) {
  print(
    ggplot(data, aes_string(x = var, y = "protective_behaviour")) +
      geom_point(alpha = 0.6) +
      geom_smooth(method = "lm", colour = "blue") +
      labs(title = paste("Linearity Check:", var),
```

```
        x = var,
        y = "Protective Behaviour") +
    theme_minimal()
  )
}

##Normality
model <- lm(protective_behaviour ~ awareness + vulnerability + severity +
            benefits + response_efficacy + self_efficacy + costs, data = data)

#Q-Q plots
qqnorm(residuals(model), main = "Q-Q Plot of Residuals")
qqline(residuals(model), col = "red", lwd = 2)

#Shapiro-Wilk
shapiro.test(residuals(model))

##Homoscedasticity
#Residuals vs Fitted Values
plot(model, which = 1)

#Breusch-Pagan
install.packages("lmtest")
library(lmtest)

bptest(model)

##Multicollinearity
#VIF
install.packages("car")
library(car)
vif(model)

##Independence
#Durbin-Watson
dwtest(model)

###Inferential Statistics
##Multiple Linear Regression
summary(model)

data_std <- as.data.frame(lapply(data, scale))
model_std <- lm(protective_behaviour ~ awareness + vulnerability + severity + benefits +
response_efficacy + self_efficacy + costs, data = data_std)

#Standardised Coefficients
```

```
standardized_coefficients <- summary(model_std)$coefficients[, "Estimate"]
print(standardized_coefficients)

#Confidence Intervals
confint(model)

data <- read_xlsx("DSthesis.xlsx")
View(data)

###Demographics
#Gender
table(data$gender)
prop.table(table(data$gender))

#Nationality
table(data$nationality)
prop.table(table(data$nationality))

#English
table(data$english)
prop.table(table(data$english))

#Age
summary(data$age)
sd(data$age)
mean(data$age)
```

Appendix E

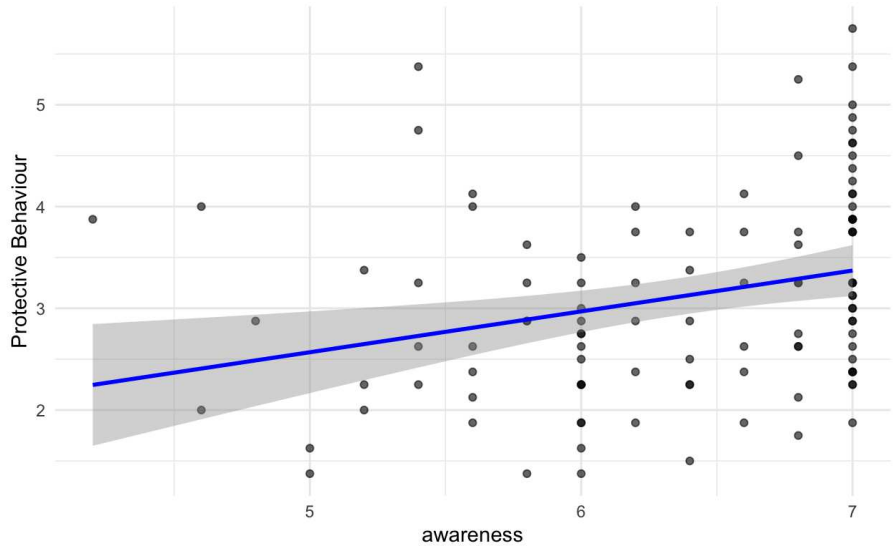
Parametric Assumptions

Linearity

First, it was assessed whether a linear relationship existed by examining scatterplots of each independent variable against protective behaviour. The plots suggested a positive linear relationship between awareness and protective behaviour (see Figure 1), perceived severity and protective behaviour (see Figure 2), response efficacy and protective behaviour (see Figure 3), and self-efficacy and protective behaviour (see Figure 4). A negative linear relationship was found for perceived costs (see Figure 5). However, there was no linear relationship between perceived vulnerability and protective behaviour (see Figure 6), and perceived benefits and protective behaviour (see Figure 7). Therefore, the assumption of linearity was rejected.

Figure 1

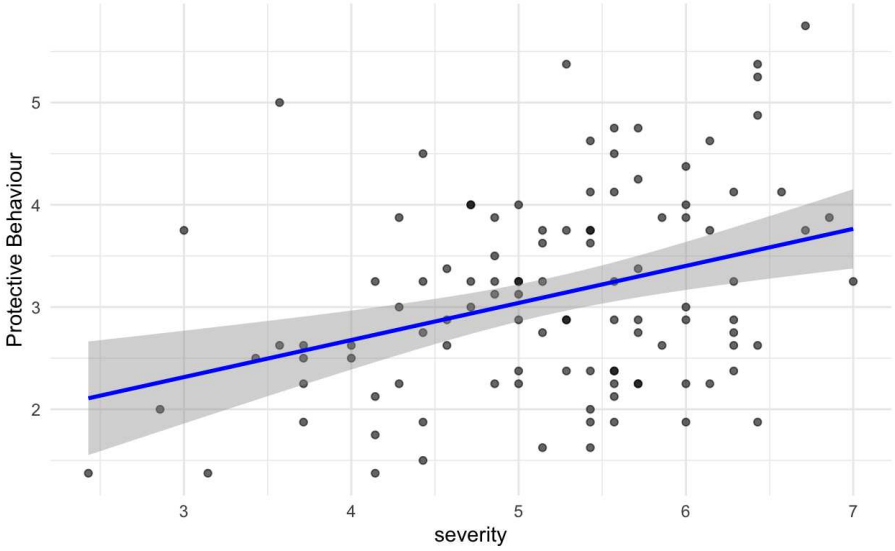
Relationship between Awareness and Protective Behaviour



Note. The dots represent individual participant scores.

Figure 2

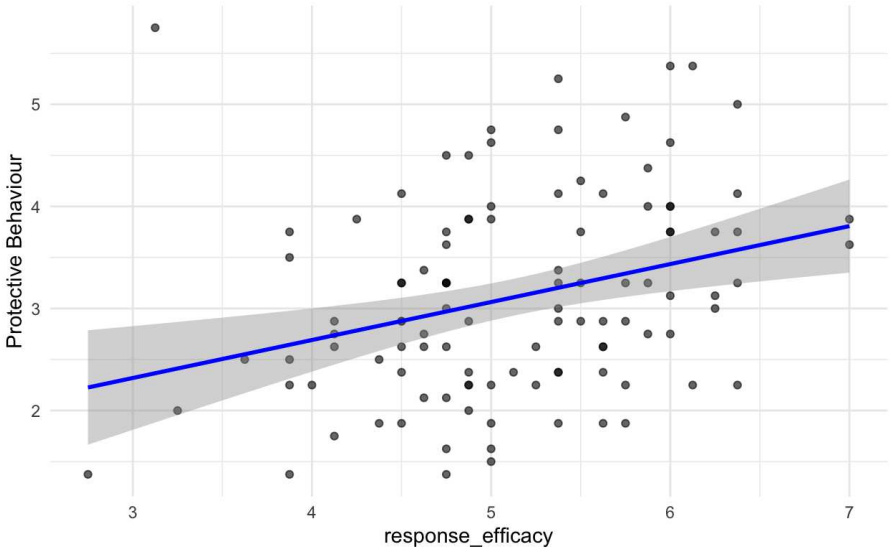
Relationship between Perceived Severity and Protective Behaviour



Note. The dots represent individual participant scores.

Figure 3

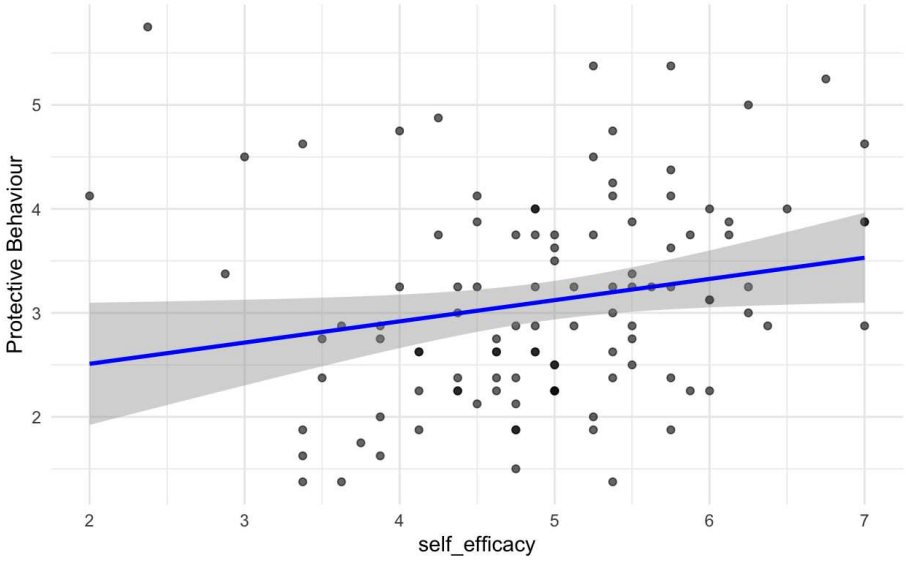
Relationship between Response Efficacy and Protective Behaviour



Note. The dots represent individual participant scores.

Figure 4

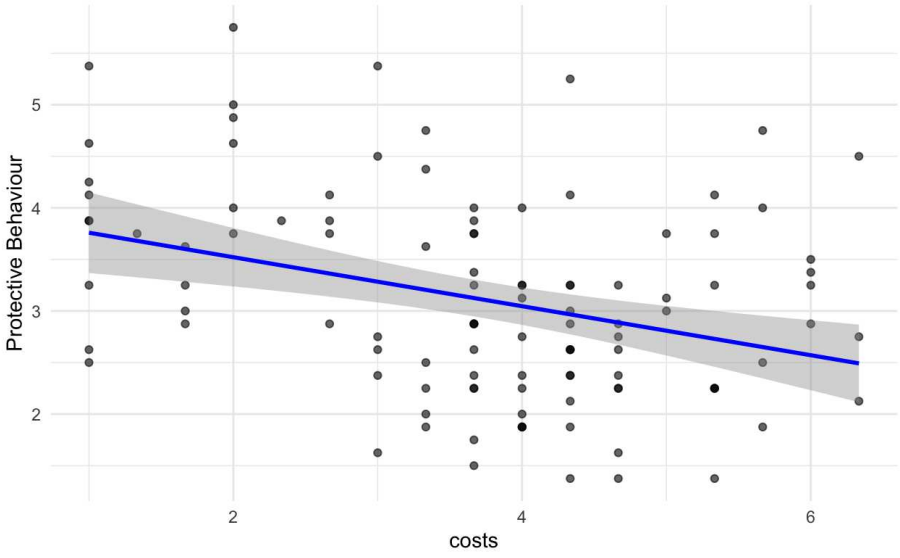
Relationship between Self-Efficacy and Protective Behaviour



Note. The dots represent individual participant scores.

Figure 5

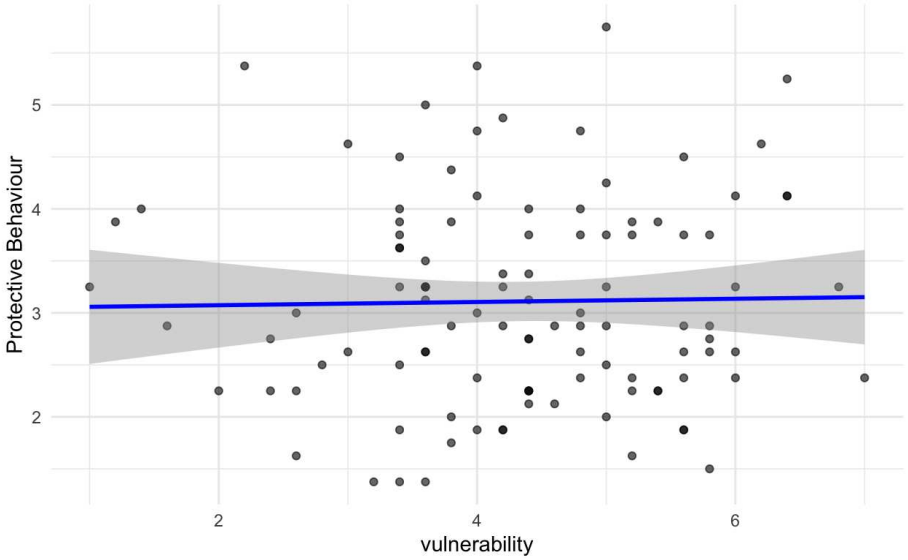
Relationship between Perceived Costs and Protective Behaviour



Note. The dots represent individual participant scores.

Figure 6

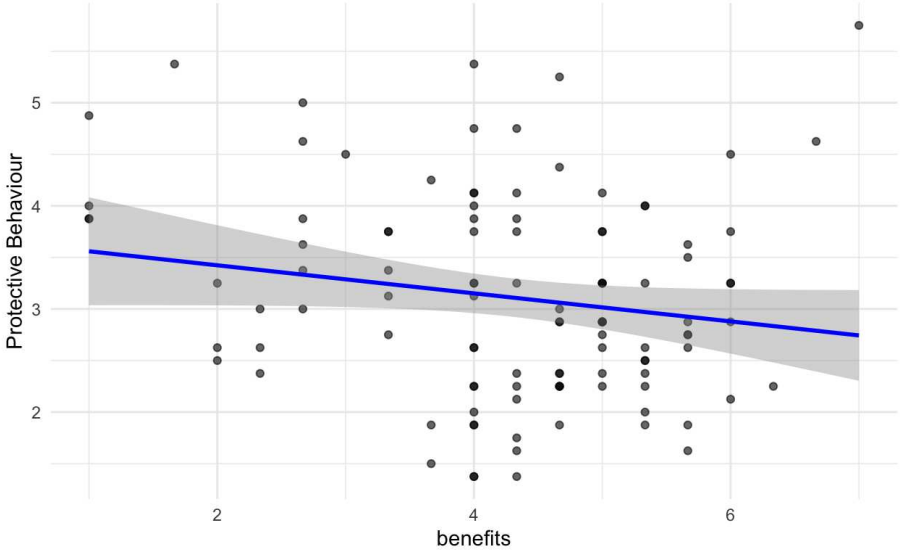
Relationship between Perceived Vulnerability and Protective Behaviour



Note. The dots represent individual participant scores.

Figure 7

Relationship between Perceived Benefits and Protective Behaviour



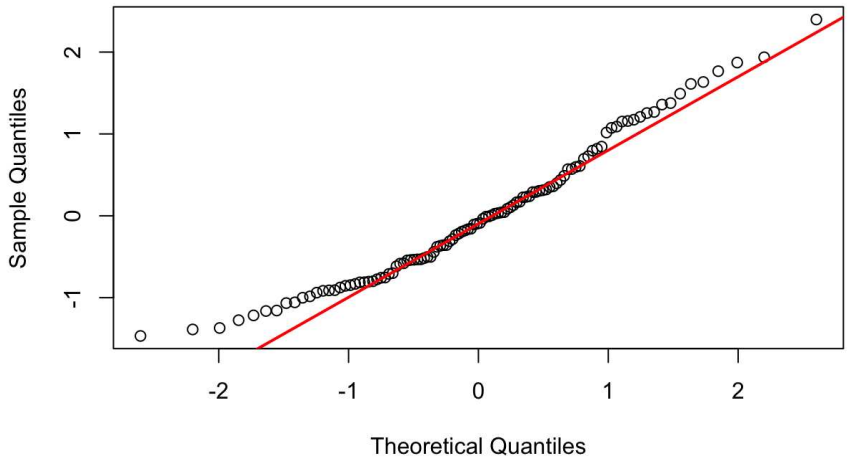
Note. The dots represent individual participant scores.

Normality

First, a Q-Q plot was created to test the normality of residuals assumption (see Figure 8). This showed a moderate deviation from normality in the tails. Additionally, a Shapiro-Wilk test (Shapiro & Wilk, 1965) was conducted to assess the distribution of the data for the variables. The results indicated that the data significantly deviated from normality ($W = 0.966$, $p < .05$). Therefore, the assumption of normality was rejected.

Figure 8

Q-Q Plot of Residuals



Note. The dots represent unstandardised residuals from a multiple linear regression model. The tails show moderate deviation from the reference line.

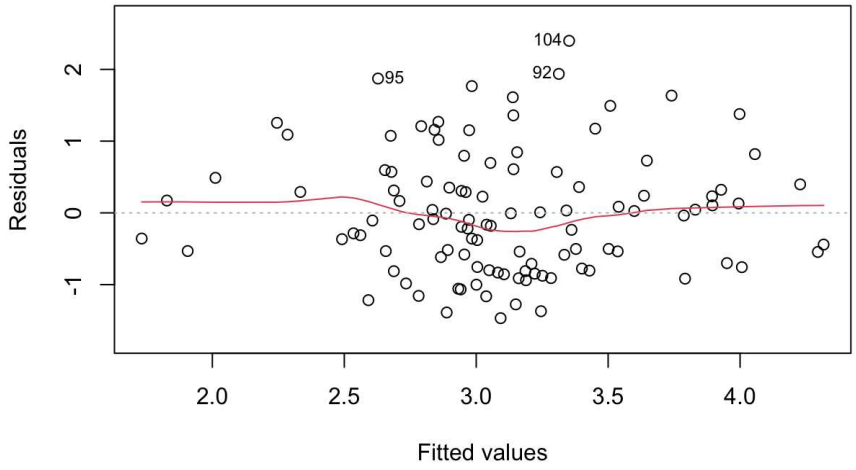
Homoscedasticity

To check the homoscedasticity of the regression model, a plot for the residuals against the fitted values was created (see Figure 9). The residuals appeared randomly scattered around zero. Additionally, a Breusch-Pagan test was performed (Breusch & Pagan, 1979). The t-statistic was

found to be $X^2(7) = 11.08$, and $p = .14$. This indicated that there was no significant heteroscedasticity. Therefore, the assumption of homoscedasticity was met.

Figure 9

Homoscedasticity of the Regression Model



Note. The circles represent the standardised residuals plotted against the fitted values. The red line indicates a LOESS smooth.

Multicollinearity

Then, the multicollinearity assumption was checked using VIFs. The results were the following: 1.27 for awareness, 1.31 for perceived vulnerability, 1.46 for perceived severity, 1.42 for perceived benefits, 1.55 for response efficacy, 1.33 for self-efficacy, and 1.42 for perceived costs. All values are below five, indicating no problematic multicollinearity. Therefore, the multicollinearity assumption was met.

Independence

Last, a Durbin-Watson test was conducted to assess the independence of residuals. The test was not significant, $DW = 2.26$, $p = .92$. This indicated that there was no significant autocorrelation for the model (Durbin & Watson, 1950). Therefore, the assumption of independence of errors was met.