Smart Device, Smart Security? Antecedents of Smart Device Security Behaviour and Future Intentions

Michelle Walterscheid, *University of Twente* Nicole Huijts, *University of Twente*
Jeroen van der Ham – de Vos, *University of Twente* Mariëlle Stel, *University of Twente*

Abstract

This study explores which psychological factors hinder or facilitate users' past security behaviours towards smart devices (i.e. smart speakers or smart doorbells), as well as their future intentions to secure their smart devices further. Using online surveys, data was collected in three Western-European countries: the Netherlands, Germany, and the UK. Initial analyses showed that being a primary user, subjective knowledge, self-efficacy and objective knowledge positively affected past security behaviour across most countries and devices. For future intentions, perceived severity, perceived vulnerability, subjective norms and response efficacy had a positive effect while response cost had a negative effect. Our findings are informative for future interventions aiming to raise users' willingness to secure their devices, giving insights into which factors to facilitate and which to hinder.

1. Introduction

Each year the number of homes with smart devices increases as their affordability and usability rises. In Europe alone, there were approximately 200.7 million smart homes in 2023, and this number is forecast to increase to 300.9 million by 2029 [9]. However, with the number of smart homes rising, the prevalence of cyberattacks is also likely to rise. Once devices are compromised they can endanger both safety and privacy of a household. Data can be stolen and abused for identity theft and blackmail [1, 11], devices can be taken over to be used for DDoSing attacks [10], to spy on users [12], and potentially even be overheated to start a fire [2, 4]. Luckily, the more severe cases have only been observed in case studies for now [1], and there is a range of protective actions that users can take, such as using a strong and unique password or limiting the devices' connection to the internet [6]. However, recent findings imply that users do little to protect themselves, increasing the likelihood of successful attacks [5]. It is somewhat unclear what factors could support or undermine users' willingness to take action to protect themselves. Recent studies suggest that variables included in the protection motivation theory (PMT) such as perceived severity, self-efficacy and response costs affect intentions to secure smart devices [3, 7, 8]. However, what roles other factors outside this model, such as trust and knowledge, could play is less known. Thus, we aim to construct and test a framework using the PMT as a basis, and extending it with relevant factors that determine users' willingness to take security measures. After an extensive literature search, we propose to examine the following constructs as predictors of protective action and future intentions: perceived vulnerability, perceived severity, perceived benefits, self-efficacy, response efficacy, response costs, social norms (i.e. descriptive norms and subjective norms), trust in the manufacturer, subjective knowledge, objective knowledge and user type. The purpose of this report is to get a comprehensive overview of factors that either support or negate security behaviour towards smart speakers and smart doorbells both in the past and in the future via an online survey, distributed among residents of Germany, the Netherlands and the UK. Thus our study had the following research question:

RQ1: Which factors facilitate or hinder past security behaviours and future intentions to secure smart speakers and smart doorbells?

2. Methods

We focused on users of online recruitment panels (i.e. Panelclix for the Dutch sample, Prolific for the UK sample, and Norstat for the German sample). Participants were compensated in line with the standard reimbursement policies of the respective recruitment panels, resulting in payments ranging from 1.00 € to 1.70€. In total, 2390 participants were recruited 795 from the Netherlands, 792 from Germany and 803 from the UK.

A cross-sectional survey design was used with perceived severity, perceived vulnerability, perceived benefits, self-efficacy, response-efficacy, response costs, objective knowledge, subjective knowledge, descriptive norms, subjective norms, trust in the manufacturer, and user type being predictors. Past security behaviour and future intentions were dependent variables.

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2026. August 23–26, 2026, Hannover, Germany.

The scales measuring the variables were either self made (i.e. objective knowledge, past security behaviour, future intentions) or adapted from existing works by rephrasing the items to fit into the smart device context [13, 14, 15, 16, 17]. All scales except objective knowledge and past security behaviour were measured on a 7-point Likert scale (1 = strongly disagree – 7 = strongly agree). Objective knowledge was measured with two scales, a dummy scale (1 = correct, 0 = incorrect) and a 6-point Likert confidence scale (1 = very unconfident (or just guessing) – 6 = very confident). If the participants answer was correct (correct = 1) and given with confidence (3 = a little confident – 6 = very confident), one point was added to the knowledge score, which has a possible maximum score of 25 points. Past security behaviour had the options "yes" = 1, "No" = 2, "Unsure" = 3, and smart doorbell users had an additional fourth option "Not applicable for my smart doorbell" = 4, since smart doorbells differ per brand and certain actions may not be possible (e.g. no account needed to operate the doorbell, hence no password can be created). Options 3 and 4 were treated equivalent to a "No" answer. One point was added to the security behaviour score, for each "yes" answer, and the possible maximum score was eight.

In total, 12 linear regression models were run. The models cover each country (UK, Netherlands, Germany), each device (smart speakers and smart doorbells), and both past security behaviour and future intentions to secure. The study was approved by the Utwente BMS ethics committee (review application nr. 252041)

3. Results

3.1 Past security behaviour

For past security behaviour, subjective knowledge was a significant positive predictor for all countries for smart speakers and self-efficacy was a significant positive predictor for all countries for smart doorbells (see Appendix A). Furthermore, being the primary user and objective Knowledge was a significant predictor for both Dutch and Germans for both smart devices. Subjective knowledge and being the primary user tended to be the strongest predictors for past security actions, while there is no consistent weakest predictor across countries or devices.

3.2 Future intention

For future intention Perceived severity, and subjective norms were significant positive predictors across countries for smart speakers (see Appendix A). Response cost was a significant negative predictor for both the UK and the Netherlands across smart devices. For smart speakers subjective norms tend to be the strongest positive predictor, while for smart doorbells it tends to be perceived severity.

4. Discussion

Our findings provide input to future interventions, specifically what factors should be focused on in order to increase the likelihood of users securing their devices. We would recommend emphasizing the severity of the consequences of compromised devices and the likelihood of this occurring. It also seems important that interventions help users feel confident in taking security measures. Furthermore, interventions could emphasize the ease of performing certain security measures, for example, creating a strong password is a one and done measure, to reduce perceived costs. Additionally, people should also be made aware of the effectiveness of the security measures. Subjective norm has also been found to be an important factor, one could attempt to increase the perception that people in general think it is important to secure smart devices due to their security and privacy issues. It should also be kept in mind that it is mainly the primary user who is responsible for the device and capable of making changes. Thus, secondary users would require a different approach as they would either have to convince the primary user of taking these actions or arrange access for themselves. To summarize, in order to encourage users to take security actions for their devices, it is important that they feel knowledgeable and capable enough to take actions and it is also important to increase perceptions of severity and likelihood of cyberattacks and to reduce the apparent cost of such actions by emphasizing that they require little time and effort.

5. Conclusion

This study examined factors influencing smart device security behaviour and future intentions to secure smart devices across three western European countries. We found that the most common and strongest predictors of past security behaviour across most countries are user type, subjective knowledge, objective knowledge and self-efficacy, in other words, knowledge about smart home cybersecurity and about taking protective actions and confidence in that knowledge most strongly predict past security measures. For future intentions perceived severity, perceived vulnerability, response efficacy, subjective norms and response costs play the more important role. Thus, interventions should aim to increase perceptions of danger and reduce perceived effort tied to taking protective measures.

Acknowledgements

This study was funded by the Dutch Institute for Vulnerability Disclosure (DIVD).

References

[1] John M. Blythe and Shane D. Johnson. A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal*, 34(1):97–125, 2021.

[2] Yuxin Chen and Bo Luo. S2A: secure smart household appliances. in P*roceedings of the second ACM conference on Data and Application Security and Privacy*, pages 217–228, 2012.

[3] Marc Dupuis and Mercy Ebenezer. Help Wanted: Consumer privacy behavior and smart home internet of things (iot) devices. in *Proceedings of the 19th Annual SIG Conference on Information Technology Education*, pages 117–122, 2018.

[4] Julie Greensmith. Securing the Internet of Things with Responsive Artificial Immune Systems. in *Proceedings of the 2015 Annual Conference on Genetic and Evolutionary Computation*, pages 113–120, 2015.

[5] Julie M. Haney, Susanne M. Furman, and Yasemin Acar. Smart Home Security and Privacy Mitigations: Consumer Perceptions, Practices, and Challenges. in *International Conference on Human-Computer Interaction,* pages 393–411, 2020.

[6] Anna Lenhart, Sunyup Park, Michael Zimmer, and Jessica Vitak. You Shouldn't Need to Share Your Data': Perceived Privacy Risks and Mitigation Strategies Among Privacy-Conscious Smart Home Power Users. *Proceedings of the ACM on Human-Computer Interaction*, *7*(CSCW2), pages 1–34, 2023.

[7] Alaa Nehme and Joey F. George. Approaching IT Security & Avoiding Threats in the Smart Home Context. *Journal of Management Information Systems,* 39(4):1184–1214, 2022.

[8] Sarah Prange, Ceenu George, and Florian Alt. Design Considerations for Usable Authentication in Smart Homes, in *Proceedings of Mensch und Computer 2021*. pages 311–324, 2021.

[9] Statista. Smart home: market & analysis, 2024.

[10] Bhagyashri Tushir, Hetesh Sehgal, Rohan Nair, Behnam Dezfouli, and Yuhong Liu. The Impact of DoS Attacks onResource-constrained IoT Devices:A Study on the Mirai Attack. *arXiv preprint arXiv:2104.09041,* 2021.

[11] Roey Tzezana. Scenarios for crime and terrorist attacks using the internet of things. *European Journal of Futures Research*, 4(1):18, 2016.

[12] Roey Tzezana. High-probability and wild-card scenarios for future crimes and terror attacks using the Internet of Things. *foresight*, 19(1):1–14, 2017.

[13] Alaa Nehme & Joey F. George. Approaching IT security & avoiding threats in the smart home context. *Journal of Management Information Systems*, 39(4):1184-1214, 2022.

[14] Xuequn Wang, Tanya J. McGill, & Jane E. Klobas. I want it anyway: Consumer perceptions of smart home devices. *Journal of Computer Information Systems,* 60(5):437–447, 2020.

[15] Hee S. Park & Sandi W. Smith. Distinctiveness and influence of subjective norms, personal descriptive and injunctive norms, and societal descriptive and injunctive norms on behavioral intent: A case of two behaviors critical to organ donation. *Human Communication Research,* 33(2):194-218. 2007.

[16] Catherine L. Anderson & Ritu Agarwal. Practicing Safe Computing: a Multimethod Empirical Examination of Home Computer User Security Behavioural Intentions1. *MIS quarterly*, 34(3):613-643, 2010.

[17] Lies De Kimpe, Michel Walrave, Pieter Verdegem, & Koen Ponnet. What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology,* 41(8): 1796-1808, 2022.

A Appendix

Table 1: Linear regression models of all predictors of past security behaviour, split by smart device type (i.e. smart speaker and smart doorbell) and by country i.e. UK (N =803), NL (N =795), GER (N =792)

	UK			NL			GER		
Smart speaker	*ß*	*SE*	*p*	*ß*	*SE*	*p*	*ß*	*SE*	*p*
Perceived severity	.04	.07	.429	.02	.10	.657	-.00	.08	.942
Perceived vulnerability	-.00	.09	.923	-.01	.10	.801	-.05	.10	.286
Perceived benefit	.03	.10	.450	.04	.10	.375	.04	.10	.385
Self-efficacy	.09	.13	.175	**.20**	**.12**	**.005**	**.15**	**.09**	**.013**
Response efficacy	-.01	.13	.800	-.07	.14	.233	.06	.12	.263
Response cost	**-.19**	**.08**	**.001**	-.04	.09	.377	.02	.09	.720
Descriptive norm	-.02	.09	.698	.03	.11	.560	.07	.10	.119
Subjective norm	.05	.08	.355	.09	.10	.090	.09	.09	.107
Objective knowledge	.06	.02	.255	**.14**	**.02**	**.004**	**.23**	**.02**	**.001**
Subjective knowledge	**.35**	**.10**	**.001**	**.26**	**.11**	**.001**	**.25**	**.10**	**.001**
Trust in manufacturer	.06	.10	.235	.01	.12	.761	.00	.11	.962
User type (primary)	.26	.31	.100	**.47**	**.38**	**.007**	**.33**	**.26**	**.007**
Smart doorbell	*ß*	*SE*	*p*	*ß*	*SE*	*p*	*ß*	*SE*	*p*
Perceived severity	.00	.07	.997	.01	.09	.934	**.13**	**.07**	**.007**
Perceived vulnerability	-.01	.08	.794	-.01	.10	.791	-.09	.09	.595
Perceived benefit	.07	.12	.120	.02	.12	.726	-.03	.11	.511
Self-efficacy	**.16**	**.09**	**.006**	**.20**	**.12**	**.003**	**.14**	**.10**	**.032**
Response efficacy	-.05	.12	.315	**.12**	**.13**	**.028**	.11	.12	.058
Response cost	-.09	.08	.055	-.00	.09	.852	.09	.09	.082
Descriptive norm	.03	.09	.570	.04	.12	.434	.10	.10	.053
Subjective norm	**.16**	**.08**	**.003**	**.12**	**.10**	**.026**	.06	.08	.275
Objective knowledge	.05	.02	.276	**.15**	**.02**	**.002**	**.22**	**.02**	**.001**
Subjective knowledge	**.24**	**.09**	**.001**	.12	.11	.052	**.21**	**.10**	**.001**
Trust in manufacturer	-.04	.09	.381	**.11**	**.12**	**.018**	.00	.10	.899
User type (primary)	-.05	.40	.205	**.84**	**.49**	**.001**	**.34**	**.31**	**.029**

Note. *Significant effects are in bold*

Table 2: Linear regression models of all predictors of future intention, split by smart device type (i.e. smart speaker and smart doorbell) and by country i.e. UK (N =803), NL (N =795), GER (N =792)

	UK			NL			GER		
Smart speaker	*ß*	*SE*	*p*	*ß*	*SE*	*p*	*ß*	*SE*	*p*
Perceived severity	**.17**	**.06**	**.001**	**.14**	**.07**	**.001**	**.19**	**.06**	**.001**
Perceived vulnerability	**.14**	**.07**	**.010**	.00	.07	.984	.08	.07	.127
Perceived benefit	**.12**	**.08**	**.026**	.07	.07	.182	.05	.08	.323
Self-efficacy	-.00	.09	.915	.09	.09	.233	**-.19**	**.07**	**.002**
Response efficacy	**.13**	**.10**	**.043**	**.17**	**.10**	**.006**	.09	.10	.080
Response cost	**-.14**	**.07**	**.011**	**-.13**	**.07**	**010**	-.10	.08	.055
Descriptive norm	.05	.07	.411	.01	.08	.770	.04	.08	.475
Subjective norm	**.12**	**.06**	**.032**	**.20**	**.07**	**.001**	**.26**	**.07**	**.001**
Objective knowledge	.02	.01	.709	.01	.01	.839	.10	.08	.058
Subjective knowledge	-.06	.08	.388	.05	.08	.439	.12	.08	.055
Trust in manufacturer	**-.12**	**.08**	**.039**	.09	.08	.081	.06	.08	.274
User type (primary)	.10	.25	.583	.16	.27	.400	.10	.20	.463
Smart doorbell	*ß*	*SE*	*p*	*ß*	*SE*	*p*	*ß*	*SE*	*p*
Perceived severity	**.21**	**.05**	**.001**	.09	.07	.074	**.24**	**.06**	**.001**
Perceived vulnerability	**.15**	**.06**	**.001**	**.12**	**.08**	**.021**	.07	.08	.170
Perceived benefit	**.15**	**.09**	**.002**	-.00	.09	.887	.00	.10	.964
Self-efficacy	.09	.07	.159	-.08	.09	.393	.00	.09	.937
Response efficacy	.06	.09	.300	**.23**	**.10**	**.001**	**.13**	**.10**	**.035**
Response cost	**-.13**	**.06**	**.011**	**-.14**	**.07**	**.005**	-.05	.09	.381
Descriptive norm	.10	.07	.100	.08	.09	.138	.05	.10	.379
Subjective norm	**.12**	**.06**	**.038**	**.16**	**.07**	**.007**	.09	.07	.124
Objective knowledge	.04	.01	.368	.09	.01	.091	-.02	.01	.670
Subjective knowledge	-.11	.07	.080	-.07	.08	.263	.11	.08	.102
Trust in manufacturer	.04	.07	.418	-.06	.09	.211	.00	.09	.993
User type (primary)	-.01	.32	.961	.26	.38	.310	-.05	.28	.749

Note. *Significant effects are in bold*