National Cyber Security Centre
*Ministry of Justice and Security*

# Security by Behavioural Design:

## A Feasibility Study

**Report for NCSC-NL**

Dr. Tommy van Steen

Dr. Els De Busser

Institute of Security and Global Affairs

Leiden University

The Netherlands

# Table of contents

# Background

To improve end-user behaviour, many organisations turn to awareness campaigns or training initiatives. The first uses posters, flyers, slogans and other types of communication to share the importance of cybersecurity with employees. However, the effectiveness of such campaigns is unknown (van Steen et al., 2020). Training end-users can be effective, but not all behaviours require extensive skills. One other method to improve end-users' behaviour is to design software in such a way that end-users are more likely to behave in a secure fashion.

This approach, which we call "Security by Behavioural Design" (van Steen & De Busser, 2021), uses techniques from the nudging literature (Thaler & Sunstein, 2009; van Steen, 2022) to improve the cybersecurity behaviour of end-users. Thaler and Sunstein (2009, p.8) define nudging as "any aspect of the choice architecture that alters people's behaviour in a predicable way without forbidding any options or significantly changing their economic incentives". This means that the way choices are presented, worded, or even completely removed, can influence the choices people make and therefore improve cybersecurity within organisations.

Security by behavioural design adopts these principles to present end-users with security options in such a way that they are more likely to choose the secure alternative over a riskier one. For example, people could be shown a set of options where the secure and therefore preferred option is the default, as inertia can cause end-users to stick to that default option instead of changing their settings. Other methods include highlighting the behaviour of peers, which makes people more likely to act in a similar fashion, a concept known as social proof (see for instance Das et al., 2014), and considering which options are available in the first place can also affect the behaviour of end-users, with Facebook offering a like-button, but not a dislike-button being a famous example of such an approach. How software is designed, and the lay-out and options presented in the user interface, can then be a tool to improve security-related behaviours. Compared to simply blocking certain options or actions, known as 'techno-regulation' or 'affordances' (Lessig, 2008; Norman, 2013), the use of security by behavioural design allows for more freedom on the part of the end-user to act in their desired manner. This can be of importance to reduce the risk of end-users turning to shadow security practices, the use of unauthorised workarounds (Kirlappos et al., 2014), to retain their productivity.

In a previous project for NCSC-NL, we mapped the studies that investigated the effectiveness of security by behavioural design principles. These studies suggest that cybersecurity behaviour of end-users can be substantially improved by tweaking the design of the software they interact with (van Steen & De Busser, 2021). While these studies covered a range of cybersecurity behaviours, most tended to focus on privacy settings and creating strong(er) passwords. The findings suggest that both privacy and password strength can be improved when applying security by behavioural design principles when designing new software solutions, while other behaviours might require more research before robust conclusions can be drawn. What these studies have in common, is that they were mostly conducted by scientists in artificial settings, such as mock-ups of privacy setting screens for a hypothetical social media platform (Cho et al., 2019; Wang et al., 2014), or screens where people could create a password with the help of nudges to increase password strength (Peer et al., 2020). These settings are useful for determining a proof of concept and eliminating other factors that might affect the decision-making process of end-users, resulting in stronger evidence for the mechanism that is tested, i.e., the influence of the new design principles on security behaviour. To determine the effectiveness in a real-world setting, more advanced testing would be required. Ideally, these principles should be included in a software design cycle, where the effectiveness is investigated using A/B tests with either a specific test population, or a larger set of end-users.

Alongside a real-world test of the effectiveness of these initiatives,

there is also a need to investigate the feasibility of implementing these solutions in practice. Do organisations see the benefits of using security by behavioural design principles in their software design cycle? Do they have the expertise to implement these solutions? And how would this work when the software is not developed in house but purchased from an external vendor? The solutions as outlined in the previous report might prove to be successful, but if the implementation is not supported within the organisation, for example because required tools are not available, the real-world success is expected to be minimal. Therefore, the goal of this project is to investigate the feasibility of implementing security by behavioural design principles in the design of software within Dutch organisations.

The research question we aim to answer is threefold:

1. Do organisations view security by behavioural design as a promising avenue that should be explored?
2. To what extent are security by behavioural design principles currently used in the development of new software?
3. Wat is needed to implement these principles in the software design cycle?

# Methods

## Research design

To investigate the feasibility of implementing security by behavioural design principles in Dutch organisations, we conducted a series of interviews with practitioners within the Netherlands. The aim of the interviews was to investigate the current practices relating to improving end-user cybersecurity behaviour, with a specific focus on the development and/or adjustment of software to support secure behaviour. The interviews were analysed in line with the set-up of the questions, and contrasted between types of respondents where relevant. To preserve anonymity, no recordings of the interviews were made and no participants are quoted literally in the report.

## Participants

The participants were recruited through the network of the NCSC and the researchers involved in the project, and in one case through a recommendation by one of the interviewees. Often, a gatekeeper within an organisation was approached to access relevant participants. These gatekeepers helped us getting to the right people within the organisation, and were our first point of contact in the respective organisations. Prospective participants were informed about the principle of security by behavioural design and our interest in interviewing them in relation to their experiences with this approach. If prospective participants showed interest in taking part, an interview was planned. In case of a non-response after an initial show of interest, prospective participants were contacted a second time. When again no response was received, they were considered to have declined to take part.

We conducted 9 interviews. In two cases, participants preferred to take part in the interview with a colleague, leading to a total of 11 participants in the interviews. Participants were assured of their anonymity, took part voluntarily and could stop at any time. All interviews were conducted online, using Microsoft Teams and lasted between 45 minutes and 1 hour. To preserve the anonymity of the participants, no job roles or organisations are mentioned in the report. However, in broad terms, the participants can be categorised into three categories: 1) people who work or advise on the technical development of software, 2) people who have the responsibility to acquire relevant software for their organisation, where vendors present their proposed software for specific purposes, and 3) people who work on the topic of end-user behaviour. This last category included behavioural change specialists who work on compliance and security related topics, as well as user experience (UX) experts. Most participants worked on software and systems designed for internal use by colleagues and not for external use by clients or customers. This is noteworthy, as internal software and systems can be designed in a way that might require training or some information on how to operate the system, while external faced software for clients or consumers would need to be more fool proof and intuitive by nature to avoid end-users moving to another platform for their activity.

## Interview questions

The interviews were organised as semi-structured interviews. This form of interviewing allowed us to structure the interviews broadly, while allowing for flexibility if a participant brought up something we would like to know more about, or when a specific participant might not be knowledgeable on aspects of the interview questions so that some questions could be skipped over if necessary. The set of interview questions were designed by the researchers, with feedback and proposed adjustments by NCSC staff before the data collection commenced. The questions concerned the ways in which organisations might currently use security by behavioural design principles to guide their software design. This included questions around whether or not they were implementing these methods already, where in the design process these principles would fit best, who is responsible for the implementation and whether they have the expertise to implement these solutions successfully. The full set of interview questions can be found in Appendix A.

# Results

## General views on security by behavioural design

All interviewees expressed a positive attitude towards using security by behavioural design to improve the cybersecurity behaviour of end-users. Overall, they suggested that beyond the technical aspects of cybersecurity, adding more focus on the human factor would be beneficial. This view is gaining ground across organisations, and suggests that they are moving towards a more holistic approach of cybersecurity instead of a purely technical one. Several interviewees explicitly mentioned that a focus on technical cybersecurity is too narrow when attempting to protect an organisation. When asked what organisations do to improve the security behaviour of end-users, respondents focused mostly on initiatives such as awareness campaigns and cybersecurity training. Altering the interface of the software was mentioned less often, but when asked specifically, respondents believed that this could be a suitable method to improve cybersecurity behaviours.

## Important factors in addressing the human factor in cybersecurity

The participants expressed various views on what they considered to be factors of importance when addressing the human factor in cybersecurity, in other words, which factors did they deem to be important to successfully improve the cybersecurity behaviour of end-users? The expressed sentiments related to three factors: ease of use, skilled end-users and access management. First, the respondents suggested that if the secure behaviour is easy to perform, end-users are more likely to behave securely. They believe that the more complicated the security procedure is, the less likely people will be to adhere to every security step posed by policy or organisational practices. Ease of use is also an aspect in the technology acceptance model (Davis 1989), which describes what people need in order to adopt new technologies. Davis (1989) argues that the easier the technology is to use, the more likely people are to use it. In this, the respondents' views and the insights from the scientific literature align.

Second, several respondents noted that it is important to enhance the cybersecurity skills of end-users, so that it is not merely the IT department that is cyber savvy, but that end-users can weigh the various options they have in how to perform tasks, and are able to choose the secure method over a less secure alternative. Making use of the knowledge and skills of end-users, instead of merely deciding top-down what is required, is likely to result in practices that balance the need for security with the need for productivity. Participants see this as a promising solution and believe that (additional) training is essential to establish the required level of cybersecurity knowledge and skills. This also suggests that participants realise that merely making end-users aware of cyber risks is not sufficient to change behaviour, but that skills are playing a vital part.

The third aspect that was mentioned by some participants suggested that security by behavioural design could help in setting standards for access management. In several organisations, job hopping within the organisation resulted in some employees having built up a large set of access rights due to the various roles they have or have had in the past. Using security by behavioural design to limit the access of end-users was seen as a viable solution by participants. Managing access rights usually entails setting defaults in which access rights should be granted based on a job role, or automate the revocation of certain access rights after a specified amount of time has passed since leaving the department, and can be considered part of the governance of an organisations' cybersecurity. However, participants suggest that security by behavioural design can be used to explore various defaults and time sensitive revocations that could help in reducing the number of employees who have vastly more access rights than required for their job role. Participants believe that security by behavioural design can be used to better manage these defaults and automated revocations. Furthermore, they believe that it can help to better manage access by having the option of selecting a timeframe for each access right in the system where access rights are managed. If, for example, someone temporarily takes over a managerial role, the added access rights could be set at the start to be revoked again from a pre-defined date. Another way security by behavioural

design principles can be incorporated here, is to use them in guiding access managers through a list of employees that need to be checked based on time spent in the current role, number of past roles and perhaps seasonal changes to roles based on peak times or other regular changes to job tasks.

Of the three mentioned factors, especially the first factor, of making security behaviour easy, fits well with security by behavioural design principles. These principles can be used to streamline decision making processes for end-users, resulting in a better workflow and more secure decisions and actions. The second, enhancing security skills might be supported with some brief comments in a user interface, but is more likely to be the domain of cybersecurity training and information campaigns. The third factor can be addressed using security by behavioural design principles, but is likely to also be the domain of internal policies and processes that discuss who, and in which circumstances, should have access to specific data and systems.

## Examples of implemented solutions

When participants were asked whether they could give some examples of security by behavioural design solutions they might have implemented in their organisation, or have experience with, it proved difficult to do so. Most attention in organisations seemed to be on the awareness and cybersecurity training aspects of behavioural cybersecurity, instead of the use of software design to improve security behaviours. Why participants experienced difficulties in coming up with examples remains unclear. It could be that not many examples are present in their organisations, or that the development team does not automatically share new initiatives that are deployed unless they are asked about it directly. Some did mention specific security by behavioural design methods that were implemented, while others confirmed the use of some of these methods when the interviewer gave some examples.

Of the examples given by the respondents, some discussed the rules that are used for end-users to create a password, with specific expectations as to which type of characters should be included, or in one case a password strength bar was mentioned. Another example was the addition of a button in Microsoft Outlook which end-users can click on to report an email as a potential phishing email to their IT department. This button was mentioned by several participants who all suggested it might be a useful change in the user interface to have end-users report phishing emails more often and more quickly. One participant noted that the effectiveness of this button would likely be higher if there was a clear, and preferably rapid, feedback loop for the person reporting the potential phishing email. This feedback loop would entail receiving a note regarding the truthfulness of the email and, in case of a phishing email, which various elements could be checked for proof. Some other participants noted that a feedback loop was present in their organisation where the person reporting the email was informed whether or not the email was genuine and safe to open. When asked why this button was implemented, the respondents who had knowledge of the process suggested that it was an option that Microsoft was now offering and that it was implemented as it might help improve reporting phishing emails. To the respondents' knowledge, no data was available on the effectivity of this button within their organisation. However, most reported believing that the button was useful in increasing the reporting of phishing emails.

## Forcing or nudging?

One of the themes that came up during the interviews was the difficulty in deciding when a form of nudging through security by behavioural design would be suitable. For developers, if a specific choice that can be made was considered to be a risk, they preferred to block that option altogether, instead of adjusting the environment in a way that end-users are less likely to choose that option. Deciding in what instances blocking an option altogether is not feasible and alternative approaches are to be sought is difficult. In the literature, this links to the discussion around nudging and techno-regulation (van Steen, 2022), also called affordances (Norman, 2014). Can we allow end-users to choose an unsafe option, or should those options not be made available in the first place? After a more in-depth conversation with interviewees on the topic, the developers mostly suggested to first block any unsafe options, and only discuss in what format these options could be made available if the blocking proved to create an unworkable situation. This suggests that the default would be to remove any unwanted options, and only using security by behavioural design principles when blocking is deemed undesirable from a business or productivity point of view.

In addition to the discussion around forcing security or nudging people towards security, participants also wondered about the long-term effects of security by behavioural design principles. Where forcing works as well on the umpteenth instance as it did on the first instance, the same might not be the case for softer approaches. For example, a brief message alongside a set of security settings might be read attentively the first time end-users are presented with these messages, and perhaps a second time as well, but respondents wondered whether these messages would still receive the same attention after a longer period of time.

## Security by behavioural design, where does it fit and who is responsible?

The interviewees were also asked about where they saw security by behavioural design fit in the development cycle and other organisational processes. In terms of development, there seemed

to be a consensus that, in line with the general security by design concept, the behavioural form should also be taken into account as early as possible, if it is to be implemented successfully in developed software. Where the opinions differed more, was on the topic of who should take charge in deciding on its implementation in the first place. The various groups, those tasked with developing or overseeing development of software, those responsible for purchasing software, and the behavioural experts all had their own ideas around who should take charge. The developers believed that it would not be difficult to implement security by behavioural design principles, but that they would need direct instruction on where this should be implemented, what it should look like, and how it should work. The purchasers believed they could easily add these principles to their list of requirements for negotiations with vendors, but would need help from other departments in decide which requirements should be included and how these requirements should be tested. Lastly, the behavioural experts believed they could play an important role in advising how to improve cybersecurity behaviour by design, but they felt they would need more technical expertise to know what possibilities they could think of, and a better understanding of which issues were of importance to the developers, purchasers and the organisation as a whole.

# Discussion

In this study, we aimed to investigate the feasibility of implementing security by behavioural design principles in Dutch organisations. After conducting a series of interviews, we can conclude that participating organisations see the benefits of implementing these principles, but struggle with what that implementation entails and could look like.

While some initiatives have been deployed, such as specific nudges in password creation, and the addition of a reporting button for potential phishing emails, the current implementation of security by behavioural design principles is relatively limited. In the next sections, the three research questions as outlined in the background section are answered.

## 1. *Do organisations view security by behavioural design as a promising avenue that should be explored?*

The participants were all supportive of security by behavioural design as tool to improve cybersecurity behaviour of end-users. As outlined in the results section, participants believed that a stronger focus on the human factor in cybersecurity would help improve cybersecurity in organisations. Participants did not necessarily state that security by behavioural design would be the 'only' or 'preferred' solution. Most supported the notion of exploring various solutions for the behavioural aspects of cybersecurity and believed that security by behavioural design could be one extra tool in the toolbox. The optimism of participants regarding this approach, suggests that implementing these solutions would not be met with rejection based on a lack of enthusiasm or scepticism of its effectiveness. This supports the notion that security by behavioural design principles are feasible to implement into the software development cycle from a motivation point of view.

## 2. *To what extent are security by behavioural design principles currently used in the development of new software?*

In the current situation, the use of security by behavioural design principles is rather limited. While some participants did mention initiatives when pressed, it was not at all a common occurrence or participants named only one or two initiatives that they had heard about or seen before. There is potential for vastly increasing the implementation of security by behavioural design principles in the development of new software by mapping which areas of cybersecurity behaviour require specific attention and to build new solutions for these topics. The solutions that participants did mention show that passwords can be improved through the use of specific messages and rules that are delivered when a new password needs to be created. Furthermore, while not objective data has been collected to the knowledge of the participants, they believed a button to immediately report a potential phishing email was highly valuable. The example of the report button shows that the secure behaviour, in this instance reporting the potential phishing email as soon as possible, can be stimulated by making it as easy as possible to report these emails. Instead of having to forward the email to a specific account, which end-users might need to look up, or having to use an online portal for reporting, end-users could report the phishing email with a single click and without leaving their email environment.

## *3. What is needed to implement these principles in the software design cycle?*

The main barrier that needs to be overcome in order to implement these principles in the software design cycle is that of the question who should take the lead in implementing security by behavioural design principles. The software developers suggest that if they are told to implement a certain function or option, they will simply do so. This means that others would need to make that decision. These can be higher up managers, or perhaps security awareness officers who branch out to security by behavioural design in addition to awareness campaigns, e-learning modules and other training methods. Similarly, the behavioural experts suggest that they could propose solutions, but would need to be told which behavioural problem the developers are currently facing, suggesting that the imitative is more suitable to come from developers or other parties rather than the behavioural experts. Lastly, the people responsible for purchasing new software suggest that if these principles are added to their list of requirements, they could easily enforce these in their negotiations with software vendors. So, while all parties believe that they could help implement these principles, it remains unclear who should take the lead in ensuring that the implementation is smooth and successful. Additional support in making these decisions, and additional training in behavioural and technical components could be effective ways to improve the implementation of security by behavioural design principles in the software design cycle.

## Areas for future research

There are three areas for future research based on the interview data. First, while some examples of security by behavioural design are clear, it remains uncertain which behavioural theories would be applicable in designing software. Is it only the nudging theory, or are there other areas of behavioural science that might help improve the security behaviour of end-users by adjusting the user interface? This could include theories and methods from scientific disciplines such as psychology, design science, user experience research and communication science. Second, the interviewees expressed doubts regarding the long-term effectiveness of security by behavioural design initiatives. The literature as outlined in our previous report (van Steen & De Busser, 2021) does not address this topic and the practitioners were not aware of any long-term effectiveness measures in their own organisations. Therefore, longitudinal testing of the effectiveness of security by behavioural design principles would be beneficial to inform changes in the software development cycle. Third, the technical experts as well as the behavioural experts expressed a need for more collaboration between the two. The technical experts suggested that they need more expertise in the behavioural methods, while the behavioural experts felt they would need more technical expertise to decide how to best implement security by behavioural design solutions. Therefore, a final area of future research would focus on how these experts can be best brought together, so that a successful implementation of the security by behavioural design principles is achieved.

## Limitations

There are three limitations to the current project that require attention. First, it proved difficult to find participants who were able to talk about the topic of security by behavioural design. While all respondents were knowledgeable and provided useful insights, many other organisations were contacted but either declined or could not find someone in their organisation who could talk about the topic of security by behavioural design. All respondents were enthusiastic about the possibilities of these principles to improve security behaviour but it remains unclear whether this enthusiasm is restricted to the respondents who took part, or whether specialists from organisations that did not take part would have held similar views, had they taken part in the study. A certain level of selection bias cannot be ruled out in this instance. This selection bias might have resulted in an overestimation of the enthusiasm with which the participants support security by behavioural design as an effective tool to improve cybersecurity practices within their organisations. The relatively small number of participants makes a selection bias more likely, as only 9 interviews, with 11 participants, were conducted.

Second, the research consisted mostly of participants who were tasked with software development, purchasing, or behavioural solutions aimed at their own organisations. It is possible that the methods that are used, and the implementation of these methods, differs between settings where the end-users are internal, such as colleagues within their own department or wider organisation, or external, such as consumers, clients or members of the general public. For example, it could be that in software for internal use a more forced approach is considered acceptable than when the end-users are external. Often, external users will have the option of licencing other software if the current software is not user-friendly enough, while internal end-users cannot. This might have repercussions for the level of control that developers have over the decision-making processes of end-users within their software environment. While we do not have data suggesting this is the case, we cannot rule this out based on the interviews we conducted.

A third and final limitation is that we focused only on security by behavioural design principles and did not take into account the interplay that might exist between security by behavioural design, awareness campaigns and cybersecurity training. It remains unclear whether security by behavioural design would be best implemented in tandem with other methods to improve security behaviour, is considered an addition to the other methods, or should perhaps replace certain initiatives. The discussion around whether we should allow unsafe behaviour in the first place, or block these options altogether seems to suggest that a wider discussion around the place of security by behavioural design in organisations is warranted.

# Conclusion

Security by behavioural design is a promising tool to improve security behaviour of end-users. While the potential benefits are clear and supported by both literature and practitioners, a strong push is needed to implement these principles in real-world settings. Additional understanding of the relevant behavioural theories, as well as methods of implementation and testing of effectiveness would be of use in implementing these methods. Furthermore, a stronger collaboration between software developers and behavioural experts is required for the implementation to succeed. These issues can be overcome by investing more time and energy into creating teams consisting of both developers and behavioural experts, and by sharing best practices and their effectiveness more widely.

# References

Cho, H., Roh, S., & Park, B. (2019). Of promoting networking and protecting privacy: Effects of defaults and regulatory focus on social media users' preference settings. *Computers in Human Behavior, 101*, 1–13.

Das, S., Kramer, A. D. I., Dabbish, L. A., & Hong, J. I. (2014). Increasing Security Sensitivity With Social Proof: A Large-Scale Experimental Confirmation. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 739–749. https://doi.org/10.1145/2660267.2660271

Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly.* 13(3), 319-340.

Kirlappos, I., Parkin, S., & Sasse, M.A. (2014). Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security. In: *USEC'14*.

Lessig, L. (2006). *Code v2.0*. Basic Books, New York, NY.

Norman, D. (2013). The design of everyday things: Revised and expanded edition. Basic books New York, NY.

Peer, E., Egelman, S., Harbach, M., Malkin, N., Mathur, A., & Frik, A. (2020). Nudge me right: Personalizing online security nudges to people's decision-making styles. *Computers in Human Behavior, 109*. psyh.

Thaler, R. H., & Sunstein, C. R. (2009). *Nudge*. Penguin Group.

van Steen, T. van, Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity, 6*(1), Article 1. https://doi.org/10.1093/cybsec/tyaa019

van Steen, T., & De Busser, E. (2021). *Security by behavioural design: a rapid review.* Publisher: NCSC.

van Steen, T. (2022). When Choice is (not) an Option: Nudging and Techno-Regulation Approaches to Behavioural Cybersecurity. In *International Conference on Human-Computer Interaction* (pp. 120-130). Cham: Springer International Publishing.

Wang, N., Wisniewski, P., Xu, H., & Grossklags, J. (2014). Designing the Default Privacy Settings for Facebook Applications. Proceedings of the Companion Publication of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing, 249–252. https://doi.org/10.1145/2556420.2556495

# Appendix A: Interview questions

1. Do you take the behaviour of end-users into account when designing software?

2. If so: In which way do you do this?
   If not: Why not? Is this something you are planning to do in the future?

3. Where in the design process would you take this component into account?

4. Who is responsible for the implementation or who has been tasked to incorporate these components in the software?

5. Do you believe there are opportunities to change end-users' behaviour towards more secure behaviours by means of changing the software architecture? (If yes: how? If no: Is there any specific reason why not?)

6. Do you have in-house expertise to include the behavioural components at the standards you require?
   (If yes: how? If no: Is there any specific reason for that and what else could/do you do?)

7. What kind of help could NCSC-NL provide in this matter?

**Publication**
National Cyber Security
Centre (NCSC)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (0)70 751 5555

**More information**
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

February 2024