TU Delft

Delft University of Technology

Document Version
Final published version

Licence
CC BY

Citation (APA)
Van Harten, V., Ganan, C. H., Van Eeten, M., & Parkin, S. (2025). "All Sorts of Other Reasons to Do It": Explaining the Persistence of Sub-optimal IoT Security Advice. In N. Yamashita, V. Evers, K. Yatani, X. Ding, B. Lee, M. Chetty, & P. Toups-Dugas (Eds.), *CHI '25: Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems* Article 387 Association for Computing Machinery (ACM). https://doi.org/10.1145/3706598.3713719

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
In case the licence states “Dutch Copyright Act (Article 25fa)”, this publication was made available Green Open Access via the TU Delft Institutional Repository pursuant to Dutch Copyright Act (Article 25fa, the Taverne amendment). This provision does not affect copyright ownership.
Unless copyright is transferred by contract or statute, it remains with the copyright holder.

Sharing and reuse
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.



"All Sorts of Other Reasons to Do It": Explaining the Persistence of Sub-optimal IoT Security Advice

Veerle van Harten
TU Delft
Delft, Netherlands
v.t.c.vanharten@tudelft.nl

Carlos Hernandez Ganan
TU Delft
Delft, Netherlands
c.hernandezganan@tudelft.nl

Michel van Eeten
TU Delft
Delft, Netherlands
m.j.g.vaneeten@tudelft.nl

Simon Parkin
TU Delft
Delft, Netherlands
s.e.parkin@tudelft.nl

Abstract

The proliferation of consumer Internet of Things (IoT) devices has raised security concerns. In response, governments have been advising consumers on security measures, but these recommendations are not guaranteed to be implementable owing to the diverse and rapidly evolving IoT landscape, risking wasted efforts and uncertainty caused by unsuccessful attempts to secure devices. Through interviews and a workshop with 14 stakeholders involved in a Dutch national public awareness campaign, we found that while stakeholders recognized the validity of these concerns, they opted to continue the campaign with minor modifications while expecting regulatory changes to resolve the observed problem. Their justifications reveal an institutional incentive structure that overlooks well-documented user realities in security and privacy HCI research. This raises important considerations for the design and delivery of such support strategies. By fostering a collaborative dialogue, we aim to contribute to the development of user-centered security practices.

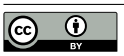
CCS Concepts

• **Security and privacy → Human and societal aspects of security and privacy**; **Usability in security and privacy**;

Keywords

cybersecurity awareness campaigns, Internet of Things (IoT) security, overproduction of advice, institutional incentives, users-centered security practices

ACM Reference Format:
Veerle van Harten, Carlos Hernandez Ganan, Michel van Eeten, and Simon Parkin. 2025. "All Sorts of Other Reasons to Do It": Explaining the Persistence of Sub-optimal IoT Security Advice. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 19 pages. https://doi.org/10.1145/3706598.3713719



This work is licensed under a Creative Commons Attribution 4.0 International License.
CHI '25, Yokohama, Japan
© 2025 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713719

1 Introduction

It has been widely observed that many consumer Internet of Things (IoT) devices are vulnerable to compromise, both out of the box and over time. In response, many governments – for example, the US, the UK, various EU member states, Australia and Japan [4, 9, 16, 20, 30, 36, 39, 53] – have launched nationwide advice campaigns, at times in collaboration with industry, to advise the public on how to configure their IoT devices to mitigate security risks as they emerge. Campaigns differ in their scope, but generally include advice on creating secure passwords and ensuring that security updates are installed.

Numerous studies have investigated the conditions under which security advice is valuable to users searching for guidance (e.g., [46, 47]). This challenge is especially urgent for consumer IoT. Compared with more established technologies such as web browsers and home operating systems, the consumer IoT space has an enormous diversity of device types, designs, configurations, and security features. New devices and risks emerge rapidly. Does providing general security advice succeed when confronted with that diversity? Redmiles et al. [46] found that across a range of categories, users lacked confidence and perceived difficulty, particularly around advice for securing the home network and advice that was overly general, e.g., 'use a password'. Van Harten et al. [55] investigated whether four recurring pieces of advice on passwords and updates from the advice campaigns of national governments are fit for purpose for IoT devices and found critical issues. Implementing the four pieces of advice was supported by *none* of the forty devices. At best, just two pieces of advice were supported by 13 of the 40 devices. In most cases, the devices did not have the properties assumed by the advice, such as update mechanisms and network-access passwords.

In other words, in the vast majority of cases, the IoT security advice was not fit for purpose. Determining if a device has the features that the advice assumes relies on technical expertise, defeating the purpose of advice being designed for non-experts. This disconnect can lead to confusion, lost time, frustration and anxiety for users [26]. Florêncio et al. highlight that when practices are widely accepted as effective without being rigorously tested, they tend to escape critical examination allowing flawed methods to persist. In security advice, this means misaligned advice, like those analyzed by Van Harten et al., continue unchecked, perpetuating ineffective advice compounding the issues they aim to resolve [22].

To address the pressing concerns surrounding the disconnect between the realities of consumer IoT devices and the advice provided to users, we conducted the first study to share these concerns, through interviews and a workshop, with key stakeholders in the advice-providing ecosystem in the Netherlands. Our goal was to explore whether advice providers recognized the problems found in general IoT security advice, and if so, what implications they drew from these problems. We conducted a workshop with nine such stakeholders with various roles in a Dutch national advice campaign, including funding, content development, dissemination, and oversight of the campaign. The workshop was preceded by scene-setting interviews (n=13) to understand the current stakeholder viewpoint and advice landscape. To support the reflection on the results of the workshop and to verify our observations, we conducted a round of post-interviews around a report that summarized the findings of the workshop (n=5). With the workshop as a focal event, we explored the following research questions: *(i) Do stakeholders agree or disagree with the quality problems observed with the advice for IoT security? (ii) Do stakeholders think that the campaign disseminating this advice should be abandoned, changed, or continued as is?*

We found that all stakeholders acknowledged that the advice was not fit for purpose for many, if not most, IoT devices. Remarkably, all stakeholders chose to accept these issues and to continue with the existing campaign or to make minor modifications that they acknowledged would not actually solve the problem that the advice was not fit for purpose. This observation parallels with previous research findings where stakeholders, when faced with similar challenges, struggle to devise effective solutions and instead resort to refining existing, albeit suboptimal, approaches [24].

We explored the reasons provided by the stakeholders for their continued support of the advice campaign. We found it is not merely inertia to improvement, but that deep-rooted institutional incentives of all stakeholders, except the users themselves, drive the production of advice regardless of whether this benefited users. Stakeholders face no institutional penalties for providing advice, but face significant penalties for *not* providing it. The provisioning of advice figures ahead of verifying whether advice is feasible and effective for diverse devices, and are the instructions a user needs. This aligns with the observations of Oliver et al., who note that academics should understand that policymaking is a political process, where decisions are made by politicians balancing various interests, and evidence-based proposals are only part of the solution [41].

Our findings underscore this political angle to consumer IoT advice, linking our work to parallel challenges observed in public health communication [10, 32]. Health authorities face a dilemma between saying nothing due to uncertainty and offering advice even if it might later turn out to have been incorrect. Under those conditions, institutional incentives sometimes prioritize the appearance of action ahead of the actual efficacy of interventions with users [37]. Although many researchers in our field view security & privacy advice as *training* [40, 45, 47], our findings suggest it aligns more closely with *policy*, subject to these same political and institutional considerations. We find that previous studies on 'security advice' have focused on individual recommendations, whereas our research investigates the surrounding infrastructure and processes that shape the creation and delivery of advice.

A critical examination of the forces shaping advice design and provisioning is needed, as well as participatory approaches to align the aims and incentives of advice-givers and policymakers with the documented efforts – especially in academic research – to improve the usability of security-related technologies. Our study highlights the tension between the need to be seen communicating and reaching users, and the need to give users actionable advice that meets their specific needs.

Next, we explore Related Work, followed by the context of the Dutch advice campaign positioned within the wider advice landscape, and then our Methodology, an overview of the stakeholder perspectives on consumer IoT security advice that were shared during the pre-interviews, workshop, and post-interviews, an analysis of these shared stakeholder perspectives, Discussion, and Conclusion.

2 Related Work

A range of advice is disseminated to users of consumer IoT devices, to signpost use of available security features, mostly protective measures to prevent compromise [6, 7, 46].

2.1 User Advice for IoT Security

Securing IoT devices is an ongoing challenge [7, 12, 15, 26, 58]. The two most common ways users can secure their devices are through passwords and the installation of updates as they are released [6, 47]. Users typically update their IoT devices for enhanced features and performance, rarely associating updates with security [26]. This is in part because of a lack of communication about the purpose of security-related updates [26, 58].

Users of IoT devices recognize the value in securing their devices [7]. They also welcome and expect device updates from the device manufacturer, as a means to mitigate security-related problems [35]. Internet Service Providers (ISPs) have emerged as intermediaries, to relay manufacturer advice to customers when needed, e.g. when compromised devices are detected [7, 48, 49] – ISPs themselves note difficulty in communicating advice to customers [49], and users can find it difficult to apply such advice [7, 48]. Notably, users can struggle to find advice that they can be sure applies to their device(s) [7].

Users see a role for governments in ensuring that manufacturers support device security [25]. While users are positive about the need for device updates [26], they hope for clearer information from manufacturers; it is noted in the same body of work [27] that users lack the technical knowledge to follow the kinds of security instructions they receive effectively. Our work builds on these findings by engaging directly with stakeholders associated with an IoT advice campaign (campaign owners, but also manufacturers and others) to determine how they see their role relative to users and the challenges of securing consumer IoT devices in the midst of various limitations.

2.2 Cybersecurity Advice Production

A driving assumption in ecosystems of advice is that the more informed a user is, the better equipped they are to secure their devices [51]. There has been much research on how users struggle with security-related technologies *despite* the wide availability of advice

targeting specific technologies, covering established controls such as passwords and updates [47] (which are also ongoing challenges with consumer IoT).

There are many dimensions to the production of security advice. A balance of generalizability and specificity is required [47], which is arguably acute for the diverse and evolving market of IoT devices. The *actionability* of advice has been found to be critical [46]; Redmiles et al. note a pronounced lack of sufficiently-detailed advice for home network devices (such as routers). IoT advice rarely refers to a specific device to which it applies [55]; paradoxically, this then rests on pre-existing expertise about device features to know if advice (intended for non-experts) applies to a device.

Meanwhile, experts struggle to agree on the exact advice to give users [47], let alone what advice to prioritize [46]. Writers of security advice are driven to provide increasing amounts of content, to activate users to address emerging threats [40]. Security advice is complex and expanding (as a "broadcast of facts" [51]), but benefits are primarily speculative [28], as for e.g., the detection of malicious websites.

Technocrats tend to be driven to generate a plethora of guidelines and recommendations to meet compliance targets [51]. Research in security and privacy advice has up to now focused on units of advice and their effectiveness [46, 47], including for consumer IoT devices [6, 7]. Emerging research has found that incentives beyond effectiveness have a role, such as the legal compliance and providing *reasonable* advice to inform stakeholders and users [62]. Herley [29] examined how the incentives of advice-providers clash with user goals and usability needs, for instance in providing advice for its own sake (regardless of whether it is applicable), as has for instance happened often with browser warnings – positing a worst-case scenario which prevents users from reaching their goals. Hadan et al. [24] note tensions between educating users about IoT, and risk-averse technologists advocating that IoT devices are never completely secure; the authors note also that policy stakeholders advocate for 'public campaigns' to educate users. Here we engage with the owners of such a public campaign, and associated stakeholders, noting a range of incentives which relate research on the effectiveness of security advice for consumer IoT devices to concerns often signaled in, e.g., the public health domain, such as sociopolitical, strategic, and communicative dimensions [10, 32].

This prior work on advice production in security has approached it as a communication problem between experts and users. Our study highlights that there are systemic pressures and institutional incentives that influence the production of IoT security advice, with stakeholders who are directly involved. We reveal how these pressures and incentives contribute to the overproduction of advice, as observed by [46], and a lack of processes to check that users can apply the advice.

3 Background – The Dutch Cybersecurity Advice Campaign

Many national campaigns are focusing on the provision of consumer-oriented security advice for IoT devices, such as in Germany, Australia, the United States, Spain, Switzerland, the United Kingdom, and Japan [4, 9, 16, 20, 30, 36, 39, 57]. In some cases, this guidance is positioned under a broader umbrella of cybersecurity awareness efforts, while in others it is a campaign distinctly focused on IoT security. Typically, the core pieces of advice focus on keeping devices up-to-date and setting strong passwords [55]. Here, we focus on efforts in the Netherlands, where we have been able to engage with relevant stakeholders.

The Dutch cybersecurity awareness campaign, veiliginternetten.nl, is an initiative of the Dutch government in collaboration with industry partners and non-profit organizations. Its primary goal is to raise awareness among Dutch citizens about adopting important cybersecurity practices, including for IoT devices. The campaign is centered around a website, physical leaflets and television ads. The core messages of the campaign emphasize the importance of keeping devices up-to-date and using secure passwords to protect against cybercriminals. Written materials relate these threats to remote access and control of IoT devices.

On the surface, the Dutch cybersecurity awareness campaign mirrors the notion of minimality as advocated in research [46], with advice narrowed down to a core set of the most important security behaviors. However, the website does provide jumping-off points to additional recommendations, ranging from router configuration to turning off devices when not in use [54]. This advice is framed as universally applicable to all smart devices despite the increasing diversity in the expanding range of IoT devices [55].

Other countries, such as the UK and the US, run similar cybersecurity awareness campaigns, e.g., the UK Cyber Aware initiative [38]. Analysis elsewhere notes that the campaigns in these countries vary in their target audiences, the behavior change techniques they reflect, and the channels through which they are delivered [57]; despite significant investment, the effectiveness of these campaigns in changing consumer behavior remains unclear [57].

4 Methodology

To explore whether stakeholders involved in a Dutch cybersecurity awareness campaign recognized the limitations of general security advice and how this recognition might influence their approach, we presented the findings of van Harten et al. to them in a workshop setting [55].

As a preparation for the workshop, pre-interviews were conducted with n=13 stakeholders to gain an initial understanding of individual perspectives. The workshop was attended by n=9 stakeholders, including eight interviewees and one additional colleague. Afterward, participants received a summary report of our findings and could participate in post-interviews to give feedback (n=5). For an overview of our approach, see Figure 1.

4.1 Participants and Recruitment

Recognizing that success measures can vary between researchers and stakeholders at the policy level [50] (in this case, advice-givers), we aimed to foster a collaborative exploration of alternative approaches that leverage the expertise of stakeholders.

We consulted a diverse group of stakeholders in various roles in and around the campaign, encompassing its funding, execution, and content development. In essence, where prior work has referred to the need for 'public campaigns' and 'consumer education' [24], we are engaging directly with the parties overseeing and producing such a campaign.

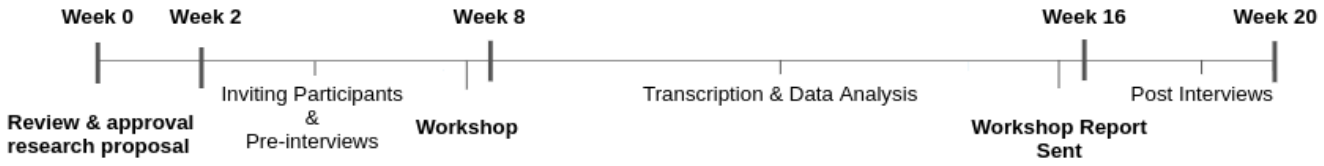


Figure 1: Timeline methodology: During each interview and workshop, we recorded the sessions for subsequent transcription and analysis.

Responsibilities ranged from preventing crime and economic damage, aiding in formulating security recommendations, and deciding on which key advice to emphasize, to participating in regulation development processes. It is important to note that stakeholders participated as organizational representatives, not as individual experts or users, thus giving us insights into institutional perspectives. This approach allowed us to explore how institutional incentive structures influence their viewpoints and actions.

Table 1 provides an overview of the stakeholder groups and their participation. Some groups play a direct role in the Dutch awareness campaign, while others have a connection or interaction with the campaign. Overall, this set of stakeholders covers the main roles in the advice ecosystem, encompassing policy, industry, consumer advocacy, and regulation, as it includes government officials and regulators shaping policy, manufacturers and an ISP driving product and service development, a consumer association advocating for users rights and safety, and a public-private partnership facilitating collaboration across sectors. Participants were sought through personal contacts and research project partners. In total, 31 practitioners were contacted. 13 of those approached then participated in the pre-interview stage. Of these, 10 confirmed their attendance for the workshop; two could not attend on the day, while one attendee brought a colleague, resulting in a total of nine participants in the workshop. However, we note that of these 9 participants, one arrived late and joined the workshop during the second round. After the workshop, the participants received an overview of our findings and were invited to participate in a post-interview (with five doing so). Table 1 provides a full overview.

4.2 Alignment IoT Advice with Device Features

The prompt for the workshop was a presentation of the findings by van Harten et al. [55], which were included in the PowerPoint slides used for the workshop [56]. By directly comparing IoT security advice with the features of a wide range of IoT devices, their work reveals a fundamental misalignment, providing a concrete foundation for stakeholders to reflect on their ongoing advice campaign. The following overview summarizes the content that we presented to the participants to set the scene for the workshop and the discussions.

The presentation centered around specific points. To assess the applicability of government cybersecurity advice to IoT devices, van Harten et al. examined the features of 40 consumer IoT devices, as described in their documentation and a wide range of support materials [55]. The advice emphasized changing default passwords, setting strong unique passwords, installing updates, and enabling automatic updates. For none of the 40 IoT devices all four pieces of advice were applicable. The maximum number of applicable advice pieces was two, which was the case for only 13 of the 40 devices. This highlights that in the majority of cases, the advice is not fit-for-purpose.

For example, many of the devices in the analysis do not have default passwords, and when they do, this is not always communicated in the support materials. This could lead to frustration for users as they search for a feature which is difficult to locate or does not even exist for the device itself. Furthermore, following advice does not necessarily lead to specific security benefits. For instance, some devices refer to parental controls as the default password. Changing that does not enhance network security. Expert knowledge may be needed to know whether advice is or is not applicable for a certain device, defeating the purpose of advice designed for non-experts.

In sum, the misalignment between advice and device capabilities raise concerns about the effectiveness of current advice campaigns. We asked our participants to reflect on the implications for the current campaign and future efforts.

4.3 Data Collection

4.3.1 Pre-interviews. Pre-interview video calls averaged approximately 30 minutes. Interviews focused on understanding a participant's professional background and their organization's stance and involvement in the area of IoT security and related user support.

We also explored the perspectives of the participants on key concerns in security and privacy: consumer responsibility for IoT device security, available resources for consumer support, and monitoring methods to track the effectiveness of support. The close of the interviews covered the findings from van Harten et al. [55] as described in Section 4.2, with participants. Concluding the interviews, respondents were asked for their insights and whether they recognized any of the findings in their work. They were also given the opportunity to suggest changes to the workshop structure and agenda topics.

4.3.2 Workshop. Multi-stakeholder workshops have been useful in examining security-related challenges, such as in the process of developing more secure software [60, 61], and in identifying misunderstandings between security managers and employees around policy compliance [3].

The setting of a workshop allows the negotiation of meaning between researchers and participants [42]. Within our research, a workshop is particularly valuable for examining institutional incentive structures and the broader implications of security advice in

Table 1: Participant Overview and Involvement.

Background	Pre-Interview	Workshop	Post-Interview
Government Official (GOV)	3	2	2
Regulator (REG)	2	2	2
Public-Private Partnership (PPP)	1	1	0
Internet Service Provider (ISP)	1	2	1
Manufacturer (MNF)	2	1	0
Consumer Association (CNS)	3	1	0
Internet Domain Registry (IDR)	1	0	0
Retailer (RET)	0	0	0
Total	**13**	**9**	**5**

Participant involvement across the study phases (Pre-Interview, Workshop, and Post-Interview) categorized by stakeholder background. Note: P–REG arrived late to the workshop and only joined the second round.

the consumer IoT domain. This has similarities to Spaa et al.'s concept of 'recipient design,' where effective communication in policy contexts requires bridging gaps between differing worldviews [50].

The workshop guideline and the workshop script are included in Appendix C and Appendix F, and the PowerPoint slides that were used can be found here [56]. Dutch served as the main language for both the interviews and the workshop. The workshop began with eight participants, as one participant arrived later during the second round. An overview of the agenda and a presentation of its objective were provided: to collaboratively evaluate and address the effectiveness of the Dutch security awareness campaign. There was a particular focus on participants' recognition and response to the identified disconnect between the provided security advice and its practical application (Section 4.2). To ensure clarity and alignment among participants, the chairperson first explicitly outlined the core issues with the provision of general advice for consumer IoT devices.

In response to the findings, group discussion then consisted of two parts. In the first part, participants ranked three courses of action: continuing the current campaign, adjusting the campaign before continuing or stopping the current campaign entirely, from most to least agreeable. The group was then divided into three smaller groups, ensuring diversity of perspectives by intentionally separating individuals from the same stakeholder groups, such as the ISP representatives and the government officials, to encourage a broader range of opinions in each group and avoid potential biases. The initial ratings provided by the participants did not influence the composition of these smaller groups.

Each group used flip charts to rank their choices and sticky notes to capture the pros and cons of each course of action. The participants ranked the courses of action again after a discussion. Finally, the entire group reconvened to share the outcomes of the small group discussions. After a short coffee break, the ninth participant joined and the group was presented with nine solution directions derived from the pre-interviews (see Table 2). The participants selected their top three choices, documented them on sticky notes, and discussed the pros and cons with their small group from the first round (the participant that arrived late joined the group that consisted of two participants.). Participants then ranked their top three choices again.

The workshop concluded with a discussion of the two most popular solution directions (elaborated on in Section 5.2.4), which were automating security features and establishing minimum security standards for IoT devices through regulation. Participants shared their perspectives on these directions, and identified the responsible party for implementation and potential actions within their organizations to support it. Participants also shared their experiences and lessons learned from the workshop.

4.3.3 Post-interviews. After the workshop, the authors shared a report summarizing the results of the pre-interviews and the workshop with the participants. The post-interviews – 15-minute short video calls – served two purposes: firstly, inviting participants to confirm or otherwise provide feedback on the research team's summary and interpretation, which included some confronting observations about participants acknowledging that the advice was not fit for purpose, yet still wanting to continue the campaign that disseminated it. We also wanted to revisit the following two topics: the disadvantages of advice for users who try to follow it even if it does not apply to their device(s) and what could be done for users who are motivated to secure their devices, but do not know enough to determine if the advice applies to their device(s) (see Appendix B).

4.4 Data Analysis

The lead author ran the workshop with the chairperson (one of the co-authors), transcribed the recordings, and documented the contents of the flip charts. During this process, data was pseudonymized to refer to participant identifiers. A multimethod qualitative text and discourse analysis (MMQTDA) approach was applied, as detailed by Alejandro et al. [2]. This approach combines Thematic Analysis (TA) and Discourse Analysis (DA) and involves the use of TA during the initial phase of the analysis, followed by DA. In this order, TA supports a sifting through the body of texts to identify prominent themes, while DA delves deeper into the relationship between identified themes and – in this case – the observed phenomenon of persistent overproduction of cybersecurity advice. One of the authors conducted the initial coding of the interviews using a 'codebook'-style approach [8]. The themes and assigned meanings were then discussed and refined in regular meetings with the

other authors, including the workshop chairperson, who provided additional context on the perspectives of the participants.

4.5 Research Ethics

The data steward of the faculty evaluated our research proposal which was subsequently reviewed and approved by the University's Human Research Ethics Committee. Consent was obtained for recording interviews and the workshop through a consent form, which detailed secure storage practices and assured participants that the recordings would only be used for transcription purposes. After transcription, the authors deleted the original recordings. All the information collected was anonymized to protect the privacy of the participants. Participants were informed about potential academic outputs and the planned sharing of summary results with participating organizations.

The workshop was conducted on our university campus at a scheduled time and required in-person attendance. Participation was voluntary, and participants were free to withdraw from the study at any time without penalty. To mitigate COVID-19 transmission risk, participants were given the option to wear face masks and maintain a 1.5-meter distance from others during the workshop. Participants could contact the lead author with any questions or concerns.

4.6 Limitations

Retailer presence was absent in the workshop, which could have limited the diversity of viewpoints and insights to be captured, potentially impacting the development of more comprehensive user-support strategies to enhance device security. Retailers – and manufacturers – are often difficult to engage with and under-researched [11, 43]. However, we did involve a manufacturer and a consumer association representative.

Although the number of participants was relatively small, we included key contributors vital to the operation of the Dutch security awareness campaign, ensuring representation of those directly involved in the dissemination of IoT security advice in the Netherlands. While our study was geographically concentrated in the Netherlands, the findings hold relevance to other countries currently applying a campaign-based approach to security advice [4, 9, 16, 20, 30, 36, 39, 53]. The challenge of providing general IoT security advice is thus not unique to any one country, as the diversity of IoT devices and their configurations makes it difficult to provide universally applicable advice. Nonetheless, the limitations of this regional focus present an opportunity for future research to broaden the scope.

5 Stakeholder Views

Here, we reflect on the complex considerations underpinning participants' views on providing security advice for consumer IoT devices. This section details our MMQTDA analysis (as described in 4.4), focusing on five of the six key themes we identified within the data: (i) Responsibilities for keeping IoT devices secure, (ii) Characteristics and dynamics of the awareness campaign, (iii) Perceived challenges and impediments, (iv) Perspectives on previous research findings, and (v) Regulatory expectations and outlook, (see Appendix E for details). Building on this foundation, theme (vi) Institutional incentives, will serve as the basis for the more in-depth analysis presented in Section 6.

5.1 Pre-Interviews

The preliminary interviews captured participants' views on the current landscape of IoT security and advice. Participant identifiers are, as in Table 1, prefixed with 'P–' and their Background classifier.

5.1.1 Perspectives on consumer responsibility. Participants generally expressed a desire for users to have minimal involvement in ensuring IoT device security. However, there was nuance here, where this was seen as a shared responsibility among users, manufacturers, and government bodies. This perspective mirrors smart home user views in a US-based study [25]. Our participants expected users to enable security features when available but that they should not be overwhelmed by the burden. However, P–ISP1 pointed out that in the current situation, manufacturers prioritize ease of use over security:

> "Ideally, making a device insecure should require effort, and right now, it's the other way around in many cases."

Some participants leaned towards a more user-centric model. For example, P–MNF noted that if users fail to enable security features, the manufacturer should not be held accountable for any vulnerabilities that arise as a result. P–IDR argued that if consumers buy a device, they accept ultimate responsibility for its security:

> "The role of the consumer is often downplayed as yes, they can't do it, they don't get it. On the one hand, yes, that's right. But on the other hand, if you don't understand cars, don't buy a car."

These statements place the onus primarily on users to enable security features and maintain device security. Going beyond existing work on shared responsibility [25], our participants saw users needing to meet manufacturers halfway, needing the skills to use offered controls – participants differed on whether this was appropriate or needed to change.

There was a broad belief that keeping IoT devices up-to-date yields the most significant enhancements for all security features available to users. It was expected that this would be doable for most consumers. P–GOV2 remarked:

> "So look, say checking an update is of course kind of the most user-friendly thing to do."

However, P–REG2 was more reluctant and wondered who decides what a user should and should not be able to do. Reflecting on their organization's commitment to uphold the highest security standards for all the devices they use, they emphasized the practical limitations of user compliance.

5.1.2 Advice selection procedure and campaign monitoring. The Dutch awareness campaign [54] was explained as being a collaborative effort involving various organizations and ministries. P–PPP stated that their organization refrains from dictating the campaign's content. Proposed topics that could be of interest undergo discussion among involved parties, with technical experts weighing in

on what they consider the best security practices. Notably, this process does not include users directly. There is some interest in prioritization of advice, although P–PPP noted:

> "Now we say: do the update check, but there are still 24 things that you should actually take into account."

Essentially, even if users follow the core advice, they are still left with a long list of other security tasks. Furthermore, no explicit 'usability' check exists to determine if advice is doable for users. This finding has parallels to research with US-based advice-writers [40], where their participants did not involve users in the creation of user-centric advice as the focus is on translating existing technical advice into accessible language for home users. This approach assumes that the primary issue is one of communication, rather than a need to fundamentally rethink the advice itself based on user needs and capabilities.

The effectiveness of the campaign is assessed by monitoring the number of website visitors and click rates, using an annual nationwide sample of users through a third party questionnaire to measure how safe people feel on the Internet [31], and conducting an annual review of the website's quality by an independent third party. This review evaluates the user-friendliness of the website. However, stakeholders did not track metrics such as visitor perceptions of content and their ability to apply recommendations. P–GOV3 explained:

> "We can't go door-to-door asking, 'Did you see the commercial and did you update?', you know? It is always very difficult to really measure whether such a campaign is effective or not."

Stakeholders thus recognize users' perspectives, but processes and resources limit any opportunity for direct engagement.

5.1.3 Expectations for campaign outcomes. Participants expected that widespread adoption of security advice could lead to tangible, positive outcomes. P–GOV1, P–GOV2, and P–PPP envisaged a scenario where, in response to this widespread adoption, the emphasis could shift to disseminating a different set of security advice (distinct from the participants of [40], who reported adding more and more advice to adapt to new threats).

In terms of the broader implications for the prevalence of security breaches, several stakeholders anticipated a decrease in the number of compromised devices if users adhered to these security guidelines. Although participants did not expect their core responsibilities to change significantly, they did envision broader changes within the digital landscape as users become more security-conscious. The prevailing belief is that a lack of 'security hygiene' among users plays a pivotal role in wide-scale cyber-attacks (similar to the view in organizations [51]), including DDoS attacks.

5.1.4 Perspectives on previous research findings. All respondents acknowledged the issues of complicated and inaccessible cybersecurity advice for diverse IoT devices, as identified in Section 4. In all, there were nine suggestions across the participants, for how to improve the current situation. These ranged from streamlining and standardizing IoT device connections and security features to encouraging ISPs to block insecure protocols such as Telnet. For an overview, see Table 2.

Table 2: Overview Recommendations.

1.	Simplifying device connectivity across brands
2.	Standardize security features
3.	Urge ISPs to block insecure Internet protocols
4.	Implement restrictions on device functions
5.	Ensure manufacturers detail security features
6.	Automate key security functions
7.	Set minimum security standards through regulations
8.	Prohibiting external access
9.	Clearly communicate the security level before purchase

While the solutions aim to address the issue of advice not being fit for purpose, the recommendations in Table 2 also give shape to 'obstacles' that the stakeholders think users need to navigate: understanding the different ways in which devices can be connected, the variety of security features available, responding to the risks associated with various device configurations, and so on.

However, P–ISP1 noted that if devices were not accessible from the Internet, most of the prevailing issues would be addressed, rendering much of the advice redundant. However, P–ISP1 conceded that many consumers need a professional who can help them properly secure their IoT devices in this way and are not able to learn how to do so themselves.

Overall, participants generally agreed that while consumers should play a role in the security of their IoT devices, the responsibility for security is a burden for users, given their varied technical capabilities.

5.2 Workshop

The overarching goal of the workshop was to allow participants to critically assess the current state of consumer IoT advice and explore potential improvement strategies.

5.2.1 First round - Stakeholder responses to the summary of findings. The first round started with a recap of the research findings, emphasizing the issues identified in Section 4.2 regarding the disconnect between general security advice and the diverse IoT landscape. Participants were asked to share their perspectives on these findings and whether they recognized the described limitations in their work.

All participants acknowledged the validity of the research findings and recognized the challenges highlighted in providing effective security advice. They agreed that the diversity of IoT devices and the rapid evolution of the IoT landscape make it difficult to provide universally applicable and actionable advice. This acknowledgment, in part, answers the first research question, confirming that the stakeholders recognize the quality problems observed with the current advice as drawbacks to the current approach.

5.2.2 Collaborative exploration of the campaign's effectiveness. Each participant was provided with post-it notes to rank three options: continuing the current campaign, modifying the campaign before

continuing, or discontinuing the campaign altogether. The participants were then divided into smaller groups to discuss their rankings and the pros and cons of each option, using a flip chart to visualize their collective preferences; see Figure 2. To determine whether group discussions influenced individual opinions, participants were given a second opportunity to rank the three options. The outcomes of this reassessment were then presented and discussed with the entire group, concluding the first segment of the workshop.

Most of the participants advocated for the customization of the campaign while remaining focused on the dissemination of general-level advice.



Figure 2: Visual documentation of the participants' insights and positions based on the workshops' group discussions, captured dynamically on flip-over sheets. To address privacy concerns and protect participant anonymity, efforts were made to anonymize the data by blurring the handwriting visible in the figure.

Although the authors had presented research highlighting limitations in the provision of general security advice for IoT devices, there was no support for discontinuing the current campaign and its core pieces of advice, which answers our second research question. The concept of discontinuation was so foreign to P–GOV2 and P–PPP that they misinterpreted the term 'quitting,' suggesting that merely presenting evidence of the shortcomings of general advice is insufficient to challenge deeply held beliefs and ingrained practices [63]. This misinterpretation underscores the complexities of changing long-standing processes, even when challenged with evidence, particularly at a policy level [50]. P–PPP clarified that they had interpreted discontinuation as not stopping entirely from providing general advice to consumers but rather initiating a new campaign if the existing one proved ineffective. Their initial interpretation of the term led them to rank it as their second preference prior to the group discussions. When 'quitting' was clarified to mean abandoning the current campaign altogether, they moved this option from their second choice to their third, as in Table 3. Appendix 5 provides a more detailed overview of these group outcomes.

Other participants, including P–MNF, P–CNS, and another P–GOV, consistently ranked quitting as their least preferred option and further emphasized their stance by adding clarifying phrases to their sticky notes. These annotations included definitive statements like "not stopping," "stop current campaign – most disagree," and "Absolutely not quitting."

	Continue	Customize	Quit
1st option (BD)	3	5	0
2nd option (BD)	3	3	2
3rd option (BD)	2	0	6
1st option (AD)	2	6	0
2nd option (AD)	6	2	0
3rd option (AD)	0	0	8

Table 3: Comparative Summary of Participant Rankings in Round 1 - This table shows the distribution of rankings provided by eight participants (the ninth participant joined in the second round) for the three options, both before (BD) and after the discussion (AD). It illustrates the changes in preferences for continuing, customizing, or quitting the Dutch awareness campaign, highlighting the shift in consensus resulting from the group dialogue.

5.2.3 Clarifying complexities. During the plenary session of the first round, the chairperson actively engaged in clarifying key points, ensuring that all participants grasped the issues being discussed. After the group discussions, participants shared their belief in the vital role of educating consumers about the importance of IoT security, arguing that although the advice provided through the campaign may not be applicable to all devices, the role of the campaign in educating consumers on the importance of IoT security still had value.

There was a reliance on changes outside the campaign's control, such as standardization and regulation of devices. These external changes would then simplify the goal of providing advice that applies to more devices.

The chairperson noted an ambiguity around whether the advice provided is applicable to specific IoT devices and that this could cause users to be unsure of its relevance. All participants acknowledged this issue, but several proposed customizing the messaging by differentiating between various target groups based on user demographics and technical expertise. The chairperson cautioned that differentiating between user types would not adequately address device-specific applicability.

P–ISP1 proposed a shift in the campaign's focus, emphasizing the prevalent issue from a device abuse standpoint: the observed accessibility of IoT devices from the Internet. They recommended reorienting the campaign to advise users on how to configure their devices to prevent unauthorized access from the Internet – this is among the pieces of advice in some national campaigns but with less emphasis than updates and passwords [55]. However, the chairperson underscored the difficulty of summarizing such a complex issue into a simple piece of advice. This exchange highlighted a tension between the desire for simplicity in public messaging and the inherent complexity of securing diverse IoT devices.

As the discussion progressed, participants maintained their support for the campaign, believing that even imperfect advice plays a crucial role in raising awareness and motivating consumers to take steps to secure their IoT devices. This finding highlighted a dual purpose of the campaign, to provide advice, but also signaling and motivation.

The importance of ongoing evaluation and refinement of the campaign was also raised (Section 5.1), with there being a need to ensure that it is effective in addressing the evolving landscape of IoT security. There was a belief that these efforts would empower at least some users to improve the security of their IoT devices.

5.2.4 Second round - Focusing on regulations. During the second round, two proposed solutions that were shared during the pre interviews (Table 2) stood out: automating security features and setting minimum security standards for consumer IoT devices through regulations, with the latter being the most popular choice. During the group discussions, Group 1 hypothesized that regulation would approximately address (a figurative) 80% of the other options outlined in Table 2 and recorded this potential benefit as a pro on their flip chart.

A unanimous benefit identified by all groups was the proposed shift in the security responsibility of IoT devices from consumers to manufacturers. This sentiment was captured in phrases on the flip charts such as "places responsibility on manufacturers," "helps consumer because action lies with company," and "takes pressure off consumers - places responsibility on manufacturers." One of the MNF participants commented elsewhere in the workshop that they proactively took on some responsibility to inform users. In general, it was widely acknowledged that the burden of securing IoT devices should not rest solely on consumers, who often lack the technical expertise and resources to manage complex security configurations effectively. Instead, participants advocated for a model in which manufacturers have a greater responsibility for building security into their products, but also by providing clear guidance to users. This position aligns with the sentiment that IoT security is a shared responsibility involving users and manufacturers [25], where here regulatory change was seen as the way to make it happen.

5.3 Post-Interviews

The workshop participants were provided with a report summarizing our findings from the pre-interviews and the workshop. An invitation was extended to participate in a 15-minute one-to-one feedback call. The interviews aimed to address potential confusion or concerns raised during the workshop and to clarify the research viewpoint relative to the participant's views (where confusion can be natural as research and policy actors engage in understanding each other [50], as has also been seen in health policy interventions, wherein policymakers may be wary of unfamiliar information provided by researchers [10]).

Of the nine participants, five expressed interest in these follow-up interviews (See Table 1). The report was generally well-received for its clarity and relevance. However, P–REG2 felt the report was somewhat critical of those supporting the campaign's continuation, particularly in the absence of alternative solutions:

> "Yes, we also saw that it could be suboptimal, but there were all sorts of other reasons to do it. But I read your points. It still feels a bit critical towards those who voiced that opinion, while I still think, yes, but what is the alternative?"

5.3.1 "The core message is no less important". Participants acknowledged the inherent challenge of providing tailored security advice, owing to the individual nature of each device. They also acknowledged the difficulty of estimating the level of technical understanding that a consumer should ideally have in order to comprehend these intricacies fully. Nonetheless, participants asserted that the fundamental advice (around, e.g., updates) embedded in security guidance remains important, based on their collective understanding of what users need to know. Keeping IoT devices up-to-date was seen as vital, even if "the way it can be done doesn't always succeed. But still, the core message is no less important" (P–GOV2).

During these post-interviews, we delved deeper into participants' perspectives on the responsibility placed upon consumers to determine the applicability of such advice to their specific devices. P–REG1 noted poor usability as an issue, often resulting from devices being designed with a technology-centric rather than a user-centric mind. In their experience, this frequently leads to terrible graphics and a confusing user interface. An example mentioned was changing passwords on a router, which may not be intuitive or clearly guided. Two respondents highlighted the upcoming EU regulation, the Radio Equipment Directive (RED) requirements, which are expected to compel manufacturers to address such security issues [18].

5.3.2 Potential solutions. To support users trying to assess whether security advice applies to their devices, P–REG2 suggested that manufacturers regularly inform consumers about their device's security status in relation to common security concerns through brief notifications. This proposal touches on Recommendation 5 of Table 2:

> "In an ideal world, you just get a two-line message that says: 'Compared to the current main safety issues, we have noticed that your device is safe. Your device has 100% safety from the test.

Another proposal was a variant of this idea to introduce a subscription service for systematic security checks.

P–ISP2 proposed encouraging users to proactively approach their ISP to check their network's security status. P–ISP2 also suggested a product labeling system, aligning with Recommendation 9 in Table 2, similar to "better life" labels, to inform consumers about device security. Elsewhere, Vetrivel et al. found consumers are willing to pay more for products that display security and privacy features in the form of security labels [59] but acknowledged the hurdles in realizing such a system, such as maintaining the accuracy of these labels in an evolving security landscape.

Participants envisioned an ideal scenario where manufacturers would provide secure devices with comprehensive explanations about security features and enriched support to consumers needing help comprehending or implementing security advice. In line with Recommendation 7 in Table 2, P–GOV1 and P–REG1 highlighted the Cyber Resilience Act, approved on March 12, 2024, as a key piece of legislation expected to improve the general security level of IoT devices significantly. Once implemented in 2027, the CRA will enforce security measures, including device updates, across the EU [19]. These suggestions, along with the broader themes from Table 2, illustrate a recurring assumption that the core advice is sound; this sidesteps the issue of verifying its applicability across diverse devices.

5.3.3 Deferring change. The post-interviews revealed a tension in participants' reasoning. Despite acknowledging the shortcomings of the current advice and flaws in their justification for continuing the campaign, they still reaffirmed their ongoing commitment to the awareness campaign. This tension did not manifest as an outright resistance to change but rather as a focus on future solutions, rationalizing that the complexity of the current situation necessitates a 'tidying up' before any substantial reassessment could occur.

Despite acknowledging the research findings on general IoT security advice not being fit for purpose, stakeholders appear to believe that the quality of advice can be significantly enhanced by tackling issues such as device feature standardization and streamlined communication. However, these do not address the core problem: the general security advice does not explicitly instruct a user on the specific action they need to take for their particular device(s).

Although it was believed that many of the solutions in Table 2 would eventually appear as an outcome of regulations, their implementation will take time. In the meantime, users must continue to navigate the existing challenges that these solutions aim to resolve (and which are characterized in Table 2). Where there was strong support to 'customize' the current approach to advice-giving (Table 3), it would appear that users need to navigate the recommendations of Table 2 while these remain presently unresolved (and non-standardized). These then constitute specific, latent usability challenges in using consumer IoT devices, which are pushed down to the end-user. Research elsewhere already highlights that users may struggle to implement technical actions such as blocking protocols and external access [7].

6 Analysis of Stakeholder Perspectives on Consumer IoT Security Advice

In Section 5, we explored the complex considerations behind stakeholder views on consumer IoT security advice. During the first round of the workshop, the chairperson pointed out a perplexing contradiction: despite acknowledging that the current advice is not fit-for-purpose for many, if not most, of the IoT devices, participants advocated that the advice campaign be continued. In the discussion the stakeholders gave various reasons for their continued commitment to the advice campaign. These reasons were separate from the actual benefits for users and instead pointed to institutional incentives of all participating stakeholders to commission, produce, and continue the advice campaign irrespective of whether the campaign actually benefited users. In this section we analyze the incentives underlying the reasons provided by the stakeholders.

6.1 Political Pressures

Group discussions revealed political forces behind the campaign. P–GOV1 expressed concerns that stopping the campaign would not serve the target audience and would fail to meet the expectations of politicians who support such initiatives. This concern was noted on the flip chart as: 'Does not meet the needs of stakeholders and politics.'

6.2 Legal Requirements

The public sector stakeholders said that they are mandated by law to disclose risks associated with consumer IoT vulnerabilities and to offer general security advice [17, 44]. Non-compliance results in indirect penalties, whether political or reputational. It is less costly for organizations to adhere to these mandates than to justify non-compliance. In practice, this often translates into continuing to provide information to consumers as a form of accountability, as opposed to achieving a net-positive impact.

6.3 Moral Obligations

While political and legal incentives were mentioned by public sector stakeholders, a strong moral obligation to provide advice was widespread among stakeholders, also among the industry representatives. Stakeholders feel compelled to provide advice, even when its effects are questionable or potentially counterproductive:

> "We both (P–PPP and P–MNF) concluded that it is actually an obligation for the business community, right? And for the government, that you always have to help consumers and inform them" (P–PPP).

Much like the "trolley problem," (as highlighted in security and privacy [34]) stakeholders generally feel compelled to act, even if that action could inadvertently cause harm. Not providing such advice is seen as a liability. This sense of obligation aligns with themes from Neil et al. [40].

This moral imperative was also visible in the commitment to "raising awareness" of consumers. Several participants justified their efforts as benevolent attempts to alleviate user difficulties. Further reinforcing this sentiment, P–PPP, along with P–MNF stressed the importance of informing consumers so they can protect themselves:

> "To wake people up, they need to know what can go wrong" (P–PPP).

They viewed this as an obligation. It was deemed alright to occasionally question how to best raise the awareness, but not doing it was not an option.

> "You can perhaps go back to the drawing board every now and then, but only as a last option to not stop abruptly. Because this is an obligation" (P–PPP).

In other words, the activity of disseminating advice is seen as inherently positive if it makes users more aware of threats, even if users acting on the advice might not reach actual security improvements.

6.4 Externalized Cost of Advice Failures

It was expected that security advice would raise awareness among consumers and help at least some of them make informed decisions. P–GOV1 argued that even if the campaign's advice is applicable to a mere 20% of consumer IoT devices (P–GOV1 believed the actual number to be higher), this level of effectiveness was still deemed as valuable. At the same time, alternative solutions should be sought for the remaining devices. P–MNF argued: "If you reach just three people, should you stop? Or is one person enough to save the campaign?"

To put it differently: any benefit is worth considering. What this reasoning reveals is that the stakeholders only look at the potential benefits of the advice, not at the cost. These costs are externalized

to the user. This also means there is no consideration of whether the campaign produces overall net benefits – in other words, whether the benefit of helping a single person are not outweighed by the cost of advice failures to many other users.

Chua et al. [13] note that well-intended security measures can have unintended consequences that harm users or the infrastructure, which often go unchecked because good intentions are assumed to produce only good outcomes. In the context of consumer IoT security advice, the campaign's metrics were not related to the real-world application of advice. No actual user testing of the advice had been done. Instead, the focus of funders and operators of the campaign was on indirect indicators, such as the usability of the website and the number of visitors:

> "Out of the top of my head, the number of visitors to the website has been fairly stable over the past few years, around 1 million visitors per year. And there is also a usability study done on the website every year." (P–GOV1).

Such metrics relate to the role of advice as signaling action, acting to highlight the visibility of the information and why it is being provided, rather than its actual effectiveness. The costs of the advice for users whose devices do not precisely match the advice are then externalized to those same users. Those user costs are de facto valued at zero in the rationalization that a few helped users would still be valuable, means the advice has net-positive effects (echoing an economics view [28]).

6.5 Legitimacy from Assumed Future Benefits

A final incentive was that the stakeholders can already gain legitimacy today from benefits to users that might arise in the future. P–GOV1 underscored that a gestation period of advice is often required for the widespread adoption of new guidelines. The efficacy of such a message would depend on its frequency of repetition. A parallel was drawn with the Belgian 'BOB' campaign[1] to reduce drink-driving, which took two decades to become fully integrated into societal norms. It is important to note, however, that this timescale contrasts sharply with the rapid evolution of the IoT device landscape.

Similarly, stakeholders mentioned how the campaign was meant to keep evolving and could become more effective in the future. P–GOV1 noted that the Dutch campaign previously focused on educating users about the importance of strong passwords for security. This emphasis later shifted towards the significance of updating devices. However, this change was motivated by the expectation that more security benefits could be gained by encouraging the installation of updates. Striking a balance between complexity and consumer comprehension, participants proposed various strategies to enhance the impact of the campaign, including segmenting the audience to provide tailored advice for distinct user profiles, refining the overall design of the campaign, and regularly reevaluating its core objectives. In addition, workshop participants suggested customizing communication methods to engage better and resonate with the specific needs and preferences of the target demographic. When the chairperson pointed out during the workshop that tailoring to user groups would not solve the problems with the advice, this was acknowledged, but these 'improvements' were still presented as reasons to continue the campaign. Just as in Hadan et al.'s work on PKI failures, the stakeholders in our study proposed refining existing approaches that are not able to address the core issues with the current advice [24].

[1]The BOB campaign, initiated in Belgium in 1995, is a road safety program that underscores the risks of driving under the influence and advocates for the use of designated drivers. Its success has led to its adoption in various European countries, including the Netherlands.

7 Discussion

Our research uncovered a puzzling situation that suggests a discrepancy between acknowledged problems and chosen solutions. Stakeholders acknowledged that the advice is mostly not fit for purpose, yet still they persist in disseminating it. This observation was validated in an additional round of engagement with the stakeholders around the workshop summary. We explained this outcome from the institutional incentives that leads stakeholders to produce advice irrespective of net user benefits. These findings have wider relevance. Other researchers have observed an overproduction and lack of prioritization of security advice, leading to users who are overwhelmed by the sheer volume of advice [46]. They do not explain why this situation exists and persists. Our findings on the institutional incentives of public and private stakeholders provide such an explanation: advice is produced for all kinds of other reasons than helping users.

7.1 The Dilemma of IoT Security Advice

The current approach to IoT security advice is not fit-for-purpose in many cases and hence does not adequately support users. This predicament creates a fundamental dilemma for stakeholders. On one hand, there are strong incentives to raise awareness about IoT security. On the other, providing users with broad or impractical advice risks confusion and may lead to wasted effort. The current advice campaign externalize the cost of the dilemma to users, requiring them to invest time and effort to apply advice across all their devices, even if such efforts might not succeed or are even impossible. As noted by Spaa et al., policy-makers tend to neglect the time and effort required by the target audience to implement policy recommendations [50]. In the case of IoT security, this oversight is acute as users are left to navigate a complex web of partial, potentially unworkable advice. This outcome highlights the urgent need to rethink how security support is provided in a rapidly evolving digital environment.

7.2 Balancing General Guidance Across Different Contexts

Signaling that IoT security is critical without providing actionable advice risks generating uncertainty for users, as also noted by Haney et al. [26], leaving users with no tangible steps to improve their situation. We echo Herley's sentiment, that it may be more beneficial to refrain from offering advice rather than persisting with vague or impractical advice [29]. In discussing digital services, Coles-Kemp et al. [14] proposed to combine top-down advice and bottom-up engagement, which could be explored here also; from our results, a notable touchpoint would be when technical experts provide instructions, as they currently do for the Dutch campaign

(Section 5.1.2), but Coles-Kemp et al. also emphasise a distinction between telling users what security is and aligning advice with what users are foremost concerned about, where some of the recommendations from Table 2 could relate more closely, such as easing connection of different device brands, and clear communication of security level to ensure a quality device is purchased.

7.3 Overreliance on Regulations

While regulations are gradually being developed and implemented, the problems that inspired the solutions outlined in Table 2 persist. It is essential to acknowledge that achieving a universally standardized IoT market, where *all* manufacturers *collectively* align all devices with the vision, is a formidable task, as it requires the collective effort and compliance of all manufacturers. P–REG2 noted while regulations sound nice on paper, enforcing them poses significant problems because of the sheer number and diverse nature of IoT devices. These are expected to increase, further complicating these regulatory challenges. Meanwhile, users continue to rely on generalized advice that does not guarantee actionable support. There is misplaced optimism in terms of "long-term engagement" and "future adjustments" that risks being more hopeful than realistic. Rather than waiting for a fully regulated IoT market, immediate strategies are needed to effectively support users in securing their devices within the existing digital landscape so as not to bet the success of advice campaigns wholly on regulations.

7.4 Legal, Political, and Socioeconomic Dimensions of Advice

For security-HCI researchers and practitioners, the current dynamic raises critical questions: How does the legal obligation to provide security advice impact the design of user interfaces, and how is information communicated to users? Woods & Ceross [62] have noted how legal decisions increasingly motivate action in cybersecurity, more so than technical accuracy (which requires great resources, time, and concentration of expertise to verify the correct action to address specific technical threats precisely). There is also a need to bridge scientific research (in this case, HCI) and the needs of policymakers [63]. A persistent challenge is the current uncertainty around whether users can effectively apply security advice or whether they have applied it correctly as this can unintentionally feed into Fear, Uncertainty, and Doubt (FUD) [22]. Socioeconomic disparities exacerbate these issues, as individuals with fewer resources have limited support channels and networks to rely on [45]. Consequently, rather than relying on expert assumptions alone, as seen in other research on advice-makers [40], it is more productive to uncover the practical barriers users face. This approach aligns with Herley's emphasis on weighing gains, costs, and motivations in security behaviors [29], shifting the focus from correcting user actions to accommodating them as constraints within the security system.

7.5 Political Dimensions and Future Directions

Where our interviews, covered in Section 5.1, identify setting a minimum security level through regulations, this also interacts with purchase touchpoints, for instance. This can lead to having minimum security levels by default, without such a reliance on users. This can be seen in, e.g., UK regulatory efforts which demand that consumer IoT products have automated updates and non-trivial network-accessible passwords when being introduced into the market. This would go one step further than the spirit of the retail engagement of Parkin et al. [43], where sales staff would aim to ensure that customers leave with some level of protection, even if it is the protection built into their purchased device by default.

Consumer IoT advice has, up to now, been researched as a behavior change and adoption issue, where our outcomes here signal the political element of public-facing advice, foremost to be seen to be positioning guidance on pertinent societal risks. This then links the body of research on security and privacy advice (e.g., [46, 47]) to a political element which was not previously signaled. It also aligns with well-established outcomes in, e.g., health interventions [10, 32], where advice-providers feel it necessary to take action – although acting on emerging risks has been visited in security advice [40], this did not explore the political reasons for needing to do so. A lack of institutional penalties for providing advice, contrasted with significant penalties for not providing it, forms the nexus of our research question: understanding not only why the advice system is faulty but also why it perpetuates despite its known flaws. A clear area for future work is to explore how to improve consumer-facing advice for IoT devices within this framework of moral, legal, and societal incentives – which must be respected – to determine if and where improvements can be found.

7.6 Beyond Regulations: Immediate, User-Centered IoT Security Solutions

Before seeking ways to increase user involvement, we should question how much involvement is genuinely necessary. While we have primarily focused on the role of advice-givers, it is crucial to acknowledge that other stakeholders, including retailers, community organizations, and technology support services, could play a part in bridging the gap between general recommendations and device-specific guidance. Similar joined-up IoT initiatives are now being seen in, e.g., the US 'Cyber Trust Mark' initiative [52]. If these efforts still require user input, that's when involving them—or an advocate skilled in behavior change—can guide more effective support methods, while considering distinct groups, such as families securing both their network and their children's access. Future work should consult stakeholders to explore metrics that are useful for evaluating a campaign but at the same time useful for whether specific pieces of advice are helpful for users effectively making actual security changes to devices. However, the question of responsibility for verifying the applicability of advice across diverse devices remains.

7.7 Alternative Approaches to IoT Security Support

Recognizing the need to improve IoT security, we propose focusing on concrete actions that align with the emphasis of policymakers in Jewell et al.'s study on linking research to concrete impacts, costs, and benefits [32]. This approach reduces the burden on users while achieving the same goals as advice campaigns by considering user costs and benefits [29]. Below, we outline two integrated recommendations:

1. IoT Security Services One immediate option is to leverage existing (commercial) services to replace the need for user-driven advice application. These services can address the same objective as advice campaigns by removing the costs and complexities users face. Services, such as network scanning, malware detection, and device-specific vulnerability analysis are already available for end users [5, 21, 23, 33, 64]. While commercial services offer more advanced capabilities, free options can still provide valuable protection, making cybersecurity accessible to a broader audience. Such services impact ISPs or other organizations who provide these tools, rather than expecting users to manually check if advice applies to their situation. This shifts the emphasis from signaling security to concrete actions that could be taken based on device identification in the local network.

2. Offsetting the Costs of Security Actions. Building on automated solutions, stakeholders could promote mechanisms that offset the impacts, costs, and benefits of applying security advice. Automated penetration testing frameworks for smart home devices, such as those proposed by Akhilesh et al., exemplify this approach [1]. Their framework aims to enable users without technical expertise to identify and mitigate common vulnerabilities and address the core problems of ambiguity and uncertainty regarding security actions. Although the framework has not yet been tested on real users, it presents a promising direction worth further exploration as it provides actionable remediation steps directly to users. These tools minimize ambiguity and uncertainty while requiring minimal user effort compared to users relying on confusing or incomplete advice.

By reframing security advice as concrete, user-friendly options, we can achieve the dual objectives of signaling the importance of security and enabling users to take meaningful action. For example, services like "Am I Infected?" [64] demonstrate how users can be supported by helping them to assess and improve their network and device security without requiring extensive technical knowledge. This approach collected telemetry on local IoT devices and their security issues via the browser, reducing the burden on users while providing insights that can inform security initiatives.

In alignment with Herley's perspective, we argue that stakeholders should prioritize evidence-based actions over generalized advice [29]. Transitioning from abstract recommendations to actionable security solutions would ensure that the benefits of security measures are realized while respecting the constraints of diverse user contexts.

8 Conclusion

In this paper, we explored the root causes behind the pervasive overproduction of sub-optimal consumer IoT security advice. Our primary concern extends beyond the sheer volume of advice and into the underlying mechanisms allowing for its persistence. Our findings reveal that the continual overproduction of advice is driven by a blend of moral, legal, and societal incentives rather than its effectiveness. We observed a critical imbalance in the system: stakeholders face no institutional penalties for providing advice, regardless of its effectiveness, while confronting significant penalties for failing to provide it. This dichotomy contributes to a cycle of advice that is more focused on maintaining a facade of responsibility rather than achieving measurable improvements in consumer IoT security. The externalization of user costs, which is a notable concern in the field of security usability, is evident in the current approach to consumer IoT security advice. The lack of institutional incentives to consider or measure the impact of this advice on users contributes to a disconnect between the campaigns' intentions and their real-world effectiveness.

Acknowledgments

We wish to thank the participants for their willingness to engage with the research and to take part in the various stages of the study. This publication is part of the RAPID project (Grant No. CS.007) financed by the Dutch Research Council (NWO).

References

[1] Rohit Akhilesh, Oliver Bills, Naveen Chilamkurti, and Mohammad Jabed Morshed Chowdhury. 2022. Automated penetration testing framework for smart-home-based IoT devices. *Future Internet* 14, 10 (2022), 276.

[2] Audrey Alejandro and Longxuan Zhao. 2024. Multi-method qualitative text and discourse analysis: A methodological framework. *Qualitative inquiry* 30, 6 (2024), 461–473.

[3] Debi Ashenden and Darren Lawrence. 2016. Security dialogues: Building better relationships between security and business. *IEEE Security & Privacy* 14, 3 (2016), 82–87.

[4] Australian Cyber Security Centre. n.d.. Personal Cyber Security: Advanced Steps. https://www.cyber.gov.au/protect-yourself/resources-protect-yourself/personal-security-guides/personal-cyber-security-advanced-steps. [Accessed 11-2023].

[5] Bitdefender. 2024. Bitdefender - Global Leader in Cybersecurity Software — bitdefender.com. https://www.bitdefender.com/en-us/. [Accessed 11-2024].

[6] John M Blythe, Nissy Sombatruang, and Shane D Johnson. 2019. What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? *Journal of Cybersecurity* 5, 1 (2019), tyz005.

[7] Brennen Bouwmeester, Elsa Rodríguez, Carlos Gañán, Michel Van Eeten, and Simon Parkin. 2021. " The Thing Doesn't Have a Name": Learning from Emergent {Real-World} Interventions in Smart Home Security. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, Virtual Conference, 493–512.

[8] Virginia Braun and Victoria Clarke. 2021. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology* 18, 3 (2021), 328–352.

[9] Bundesamt für Sicherheit in der Informationstechnik (BSI). n.d.. Smart Home. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Internet-der-Dinge-Smart-leben/Smart-Home/smart-home_node.html. [Accessed 11-2023].

[10] Paul Cairney and Kathryn Oliver. 2017. Evidence-based policymaking is not like evidence-based medicine, so how far should you go to bridge the divide between evidence and policy? *Health research policy and systems* 15 (2017), 1–11.

[11] George Chalhoub and Ivan Flechais. 2022. Data protection at a discount: Investigating the ux of data protection from user, designer, and business leader perspectives. *Proceedings of the ACM on Human-computer Interaction* 6, CSCW2 (2022), 1–36.

[12] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. "It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–16. https://doi.org/10.1145/3411764.3445691

[13] Yi Ting Chua, Simon Parkin, Matthew Edwards, Daniela Oliveira, Stefan Schiffner, Gareth Tyson, and Alice Hutchings. 2019. Identifying unintended harms of cybersecurity countermeasures. In *2019 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, IEEE, Piscataway, NJ, USA, 1–15.

[14] Lizzie Coles-Kemp, Rikke Bjerg Jensen, and Claude PR Heath. 2020. Too much information: Questioning security in a post-digital society. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376214

[15] Lorrie Faith Cranor. 2008. A Framework for Reasoning About the Human in the Loop. In *Usability, Psychology, and Security 2008 (UPSEC 08)*. USENIX Association, San Francisco, CA, 15 pages. https://www.usenix.org/conference/upsec-08/framework-reasoning-about-human-loop

[16] Cybersecurity & Infrastructure Security Agency. 2021. Securing Internet of Things (IoT). https://www.cisa.gov/news-events/news/securing-internet-things-iot. [Accessed from CISA News & Events].

[17] Cyberwiser. 2018. National Cyber Security Agenda; A cyber secure Netherlands. https://bit.ly/3ZgFqPy. [Accessed 12-2024].

[18] European Commission. 2021. Commission Delegated Regulation (EU) .../... of 29.10.2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive. Text with EEA relevance, SEC(2021) 382 final, SWD(2021) 302 final, SWD(2021) 303 final. https://single-market-economy.ec.europa.eu/system/files/2021-10/C_2021_7672_F1_COMMISSION_DELEGATED_REGULATION_EN_V10_P1_1428769.PDF Brussels, 29.10.2021, C(2021) 7672 final.

[19] European Parliament. 2024. European Parliament legislative resolution of 12 March 2024 on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=EP%3AP9_TA%282024%290130 Cyber Resilience Act.

[20] Federal Trade Commission. n.d.. Careful Connections: Building Security in the Internet of Things. https://www.ftc.gov/business-guidance/resources/careful-connections-keeping-internet-things-secure. [Accessed 11-2023].

[21] Fing. Accessed 12-2024. Network scanner at your fingertips - Manage your home network like a pro. https://www.fing.com/.

[22] Dinei Florêncio, Cormac Herley, and Adam Shostack. 2014. FUD: A plea for intolerance. *Commun. ACM* 57, 6 (2014), 31–33.

[23] F-Secure. 2024. Connected Home Security for service providers. https://www.f-secure.com/en/partners/solutions-and-services/connected-home-security. [Accessed 11-2024].

[24] Hilda Hadan, Nicolas Serrano, Sanchari Das, and L. Jean Camp. 2019. Making IoT Worthy of Human Trust. In *Proceedings of TPRC47: The 47th Research Conference on Communication, Information and Internet Policy*. Telecommunications Policy Research Conference, Washington, DC, 12 pages. Initial draft.

[25] Julie Haney, Yasemin Acar, and Susanne Furman. 2021. "It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Berkeley, CA, USA, 411–428. https://www.usenix.org/conference/usenixsecurity21/presentation/haney

[26] Julie M Haney and Susanne M Furman. 2023. User Perceptions and Experiences with Smart Home Updates. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, Institute of Electrical and Electronics Engineers (IEEE), Piscataway, NJ, USA, 2867–2884. https://doi.org/10.1109/SP46215.2023.00045

[27] Julie M Haney, Susanne M Furman, and Yasemin Acar. 2020. Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. In *HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22*. Springer, Springer, Cham, Switzerland, 393–411. https://doi.org/10.1007/978-3-030-50309-3_26

[28] Cormac Herley. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop (NSPW'09)*. ACM, Oxford, United Kingdom, 133–144. https://doi.org/10.1145/1719030.1719050

[29] Cormac Herley. 2013. More is not the answer. *IEEE Security & Privacy* 12, 1 (2013), 14–19.

[30] INCIBE - Instituto Nacional de Ciberseguridad. n.d.. Dispositivos IoT (Internet de las cosas). https://www.incibe.es/ciudadania/tematicas/dispositivos-iot. [Accessed 11-2023].

[31] I&O Research. 2022. Cybersecurity onderzoek Alert Online 2022. Available online at https://open.overheid.nl/documenten/ronl-f9dabadc3e7b330da895c60b98cf4db8ae54c95d/pdf.

[32] Christopher J Jewell and Lisa A Bero. 2008. "Developing good taste in evidence": facilitators of and hindrances to evidence-informed health policymaking in state government. *The Milbank Quarterly* 86, 2 (2008), 177–208.

[33] Kaspersky. 2024. Securing Your Smart Home. https://www.kaspersky.com/resource-center/preemptive-safety/smart-home-security. [Accessed 11-2024].

[34] Tadayoshi Kohno, Yasemin Acar, and Wulf Loh. 2023. Ethical frameworks and computer security trolley problems: Foundations for conversations. In *Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, USA, 5145–5162.

[35] Lorenz Kustosch, Carlos Gañán, Mattis Van't Schip, Michel Van Eeten, and Simon Parkin. 2023. Measuring Up to (Reasonable) Consumer Expectations: Providing an Empirical Basis for Holding {IoT} Manufacturers Legally Responsible. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, USA, 1487–1504.

[36] Ministry of Internal Affairs and Communications. n.d.. End User Security Guidelines. https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/enduser/enduser_security01_13.html. [Accessed 11-2023].

[37] T. Mitchell. 2021. How Do You Communicate Uncertainty and Promote Public Health—During COVID-19 and Beyond? https://hsph.harvard.edu/exec-ed/news/how-do-you-communicate-uncertainty-and-promote-public-health-during-covid-19-and-beyond/. [Accessed 11-2024].

[38] National Cyber Security Centre. n.d.. *Top tips for staying secure online*. (NCSC). https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates [Accessed 07-2024].

[39] National Cyber Security Centre Switzerland. n.d.. Cyber Tipp: IoT. https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2023/cybertipp-iot.html [Accessed 11-2023].

[40] Lorenzo Neil, Harshini Sri Ramulu, Yasemin Acar, and Bradley Reaves. 2023. Who Comes Up with this Stuff? Interviewing Authors to Understand How They Produce Security Advice. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. USENIX Association, Anaheim, CA, 283–299. https://www.usenix.org/conference/soups2023/presentation/neil

[41] Kathryn Oliver and Paul Cairney. 2019. The dos and don'ts of influencing policy: a systematic review of advice to academics. *Palgrave Communications* 5, 1 (2019), 1–11.

[42] Rikke Ørngreen and Karin Tweddell Levinsen. 2017. Workshops as a research methodology. *Electronic Journal of E-learning* 15, 1 (2017), 70–81.

[43] Simon Parkin, Elissa M Redmiles, Lynne Coventry, and M Angela Sasse. 2019. Security when it is welcome: Exploring device purchase as an opportune moment for security behavior change. In *Proceedings of the Workshop on Usable Security and Privacy (USEC'19)*. Internet Society, Internet Society, San Diego, CA, USA, 10 pages. https://doi.org/10.14722/usec.2019.23024

[44] European Parliament and Council of the European Union. 2022. NIS 2 Directive (Directive (EU) 2022/2555). https://eur-lex.europa.eu/eli/dir/2022/2555. [Accessed 12-2024].

[45] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2017. Where is the digital divide? A survey of security, privacy, and socioeconomics. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, Denver, CO, USA, 931–936. https://doi.org/10.1145/3025453.3025673

[46] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. 2020. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In *Proceedings of the 29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Boston, MA, USA, 89–108. https://www.usenix.org/conference/usenixsecurity20/presentation/redmiles

[47] Robert W Reeder, Iulia Ion, and Sunny Consolvo. 2017. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy* 15, 5 (2017), 55–64.

[48] Elvira Rodríguez, Arman Noroozian, Michel van Eeten, and Carlos Hernandez Gañán. 2021. Superspreaders: Quantifying the Role of IoT Manufacturers in Device Infections. Presented at the Annual Workshop on the Economics of Information Security (WEIS).

[49] Nissy Sombatruang, Tristan Caulfield, Ingolf Becker, Akira Fujita, Takahiro Kasama, Koji Nakao, and Daisuke Inoue. 2023. Internet Service Providers' and Individuals' Attitudes, Barriers, and Incentives to Secure IoT. In *Proceedings of the 32nd USENIX Security Symposium*. USENIX Association, Anaheim, CA, USA, 19 pages.

[50] Anne Spaa, Abigail Durrant, Chris Elsden, and John Vines. 2019. Understanding the Boundaries between Policymaking and HCI. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3290605.3300314

[51] Geordie Stewart and David Lacey. 2012. Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security* 20, 1 (2012), 29–38.

[52] The White House (US). 2023. Biden–Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers. https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/. [Accessed 08-2024].

[53] UK Parliament. 2021. Product Security and Telecommunications Infrastructure Bill. https://bills.parliament.uk/bills/3069 [Accessed 11-2023].

[54] Ministerie van Economische Zaken en Klimaat. n.d.. Doe je updates. https://veiliginternetten.nl/doejeupdates/. [Accessed 11-2023].

[55] Veerle van Harten, Carlos Hernández Gañán, Michel van Eeten, and Simon Parkin. 2023. Easier Said Than Done: The Failure of Top-Level Cybersecurity Advice for Consumer IoT Devices. arXiv:2310.00942 [cs.CR]

[56] Veerle van Harten and Michel van Eeten. 2023. Cybersecurity Workshop Smart Devices. https://doi.org/10.5281/zenodo.14872940 PowerPoint presentation.

[57] Tommy Van Steen, Emma Norris, Kirsty Atha, and Adam Joinson. 2020. What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity* 6, 1 (2020), tyaa019.

[58] Kami E Vaniea, Emilee Rader, and Rick Wash. 2014. Betrayed by updates: How negative experiences affect future security. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, Toronto, ON, Canada, 2671–2674. https://doi.org/10.1145/2556288.2557275
[59] Swaathi Vetrivel, Brennen Bouwmeester, Michel van Eeten, and Carlos H Gañán. 2024. {IoT} Market Dynamics: An Analysis of Device Sales, Security and Privacy Signals, and their Interactions. In *Proceedings of the 33rd USENIX Security Symposium*. USENIX Association, Philadelphia, PA, USA, 7031–7048.
[60] Charles Weir, Ingolf Becker, and Lynne Blair. 2021. A passion for security: Intervening to help software developers. In *ICSE-SEIP '21: Proceedings of the 43rd International Conference on Software Engineering: Software Engineering in Practice*. IEEE, IEEE, Madrid, Spain, 21–30. https://doi.org/10.1109/ICSE-SEIP52600.2021.00011
[61] Charles Weir, Ingolf Becker, and Lynne Blair. 2023. Incorporating software security: using developer workshops to engage product managers. *Empirical Software Engineering* 28, 2 (2023), 21.
[62] Daniel W Woods and Aaron Ceross. 2021. Blessed are the lawyers, for they shall inherit cybersecurity. In *Proceedings of the 2021 New Security Paradigms Workshop*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3498891.3501257
[63] Qian Yang, Richmond Y Wong, Steven Jackson, Sabine Junginger, Margaret D Hagan, Thomas Gilbert, and John Zimmerman. 2024. The Future of HCI-Policy Collaboration. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, Honolulu, HI, USA, 1–15. https://doi.org/10.1145/3613904.3642771
[64] Yokohama National University (YNU). 2024. am I infected? https://amii.ynu.codes/. [Accessed 12-2024].

A Pre-Interview Questionnaire on IoT Security and Consumer Support

A.1 Background Information

A.1.1 Position and Role:

- What is your position
- How long have you been working in your current role or organization?
- Can you provide a brief description of your position, including main duties and responsibilities?
- Are you the key decision maker or influencer in your organization regarding IoT security and consumer support?

A.1.2 Organizational Overview:

- Are you familiar with current industry standards and guidelines for IoT security?
- Please provide a brief overview of your organization, covering its objectives, funding sources, and the number of employees.

A.2 User Support and Security of IoT Devices

A.2.1 Consumer Role and Resources:

- What is your organization's stance on the role of consumers in ensuring the safety of consumer IoT devices?
- Does your organization provide resources to consumers to improve the security of consumer IoTs? If so, could you share them?

A.2.2 Monitoring Consumer Support:

- Does your organization monitor how well consumers feel supported in securing their consumer IoTs? If so, how is this monitored, and what are the recent findings?

A.2.3 Benefits and Impact:

- What benefits would your organization experience if consumers could enhance the security of their consumer IoTs? What changes would you expect to notice in your work?

A.3 Feedback on Previous Research Findings

A.3.1 Research Findings Prior Research:

- What is your opinion on the research findings we shared? Are they recognizable to you?
- If yes, what do you think should be done to improve the situation? If no, why do you think they are not recognizable?

B Post-Workshop Interview Questions

The workshop participants were invited to a brief call (maximum 15 min) to discuss and provide feedback on our conclusions that were sent to them in the form of a report. First, we sought their general impressions of the report to gauge the extent to which they agreed with the write-up of our findings from the workshop. Subsequently, the following two topics were addressed during these calls:

B.1 Disadvantages of Advice That is Not Fit for Purpose

- Discuss the challenges you expect users would face when attempting to follow security advice that is not relevant or applicable to their specific devices. What disadvantages or issues would you expect to observe in these scenarios?

B.2 Supporting Knowledge-Deficient, Motivated Users

- What strategies or measures could be implemented to assist users who are motivated to secure their devices, but lack sufficient knowledge to determine if the given advice is applicable to their devices?

C Workshop Guideline

C.1 Introduction

C.1.1 Purpose and Goals. The workshop aimed to collaboratively evaluate the effectiveness of the Dutch security awareness campaign, focusing on participants' recognition of the disconnect between provided security advice and its practical application.

C.2 Workshop Design

C.2.1 Format. The workshop was structured in two main parts:

(1) Ranking Courses of Action: Participants ranked three potential paths: (1) continuing the current campaign, (2) adjusting it before proceeding, or (3) stopping it entirely. This was followed by small group discussions using flip charts and sticky notes to document pros and cons and a plenary session to share outcomes.

C.2.2 Agenda.

(1) Evaluating Solution Directions: After a coffee break, participants evaluated nine potential solution directions outlined in Table 2, derived from pre-interviews. They selected their top three choices and discussed them in small groups. A final ranking session determined the most favored solutions:

Time	Activity
14:00	Introduction: Overview of workshop goals and format.
14:10	Brainstorm Session Part I: Identify challenges and propose initial solutions.
14:35	Break.
14:45	Brainstorm Session Part II: Refine solutions, focusing on practical implications.
15:25	Break.
15:35	Summary and Conclusion: Recap key findings, with an open floor for final comments.

Table 4: Workshop Schedule

automating security features and establishing minimum security standards for IoT devices through regulation.

C.2.3 Duration. The workshop was scheduled for 2 hours, utilizing structured ranking, group discussions, and plenary sessions.

C.3 Target Audience and No. of Participants

The workshop targeted key contributors to the Dutch security awareness campaign, aiming to involve a max. of 15 participants. The final participant count was nine, representing essential stakeholders.

C.4 Preparation

C.4.1 Timeline and Planning.

- Development of research proposal: September – December
- Ethics approval and participant outreach: January – February
- Workshop preparations and event: February.

C.4.2 Presenter Selection. The lead author facilitated the workshop, supported by the chairperson, who guided discussions and ensured clarity. The lead author managed the documentation of outputs.

C.5 Implementation

C.5.1 Facilitation Techniques and Activities. Active learning was encouraged through group discussions, hands-on activities, and open-floor sharing during plenary sessions. Group discussions utilized flip charts and sticky notes for capturing insights, along with structured ranking exercises and interactive plenary sessions. See [56] for the PowerPoint slides used during the workshop.

C.5.2 Steps Taken by the Chairperson to Maintain Impartiality. The chairperson took several steps to maintain impartiality and avoid dominant voices during discussions:

- Balanced Contribution: The chairperson actively monitored participation and encouraged quieter participants to share their views.
- Group Division Strategy: Participants from the same organization were intentionally separated to ensure diverse perspectives.
- Neutral Questioning: The chairperson used open-ended questions to maintain an unbiased tone.
- Summary of Contributions: Contributions were summarized to ensure understanding and prevent dominance.
- Guiding the Discussion Back on Topic: The chairperson gently guided the conversation back on topic when needed.

C.6 Evaluation

C.6.1 Gathering Participant Feedback. Feedback was collected through the group discussions and post-interviews.

C.6.2 Key Elements.

Clear Objectives and Outcomes. The workshop aimed to evaluate the campaign's effectiveness and identify feasible improvement directions.

Participant Roles and Expectations. Participants engaged in ranking, discussing, and identifying solutions. The roles included:

- Government Officials (GOV): Provided insights on regulatory requirements.
- Regulators (REG): Contributed perspectives on policy alignment.
- Public-Private Partnership Representatives (PPP): Highlighted collaboration opportunities.
- Internet Service Providers (ISP): Provided network infrastructure expertise.
- Manufacturers (MNF): Focused on product security standards.
- Consumer Association Representatives (CNS): Highlighted consumer concerns.

C.7 Ethical Considerations

Informed consent was obtained for recording the workshop, with all data anonymized. Participants could withdraw at any time without penalty.

D First Round - Detailed Flip Chart Distributions

Group	Participant Type	1st Choice	2nd Choice	3rd Choice
Preferences Before Discussion				
Group 1	P–REG1	Adjust	Continue	Quit
	P–ISP1	Adjust	Continue	Quit
	P–GOV1	Continue	Adjust	Quit
Group 2	P–PPP	Adjust	Quit	Continue
	P–MNF	Continue	Adjust	Quit
Group 3	P–CON	Continue	Adjust	Quit
	P–GOV2	Adjust	Quit	Continue
	P–ISP2	Adjust	Continue	Quit
Preferences After Discussion				
Group 1	P–REG1	Adjust	Continue	Quit
	P–ISP1	Adjust	Continue	Quit
	P–GOV1	Continue	Adjust	Quit
Group 2	P–PPP	Adjust	Continue	Quit
	P–MNF	Adjust	Continue	Quit
Group 3	P–CON	Continue	Adjust	Quit
	P–GOV2	Adjust	Continue	Quit
	P–ISP2	Adjust	Continue	Quit

Table 5: Summary of Flip Chart Contributions from Group Discussions - Round 1. This table zooms in on the distribution of preferences to continue, adjust or quit the campaign across groups and participant types before and after the group discussions.

E Codebook

Main Themes	Definitions	Example Quotes
Responsibilities for keeping IoT devices secure	Covers the provision, implementation, and support in this implementation of security measures to protect consumer IoT from unauthorized access, data breaches, and cyberattacks, ensuring their safe and private operation.	"They need to be involved, right? Piece by piece, education can lead to awareness, and you do notice that. It's also been getting better lately, hasn't it? There's also a bit of awareness." (Source: P–ISP1)
Characteristics & dynamics of awareness campaign	Refers to the attributes and processes involved in the development and implementation of awareness campaigns aimed at educating the public about cybersecurity risks and practices. It encompasses the campaign's objectives, target audience, communication channels, messaging strategies, evaluation methods, and ongoing adjustments based on feedback and evolving threats.	"Yes, and they don't pay us, because we're not paid by private parties. Otherwise, there could be a conflict of interest, right? If I don't do my job well, or if I don't write well enough about [app name], then [app name] would say, 'You're not getting paid.' No, it's actually a subsidy." (Source: P–PPP)
Perspectives on previous research findings	Responses of those involved in the Dutch public awareness campaigns on previous research findings that highlight the issues with general security advice which often is not verified with users as being feasible or effective.	"Well, what I think of it is that it is in any case not surprising." (Source: P–CNS)
Perceived challenges & impediments	Understanding stakeholder challenges in enhancing consumer IoT security.	"I think that the expectations of consumers are far too high. Yes. The idea that people will change their passwords themselves and also understand that 'admin admin' is not a good password. That is simply not realistic." (Source: P–CNS)
Regulatory expectations & outlook	Expectations on the changing regulatory landscape and how this influences the management of cybersecurity risks. It encompasses the latest regulatory developments, emerging compliance requirements, and the potential impact of these changes on consumers. This theme also considers the future direction of cybersecurity regulations and the challenges and opportunities they present.	"And even if that regulation does exist, right? I mean, what, they're not going to test every product, enforcing it is another story." (Source: P–REG2)
Institutional incentives	Navigating policy, compliance, and motivations in consumer IoT security advice.	"We must strengthen the ecosystem and... for users, and then you're talking about citizens, consumers, but also about businesses, smaller businesses." (Source: P–GOV1)

Table 6: Codebook with main themes, definitions, and example quotes.

F Workshop Script

Est. Time	What to Ask and Tell	Description
	Before the Workshop	
Preparation	Organizers	Ensure materials (flip charts, sticky notes) are ready, and the room is set up for discussions.
Distribute Pre-Workshop Materials	Participants	Provide an overview of workshop goals, structure, and expectations. Ask participants to review preliminary reading materials.
	During the Workshop	
10 mins	Introduction and Consent	Tell participants about the workshop's purpose, expected outcomes, and ethical considerations. Ask for informed consent before proceeding.
"Hello! Thank you for joining today's workshop. Our goal is to evaluate the effectiveness of the Dutch security awareness campaign and assess whether the advice provided is practical. This session is designed to encourage discussion and collaboration. Before we begin, I'd like to go over some ethical considerations—participation is voluntary, and all responses will be anonymized."		
25 mins	Ranking Courses of Action	Ask participants to rank three options: (1) continue the campaign, (2) adjust and proceed, or (3) stop it entirely. Facilitate small group discussions using flip charts and sticky notes to document reasoning. Ask groups to share insights in a plenary session.
"Let's start by ranking the possible actions we can take regarding the security awareness campaign. You have three choices: continuing as is, making adjustments, or stopping entirely. Please use the sticky notes to jot down the pros and cons of each option, then rank them accordingly. After this, we'll discuss your rankings in small groups."		
10 mins	Break	Allow participants time to process discussions and network informally.
40 mins	Evaluating Solution Directions	Ask participants to evaluate nine proposed solutions. Have them select their top three and discuss their viability in small groups. Ask them to explain their rankings and collectively decide on the most favored solutions.
10 mins	Break	Allow participants time to process discussions and network informally.
"Now, we will focus on potential solutions. Based on previous interviews, nine possible directions were shared with us. Please review these solutions and pick the three you find most promising. Consider feasibility, effectiveness, and impact. We will then discuss our choices in small groups before ranking them collectively."		
15 mins	Summary and Conclusion	Summarize key insights, reiterate important points, and ask for final reflections. Open the floor for any remaining comments.
"Before we wrap up, let's summarize our key takeaways. What were the strongest solutions? Do you feel our discussion today provided valuable insights? If there are any last thoughts or reflections, now is the time to share."		
	Follow-up After the Workshop	
10 mins	Participant Feedback	Ask participants about their experience, what worked well, and areas for improvement. Collect structured feedback through discussions or a short survey.
"We appreciate your participation today. Before you leave, we'd love to hear your thoughts on how the session went. What did you find useful? What could be improved? Your feedback will help refine future workshops."		
Documentation	Organizers	Compile notes from flip charts, rankings, and discussions. Ask participants if they have any additional insights to share before finalizing the documentation.

Table 7: Workshop Schedule