

USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Who Can Actually Follow IT-Security Advice? Exploring the Usability of IT-Security Advice

Dennis Lawo, Jenny Hindrichs, and Gunnar Stevens, *University of Siegen*

https://www.usenix.org/conference/soups2026/presentation/lawo

This paper is included in the Proceedings of the Twenty-Second Symposium on Usable Privacy and Security.

August 24–26, 2026 • Hannover, Germany

ISBN 978-1-939133-59-5

Open access to the Proceedings of the Twenty-Second Symposium on Usable Privacy and Security is sponsored by USENIX.

Who Can Actually Follow IT-Security Advice? Exploring the Usability of IT-Security Advice

Dennis Lawo
University of Siegen

Jenny Hindrichs
University of Siegen

Gunnar Stevens
University of Siegen

Abstract

Individuals are increasingly expected to rely on publicly available IT-security advice to protect themselves against cyberattacks and data breaches. However, little is known about how usable such IT-security advice is in practice for ordinary users. In this paper, we empirically evaluate the perceived usability of IT-security advice drawn from multiple publicly available sources. Based on an adapted System Usability Scale survey and qualitative analysis, we explored the perceived usability of IT security advice. Our results show substantial variation in usability across pieces of advice. User characteristics such as age, education, and self-assessed IT-knowledge are associated with differences in perceived usability, whereas traditional text-metrics show limited explanatory power. We discuss implications for the user-centred design and evaluation of IT-security advice. This work contributes to the usable security literature by providing empirical evidence on policy usability and by highlighting the role of user differences in the perceived usability of IT-security advice.

1 Introduction

Advancing digitalisation and ubiquitous computing have fundamentally reshaped societies, creating new opportunities but also new risks. Cyberattacks, data leaks, and security breaches are now everyday occurrences that threaten not only organisational infrastructures but also the well-being of individual users [3, 67]. In response, organisations, governments, and civil actors have issued a growing number of IT-security advisories to mitigate these threats [44, 58]. Similar to traditional information security policies (ISPs), this advice aims to ensure the confidentiality, integrity, and availability of information assets [51, 58], yet the effectiveness depends critically on whether users can understand and apply them in practice [72, 77].

However, usability is not well integrated into the design process for IT-security advice [72]. This comes at the cost of a lack of end-user centricity, e.g., consideration of their individual contexts, such as age, education, or IT-skills [40, 72, 77]. A one-size-fits-all advice is unlikely to be usable, but context and user-specific advice is required [77]. In general, the usability of IT-security advice has received little attention. Usability, understood as a relational property between artefacts, users, and contexts [12, 60], is crucial: even technically sound policies fail if they are inaccessible, overly complex, or misaligned with everyday practices [89, 96]. Recent conceptual work has argued for reconceptualising ISPs as Usable Information Security Policies (UISPs), integrating usability alongside compliance [56, 57]. However, empirical evidence on ISP (perceived) usability remains scarce.

In light of this gap, we address the following research questions:

- **RQ1:** How do end-users perceive the usability of IT-security advice?
- **RQ2:** Which end-user characteristics influence perceived usability?
- **RQ3:** What textual design aspects influence perceived usability?

To answer these questions, we conducted an exploratory mixed-methods study evaluating the usability of 29 pieces of IT-security advice falling into the category of governmental, civil associations, and commercial online services. Adapting the Information Security Policy Usability Scale (ISPUS) [57], we collected assessments of the pieces of IT-security advice from 348 participants. We complemented this quantitative evaluation with a qualitative analysis of policy texts, focusing

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

on risk communication, topic and problem framing, institutional self-positioning, and user subject positions.

Our quantitative exploratory analyses reveals that user characteristics (age, education, IT/security knowledge) and policy identity explain significantly more variance in usability scores than text features such as readability or sentence length. Moreover, our analysis provides evidence for an over- and under-assessment of IT-skills in relation to perceived usability. Complementing these findings, our qualitative analysis reveals recurring deficits: measures are often framed as abstract norms without causal justification, lack operational detail, and rely heavily on sustained user cognitive attention, which may hinder comprehension and possibility-to-follow.

This paper contributes to the SOUPS discourse by an exploratory mixed-methods analysis of the usability of public IT-security advice. We show that user characteristics, not traditional text metrics, are the primary drivers of perceived usability. Because perceived usability is a prerequisite for engagement, as prior SUS research indicates [76, 92], understanding these user-driven differences is essential. By adapting and applying the ISPUS scale in an exploratory manner, without aiming to fully validate the instrument or evaluate specific advice items, we provide an initial foundation and concrete directions for designing more inclusive, user-centred security communication.

2 Related Work

2.1 End-User IT-Security Advice

IT-security advice has been a topic of interest within many studies [20, 32, 36, 41, 48, 83, 85–87, 102, 104], e.g., studies focusing on the creation of advice [72], the types of advice [44], or the usability of advice [58]. Security advice for end-users comes in various forms, e.g., as governmental guidelines, product manuals, training, or community-based communications [44, 58]. Thus, IT-security advice for end-users comes in various forms and ranges from formal [53, 54, 66, 93, 106, 109] to informal [35, 42, 55, 74, 81, 83, 99, 103] communication styles. Thus, these forms and styles affect the security knowledge, perceptions, and behaviours of end-users [14, 17, 74, 80, 84, 85]. Although end-user advice, follow a similar logic as an ISPs for end-users in organisations, behaviours are not influenced by motivators, such as legal sanctions [58], but positive motivators, e.g., gamification [23, 25, 37], or facilitating factors, e.g., a high usability [45, 64, 79, 108]. Although the latter are also relevant in organisational contexts [58].

Accordingly, many researchers have analysed the quality of security advice for experts [1, 2, 39] and non-experts [4, 71, 86].

One prevailing issue is the usability of security advice [58, 72, 77]. From the research on traditional ISPs, the importance of content, i.e., actionability [6, 27, 38, 63, 95], relevancy for the work practices [26, 49, 95], and congruency [38, 49, 65] with other types of documents, presentation, i.e., avoidance of information overload and a clear communicative structure [7, 21, 49] as well as an ease or reading and understanding [8, 38], and Management, i.e. well-defined processes to keep the advice up-to-date with relevant and state-of-the-art information [6, 49, 63, 100]. Regarding end-user advice in non-organisational settings, there is little research on the usability of such artefacts. Although less in focus, research on end-user security advice confirms the importance of comprehensiveness [33], understandability [91], as well as the findability of information [33, 91].

Neil et al. [72], for example, found that most authors consider usability; however, they do not follow a specific method or goal, and sometimes even consider their own perspective a good indicator. Moreover, they found that authors struggle with broad audiences and diverse technical contexts, leading to general-purpose rather than relevant advice. However, such alignment is crucial, as users have diverse educational and ability backgrounds [40]. Moreover, their security attitudes substantially differ [104]. Given this, a one-size-fits-all advice is unlikely to be usable, but context and user-specific advice is required [77]. Moreover, non-experts should be granted a level of accessibility [40, 70] and the ability to prioritize advice [77].

In summary, there is a large corpus of research on ISPs and security advice, but putting advice into practice is difficult, "as usability is still a hurdle to achieving security" [77].

2.2 Measuring Usability of Security Advice

Ensuring that security advice is usable not only promotes effective daily use but also reduces users' cognitive load. This prevents security fatigue and enhances satisfaction with the artefact's use. Systematic usability evaluation within the process of designing advice, therefore, helps to uncover critical incidents and obstacles that might cause ignorance of the advice [58, 72, 77].

However, usability presents a theoretical construct that is hard to measure [90]. Often, usability is misunderstood as an inherent characteristic of an artefact, yet it is an emergent, relational property that depends on interactions of users, products, tasks, and environments [12, 60]. Usability is not an inherent product characteristic but an emergent property arising from the interaction between users, goals, artefacts, and context [13, 29].

The user-centred design methodology advocates an iterative approach, with multiple design and evaluation cycles, in which the usability of an artefact is assessed during and after the design process using formative and summative methods [22, 34, 107].

Formative evaluation methods aim to provide feedback on the ongoing artefact design to improve its effectiveness and relevance [43]. Most commonly, the methods used are qualitative and aim to gain a deep understanding of the artefact's strengths and weaknesses, such as interviews [47], focus

groups [50], contextual inquiries [82], heuristic analyses [75], and think-aloud testing [107] to identify weaknesses in early design iterations and improve presentation and contextual fit. Moreover, formative advice or ISP evaluations primarily focus on individual aspects of the presentation, such as readability [8, 38]. The goal of such evaluation is to gather feedback to enhance the presentation, making it more likely that users understand and follow the advice/ISP.

Summative evaluation focuses on assessing the overall usability of an artefact, e.g., the advice, once it has been fully developed and implemented [11, 28]. This type of evaluation utilises comprehensive metrics to provide a conclusive judgement on the usability of individual directives or the entire artefacts. By providing a summative score, stakeholders can determine whether the advice meets the usability standards. Moreover, they can identify areas for further improving the content or aligning it with the context. Regarding this, objective metrics are externally observable characteristics, such as the number of errors in a given task [59], the number of tasks successfully completed by the user [88], or the time required to complete a task [98]. They provide reliable indicators of usability, particularly of task performance effectiveness and efficiency. Yet, they do not capture the subjective aspects of usability, such as user satisfaction, perceived work conditions, or perceived barriers. Subjective metrics, in contrast, are evaluative measures that collect user feedback through structured questionnaires or rating scales on perceptions, opinions, or judgments, such as the Single Ease Use (SEQ) questionnaire [105]. In the ISP context, questionnaires on compliance behaviour [68, 94] are used. However, such methods primarily measure adherence rather than the broader usability factors that influence compliance. A holistic usability metric should consider a range of indicators that influence how easily and effectively employees can comply with these policies. For such a holistic usability measure, Lawo and Stevens suggest adapting the System Usability Scale (SUS) [57], which has already been used in other security-related fields [73].

2.3 Information Security Policy Usability Scale

The SUS has long been recognised for its versatility, reliability, and applicability across a wide range of systems and environments [18, 61], including security-related domains such as the evaluation of safety signs [73]. Its ability to consolidate multiple usability dimensions into a single, interpretable score [10] makes it a promising foundation for assessing the usability of ISPs and security advice [57, 58].

In line with prior adaptations of the SUS to new contexts [46, 73], Lawo and Stevens [57] adapted the theoretical constructs to the domain of ISP compliance and then adjusted the wording of each item accordingly. This was necessary because the original SUS items assume the *use* of a *system*, whereas ISPs require *compliance* with organisational rules and guidance. Thus, terms such as "use" and "system" were systematically replaced with "comply" and "information security policy," to align the questionnaire with established determinants of ISP usability. Table 1 presents the original SUS items alongside their ISPUS counterparts.

The ISPUS is administered analogously to the SUS [52]: participants are presented with an ISP or an excerpt and a request to reflect on prior experiences. Based on these impressions, they complete the ten-item questionnaire, which is scored using the standard SUS procedure [61]. The resulting score provides a normalised measure of usability, enabling systematic comparison across policies, organisations, or user groups.

Although the ISPUS offers a theoretically grounded and systematically adapted instrument, it has not yet undergone empirical validation. To date, no study has evaluated its psychometric properties, practical applicability, or sensitivity to differences in design.

3 Methodology

To investigate the usability of IT-security advice, we adopted a mixed-methods approach that combines quantitative and qualitative analyses. This design allows us to capture both measurable differences in usability perceptions across user groups and policies, as well as deeper insights into the structural and linguistic characteristics of the policies themselves. The quantitative component is based on survey data collected with the ISPUS, while the qualitative component involves textual analysis of the policies. Together, these methods provide a comprehensive understanding of how ISPs are perceived and experienced by individuals.

3.1 Quantitative Study

3.1.1 Survey Design

To assess the perceived usability of individual pieces of IT-security advice as a prerequisite for engagement [76, 92], we used an adapted ISPUS as proposed by [57]. ISPUS adapts the System Usability Scale (SUS) [18] to the context of information security policies and measures, treating usability as a relational property between users, rule content, and application situation. Such minimal and contextualizing adaptations of the SUS have proven to measure usability in different context, e.g., safety signs [73]. For this study, we slightly adjusted the wording of the ISPUS items to inquire into the usability of IT-security advice, i.e., *ISP* was replaced with *IT-security advice* and *comply* with *follow*. This adaptation was accompanied by an internal review and a small pilot with ten participants to ensure clarity and comprehensibility of the adapted items.

Participants rated the statements on a five-point Likert scale (1 = strongly disagree, 5 = strongly agree). Positive and negative items were alternated to reduce response bias. The re-

Table 1: The original SUS Statements [18], the ISPUS statements [57], and the IT-Security ISPUS adaptation.

#	Original SUS Question	ISPUS Question	Adapted ISPUS Question
01	I think that I would like to use this system frequently.	I think that I would like to comply with this ISP frequently.	I think that I would like to follow this IT-security advice frequently.
02	I found the system unnecessarily complex.	I found the ISP unnecessarily complex.	I found the IT-security advice unnecessarily complex.
03	I thought the system was easy to use.	I thought the ISP was easy to comply with.	I thought the IT-security advice was easy to comply with.
04	I think that I would need the support of a technical person to be able to use this system.	I think that I would need the support of a colleague or supervisor to be able to comply this ISP.	I think that I would need the support of a IT-skilled person to be able to comply this IT-security advice.
05	I found the various functions in this system were well integrated.	I found the ISP to be well integrated into my daily work procedures.	I found the IT-security advice to be well integrated into my daily life.
06	I thought there was too much inconsistency in this system.	I thought there were too many inconsistencies within this ISP.	I thought there were too many inconsistencies within this IT-security advice.
07	I would imagine that most people would learn to use this system very quickly.	I would imagine that most people would learn to comply with this ISP very quickly.	I would imagine that most people would learn to comply with this IT-security advice very quickly.
08	I found the system very cumbersome to use.	I found this ISP very cumbersome to comply with.	I found this IT-security advice very cumbersome to comply with.
09	I felt very confident using the system.	I felt very confident in correctly complying with this ISP.	I felt very confident in correctly complying with this IT-security advice.
10	I needed to learn a lot of things before I could get going with this system	I needed to learn a lot of things before I could comply with this ISP.	I needed to learn a lot of things before I could comply with this IT-security advice.

sponses were aggregated according to SUS logic and transformed to a scale from 0 to 100, with higher values indicating higher perceived usability.

In addition, we collected demographic and experience-related characteristics in order to analyse their influence on usability perception (RQ2). These included age, gender (male, female, diverse), highest educational qualification (coded according to the German Qualifications Framework [24]), self-assessed knowledge of handling digital devices (five-point scale from 'no knowledge' to 'very good knowledge'), knowledge of IT-security and data protection (also a five-point scale), and professional status (employee, civil servant, job seeker, student, pupil, pensioner, other).

The questionnaire was designed so that all participants were informed about the aim, procedure, and data protection provisions of the study, and they had to give their voluntary, informed consent to participate. Demographic data was then collected. All participants then evaluated three security advisories, one after the other. At the beginning of each evaluation round, the relevant rule or associated IT-security advice was displayed, accompanied by a brief instruction to read the advice carefully, reflect on its significance for their everyday lives, and then assess its suitability for everyday use using the adapted ISPUS items. This procedure was repeated identically for all three randomly assigned rules.

The IT-security advice presented in the following, was selected in line with Holton [44] and Lawo et al. [58] to cover the most common categories of IT-security advise. See appendix for details.

- Governmental Sources:
  - 8 pieces of advice from Federal Office for Information Security: Smart home – securely connecting your living space [19]
  - 10 pieces of advice from European Agency for Cybersecurity: Cyber Hygiene [30]
- Civil Associations:
  - 7 pieces of advice from European Consumer Centres Network: Data protection on the Internet: How can I protect my data? [31]
- Commercial Online Services:
  - 6 pieces of advice from PayPal: Help us protect your PayPal account [78]

3.1.2 Data Collection

Data was collected via the online survey platform `QuestionPro`[1]. The platform provided a representative sample of the German population for our survey. Participants had

[1] https://www.questionpro.com/

to be at least 18 years old and have sufficient German language proficiency. Before the study began, all participants were informed about its purpose, procedure and data protection regulations and had to actively agree to participate. Remuneration was paid in accordance with QuestionPro's standard terms and conditions. All participants received the questionnaire as described in the previous section and followed the same process: first, demographic information was collected, then participants evaluated three IT-security advice items one after the other using the ISPUS items. Participants were randomly assigned to these pieces of advice three pieces of advice from the full set. We did not stratify by source category nor did we ensure per-item level representativeness of the sample. A total of 565 people took part in the study. After removing incomplete or duplicate entries, an adjusted sample of 348 valid responses remained. To remove non-reliant answers, we filtered for a test question that asked to select a specific likert-value. Depending on the advice, between 25 and 41 complete assessments were valid. The imbalance in per-item responses reflects natural variation in random draws and platform-specific dropout patterns.

3.1.3 Analysis

The analysis included descriptive evaluations, reliability and validity tests, and regression models to answer the research questions.

First, we calculated descriptive statistics for all ISPUS items and the correlations between individual items and total scores to obtain initial indications of response distributions and item consistency.

The ISPUS [57] has not yet been subjected to a systematic psychometric evaluation, and no evidence is available regarding its measurement properties in the context of information-security advice. Because the present study employs an adapted version of the instrument tailored specifically to this domain, the reliability and dimensionality of the modified scale cannot be assumed. A psychometric assessment was therefore necessary to examine whether the adapted ISPUS functions as a coherent and reliable measure in this application context. To evaluate the internal consistency of the adapted scale, we calculated Cronbach's α. Values above $\alpha > .70$ are generally interpreted as an indicator of sufficient reliability. In addition, we explored the instrument's dimensionality by conducting an exploratory factor analysis and inspecting the eigenvalues of the extracted components. Inline with prior SUS research, we expect a dominant main component with factor loadings of at least $> .40$, as well as a smaller factor. All other factors should be neglectable, as the SUS is known for the factors usability and learnability.

To investigate the influence of the advice's structural and linguistic features, we supplemented the dataset with automatically calculated text metrics. These included readability indices (Flesch Reading Ease, Wiener Sachtextformel), word, sentence and syllable counts, character and letter counts, polysyllable and monosyllable counts, average sentence length, type-token ratio and the proportion of passive sentence constructions. The calculations were performed using `textstat`[2] and `spaCy`[3]. Prior to the regression analyses, we performed a variance inflation factor (VIF) [5] analysis to identify multicollinearity. Highly correlated variables were removed to obtain a non-redundant subset of text features for the models. To answer RQ2, we estimated several OLS models with the ISPUS score as the dependent variable. The models included user characteristics, text characteristics, and policy identities (Advice ID) as well as combinations of these predictor groups. The reference categories were male (gender), unemployed (employment status), and the rule with the `ID-22`. We reported unstandardised coefficients, robust standard errors, and AIC/BIC values. In addition, we performed pairwise ANOVA model comparisons to evaluate relative model goodness.

To investigate the factors influencing the perceived usability of information security advice, several linear regression models containing different predictor groups were specified. In addition, a residual approach was chosen to separate objective competence from subjective over- or underestimation. To this end, self-assessments of IT and information security competence were regressed on age and educational level. The resulting residuals (`IT_over_under`, `SEC_over_under`) capture the individual deviation between expected and reported competence. Positive values can represent a relative overestimation, negative values a underestimation. Using these residuals instead of the original self-assessments prevents age-related differences in self-confidence from distorting the models and makes it possible to examine the independent contribution of subjective competence perception to perceived usability more precisely. Overall, this approach allows for a systematic exploratory analysis of the contribution of user characteristics, text characteristics, and differences between the individual pieces of advice to the explanation of the ISPUS score.

A total of eight models were estimated:

- **Model M1:** User characteristics only
- **Model M2:** Text characteristics only
- **Model M3:** ISP-specific fixed effects (*Advice ID*) only
- **Model M4:** User characteristics + text characteristics
- **Model M5:** User characteristics + Advice ID
- **Model M6:** Text characteristics + Advice ID
- **Model M7:** All Features
- **Model M8:** User characteristics + Advice ID + Residual of Self-Assessment

[2] https://textstat.org/
[3] https://spacy.io/

The user characteristics included demographic variables (age, gender, education, occupational status) as well as the self-assessments of IT competence and information security knowledge. The final set of text characteristics included measures of linguistic complexity such as the Wiener Sachtextformel, the type-token ratio, average sentence length, word count, and the proportion of passive sentences. The variable Advice_ID models systematic differences between the individual information security advice presented. A two-stage approach was chosen for the exploration. The models were compared using `anova_lm` [97] to test whether the addition of additional predictors leads to a significant reduction in the sum of squares of residuals. This comparison is based on the differences in degrees of freedom and residual sums of squares, as well as the resulting F-value. Since not all models are nested within each other, the Akaike Information Criterion (AIC) and the Bayesian Information Criterion (BIC) were also used. Both information criteria evaluate model quality while accounting for model complexity, enabling a fair comparison even between models with different variable sets. This approach allows a structured assessment of the relative importance of the various predictor groups and identifies the model structure that offers the best explanatory power for usability.

3.2 Qualitative Study

To complement the quantitative analysis, we conducted a qualitative study of the policies' textual characteristics. Because surface-level text metrics proved insufficient, we conducted an in-depth qualitative analysis of communicative structure. Therefore, we analysed the policy texts themselves to uncover recurring framing patterns, structural deficits, and implicit assumptions that may hinder comprehension and possibility-to-follow. We examined the 29 pieces of IT-security advice included in our survey, drawn from four sources of consumer-facing security guidance. Each rule was treated as an individual text unit and imported into MAXQDA to support iterative coding, memoing, and the organisation of thematic categories throughout the analysis process.

The analysis was conducted on the original German-language advice texts. All coding and interpretative discussions were performed using the original wording to preserve linguistic nuance and contextual meaning. English translations of selected excerpts were produced only for publication purposes and translated as closely as possible to the original phrasing. Nevertheless, minor shifts in tone or connotation introduced through translation cannot be fully excluded.

The qualitative analysis was conducted by researchers who are native German speakers with experience in qualitative analysis and usable security research. This linguistic and domain familiarity supported the interpretation of culturally embedded expressions and security-related terminology within the analysed advice texts.

Our analysis follows an interpretative, reflexive thematic analysis approach [16], aimed at identifying recurring communicative. Coding was primarily inductive and iterative, involving repeated readings of the material, open coding, and collaborative refinement of emerging themes. At the same time, the analysis was theoretically informed by the related work presented above on security communication, usable security, and information security policy usability, introducing a light deductive influence during interpretation and category refinement.

Consistent with reflexive thematic analysis, we did not aim to establish statistical intercoder reliability, as meaning was understood as interpretatively constructed through collaborative analysis rather than independently discovered. Multiple codes could be assigned to a single text segment where analytically appropriate.

The final analysis was organised around four analytical perspectives:

- **Risk communication:** We analysed how risks were framed, including urgency, the explicitness of harm descriptions, and whether recommended actions were causally justified.
- **Topic and problem framing:** We analysed which security topics were addressed (e.g., passwords, phishing, IoT, encryption) and how concretely the problem was specified.
- **Institutional self-positioning:** We analysed how the issuing institution positioned itself, for example as an expert authority, an advisory actor, or a warning body, and how legitimacy was established through language.
- **User subject positions:** We examined how users were constructed through the texts, including implied responsibilities, expected competencies, and the role of cognitive attention demands as a security mechanism.

In addition, we conducted a focused comparative analysis of highly and poorly rated advice items, based on their quantitative distributions (see M5 and M7), to explore structural differences between the two cases.

By combining quantitative and qualitative perspectives, we aim to provide a holistic understanding of ISP usability. While regression and ANOVA highlight statistical predictors of usability scores, the qualitative analysis reveals the communicative mechanisms behind these perceptions, including the normalization of security as routine, reliance on user vigilance, and the frequent absence of operational guidance.

3.3 Ethics Statement

This study was approved by the Ethics Committee of the authors' home University through the expedited (fast-track) review process. We complied with the General Data Protection Regulation. The data was collected anonymously, and

we informed our participants about the study and our data collection process before they began participating.

4 Results

4.1 Validity Check

The results of the reliability and factor analyses show that adapting the SUS items to the context of IT-security notices did not cause any fundamental change in the expected measurement behaviour. The high value of Cronbach's $\alpha = .85$ is within the range of typical SUS reliabilities [11] and confirms that the modified items continue to capture a coherent and internally consistent construct.

The factor structure also corresponds to the patterns known from the SUS literature [62]. The clear dominance of the first factor (eigenvalue = 5.73) and a second factor above the Kaiser threshold [15] (eigenvalue = 3.33) reflect the frequently reported structure in which SUS is interpreted either as a one-dimensional measure or as a two-dimensional model (usability and learnability [62]). The remaining factors are clearly below the relevance threshold and explain only marginal variance, which is also consistent with previous findings on SUS. This shows that the transfer of SUS logic to ISPUS has not created any structural breaks. Psychometrically, the scale behaves as expected for SUS-based instruments, with a strong main component as well as a second weaker factor and consistently sufficient factor loadings. On this basis, it can be assumed that the content adjustments made (contextualisation to IT-security advice) have not changed the basic measurement properties. The results, therefore, support the validity of the measurement and confirm that ISPUS reliably reflects the intended construct.

4.2 Descriptive Statistics

Before turning to the regression analyses, we first report descriptive statistics of the sample and the ISPUS scores. A total of 348 participants completed the survey. Table 4.2 summarises the demographic characteristics of the sample.

Variable	Mean	SD
Age	46.90	18.81
Computer Literacy (Self-Assessment)	3.34	0.99
IT-Sec. Literacy (Self-Assessment)	3.01	1.03

Table 2: Descriptive statistics of continuous demographic variables.

Regarding gender, 51% of participants selected male, 48% female, and 1% diverse. Occupational status was distributed as follows: 55% in employee, 4% in civil servants, 8% in unemployed, 5% in student, 4% in pupil, 20% in pensioner, and 4% in misc. Highest education was distributed as follows: 1% in none, 10% in lower secondary school, 21% in higher secondary school, 37% in high school or professional training, 17% in bachelor, 13% in master, and 1% in PhD.

The average ISPUS score across all policies was 61.45 (SD = 18.66), indicating moderate usability perceptions (if we apply the marginal acceptable range of the SUS-Score as a heuristic [10]) Figure 1 illustrates the distribution of ISPUS scores across exemplary pieces of advice, with Advice 3 having the minimum score and Advice 24 having the maximum score.

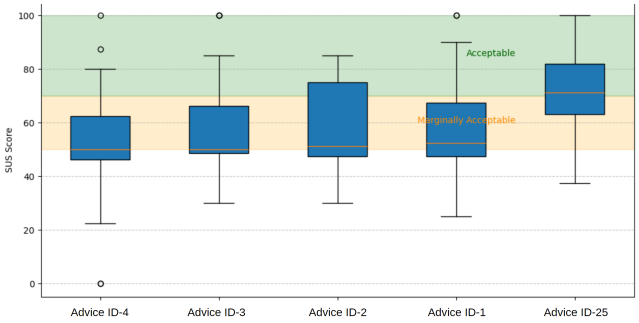


Figure 1: Boxplots of exemplary pieces of IT-security advice.

4.3 Exploratory Analysis

To examine the relative influence of user characteristics, text characteristics, and policy identity on ISPUS scores, we estimated eight OLS models (M1–M8). The models differ systematically in the predictor groups they contain, allowing us to determine their respective contributions to the explained variance.

Model M1 (User Features). Model M1 contains only user characteristics and achieves $R^2 = 0.111$ (adj. $R^2 = 0.100$). Several predictors showed significant correlations with the ISPUS scores: older age (coef = 3.64, $p < .001$), higher education (coef = 1.96, $p = .003$), better IT device skills (coef = 1.83, $p = .033$) and higher IT/security skills (coef = 3.26, $p < .001$) were each associated with higher ratings. Among the occupational groups, only civil servants had significantly lower ratings than the reference category (unemployed) (coef = –7.90, $p = .033$). Gender was not significant.

Model M2 (Text Features). Model M2 comprises text features only and, with $R^2 = 0.021$, has the lowest explained variance of all models. None of the text features – neither readability (e.g. wiener_grade: coef = 0.71, $p = .307$) nor word count (coef = –0.38, $p = .708$), sentence length (coef = 0.14, $p = .836$), lexical diversity (coef = 1.46, $p = .112$) or passive voice (coef = –0.96, $p = .203$) – was significant. This shows that surface-level linguistic properties of the rules have little influence on perceived usability.

Model M3 (Advice ID). Model M3 contains only the policy identity and achieves $R^2 = 0.095$. Several rules differed

significantly from the reference rule (Advice ID 22). Lower ratings were found for Advice ID 5 (coef = –10.55, $p = .024$), Advice ID 7 (coef = –10.65, $p = .020$), Advice ID 12 (coef = –9.27, $p = .045$), Advice ID 25 (coef = –9.79, $p = .027$) and Advice ID 28 (coef = –10.70, $p = .014$). A higher rating was given to `ID-16` (coef = 9.77, $p = .038$). These differences illustrate that the content and structural design of the rules has a relevant influence on the perception of usability.

Model M4 (User and Text Features). Model M4 combines user and text characteristics and achieves $R^2 = 0.129$ (adj. $R^2 = 0.112$). The text characteristics remained insignificant (all $p > .20$). The significant user characteristics largely corresponded to model M1: age (coef = 3.55, $p < .001$), education (coef = 1.88, $p = .004$), IT device knowledge (coef = 1.84, $p = .031$) and IT/security knowledge (coef = 3.31, $p < .001$). Here, too, civil servants rated the rules significantly lower (coef = –7.74, $p = .036$).

Model M5 (User Features and Advice ID). Model M5 combines user characteristics and policy identity and, with $R^2 = 0.209$ (adj. $R^2 = 0.172$), has the highest explained variance of all models. Older age (coef = 3.61, $p < .001$), higher education (coef = 1.89, $p = .003$), better IT device skills (coef = 2.00, $p = .017$) and higher IT/security skills (coef = 3.54, $p < .001$) led to higher ISPUS scores. Civil servants rated the rules significantly lower (coef = –7.21, $p = .047$).

Policy identity also had a significant effect: `ID 7`(coef = –9.77, $p = .025$), `ID 12` (coef = –8.62, $p = .049$), `ID 28` (coef = –9.01, $p = .029$) and `ID 5` (coef = –8.37, $p = .059$, marginal) were rated lower, while `ID 16` (coef = 11.54, $p = .010$) and `ID-20` (coef = 8.86, $p = .041$) received significantly higher ratings.

Model M6 (Text Features and Advice ID).

Model M6 combines text features and policy identity, but showed numerical instabilities (extreme coefficients in the range 10^{12} to 10^{14}). These values indicate strong multicollinearity between text features and fixed effects, which is why the model is not interpretable and will not be considered further.

Model M7 (User Features, Text Features and Advice ID). Model M7 represents the complete model by combining user characteristics with policy identity. With an $R^2 = 0.209$ (adj. $R^2 = 0.172$), it explains as much variance as M5. The results show that both individual differences among participants and the specific rule systematically influence ISPUS scores.

Older age was associated with higher ratings (coef = 3.61, $p < .001$), as were higher education (coef = 1.89, $p = .003$), better IT device skills (coef = 2.00, $p = .017$) and higher IT/security skills (coef = 3.54, $p < .001$). Civil servants, on the other hand, rated the rules significantly lower than the reference group (coef = –7.21, $p = .047$). Policy identity also had a significant effect: some rules were rated significantly lower than the reference rule, including `ID-7` (coef = –9.77, $p = .025$), `ID-12` (coef = –8.62, $p = .049$) and `ID-28` (coef = –9.01, $p = .029$), while other rules such as `ID-16` (coef = 11.54, $p = .010$) and `ID-20` (coef = 8.86, $p = .041$) received significantly higher ratings.

Model M8 (User Features, Advice ID, and Self-Assessment Residuals). In addition, a residual model (M8) was estimated in which self-assessments of IT and information security competences were replaced by residuals from regression models based on age and education. This approach was chosen because age and self-assessment were negatively correlated, but both had positive effects on the ISPUS rating in the regression model. The residuals (`IT_over_under` and `SEC_over_under`) capture the individual overestimation or underestimation relative to the demographically expected competence. The residual model achieved the same explained variance as M5/M7 ($R^2 = 0.209$). Both residual variables were significant predictors: a relative overestimation of IT competence led to higher ISPUS values (coef = 2.00, $p = .017$), as did an overestimation of security competence (coef = 3.54, $p < .001$). Age is not correlated with such over-/underestimation.

Table 3: Model fit statistics for regression models M1–M8.

Model	R^2	Adj. R^2	AIC	BIC
M5/M7/M8	0.209	0.172	7709	7906
M4	0.129	0.112	7750	7836
M1	0.111	0.100	7758	7820
M3	0.095	0.066	7806	7945
M6	0.093	0.064	7809	7948
M2	0.021	0.015	7831	7860

The ANOVA comparisons confirm the overall pattern observed in the regression analyses. The full models M5, M7, and M8 (User + Advice ID, with or without text features or residualised competence estimates) clearly outperform all text-based models. The comparison between M7 and M2 (Text only) shows a substantial reduction in residual variance ($\Delta SSR = -59{,}076$), demonstrating that text features alone explain very little variance in ISPUS scores. Likewise, M5/M7/M8 improve model fit compared to the user-only model M1 ($\Delta SSR = -30{,}656$), indicating that advice identity contributes additional explanatory power beyond user characteristics.

Model M4 (User + Text) also significantly outperforms the text-only model M2 ($\Delta SSR = -33{,}972$), reinforcing that user characteristics are far more relevant than textual features. The comparison between M2 and M3 (Advice ID only) shows that policy identity has a stronger effect on ISPUS scores than text characteristics. Finally, the comparison between M3 and M1 shows no meaningful difference, suggesting that user characteristics and policy identity explain similar amounts of variance when considered separately.

The residual model M8, in which the self-assessed IT and information security competence was replaced by residuals

capturing individual over- or underestimation, achieved the same explanatory power as M5 and M7 ($R^2 = 0.209$). The significant effects of `IT_over_under` and `SEC_over_under` might indicate that subjective confidence—rather than objective competence—substantially contributes to perceived usability. However, as no job-related IT competency indicators were collected, the residuals may also reflect objective but unobserved expertise. The positive effect of the residuals on the ISPUS rating can therefore be explained by both self-confidence and actual professional competence. Importantly, including these residuals did not alter the effects of age, education, or policy identity, confirming the robustness of the overall model structure.

Table 4: Pairwise ANOVA comparisons between regression models M1–M8 (M6 excluded). Negative ΔSSR values indicate improved fit for the more complex model. M5, M7, and M8 are merged because they are identical in their properties.

Comparison	Δdf	ΔSSR	Interpretation
M1 vs. M2	7	28,420	M1 > M2
M1 vs. M3	−16	5,075	M3 ∼ M1
M1 vs. M4	−5	−5,552	M4 ∼ M1
M1 vs. (M5/7/8)	−28	−30,656	M5/7/8 > M1
M2 vs. M3	23	23,345	M3 > M2
M2 vs. M4	12	33,972	M4 > M2
M2 vs. (M5/7/8)	35	59,076	M5/M/8 » M2
M3 vs. M4	−11	10,627	M4 > M3
M3 vs. (M5/7/8)	−12	−35,731	M5/7/8 > M3
M4 vs. (M5/7/8)	−23	−25,104	M5/7/8 > M4

4.4 Qualitative Findings

4.4.1 Informative Framing and Institutional Authority

Based on our qualitative thematic coding with attention to recurring argumentative structures, we identified consistent patterns in how security is communicated across the 29 policies. A central observation concerns the overall tone of communication. Across the dataset, policies adopt an informative and advisory style. Rather than relying on fear appeals or catastrophic threat narratives, the documents frame security as neutral knowledge and practical guidance. Sanctioning language was absent, and the institutional authority was rather constructed implicitly through the provision of "correct" information and recommendations. This framing positions the issuing institutions as expert knowledge providers rather than disciplinary actors. At the same time, it normalizes security as routine behaviour rather than an exceptional response to a crisis.

4.4.2 Responsibility Shift to Users

Despite the neutral tone, the policies consistently position users as the primary agents of security. While this is expected, given that the advice is explicitly directed at end users, it remains analytically relevant because it frames security primarily as user responsibility and presupposes user capability. Users are expected to implement protective measures and respond appropriately to risks. This framing presupposes that users are capable of understanding, interpreting, and operationalizing security advice. However, prior work [9, 96] and our findings suggest that such comprehension cannot be assumed across user groups. In effect, responsibility for security is individualized. Structural or systemic factors are rarely addressed.

4.4.3 Limited Causal Justification and Operational Guidance

A recurring limitation concerns the structure of advice. Many policies specify what users should do, but provide limited step-by-step guidance on how to carry out these actions or why they are necessary. Only a minority of documents follow an explicit causal structure, such as: risk X leads to harm Y, therefore, measure Z is required (e.g., `ID-2`). In many cases, security measures are presented as general normative best practices rather than as responses to clearly articulated threats. For example, `ID-29` states: "If available, enable fingerprint or Face ID authentication for any account that offers this method." Similarly, `ID-18` advises: "Monitor accounts and devices: Regularly check your financial accounts and online profiles for suspicious activity. Use security software to monitor your devices for unauthorized access or unusual behaviour." In these examples, security is framed as inherently desirable, yet the underlying risks and harms are not explicitly articulated.

4.4.4 Abstract Threat Descriptions and High Cognitive Demands

Another pattern concerns the abstraction level of threat descriptions. Concrete, relatable examples are rare. When metaphors are used, they appear to support comprehension, such as the "tunnel" metaphor for VPNs (`ID-5`) or the password-toothbrush analogy ("Passwords are like toothbrushes: you should choose them carefully, not share them, change them regularly, and be sure to use them"; `ID-19`). However, most policies rely on abstract formulations such as "Be careful with [...]" or "Be cautious [...]" (e.g., `ID-7`, `ID-25`). The majority of policies implicitly treat attention and awareness as a primary security mechanism. Users are instructed to verify identities, reflect on requests, and remain cautious. For instance, `ID-12` expects users to verify email senders but provides limited guidance on what concrete indicators should be examined. This places substantial cognitive demands on users in everyday contexts. Sustained high levels of attention,

however, are widely recognized as unrealistic under routine conditions and in the face of cognitive load.

4.4.5 Differences Between Highly and Poorly Rated Advice

To further contextualize these findings, we compared a subset of highly rated and poorly rated advice items from the usability distribution (M5 and M7). Low-rated advice (ID-5, ID-7, ID-12, and ID-28) often assumes technical background knowledge, provides limited operational detail, and relies on abstract preventive framing. For example, the VPN advice in ID-5 uses the aforementioned tunnel metaphor but does not clearly explain why a VPN is needed or how to install it. Similarly, ID-7 refers to USB and LAN ports without describing what they look like or defining these terms, and offers only general guidance ("Be careful with [...]") rather than concrete steps. ID-12 and ID-28 rely heavily on user attention while providing few actionable cues for identifying suspicious situations. In contrast, higher-rated advice (ID-16 and ID-20) tends to be actionable without requiring technical expertise and often provides concrete heuristics. ID-16 focuses on staying informed and sharing security knowledge, which may be perceived as feasible across skill levels. ID-20 includes a memorable strategy for generating passwords based on the first letters of each word of a song title, offering users a directly applicable method rather than an abstract requirement. This comparison suggests that usability is not only shaped by the presence of advice, but by its level of operationalisation, cognitive demand, and assumed technical knowledge. To complement our qualitative findings, Table 5 provides an overview of recurring advice characteristics associated with low and high ratings.

Pattern	Low-rated advice	High-rated advice
Technical assumptions	Requires technical vocabulary without explanation (e.g., VPN, home network, USB/LAN ports) (ID-5, ID-7).	Avoids technical prerequisites or focuses on everyday actions that are feasible across skill levels (ID-16).
Operationalisation	States what to do but provides limited step-by-step guidance on how to implement the measure (ID-5, ID-7, ID-28).	Provides concrete heuristics or strategies that users can directly apply (ID-20).
Cognitive demands	Relies on abstract calls for caution and sustained attention without providing concrete cues (e.g., email sender verification) (ID-12).	Reduces cognitive burden by offering practical shortcuts and memorable strategies (ID-20).

Table 5: Qualitative differences between high- and low-rated advice items. Low-rated advice often assumes technical knowledge, lacks operational guidance, and places high cognitive demands on users, whereas high-rated advice tends to provide actionable heuristics and feasible everyday practices.

4.5 Summary of Findings

How do end-users perceive the usability of IT-security advice? Perceived usability was rated as moderate overall (ISPUS $M = 61.45$), with substantial variation across individual advice items. Qualitative patterns show that higher-rated advice is concrete and actionable, whereas lower-rated advice assumes technical knowledge or relies on abstract calls for caution.

Which end-user characteristics influence perceived usability? Perceived usability ratings were significantly associated with age, education, and self-assessed IT/IT-security knowledge. Older participants, those with higher education, and those who rated their own skills more positively tended to give higher usability scores. Civil servants rated advice lower than other groups, while gender showed no effect. Residual analyses further indicate that subjective confidence in one's abilities also contributes to higher ratings.

What textual design aspects influence perceived usability? Traditional readability metrics showed little explanatory power; none of the linguistic surface features were significant predictors. Qualitative findings suggest instead that usability is shaped by operational clarity, cognitive demands, and the level of technical complexity assumed by the advice.

5 Discussion

5.1 Usable IT-Security Advice as a Relational Artefact

Our findings show that the usability of IT-security advice cannot be understood as a static property of a text, but rather as a relational interaction among users, content, and situational contexts. While this perspective is well established in usability research [12, 60], it has been studied only sparingly in the context of IT-security advice to date. Earlier work on organisational ISPs [27, 38, 49, 57] as well as IT-security advice [58, 72, 77] repeatedly points to a lack of usability, while its structural characteristics remained unclear.

Neil et al. [72] show that authors of security advice often work without a clear methodological basis, combining content from various external sources and rarely prioritising it systematically. Our results complement these findings by showing how these production processes are reflected in end-users' perceptions. In particular, classic text metrics, such as readability indices or sentence length, hardly explain any variance in perceived usability, whereas the lack of contextual-

isation and user-centricity do. This finding is consistent with work showing that comprehensibility alone is not sufficient to promote security-related behaviour [86]. Instead, our results confirm the assumption that usability in an IT-security context is essentially characterised by action orientation, clarity of responsibilities, and contextual relevance. Our comparison of high and low-rated advice further illustrates this relational perspective. Low-rated advice often required technical background knowledge or sustained cognitive effort (e.g., `ID-5`, `ID-7`, `ID-12`), whereas higher-rated advice provided concrete heuristics or everyday practices that were feasible without specialized expertise (e.g., `ID-16`, `ID-20`). This suggests that usability emerges not merely from textual clarity, but from the alignment between assumed user capabilities and actual user resources. In this sense, usability is co-constructed between advice design and user context.

This becomes even clearer when considering demographic differences. Our quantitative results show that higher age is associated with higher perceived usability, and similar patterns emerge for education and self-assessed IT/security knowledge. These findings indicate that usability perceptions are shaped not only by textual properties but also by users' accumulated experience, confidence, and familiarity with IT-security. This pattern resonates with Morrison et al.'s [69] findings on older adults' engagement with cyber-security behaviours, where confidence, perceived competence, and available support strongly influenced whether protective actions were seen as feasible or overwhelming. Their themes mirror the dynamics we observe in our data, i.e., usability is not only a function of textual design but also of users' self-efficacy and prior experience. Interestingly, users who overestimate their abilities also perceive the advice as more usable, indicating that insufficient understanding can produce an inflated sense of ease and obscure the real implications of the text (see also [101]).

Our study shows that much of the advice implicitly assumes idealised users, technically savvy, educated, and stuck within similar (technological) contexts. These implicit subject positions reproduce digital inequalities, as prior research [40, 77] also emphasises. We thus expand the usability discussion to include a social perspective: usability is not only a question of design, but also of social inclusion of security. For example, among less educated citizens.

5.2 Implications for the Design of Usable IT-Security Advice

The results of this study show that IT-security advice must be tailored more closely to end users' needs and abilities. In particular, the average usability score falls in the marginally acceptable range [10], indicating opportunities for improvement. Our qualitative comparison further suggests that authors should (1) avoid unexplained technical terminology, (2) explicitly link recommended measures to concrete risks and harms, (3) provide step-by-step guidance where feasible, and (4) reduce reliance on sustained user attention by offering actionable heuristics.

The literature shows that many authors do take usability into account, but without a systematic method or objective [72]. Our results underscore that different user groups, especially in terms of age, education and IT-skills, have very different prerequisites. A universal approach is therefore not suitable for reaching broad population groups. It is also crucial to recognise that advice must be formulated in an end-user-specific and context-specific manner. On the one hand, this is consistent with findings from ISP research, which emphasise that clear responsibilities, concrete steps, and a comprehensible structure are crucial for implementation [21, 27]. On the other hand, it is clear that traditional readability metrics should not be used as sole indicators of quality. Our results show that these metrics explain very little variance in perceived usability. Instead, authors should use more comprehensive usability measurement tools, such as the ISPUS adaptation [57], and supplement them with qualitative tests. This aligns with the call for systematic, iterative evaluation in the spirit of user-centred design [22, 107]. Finally, there is much to be said for segmenting or personalising advice. The literature shows that users have different security needs, attitudes, and abilities [40, 77]. Multi-level, adaptive, or target-group-specific formats could better reflect these differences and increase the effectiveness of security-related communication.

5.3 Limitations

This study has several limitations that must be taken into account when interpreting the results. First, the sample is based exclusively on the German population. Although this is useful for studying a national communication ecosystem, cultural differences in security mental models, language comprehension, or trust in institutions may limit the transferability of the results to other countries. Although the adapted version of the SUS (ISPUS) scale showed similar psychometric characteristics (Cronbach's $\alpha = .85$; factor structure consistent with SUS literature), our research does not provide a conclusive validation, but initial evidence only. Similarly, the SUS acceptability range was used as a heuristic reference, without any broad scale measurement of their transferability. Thus the instrument and its construct validity needs to be further validated for the use in the context if IT-security advice.

The regression analysis applied to the ISPUS results was theory-informed but exploratory, thus no formal multiple-comparison corrections were applied. Future work should, therefore, more strongly move beyond exploration and include confirmatory hypothesis testing and appropriate multiple-comparison corrections to ensure the robustness of the findings. Another methodological aspect concerns the presentation of the advice examined. All texts were presented in a uniform visual format without changing their original structure, such as bullet points, highlighting, or visual struc-

turing elements. This allowed us to ensure that differences in usability within our exploration, but ignored visual guidance and/or the positive influence of aesthetics.

All analysed advice texts originated from German or European institutions. Consequently, the communicative style, assumptions about user responsibility, and framing of security practices are embedded within a specific cultural and institutional context. These contextual factors likely influenced both the tone of the advice and participants' interpretations of usability, which may limit direct transferability to other national or linguistic settings.

6 Conclusion

This paper shows that the perceived usability of end-user IT-security advice depends much more on user characteristics and structural text decisions than previously assumed. By applying an adapted ISPUS scale to 29 real-world pieces of IT-security advice and combining quantitative modelling with qualitative text analysis, we make an empirically based contribution to the discussion on usable IT-security advice. Our results illustrate that classic readability measures hardly explain how usable security advice actually is, while age, education, IT competence, and the specific design of individual pieces of advice are key influencing factors. We contribute empirical evidence to a research gap repeatedly identified in both the ISP literature and work on end-user advice.

At the same time, our qualitative findings reveal recurring design deficits that help explain these patterns. Many advice items are framed as general best practices without explicit causal justification, provide limited operational guidance, and rely heavily on sustained user attention. As a result, the advice often presupposes idealised users with technical background knowledge and stable cognitive resources, which risks reproducing digital inequalities by making security less accessible for parts of the population, thereby unintentionally creating exclusion. By identifying structural and contextual patterns that hinder implementation, we recommend concrete starting points for developing more inclusive, action-oriented advice. Our findings underscore that user-centred design is not an optional add-on but a prerequisite for effective IT-security practices in everyday life.

Looking ahead, this work opens up several trajectories for future research, including the systematic validation of the adapted ISPUS scale, investigations into alternative visual presentation formats to experimental studies that capture actual behaviour rather than just perceptions. We hope that our findings will encourage the SOUPS community to view security advice even more as socio-technical artefacts and to continue research on usability to ensure that good security recommendations not only exist but are also truly actionable.

Acknowledgments

This research was funded by the German Federal Ministry of Research, Technology, and Space (BMFTR) under the project BeDeNUTZ (project number: 16KIS1892). We would like to thank the BMFTR for its support.

References

[1] Acar, Yasemin and Backes, Michael and Fahl, Sascha and Kim, Doowon and Mazurek, Michelle L and Stransky, Christian. You get where you're looking for: The impact of information sources on code security. In *2016 IEEE symposium on security and privacy (SP)*, pages 289–305. IEEE, 2016.

[2] Acar, Yasemin and Stransky, Christian and Wermke, Dominik and Weir, Charles and Mazurek, Michelle L and Fahl, Sascha. Developers need support, too: A survey of security advice for software developers. In *2017 IEEE Cybersecurity Development (SecDev)*, pages 22–26. IEEE, 2017.

[3] Admass, Wasyihun Sema and Munaye, Yirga Yayeh and Diro, Abebe Abeshu. Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2:100031, 2024.

[4] Akhawe, Devdatta and Felt, Adrienne Porter. Alice in warningland: A Large-Scale field study of browser security warning effectiveness. In *22nd USENIX security symposium (USENIX Security 13)*, pages 257–272, 2013.

[5] Akinwande, Michael Olusegun and Dikko, Hussaini Garba and Samson, Agboola. Variance inflation factor: As a condition for the inclusion of suppressor variable (s) in regression analysis. *Open journal of statistics*, 5(7):754–767, 2015.

[6] Al-Hamdani, Wasim A and Dixie, Wendy D. Information security policy in small education organization. In *2009 Information Security Curriculum Development Conference*, pages 72–78, 2009.

[7] Al-Mukahal, Hasan M and Alshare, Khaled. An examination of factors that influence the number of information security policy violations in Qatari organizations. *Information & Computer Security*, 23(1):102–118, 2015.

[8] Alkhurayyif, Yazeed and Weir, George RS. Evaluating readability as a factor in information security policies. *International Journal of Trend in Research and Development*, pages 54–64, 2017.

[9] An, Qin and Hong, Wilson Cheong Hin and Xu, XiaoShu and Zhang, Yunfeng and Kolletar-Zhu, Kimberly. How education level influences internet security knowledge, behaviour, and attitude: A comparison among undergraduates, postgraduates and working graduates. *International Journal of Information Security*, 22(2):305–317, 2023.

[10] Bangor, Aaron and Kortum, Philip and Miller, James. Determining what individual SUS scores mean: Adding an adjective rating scale. *Journal of usability studies*, 4(3):114–123, 2009.

[11] Bangor, Aaron and Kortum, Philip T and Miller, James T. An empirical evaluation of the system usability scale. *Intl. Journal of Human–Computer Interaction*, 24(6):574–594, 2008.

[12] Bevan, Nigel and Carter, James and Harker, Susan. ISO 9241-11 revised: What have we learnt about usability since 1998? In *Human-Computer Interaction: Design and Evaluation: 17th International Conference, HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015, Proceedings, Part I 17*, pages 143–151. Springer, 2015.

[13] Bevan, Nigel and Kirakowski, Jurek and Maissel, Jonathan. What is usability. In *Proceedings of the 4th International Conference on HCI*, pages 1–6, 1991.

[14] Boyd, Maia J and Sullivan Jr, Jamar L and Chetty, Marshini and Ur, Blase. Understanding the security and privacy advice given to black lives matter protesters. In *Proceedings of the 2021 CHI conference on human factors in computing systems*, pages 1–18, 2021.

[15] Braeken, Johan and Van Assen, Marcel A.L.M. An empirical Kaiser criterion. *Psychological Methods*, 22(3):450, 2017.

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

[17] Bravo-Lillo, Cristian and Cranor, Lorrie Faith and Downs, Julie and Komanduri, Saranga. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):18–26, 2010.

[18] Brooke, John. SUS-A quick and dirty usability scale. *Usability evaluation in industry*, 189(194):4–7, 1996.

[19] Bundesamt für Sichterheit in der Informationstechnik. Smarthome – den Wohnraum sicher vernetzen. 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: 2025-02-01.

[20] Busse, Karoline and Schäfer, Julia and Smith, Matthew. Replication: No one can hack my mind revisiting a study on expert and non-expert security practices and advice. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 117–136, 2019.

[21] Corpuz, Maria and Barnes, Paul. Integrating information security policy management with corporate risk management for strategic alignment. In *The 14th World Multi-Conference on Systemics, Cybernetics, and Informatics, Proceedings Volume III*, pages 337–342. International Institute of Informatics and Systemics, 2010.

[22] Creusen, Mariëlle and Hultink, Erik Jan and Eling, Katrin. Choice of consumer research methods in the front end of new product development. *International Journal of Market Research*, 55(1):81–104, 2013.

[23] Denning, Tamara and Lerner, Adam and Shostack, Adam and Kohno, Tadayoshi. Control-Alt-Hack: The design and evaluation of a card game for computer security awareness and education. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, pages 915–928, 2013.

[24] Deutscher Qualifikationsrahmen —- DQR. Deutscher Qualifikationsrahmen für lebenslanges Lernen (DQR). https://www.dqr.de/dqr/de/home/home_node.html, 2025. Accessed: 2026-02-20.

[25] Dincelli, Ersin and Chengalur-Smith, InduShobha. Choose your own training adventure: Designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. *European Journal of Information Systems*, 29(6):669–687, 2020.

[26] Doherty, Neil F and Fulford, Heather. Do information security policies reduce the incidence of security breaches: an exploratory analysis. *Information Resources Management Journal (IRMJ)*, 18(4):21–39, 2005.

[27] Doherty, Neil F and Fulford, Heather. Aligning the information security policy with the strategic information systems plan. *Computers & Security*, 25(1):55–63, 2006.

[28] Dumas, Joseph F and Redish, Janice C. *A practical guide to usability testing*. Greenwood Publishing Group Inc., 1993.

[29] Dzida, Wolfgang and Freitag, Regine. Usability Testing—the DATech Standard. *Software Quality: State of the Art in Management, Testing, and Tools*, pages 160–177, 2001.

[30] European Union Agency for Cybersecurity. Cyber Hygiene. https://www.enisa.europa.eu/topics/cyber-hygiene. Accessed: 2025-02-01.

[31] Europäisches Verbraucherzentrum Deutschland. Datenschutz im Internet: Wie kann ich meine Daten schützen? https://www.evz.de/einkaufen-internet/datenschutz/datenschutz-im-internet.html, 2025. Accessed: 2025-02-01.

[32] Fagan, Michael and Khan, Mohammad Maifi Hasan. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 59–75, 2016.

[33] Feng, Yuanyuan and Yao, Yaxing and Sadeh, Norman. A design space for privacy choices: Towards meaningful privacy control in the internet of things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–16, 2021.

[34] Fernandez, Adrian and Insfran, Emilio and Abrahão, Silvia. Usability evaluation methods for the web: A systematic mapping study. *Information and Software Technology*, 53(8):789–817, 2011.

[35] Fulton, Kelsey R and Gelles, Rebecca and McKay, Alexandra and Abdi, Yasmin and Roberts, Richard and Mazurek, Michelle L. The effect of entertainment media on mental models of computer security. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 79–95, 2019.

[36] Geeng, Christine and Harris, Mike and Redmiles, Elissa and Roesner, Franziska. "Like Lesbians Walking the Perimeter": Experiences of US LGBTQ+ Folks With Online Security, Safety, and Privacy Advice. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 305–322, 2022.

[37] Gjertsen, Eyvind Garder B and Gjære, Erlend Andreas and Bartnes, Maria and Flores, Waldo Rocha. Gamification of Information Security Awareness and Training. In *ICISSP*, pages 59–70, 2017.

[38] Goel, Sanjay and Chengalur-Smith, InduShobha N. Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems*, 19(4):281–295, 2010.

[39] Gorski, Peter Leo and Iacono, Luigi Lo and Wermke, Dominik and Stransky, Christian and Möller, Sebastian and Acar, Yasemin and Fahl, Sascha. Developers deserve security warnings, too: On the effect of integrated security advice on cryptographic API misuse. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 265–281, 2018.

[40] Habib, Hana and Li, Megan and Young, Ellie and Cranor, Lorrie. "Okay, whatever": An evaluation of cookie consent interfaces. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–27, 2022.

[41] Herley, Cormac. 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*, pages 133–144, 2009.

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

[43] Hix, Deborah and Hartson, H Rex. Formative evaluation: Ensuring usability in user interfaces. *Virginia Polytechnic Institute & State University, United States*, 1992.

[44] Holton, Nirosha and Furnell, Steven. Assessing the provision of public-facing cybersecurity guidance for end-users. In *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*, pages 161–168. IEEE, 2020.

[45] Holtz, Leif-Erik and Zwingelberg, Harald and Hansen, Marit. Privacy policy icons. In *Privacy and Identity Management for Life*, pages 279–285. Springer, 2011.

[46] Holzinger, Andreas and Carrington, André and Müller, Heimo. Measuring the quality of explanations: the system causability scale (SCS) comparing human and machine explanations. *KI-Künstliche Intelligenz*, 34(2):193–198, 2020.

[47] Hopf, Christel. Qualitative interviews: An overview. *A Companion to Qualitative Research*, 203(8):100093, 2004.

[48] Ion, Iulia and Reeder, Rob and Consolvo, Sunny. "... No one can hack my Mind": Comparing expert and non-expert security practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 327–346, 2015.

[49] Karlsson, Fredrik and Hedström, Karin and Goldkuhl, Göran. Practice-based discourse analysis of information security policies. *Computers & Security*, 67:267–279, 2017.

[50] Kitzinger, Jenny. Qualitative research: introducing focus groups. *British Medical Journal*, 311(7000):299–302, 1995.

[51] Knapp, Kenneth J and Morris Jr, R Franklin and Marshall, Thomas E and Byrd, Terry Anthony. Information security policy: An organizational-level process model. *Computers & Security*, 28(7):493–508, 2009.

[52] Kortum, Philip T and Bangor, Aaron. Usability ratings for everyday products measured with the system usability scale. *International Journal of Human-Computer Interaction*, 29(2):67–76, 2013.

[53] Kumaraguru, Ponnurangam. *Phishguru: A system for educating users about semantic attacks*. Carnegie Mellon University, 2009.

[54] Kumaraguru, Ponnurangam and Cranshaw, Justin and Acquisti, Alessandro and Cranor, Lorrie and Hong, Jason and Blair, Mary Ann and Pham, Theodore. School of phish: A real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, 2009.

[55] Kumaraguru, Ponnurangam and Sheng, Steve and Acquisti, Alessandro and Cranor, Lorrie Faith and Hong, Jason. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2):1–31, 2010.

[56] Lawo, Dennis and Neifer, Thomas and Esau-Held, Margarita and Stevens, Gunnar. Digital Sovereignty: What it is and why it matters for HCI. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–7, 2023.

[57] Lawo, Dennis and Stevens, Gunnar. Information Security Policy Usability Scale: A Questionnaire for Evaluating the Usability of Information Security Policies. In *Mensch und Computer 2024-Workshopband*, pages 10–18. Gesellschaft für Informatik e.V., 2024.

[58] Lawo, Dennis and Stevens, Gunnar. From usable design characteristics to usable information security policies: a reconceptualisation. *i-com*, 24(1):107–124, 2025.

[59] Lee, Ying-Lien and Hsu, Chih-Hsiang. Usability study of text-based CAPTCHAs. *Displays*, 32(2):81–86, 2011.

[60] Lewis, James R. Usability: lessons learned... and yet to be learned. *International Journal of Human-Computer Interaction*, 30(9):663–684, 2014.

[61] Lewis, James R. The system usability scale: past, present, and future. *International Journal of Human–Computer Interaction*, 34(7):577–590, 2018.

[62] Lewis, James R and Sauro, Jeff. The factor structure of the system usability scale. In *International Conference on Human Centered Design*, pages 94–103. Springer, 2009.

[63] Lopes, Isabel and Oliveira, Pedro. Applying action research in the formulation of information security policies. In *New Contributions in Information Systems and Technologies: Volume 1*, pages 513–522. Springer, 2015.

[64] Mathis, Florian and Vaniea, Kami and Khamis, Mohamed. Prototyping usable privacy and security systems: Insights from experts. *International Journal of Human–Computer Interaction*, 38(5):468–490, 2022.

[65] Maynard, S and Ruighaver, Anthonie B. What makes a good information security policy: a preliminary framework for evaluating security policy quality. In *Proceedings of the Fifth Annual Security Conference, Las Vegas, Nevada USA*, pages 19–20, 2006.

[66] Mekhail, Christine and Zhang-Kennedy, Leah and Chiasson, Sonia. Visualizations to teach about mobile online privacy. In *Persuasive Technology Conference (poster)*, 2014.

[67] Montasari, Reza. Cyber threats and the security risks they pose to national security: An assessment of cybersecurity policy in the United Kingdom. *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity*, pages 7–25, 2023.

[68] Moody, Gregory D. and Siponen, Mikko and Pahnila, Seppo. Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1), 2018.

[69] Morrison, Benjamin and Coventry, Lynne and Briggs, Pam. How do Older Adults feel about engaging with Cyber-Security? *Human Behavior and Emerging Technologies*, 3(5):1033–1049, 2021.

[70] Morville, P. User Experience Design. *Semantic Studios LLC*, 2004.

[71] Neil, Lorenzo and Bouma-Sims, Elijah and Lafontaine, Evan and Acar, Yasemin and Reaves, Bradley. Investigating web service account remediation advice. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 359–376, 2021.

[72] Neil, Lorenzo and Ramulu, Harshini Sri and Acar, Yasemin and Reaves, Bradley. 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)*, pages 283–299, 2023.

[73] Ng, Annie WY and Lo, Honour WC and Chan, Alan. Measuring the Usability of Safety Signs: A use of system usability scale (SUS). In *Proceedings of the International MultiConference of Engineers and Computer Scientists*, volume 2, pages 1296–1301, 2011.

[74] Nicholson, James and Coventry, Lynne and Briggs, Pamela. "If it's important it will be a headline" Cybersecurity Information Seeking in Older Adults. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–11, 2019.

[75] Nielsen, Jakob. Finding usability problems through heuristic evaluation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 373–380, 1992.

[76] O'Brien, Heather L and Toms, Elaine G. The development and evaluation of a survey to measure user engagement. *Journal of the American Society for Information Science and Technology*, 61(1):50–69, 2010.

[77] Ortloff, Anna-Marie and Tang, Jenny and Arumugam, Arthi and Huschina, Daniel and Geierhaas, Lisa and Martius, Florin and Jansen, Luisa and Von Der Twer, Kolja and Jungbluth, Lilly and Smith, Matthew. Replication: "No one can hack my mind"-10 years later: An update and outlook on experts' and non-experts' security practices and advice. In *Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025)*, pages 435–454, 2025.

[78] PayPal. Hilf uns, dein PayPal-Konto zu schützen. https://www.paypal.com/de/security/protect-your-account, 2025. Accessed: 2025-02-01.

[79] Prange, Sarah and Von Zezschwitz, Emanuel and Alt, Florian. Vision: Exploring challenges and opportunities for usable authentication in the smart home. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 154–158. IEEE, 2019.

[80] Rader, Emilee and Wash, Rick. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, 1(1):121–144, 2015.

[81] Rader, Emilee and Wash, Rick and Brooks, Brandon. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, pages 1–17, 2012.

[82] Randall, David and Harper, Richard and Rouncefield, Mark. *Fieldwork for design: theory and practice*. Springer Science & Business Media, 2007.

[83] Redmiles, Elissa M and Kross, Sean and Mazurek, Michelle L. How I learned to be secure: A census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 666–677, 2016.

[84] Redmiles, Elissa M and Kross, Sean and Mazurek, Michelle L. 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*, pages 931–936, 2017.

[85] Redmiles, Elissa M and Malone, Amelia R and Mazurek, Michelle L. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 272–288. IEEE, 2016.

[86] Redmiles, Elissa M and Warford, Noel and Jayanti, Amritha and Koneru, Aravind and Kross, Sean and Morales, Miraida and Stevens, Rock and Mazurek, Michelle L. A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 89–108, 2020.

[87] Rotthaler, Anna Lena and Ramulu, Harshini Sri and Simko, Lucy and Fahl, Sascha and Acar, Yasemin. "It's Time. Time for Digital Security.": An End User Study on Actionable Security and Privacy Advice. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 2228–2245. IEEE, 2025.

[88] Rummel, Bernard. About time: a practitioner's guide to task completion time analysis. *Journal of Usability Studies*, 15(3):124–134, 2020.

[89] Safa, Nader Sohrabi and Von Solms, Rossouw and Furnell, Steven. Information security policy compliance model in organizations. *Computers & Security*, 56:70–82, 2016.

[90] Sauro, Jeff and Kindlund, Erika. A method to standardize usability metrics into a single score. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pages 401–409, 2005.

[91] Schaub, Florian and Cranor, Lorrie Faith. Usable and useful privacy interfaces. *An Introduction to Privacy for Technology Professionals*, pages 176–299, 2020.

[92] Seo, Kwang-Kyu and Lee, Sangwon and Chung, Byung Do and Park, Changsoon. Users' emotional valence, arousal, and engagement based on perceived usability and aesthetics for web sites. *International Journal of Human-Computer Interaction*, 31(1):72–87, 2015.

[93] Sheng, Steve and Magnien, Bryant and Kumaraguru, Ponnurangam and Acquisti, Alessandro and Cranor, Lorrie Faith and Hong, Jason and Nunge, Elizabeth. Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, pages 88–99, 2007.

[94] Siponen, Mikko T. Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. *Information Management& Computer Security*, 8(5):197–209, 2000.

[95] Stahl, Bernd Carsten and Doherty, Neil F and Shaw, Mark. Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal*, 22(1):77–94, 2012.

[96] Stanton, Jeffrey M. and Stam, Kathryn R. and Mastrangelo, Paul and Jolton, Jeffrey. Analysis of end user security behaviors. *Computers & Security*, 24(2):124–133, 2005.

[97] Statsmodels Developers. statsmodels.stats.anova.anova_lm. https://www.statsmodels.org/stable/generated/statsmodels.stats.anova.anova_lm.html. Accessed: 2026-05-28.

[98] Suzuki, Shunsuke and Bellotti, Victoria and Yee, Nick and John, Bonnie E and Nakao, Yusuke and Asahi, Toshiyuki and Fukuzumi, Shin'ichi. Variation in importance of time-on-task with familiarity with mobile phone models. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2551–2554, 2011.

[99] Turner, Sarah and Nurse, Jason and Li, Shujun. When Googling it doesn't work: The challenge of finding security advice for smart home devices. In *International Symposium on Human Aspects of Information Security and Assurance*, pages 115–126. Springer, 2021.

[100] Tuyikeze, Tite and Flowerday, Stephen. Information Security Policy Development and Implementation: A Content Analysis Approach. In *Haisa*, pages 11–20, 2014.

[101] Wagner, Amina and Mesbah, Neda. Too Confident to Care: Investigating Overconfidence in Privacy Decision Making. In *Proceedings of the 27th European Conference on Information Systems (ECIS)*, Stockholm & Uppsala, Sweden, June 8–14 2019. Association for Information Systems.

[102] Wash, Rick. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, pages 1–16, 2010.

[103] Wash, Rick and Cooper, Molly M. Who provides phishing training? Facts, stories, and people like me. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2018.

[104] Wash, Rick and Rader, Emilee. Too much knowledge? Security beliefs and protective behaviors among united states internet users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 309–325, 2015.

[105] Wetzlinger, Werner and Auinger, Andreas and Dörflinger, Michael. Comparing effectiveness, efficiency, ease of use, usability and user experience when using tablets and laptops. In *Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience: Third International Conference, DUXU 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014, Proceedings, Part I 3*, pages 402–412. Springer, 2014.

[106] Williams, Laurie and Meneely, Andrew and Shipley, Grant. Protection poker: The new software security "game". *IEEE Security & Privacy*, 8(3):14–20, 2010.

[107] Wronikowska, Marta Weronika and Malycha, James and Morgan, Lauren J and Westgate, Verity and Petrinic, Tatjana and Young, J Duncan and Watkinson, Peter J. Systematic review of applied usability metrics within usability evaluation methods for hospital electronic healthcare record systems: Metrics and Evaluation Methods for eHealth Systems. *Journal of Evaluation in Clinical Practice*, 27(6):1403–1416, 2021.

[108] Yamagishi, Rei and Fujii, Shota. Survey and Analysis of User Perceptions of Security Icons. In *Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference*, pages 202–209, 2024.

[109] Zhang-Kennedy, Leah and Chiasson, Sonia and Biddle, Robert. The role of instructional design in persuasion: A comics approach for improving cybersecurity. *International Journal of Human-Computer Interaction*, 32(3):215–257, 2016.

Appendix IT-Security Advice

- ID-1 (BSI): Aktuelle Software und Sicherheitsupdates. Schon vor dem Kauf eines IoT-Geräts sollte darauf geachtet werden, dass der Hersteller Softwareupdates über die zu erwartende typische Nutzungsdauer des Geräts bereitstellen wird. Erkundigen Sie sich für jedes Gerät, ob und wie die Updates durchgeführt

werden. In den meisten Fällen geschieht das automatisch oder manuell über eine zugehörige App oder die Web-Oberfläche des Gerätes. Aktivieren Sie nach Möglichkeit automatische Updates bei Ihrem Gerät, um dessen Sicherheitsfunktionen stets aktuell zu halten. IoT-Geräte, für die keine Updates zur Verfügung gestellt werden, stellen ein Sicherheitsrisiko dar. Bei ihnen bleiben Schwachstellen offen und können ausgenutzt werden, Fehler in der Software können nicht korrigiert werden. Angreifer können sich auf diese Weise Zugang zu den Geräten verschaffen und sie möglicherweise fremdsteuern. Wenn Ihr Gerät nicht mehr mit Sicherheitsupdates versorgt wird, sollten Sie es austauschen.

- ID-2 (BSI): Zentrale Firewall und Routersicherheit. Die Firewall in Ihrem Router schützt Ihr Heimnetzwerk vor Angriffen über das Internet. Überprüfen Sie, ob Ihr Router eine Firewall integriert hat und aktivieren Sie diese. Schützen Sie auch Ihren Router, indem Sie das dort voreingestellte Passwort ändern, verfügbare Updates einspielen und auf aktuelle Firmware achten. Das Aktivieren der Firewall sowie die Änderung des Passworts können Sie in den Einstellungen des Routers vornehmen. Im Handbuch Ihres Routers ist die Internetadresse (oftmals eine IP-Nummer) vermerkt, die Sie aus Ihrem LAN bzw. WLAN heraus aufsuchen müssen, um direkten Zugriff auf den Router zu erhalten.
- ID-3 (BSI): Keine Standardpasswörter verwenden. Ein viel genutztes Einfallstor für Angreifer sind an das Internet angeschlossene Geräte, die keinen Passwortschutz besitzen oder nur mit voreingestellten Standardpasswörtern geschützt sind. Solche Geräte sind besonders anfällig für das unbefugte Aufspielen von Schadsoftware. Infizierte Geräte können beispielsweise Teil eines Botnetzes werden: Das ist ein Netzwerk aus sehr vielen Geräten, das Angreifer per Fernsteuerung zusammenschließen und für verschiedene Aktionen nutzen können. In den meisten Fällen ist es sehr schwer nachzuvollziehen, ob ein Gerät mit Schadsoftware infiziert ist. Achten Sie daher darauf, dass Sie beim erstmaligen Anschließen eines IoT-Geräts ein eigenes, individuelles Passwort setzen. Geben Sie Ihre Passwörter niemals an Dritte weiter. Worauf Sie beim Erstellen eines sicheren Passwortes achten müssen: Je länger das Passwort ist, desto besser. Das Passwort sollte mindestens acht Zeichen lang sein. Für die Absicherung eines WLAN werden mindestens 20 Zeichen empfohlen. Für ein Passwort können in der Regel alle verfügbaren Zeichen genutzt werden, also Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Das vollständige Passwort sollte nicht im Wörterbuch vorkommen. Gängige Zahlenfolgen oder Tastaturmuster kommen ebenfalls als sicheres Passwort nicht in Frage. Einfache Ziffern oder Sonderzeichen vor oder nach einem normalen Wort zu ergänzen, ist nicht empfehlenswert. Ein Passwortmanager kann die Handhabung unterschiedlicher Passwörter erleichtern. Wird eine Zwei-Faktor-Authentisierung angeboten, können Sie damit den Zugang zu Ihrem Gerät zusätzlich absichern. Dabei wird neben der Passworteingabe ein zusätzlicher Faktor abgefragt, beispielsweise in Form einer Hardware-Komponente, die als Schlüssel fungiert. Das können das Smartphone, eine Chipkarte oder ein spezieller USB-Stick sein. Auch ein Fingerabdruck oder eine vom Anbieter versendete SMS mit einem Einmalcode kann als zweiter Faktor genutzt werden.
- ID-4 (BSI): Verschlüsselte Kommunikation und lokale Nutzung. Achten Sie darauf, dass Ihre IoT-Geräte sensible Informationen verschlüsselt übertragen. Dritte können diese Daten sonst abfangen und auslesen. Erkundigen Sie sich vor dem Kauf, ob das Gerät verschlüsselte Kommunikation unterstützt.Verbinden Sie Ihr Smarthome nur mit dem Internet, wenn ein Fernzugriff unbedingt notwendig ist. In vielen Fällen reicht es aus, wenn Sie auf Ihre IoT-Geräte nur innerhalb Ihres Heimnetzes zugreifen können. Das Smartphone oder der Computer, mit dem Sie Ihre IoT-Geräte steuern, muss natürlich ebenfalls direkt in Ihr Heimnetz eingebunden sein. Einige Smarthome-Basisstationen bieten die Möglichkeit, die Kommunikation mit dem Internet zu unterbinden. Ein Gerät, das nicht über das Internet zugänglich ist, stellt ein deutlich geringeres Risiko dar. Für Rollläden oder Beleuchtung lassen sich beispielsweise Zeitpläne und Szenarien hinterlegen, die eine Steuerung völlig ohne Internetanbindung ermöglichen. So lässt sich etwa während eines Urlaubs die Anwesenheit von Bewohnerinnen oder Bewohnern vortäuschen.Sofern an Ihrem Router die Einstellung UPnP (Universal Plug and Play) aktiviert ist, sollten Sie diese deaktivieren, damit Ihre IoT-Geräte nicht unkontrolliert ins Internet kommunizieren können.
- ID-5 (BSI): VPN einrichten. Ein Virtuelles Privates Netzwerk (VPN) ist eine besonders gesicherte Verbindung zwischen zwei Punkten. Dabei wird ein sicherer “Tunnel” von beispielsweise einem Smartphone durch das öffentliche Internet zu Ihrem Heimnetz bzw. Ihrem Router aufgebaut. Die Besonderheit des VPN ist hierbei, dass der aufgebaute Tunnel nur einen Eingang und einen Ausgang aufweist und so keine Daten auf dem Weg abfließen können. Zudem ist Ihr Heimnetz durch das VPN nur mit von Ihnen freigeschalteten Geräten erreichbar. Moderne Router bieten die Möglichkeit, ein einfaches VPN einzurichten.
- ID-6 (BSI): Separates Heimnetz. Das sogenannte Segmentieren des Netzwerkes ist in Industrienetzen bereits Standard und kann auch im Heimnetz angewandt werden. Hierbei werden die IoT-Geräte in einem separaten Netzwerk betrieben, das keine Verbindung zu sensiblen Daten oder Geräten wie etwa Ihrem Computer hat. Viele Heimrouter bieten die Möglichkeit, ein separates WLAN einzurichten, in dem dann nur IoT-Geräte eingebunden werden. Dieses WLAN ist logisch von Ihrem Heimnetz getrennt und stellt somit eine einfache Möglichkeit dar, Ihre IoT-Geräte in einem separaten Netzwerk zu betreiben. Für Geräte, die Zugriff auf Daten in Ihrem Heimnetz benötigen, ist die Verlagerung in ein separates Netz nicht sinnvoll. Ein Beispiel hierfür ist Ihr Smart-TV, wenn Sie mit diesem auch auf Ihre im Netzwerk gespeicherten Mediendateien zugreifen möchten. Einige Router bieten keine Netzwerksegmentierung an, aber ein Gäste-WLAN. Dann können Sie auch überlegen, ob Sie die IoT-Geräte in dieses einbinden. In dem Fall sollte das Gäste-WLAN jedoch ausschließlich für IoT-Geräte genutzt und die Zugangsdaten nicht an Dritte weitergegeben werden.
- ID-7 (BSI): Physikalische Sicherheit. Achten Sie darauf, dass Fremde von außen keinen physischen Zugriff auf Ihre Geräte erhalten können. USB- oder LAN-Ports sollten nicht frei zugänglich sein, da diese Dritten als Einfallstor in Ihr Netzwerk und auf Ihre Daten dienen können.
- ID-8 (BSI): Bewusster Einsatz von IoT-Geräten. Machen Sie sich bewusst, wie Ihr Gerät arbeitet, welche Daten Sie mit der

Nutzung Ihres Geräts generieren und wo diese gespeichert werden. Dies ist eine wichtige Grundlage für den bewussten Einsatz von IoT-Geräten. Folgende Fragen helfen dabei, das Gerät und die potentiellen Risiken seines Einsatzes besser einzuschätzen: Welche Sensoren, wie z.B. eine Kamera oder ein Mikrofon, hat das Gerät? Welche Daten werden aufgezeichnet und gespeichert? Kann nachvollzogen werden, wo die Daten gespeichert werden? Werden diese Daten versendet oder mit anderen Anwendungen geteilt? Welche potenziellen Risiken könnten mit der Nutzung des Geräts einhergehen und bin ich bereit, diese zu tragen? Die Antworten auf diese Fragen helfen Ihnen auch, eine Abwägung zwischen Komfort, Funktionalität und Aspekten der Sicherheit zu treffen. Entscheiden Sie bewusst, ob Sie auf Sicherheit verzichten wollen, um bestimmte Funktionalitäten zu nutzen.

- ID-9 (ENISA): 1. Verwenden Sie sichere Passwörter: Erstellen Sie sichere und einzigartige Passwörter, die schwer zu erraten sind (verwenden Sie eine Mischung aus Buchstaben, Zahlen und Sonderzeichen). Vermeiden Sie die Verwendung desselben Passworts für mehrere Konten.Verwenden Sie einen Passwort-Manager, um sichere Passwörter zu speichern und zu erstellen.Überprüfen Sie, ob eines Ihrer Konten in bestehenden Datenpannen auftaucht, und ändern Sie Ihre Passwörter für die entsprechenden Dienste.
- ID-10 (ENISA): 2. Aktivieren Sie die Zwei-Faktoren-Authentifizierung (2FA): Fügen Sie eine zusätzliche Sicherheitsebene hinzu, indem Sie 2FA für Ihre Konten aktivieren-Verwenden Sie Authentifizierungs-Apps oder SMS-Codes, um Ihre Identität zu überprüfen.
- ID-11 (ENISA): 3. Regelmäßige Software-Updates: Halten Sie Ihr Betriebssystem, Ihre Anwendungen und Ihre Antiviren-Software auf dem neuesten Stand. Aktivieren Sie nach Möglichkeit automatische Updates, um sicherzustellen, dass Sie über die neuesten Sicherheits-Patches verfügen.
- ID-12 (ENISA): 4. Seien Sie vorsichtig mit E-Mails und Links: Vermeiden Sie das Anklicken von Links oder das Herunterladen von Anhängen aus unbekannten oder verdächtigen E-Mails.Überprüfen Sie die Identität des Absenders, bevor Sie auf E-Mail-Anfragen nach sensiblen Informationen antworten. Nehmen Sie sich Zeit, um über eine Anfrage nach Ihren persönlichen Daten nachzudenken und zu prüfen, ob die Anfrage angemessen ist.
- ID-13 (ENISA): 5. Sichern Sie wichtige Daten: Sichern Sie regelmäßig Ihre wichtigen Dateien auf einem externen Laufwerk oder in einem Cloud-Speicher. Stellen Sie sicher, dass die Sicherungen sicher gespeichert und auf Datenwiederherstellung getestet sind.
- ID-14 (ENISA): 6. Sichern Sie Ihr Wi-Fi-Netzwerk: Verwenden Sie eine starke Verschlüsselung (WPA3) für Ihr Wi-Fi-Netzwerk. Ändern Sie das Standardpasswort Ihres Routers und verwenden Sie ein sicheres Passwort. Deaktivieren Sie die Fernverwaltung und unnötige Dienste auf Ihrem Router.
- ID-15 (ENISA) 7. Verwenden Sie Antiviren- und Anti-Malware-Software: Installieren Sie seriöse Antiviren- und Anti-Malware-Software auf Ihren Geräten.Führen Sie regelmäßig Scans durch, um Bedrohungen zu erkennen und zu entfernen.
- ID-16 (ENISA): 8. Informieren Sie sich selbst und andere: Informieren Sie sich über die neuesten Bedrohungen und Trends im Bereich der Cybersicherheit. Nehmen Sie an Schulungen und Sensibilisierungsprogrammen für Cybersicherheit teil. Teilen Sie Ihr Wissen mit Familie, Freunden und Kollegen, um eine gute Cyberhygiene zu fördern.
- ID-17 (ENISA): 9. Begrenzen Sie die Weitergabe persönlicher Informationen: Achten Sie darauf, welche persönlichen Informationen Sie online weitergeben. Prüfen Sie die Datenschutzeinstellungen in sozialen Medien und anderen Online-Diensten.
- ID18 (ENISA): 10. Überwachen Sie Konten und Geräte: Überprüfen Sie regelmäßig Ihre Finanzkonten und Online-Profile auf verdächtige Aktivitäten. Verwenden Sie Sicherheitssoftware, um Ihre Geräte auf unbefugten Zugriff oder ungewöhnliches Verhalten zu überwachen.
- ID-19 (Europäisches Verbraucherzentrum Deutschland): Wodurch zeichnet sich ein gutes Passwort aus? Passwörter sind wie Zahnbürsten: Man sollte sie sorgfältig auswählen, nicht teilen, regelmäßig wechseln und unbedingt benutzen. Wenn Sie Ihre Daten im Internet so gut wie möglich schützen möchten, sollten Sie folgende Punkte in Ihrem zukünftigen Passwort berücksichtigen. Verwenden Sie mindestens acht Zeichen.Ziffern, Groß- und Kleinbuchstaben sowie Sonderzeichen $(!?_{\&} - \#)$ nutzen. Nehmen Sie keinen Bezug auf persönliche Daten (zum Beispiel Geburtsdatum, Adresse oder den eigenen Namen). Vermeiden Sie Begriff aus dem Wörterbuch. Ein Kennwort sollte für jedes Benutzerkonto nur einmal verwendet und regelmäßig geändert werden (am besten alle drei bis sechs Monate).
- ID-20 (Europäisches Verbraucherzentrum Deutschland): Wie erstelle ich ein sicheres Passwort? Grundsätzlich kann jeder ein sicheres Passwort erstellen. Es gibt jedoch zahlreiche Tools (Passwort-Manager und Passwort-Generatoren), die Ihnen unter die Arme greifen können. Wir geben einen Überblick, wie es mit der Passwort-Erstellung klappt. Formulieren Sie einen einfach zu merkenden Satz, zum Beispiel einen Musiktitel wie "Mit 66 Jahren, da fängt das Leben an!" Die Anfangsbuchstaben jedes Wortes sowie die Zeichen und Ziffern ergeben dann Ihr Passwort. In diesem Fall also: M66J,dfdLa!Im Internet gibt es übrigens nützliche Hilfsmittel zum Herunterladen, mit denen man sichere Passwörter erstellen kann (Passwort-Generatoren). Nutzen Sie - wenn möglich - die Zwei-Faktor-Authentifizierung. Sie dient als Nutzeridentifikation und bietet somit einen weiteren Schutz vor Hackern. Speichern Sie Ihr Passwort niemals auf Ihrem PC ab, sondern höchstens auf einem anderen Medium (zum Beispiel Notizblock). Geben Sie Ihr Passwort nicht an Dritte weiter! Verwenden Sie keine gängigen Tastaturfolgen wie wertzuiopü oder logische Zahlenreihen wie 12345678 - auch wenn das die beliebtesten (und damit am leichtesten zu knackenden) Passwörter sind.
- ID-21 (Europäisches Verbraucherzentrum Deutschland): Auf eine verschlüsselte Verbindung achten. Kein System ist hundertprozentig sicher. Es hilft aber, eine gesicherte Verbindung zur Übermittlung von sensiblen Daten zu wählen - gerade bei Bankverbindungen und persönlichen Angaben. Achten Sie deshalb beim Surfen im Netz auf die https-Verschlüsselung in der Adresszeile. Besteht eine sichere Verbindung, wird diese

durch ein Schloss-Symbol im Browser dargestellt. Bei E-Mail-Programmen sollte eine SSL-Verschlüsselung vorhanden sein. Bei den meisten Anbietern ist das heutzutage Standard.

- ID-22 (Europäisches Verbraucherzentrum Deutschland): Ausloggen nicht vergessen. Loggen Sie sich immer aus Ihren Benutzer-Accounts aus, um anderen Personen den Zugang zu Ihren Daten und Kunden-Konten zu verwehren. Das gilt insbesondere dann, wenn Sie sich in öffentlich zugängliche WLAN-Hotspots einwählen oder sich in Internet-Cafés aufhalten.
- ID-23 (Europäisches Verbraucherzentrum Deutschland): Browser-Chronik löschen. Die Chronik des Browsers setzt sich aus Cookies, Cache, Suchbegriffen sowie der Seiten- und Download-Chronik zusammen. Wir empfehlen den Browser so einzustellen, dass beim Beenden der Sitzung die komplette Chronik und sonstige Daten (Offline-Daten, Passwörter usw.) gelöscht werden. So verhindern Sie, dass das eigene Surf-Verhalten und persönliche Daten über mehrere Sitzungen hinweg nachvollzogen werden können. Wenn Sie dies regelmäßig machen, ist es auch nicht mehr so wichtig, sogenannte permanente Cookies aus Sicherheitsgründen abzulehnen. Dies können Sie natürlich trotzdem zusätzlich tun, wenn Sie während einer Sitzung eine Zurückverfolgung und / oder Auswertung Ihres Surfverhaltens verhindern wollen.
- ID-24 (Europäisches Verbraucherzentrum Deutschland): Werfen Sie einen Blick in die Datenschutzerklärung. Zu lang? Zu kompliziert? Zu unverständlich? Dennoch sollten Sie immer einen Blick in die Datenschutzerklärung werfen, um nachvollziehen zu können, welche Ihrer Daten vom Unternehmen erhoben werden. Einen einheitlichen Rahmen für den Datenschutz in der EU gibt die Datenschutzgrundverordnung (DSGVO) vor. Vor dem Abschluss eines Kaufvertrags im Internet werden Sie immer dazu aufgefordert ein Häkchen zu setzen, dass Sie die Datenschutzerklärung und die Allgemeinen Geschäftsbedingungen (AGB) durchgelesen haben. Wenn wir ehrlich sind: In den wenigsten Fällen liest man sich diese jedoch durch. Dennoch sollten Sie sich immer mit der Datenschutzerklärung vertraut machen, sodass Sie sich im Anschluss folgende Fragen beantworten können: Wer ist die verantwortliche Stelle für die Datenverarbeitung im Unternehmen? An wen kann ich mich bei Fragen wenden? Ist nachvollziehbar, welche Daten zu welchem Zweck und in welchem Umfang gespeichert werden? Ist ersichtlich, ob und an wen die Daten weitergegeben werden? Werden persönliche Daten auch außerhalb der EU verwendet? Wenn ja, was passiert dort mit meinen Daten?
- ID-25 (PayPal): Informationen über Nachrichten zum Wiederherstellen des Passworts. Wenn du eine E-Mail oder SMS erhältst, in der du aufgefordert wirst, dein Passwort zu ändern, könnte es sich um Phishing handeln. Sei vorsichtig und klicke nicht auf den Link in der Nachricht. Öffne stattdessen ein Browserfenster, gib paypal.com ein und melde dich bei PayPal an. Dies ist der sichere Weg, um dein Passwort wiederherzustellen.
- ID-26 (PayPal): Sichere Passwörter: Die Komplexität von Passwörtern ist nur eine Komponente sicherer Passwörter. Verwende Passwörter nicht mehrfach, denn wenn du dasselbe Passwort für mehrere Konten verwendest, muss ein Hacker nur auf eine Website zugreifen, um deine Daten zu stehlen und Zugriff auf jedes Konto zu erhalten, das dieses Passwort verwendet. Längere Passwörter sind stärker, daher sollten sie mindestens 12 Zeichen lang sein. Erstelle eine Passphrase mit drei oder mehr Wörtern solche Phrasen sind leichter zu merken und schwerer zu knacken. Sei kreativ und verwende keine gängigen Wörter oder persönlichen Daten, auf die Hacker leicht zugreifen können, wie Geburtsdaten, Familien- oder Haustiernamen und Telefonnummern.
- ID-27 (PayPal): Passwort-Manager: Es kann eine Herausforderung sein, dir all deine Passwörter zu merken. Eine Passwort-Manager-App kann Passwörter auf allen Geräten speichern und synchronisieren. Du musst dir nur ein Master-Passwort merken, also stelle sicher, dass dieses Passwort so komplex, einzigartig und einprägsam wie möglich ist.
- ID-28 (PayPal): Wann solltest du dein Passwort ändern? Es ist wichtig, dass du dein Passwort unter folgenden Umständen sofort änderst:Du bemerkst nicht genehmigte Aktivitäten in deinem Konto. Du hast den Verdacht, dass jemand Unseriöses deine Daten hat. Du hast in deinem E-Mail-Konto oder anderen Online-Konten etwas Verdächtiges festgestellt. Du hast kürzlich Malware gefunden und entfernt. Du hast eine Benachrichtigung von PayPal erhalten, in der du aufgefordert wirst, dein Passwort aufgrund ungewöhnlicher Aktivitäten zu ändern.
- ID-29 (PayPal): Biometrische Authentifizierung: Falls verfügbar, aktiviere die Authentifizierung per Fingerabdruck oder Face ID für jedes Konto, das dieses Verfahren anbietet.