Making Encryption Feel Secure: Investigating how Descriptions of Encryption Impact Perceived Security

Verena Distler
HCI Research Group
University of Luxembourg
Esch-sur-Alzette, Luxembourg
verena.distler@uni.lu

Carine Lallemand
HCI Research Group
Dep. of Industrial Design
University of Luxembourg
Eindhoven University of Technology
Esch-sur-Alzette, Luxembourg
Eindhoven, Netherlands
carine.lallemand@uni.lu

Vincent Koenig
HCI Research Group
University of Luxembourg
Esch-sur-Alzette, Luxembourg
vincent.koenig@uni.lu

***Abstract*—When communication about security to end users is ineffective, people frequently misinterpret the protection offered by a system. The discrepancy between the security users perceive a system to have and the actual system state can lead to potentially risky behaviors. It is thus crucial to understand how security perceptions are shaped by interface elements such as text-based descriptions of encryption. This article addresses the question of how encryption should be described to non-experts in a way that enhances perceived security. We tested the following within-subject variables in an online experiment (N=309): a) how to best word encryption, b) whether encryption should be described with a focus on the process or outcome, or both c) whether the objective of encryption should be mentioned d) when mentioning the objective of encryption, how to best describe it e) whether a hash should be displayed to the user. We also investigated the role of context (between subjects). The verbs "encrypt" and "secure" performed comparatively well at enhancing perceived security. Overall, participants stated that they felt more secure not knowing about the objective of encryption. When it is necessary to state the objective, positive wording of the objective of encryption worked best. We discuss implications and why using these results to design for perceived lack of security might be of interest as well. This leads us to discuss ethical concerns, and we give guidelines for the design of user interfaces where encryption should be communicated to end users.**

***Index Terms*—Usable Security and Privacy, User Experience, Encryption**

1. Introduction

Effective communication about security is crucial to shape security perceptions purposefully and, ultimately, to reduce risky behaviors. Indeed, when interfaces communicate security states in a potentially misleading way, people may misinterpret the protection offered by a tool, which may hinder adoption [2]. Efforts to model misalignment between a user's mental model and the system's security state [16] [23] show that lack of alignment can lead to "false sense of insecurity", or on the contrary, a "false sense of security" [23]. While previous work shows that visible indicators of encryption, in their case a waiting screen displaying "encrypting your vote" and a hash, may have a positive impact on perceived security [11], it is currently unclear precisely *how* encryption should be communicated to people with the goal of triggering perceived security.

To address this objective, we conducted an online experiment with 5 within subjects variables: a) wording of encryption b) process or outcome-focussed description (or both) c) whether the objective of encryption should be mentioned d) when mentioning the objective of encryption, how to best describe it e) whether a hash should be displayed to the user. To understand whether the perceived security of these options depended on context, we used three contexts as a between subjects variable (online banking, e-voting, online pharmacy).
This paper makes the following contributions:

- We present a relative ranking of the perceived security of various text samples describing encryption to users.
- We provide suggestions to support the communication of encryption to users in a way that enhances perceived security.

2. Related Work

Improving the user-friendliness of encryption has been important concern in the usable security and privacy community given that encryption approaches sometimes demand too much user effort and thus do not not lead to adoption. More convenient encryption approaches are frequently seen as "good enough" for everyday use [4]. Interestingly, the adoption of secure messaging applications depends largely on social factors, rather than security and privacy concerns. [8]

Going beyond improving the usability and UX of encryption tools, there is an ongoing debate in the usable security and privacy community on whether security mechanisms such as encryption should be visible to users. Consensus has not been reached so far, and the answer seems to be "it depends". When users cannot see underlying security mechanisms, the advantage is that they do not need to understand what the security mechanisms entails.

The resulting lack of knowledge can however lead to security-relevant misunderstandings [3], and some authors have argued that security and privacy should be highly visible [12] and scrutable [20] in order to keep the human in the loop [22].

2.1. Consequences of invisible and ineffectively communicated encryption

Wu and Zappala [26] describe how the invisibility of encryption can lead people to make up their own, frequently inaccurate or outright wrong, mental models (or "folk models" [25]) of encryption. Such incorrect mental models and misaligned security perceptions can cause security problems when users need to interact with encryption, such as sending out unencrypted messages or emails mistakenly [21] or using less secure channels because encrypted messaging apps are not perceived as secure [15]. In addition to impacting mental models of encryption, lack of visible encryption can also influence trust and perceptions of the security of a tool. Ruoti and colleagues [21] tested prototypes of two versions of a private email system, one where technical details were hidden (e.g., key management and encryption), whereas the other version did show such information. The authors found that invisible security details (automatic key management, automatic encryption) led some users to mistakenly send out unencrypted messages, and some users doubted the trustworthiness of the email system. The authors then conducted user studies with an alternative prototype that used manual encryption. The users accepted extra steps of cutting and pasting ciphertext themselves and had more trust in the system. The authors suggest that more visible encryption may be a way to foster greater trust. Distler and colleagues [11] described similar results when comparing an e-voting application with visible encryption with a second version, where encryption was invisible. While the version with visible encryption performed worse in terms of pragmatic aspects of UX (i.e. usability), it seemed to qualitatively create a more favorable reaction for overall User Experience (UX) and perceived security.

Mental models of the security of messaging apps are often erroneous, as shown by Gerber et al. [15] who investigated how people perceive the security of end-to-end encryption for the messaging app WhatsApp in an interview study. They found that about half of the participants thought that even with E2E encryption, messages were still available in plain text to third parties. This perception that messages could be eavesdropped led to a lack of trust towards WhatsApp. The authors suggest to implement a user interface that makes E2E encryption processes more graspable for the user and increases transparency about the business model and the encryption protocol, which is not publicly available yet. The creation of metaphors with the objective of improving user understanding of encryption also seems to be a promising direction for future research, however, Demjaha et al., [10] showed that using metaphors can sometimes do more harm than good, and the authors underline the difficulties of explaining encryption to users. Similar problems are pointed out by Abu-Salma and colleagues [1], who analyzed the user interface of the secure messaging app Telegram. The interface design showed various issues, including the use of inconsistent terminology and not making all security features clear to the user. A later study showed that users lacked both trust in and awareness of encryption in secure messaging tools, even though the tool explitely informed them that encrpytion was used [9]. Communication with end users in the context of connection security seems to be similarly challenging as shown in a qualitative study on end user and administrator mental models of HTTPS. Users often confuse encryption with authentication and tend to underestimate the security benefits of HTTPS. When comparing the mental models of encryption of end users to administrators, end users have a more conceptual understanding, whereas administrators' understanding is more protocol-based [17].

2.2. How to communicate security concepts and encryption

How security concepts such as encryption should be communicated to users remains an ongoing debate. Bultel and colleagues [6] proposed various ways of teaching security concepts including various encryption modes to children or non-expert adults in an understandable manner. However, in many contexts, it is not always realistic to include full explanations of the details of encryption protocols to users who want to achieve their primary goal, unrelated to encryption. Efforts to communicate encryption in a concise manner has been made in the context of browser security indicators which communicate that data is sent through an encrypted communication protocol. Felt and colleagues found that the strings "secure" and "https" performed best at conveying security to users, accompanied by a green lock [13]. The level of detail that should be communicated to users can be difficult to define. In the warning literature [18], studies have shown that explicit (full and precise) information creates a greater perception of risk, better comprehension of the safety issues and people remember more explicit warnings [18].

Overall, it seems that visible instances of encryption may be beneficial for perceived security [11], [21] and that interface design has an important impact on people's perceived security of encryption [15]. In particular, text describing encryption-related processes often lacks consistency [1] and should be made more graspable to users for better perceived security [15].

3. Research Objectives

The objective of this study is to better understand how to describe encryption in a way that gives a feeling of perceived security to users. Given that user understanding and perceived security do not necessarily coincide, we wanted to disentangle the goals of optimizing for user understanding and perceived security. Our objective was thus not to improve user understanding of encryption, rather, we aimed at investigating the impact of various ways of wording encryption in user interfaces on perceived security. We address the following research question:

How should we describe encryption to users to create perceived security through user interfaces?

4. Methodology

We conducted a mixed design online experiment, including both an in-between subjects variable (text samples) and a between subjects variable (context). All experimental variables are described in 4.2 Material, details on participants can be found in 4.3 Participants.

4.1. Procedure

An overview of the study design is presented in Figure 1. Participants viewed various screens simulating the use of a smartphone app. In each of these contexts, we focused on the moment where the user has to send critical data (vote, money transfer, medical prescription). At this security-critical moment (shown in more detail in the appendix), participants had to confirm whether the information was correct. Finally, they were presented with various text samples (described in "Material") which they rated on a Likert scale of perceived security from 1 (not secure at all) to 10 (very secure). An example of how the question was presented to participants is shown in Figure 2, the full questionnaire is provided as supplementary material. We then asked participants how security-critical their experimental use context was in their opinion on a scale from 1 (not security-critical) to 10 (very security-critical). Question order and answer options were randomized. This paper focuses on the part of the questionnaire that addresses the perceived security of various ways of describing encryption. A separate subset of this dataset, addressing another research question concerning the perceived security of a selection of icons, has been separately analyzed by [24]. The subset of data analyzed in the present article includes only questions regarding the textual description of encryption, which were asked after the questions concerning the perceived security of icons. Given that all participants were exposed to the same icons (in random order) before answering to the questions about the perceived security of textual descriptions of encryption, we have ensured that any potential bias relating to previously answering questions about the icons was the same across all participants.

4.2. Material

4.2.1. Text Samples (Within subjects). We investigated the best wording to communicate encryption for perceived security. The objective was to keep the text samples short and concise, aiming to foster perceived security rather than technical understanding. We conducted a literature review to inform the selection of the text samples used in our experiment. The text samples were additionally reviewed by a group of seven usable security and UX experts, and subsequently pre-tested and refined with the target population in qualitative pre-tests (N = 15).

In summary, we tested 5 aspects related to possible descriptions of encryption:

	Variable	*Options*
a)	Wording of encryption	3 text samples
b)	Focus on process or outcome of encryption	3 options (Table 2)
c)	How to describe the objective of encryption	3 text samples
d)	Display or omit objective of encryption	Display or omit
e)	Hash	Display or omit

TABLE 1. SUMMARY OF THE VARIABLES AND ANSWER OPTIONS, DETAILS IN THE TEXT

a) Wording of encryption

First, we studied how to word encryption in a way that conveys security. We used the following answer options (screens in Figure 3):

- securing your data (or vote/transaction)
- encrypting your data (or vote/transaction)
- translating your data (or vote/transaction) to secret code

The verbs "encrypt" and "secure" were based on previous research [13], where they evoked perceived security.

b) Focus on process or outcome of encryption

As displayed in table 2, participants selected whether (1) process-oriented wording, (2) results-oriented wording, or (3) a combination of both made them feel more secure.

(1)	*(2)*	*First (1) , then (2)*
Encrypting your data.	Your data is encrypted.	Encrypting your data →Your data is now encrypted.

TABLE 2. DOES PROCESS ORIENTED WORDING (1), RESULTS-ORIENTED WORDING OR (3) A COMBINATION OF BOTH MAKE PEOPLE FEEL MORE SECURE?

c) How to describe the objective of encryption

We were interested in the impact of explicitness [18] on perceived security and wanted to understand if the objective of encryption should be mentioned to the user when designing for perceived security. Explicit information, in this context, can be defined as full and precise information [18]. For cases where describing the objective of encryption was necessary, we wanted to understand how to describe encryption in a way that enhances perceived security. We strived to keep these explanations short and concise, as recommended in the warning literature [18] so that users would realistically be able to read them in a smartphone app. We avoided technical jargon, which is usually not a good way to achieve explicitness for a general target audience [18]. The three versions we tested were:

Your vote is now encrypted / secure / translated to secret code...

- ... to mask your data from being viewed and read.
- ...to protect it during transit.
- ...so that only authorized parties can read it.

d) Display or omit objective of encryption

After finding out which option felt most secure in the previous question, the next question addressed whether perceived security was higher when participants were presented with the goal of encryption or when this

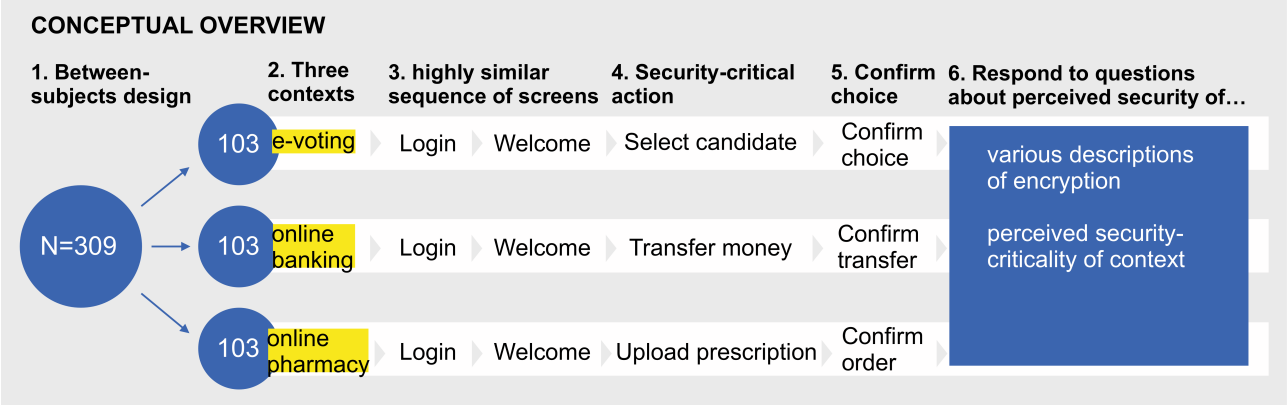


Figure 1. Overview of the study design (a separate subset of this dataset, addressing another research question, has been separately analyzed by [24])

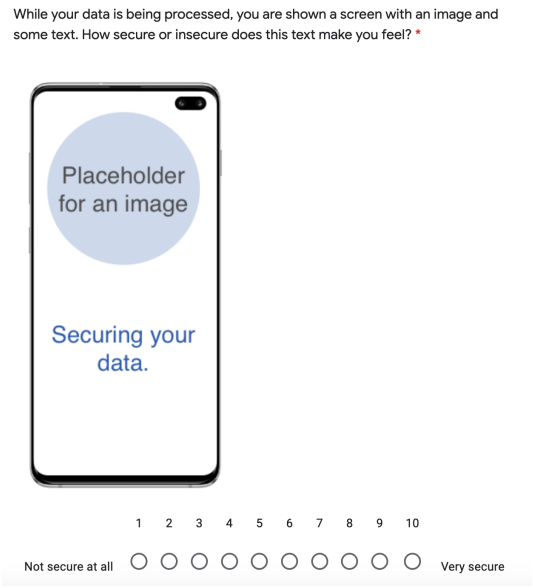


Figure 2. Sample question as presented to participants.

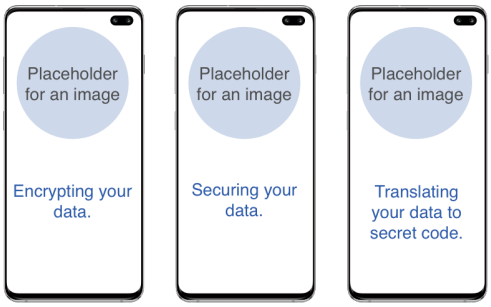


Figure 3. Participants rated the perceived security of each text sample on a scale from 1 (not secure at all) to 10 (very secure).

information was omitted. The participants chose whether overall, they preferred being presented the objective of encryption, or not.

e) Display or omit hash

In addition to the previously mentioned wordings regarding encryption, we also wanted to know whether participants felt more secure when a hash was displayed or whether the opposite was the case. We thus asked them to choose the screen they felt was more secure between one with a hash and one without a hash (see Figure 4).

Figure 4. Participants had to choose whether they felt more secure when seeing a hash or without this information.

4.2.2. Context (Between subjects). Within our experimental design, each participant was randomly assigned to one of three use contexts. In all contexts, participants were placed in a realistic scenario in which they had to take a context-dependent, security-critical action. These scenarios were (1) voting for the next national elections online (2) transferring money on a banking app (3) ordering medication through the app of an online pharmacy. All three contexts used a very similar sequence of screens so that the context was the only major factor that varied between use contexts (see Appendix, Table 13). We purposefully kept the color scheme and visual design consistent and neutral across use contexts. We did not use any official-looking logos to ensure the logo did not act as a confounding factor.

4.3. Participants

309 participants took part in our study. The average age was 34.8 years (Min = 18, Max = 76, SD = 12.6). Participants were sampled through the crowdsourcing platform Prolific. Peer and colleagues [19] found that Prolific participants produced data quality that was comparable to MTurk's and tends to include more diverse samples. We

recruited 309 adult UK citizens who were randomly split into three experimental groups of 103 participants. Each experimental group was assigned to a different security-critical context (see "Procedure").

4.3.1. Pre-tests. We conducted 3 pre-tests with 5 participants each. In these pre-tests, we asked Prolific participants to comment on the difficulty and understandability of the questionnaire, what they liked and disliked about the questionnaire. We also gathered feedback on the adequacy of the compensation, and asked them to give feedback to improve the questionnaire. This also allowed us to refine the smartphone screens shown to the participants. We excluded anyone who had participated in pre-tests, and no participant could partake in more than one group.

4.3.2. Ethics. The study has received prior approval by our university's ethics committee. Participants gave informed consent. We did not use deception. The compensation of this study (GBP 2.20 / ca. USD 2.90 for 15 minutes) equals GBP 8.80 / ca. USD 11.60 per hour, thus exceeding Prolific's minimum compensation of GBP 6.50 / ca. USD 8.50.

4.4. Data Analysis

For qualitative analyses, the first author used inductive coding to create the codebook in consultation with the other authors. We did not exclude any data points given that responses were of satisfactory quality, all datasets were complete and all qualitative answers were valid. We used an alpha level of .05 for all statistical tests. While we can conclude from the normality tests of the residuals that they don't follow a normal distribution, visually verifying the distributions of the residuals on a histogram shows that they are quite symmetrical and the analysis of variance is known to be a robust method in that case. We provide the ANOVA tables [1].

5. Results

5.1. Security-Criticality

There was a significant effect of context on criticality $F(2,306) = 4.25$, $p = .015$. Online banking was perceived as significantly more security-critical than the online pharmacy ($p = .012$) (see Table 4). No significant difference with voting could be observed ($p = .149$). No significant difference between voting and the online pharmacy could be observed ($p = .575$).

Context	*Mean*	*SD*	*Min*	*Max*
e-voting	8.88	1.62	4	10
Online Banking	9.28	1.13	4	10
Online Pharmacy	8.67	1.76	1	10
Total	8.94	1.54	1	10

TABLE 3. CRITICALITY OF CONTEXTS (1 = NOT SECURITY CRITICAL, 10 = VERY SECURITY-CRITICAL, N = 103 PER CONTEXT)

1. Link to ANOVA tables

5.2. Wording of encryption, focus on process or outcome of encryption (a) and b))

In summary, the verbs encrypt and secure were perceived as significantly more secure (table 4) than "translating to secret code" (described in more detail hereafter).

Process-focussed wording We conducted a univariate analysis of variance to understand whether there was an effect of the textual indicator on their perceived security and whether there was an effect of the experimental group (e-voting, online banking, online pharmacy). There was no significant effect of context on perceived security at the $p < .05$ level, $F(2,918) = .76$, $p = .469$. The version of the text however had a significant effect $F(2,918) = 100.6$, $p < .001$. An interaction between context and version of text could not be demonstrated, $F(4,918) = 1.48$, $p = .208$.

Result-focussed wording There was a significant effect of context on perceived security, $F(2,918) = 3.24$, $p = .040$. The version of the text also had a significant effect, $F(2,918) = 158.00$, $p < .001$. An interaction between context and version of text could not be demonstrated, $F(4,918) = .66$, $p = .620$. Post-hoc tests showed that the perceived security was significantly higher in the pharmacy use case compared to the banking use case ($p = .033$).

Post-hoc tests showed that for both process-focussed and result-focussed wording, the verbs "encrypt" and "secure" significantly outperformed "translating to secret code" ($p < .001$, Tukey HSD). In both cases, no significant difference between "encrypt" and "secure" was observed ($p = .985$ process-focussed, $p = .240$ results-focussed).

Process-oriented wording, results-oriented wording, or a combination of both (b) For 63% of participants, seeing information on the process, followed by information on the result was perceived as more secure than seeing either option in isolation (26% found result-focussed wording more secure, 11% found process-focussed wording more secure). There was no significant difference between the contexts (χ^2 (2, $N = 309$) = 8.33, $p = 0.080$).

5.3. How to describe the outcome of encryption for perceived security (c)

There was no significant effect of context on perceived security, $F(2,918) = .24$, $p = .786$. The version of the text had a significant effect, however: $F(2,918) = 17.69$, $p < .001$. An interaction between context and version of text could not be demonstrated $F(4, 918) = .87$, $p = .482$.

Post-hoc Tukey HSD tests showed that the wording "...so that only authorized parties can read it" ($M = 6.65$, $SD = 2.41$) significantly outperformed "...to mask your data from being viewed and read." ($p < .001$) and "to protect it during transit." ($p < .001$). The latter two versions did not differ significantly with regard to their perceived security ($p = .120$).

5.4. Display or omit objective of encryption (d)

Overall, 63% of participants felt more secure not knowing about the goal of encryption. In the context of voting, more participants preferred knowing about the goal

Verb used	*Process-focused or results-focused*	*Text communicating encryption*	*Mean*	*SD*
Encrypt	Process-focused	"Encrypting your transaction."	6.61	2.198
	Result-focused	"Your transaction is now encrypted."	7.19	2.198
Secure	Process-focused	"Securing your transaction.."	6.56	2.010
	Result-focused	"Your transaction is now secure."	7.40	2.114
Translate to secret code	Process-focused	"Translating your transaction to secret code."	4.44	2.289
	Result-focused	"Your transaction is now translated to secret code."	4.42	2.555
Total	Process-focused		5.87	2.390
	Result-focused		6.31	2.657

TABLE 4. DESCRIPTIVE STATISTICS OF PERCEIVED SECURITY OF TEXTUAL INDICATORS. 10 EQUALS HIGHEST POSSIBLE PERCEIVED SECURITY, 1 LOWEST PERCEIVED SECURITY.

Text Version	*Mean*	*SD*
Your transaction is now [...] so that only authorized parties can read it	6.65	2.42
Your transaction is now [...] to mask your data from being viewed and read.	5.90	2.39
Your transaction is now [...] to protect it during transit.	5.52	2.35
	6.02	2.43

TABLE 5. PERCEIVED SECURITY OF THREE TEXT VERSIONS COMMUNICATING THE RESULT OF ENCRYPTION (10 EQUALS HIGHEST POSSIBLE PERCEIVED SECURITY, 1 LOWEST PERCEIVED SECURITY).

of encryption (45% compared to 37%), but the difference was non-significant ($\chi^2(2, N = 309) = 4.55$, $p = .110$).

5.5. Display or omit hash (e)

A majority of participants (72%) felt more secure not seeing the hash. There were no significant differences between the contexts ($\chi^2(2, N = 309) = .22$, $p = 0.895$).

5.6. Why People Want to Know or Prefer Not To Know About the Goal Of Encryption

As shown in table 6, analysis of qualitative answers showed that those who **preferred not being told** about about the goal of encryption stated that on the one hand, they preferred straight-to-the-point information (see table 6) and on the other hand, it made them worry about security problems they had not previously thought about. Participants who perceived the **display of the goal of encryption as more secure** did so because they felt better informed about the process and they thought that it sounded more professional.

5.7. Summary of Results

a) Wording of encryption: The verbs "encrypt" and "secure" outperformed "translating to secret code".
b) Focus on process or outcome of encryption: Most participants preferred seeing information on the process of encryption, followed by information on the result.
c) How to describe the objective of encryption: Participants thought that,"...so that only authorized parties can read it" felt most secure as an objective of encryption.
d) Display or omit objective of encryption: 63% of participants felt more secure when they were not told about the objective of encryption.
e) Display or omit hash: 72% felt more secure when not seeing the hash.

6. Discussion

6.1. How to Describe Encryption to Users to Evoke Perceived Security

6.1.1. Wording. This study addresses the question of how to describe encryption in a way that triggers perceived security. Both "encrypting your transaction" and "securing your transaction" were perceived as significantly more secure than "translating your transaction to secret code." Indeed, the use of slightly technical vocabulary (encrypting, securing) felt reassuring and professional for participants. Previous research in the context of HTTPS indicators also found that "secure" yielded a high number of participants who felt at least somewhat safe, and the lowest number who felt not safe at all [13]. Future studies could address even more variations of wordings, such as more "extreme" statements (e.g., "highly secure"), however such descriptions might have a negative effect on the perceived security of expert users, who might thus want more information on the actual security of the system. Another relevant question for future work concerns the applicability of these results going beyond graphical interfaces, such as reassuring descriptions of encryption for voice interactions.

Displaying the goal of encryption...	*Responses*	*Representative Verbatims*
Is unnecessary, keep it simple	36 %	"I only need to know my data is secure at all times, not the reason why." (P72) "simple to read, gets the point across, no useless information" (P301)
Makes me worry	18 %	"I really don't know. It's weird. You'd think the more transparency the better, but actually, I'd rather just do the whole "ignorance is bliss" thing and just not think about the risks involved in sharing my data showing the reason for encryption provides an extra layer of worry that I was never worried about until it was mentioned." (P82)
Makes me feel better informed	22 %	"Because it makes it clearer what is being encrypted and why." (P182) "I would like to be told whether or not my data will be protected and know what/who would be able to see my data." (P79) "Because it's not just random terminology that doesn't mean anything. It explains why these processes are happening to your data which makes me feel as though security is paramount in the process."(P239)
Sounds safer and more professional	13 %	"I feel secure cause the info tells me my data is being protected" (P143)

TABLE 6. WHY PARTICIPANTS FELT MORE SECURE SEEING / NOT SEEING THE GOAL OF ENCRYPTION. PERCENTAGES DO NOT ADD UP TO 100% BECAUSE ONLY FREQUENT CODES ARE LISTED.

6.1.2. Level of detail. In our study, user perception was different when they were presented with details on the objective of encryption. Participants felt that mentioning the transfer of data, as well as mentioning the possibility of their data being viewed and read, made them worry about security more than they would have without this information. This aligns with results from the warning literature, which found that a higher level of "explicit" (full and precise) information leads to greater perception of risk or hazard [18]. While creating a greater perception of risk is intended for effective warnings, a designer's intention when communicating encryption might be the opposite, aiming to reassure users. In this case, one option might thus be to opt for a lower level of explicitness, which has the downside of potentially not informing the user sufficiently. Indeed, 63% of participants stated that they felt more secure not knowing about the objective of encryption. While this is the majority, it is worth mentioning that the remaining 37% felt reassured and kept in the loop when seeing the objective of encryption. Future studies might address whether this concerns a particular population group (e.g., more tech savvy users), or whether in certain contexts users might be more interested in receiving more detailed information on the security process.

6.1.3. Phrasing the objective of encryption. Rather than completely omitting any explicit information on the objective of encryption, designers might also choose to inform users, but ideally word the advantages of encryption in a positive, rather than directly threat-related way when designing for perceived security. Compared to "[...] to mask your data from being viewed and read." and "Your transaction is now [...] to protect it during transit." "Your transaction is now [...] so that only authorized parties can read it" was perceived as significantly more secure than information relating to "data being viewed and read" or "to protect it during transit". We hypothesize that this is due to the fact that the information focuses on the positive result of encryption, rather than potential threats during data transmission. This is coherent with previous research emphasizing that displays of security mechanisms should be meaningful for users and aligned with their goals [11], which was not the case for the majority (63%) of our users who felt felt more secure not seeing the goal of encryption.

6.2. Use of Results to Design for A Lack of Perceived Security

While the first reaction to these results may be to discard any text samples that did not create a feeling of perceived security, there is value in understanding which descriptions of encryption evoke a negative reaction, a lack of perceived security. For instance, mentioning data transmission and the possibility of data being viewed and read created a sense of worry for our participants. Previous work has shown that users sometimes show a false sense of security, when it is not warranted by a secure system state [23]. Understanding the interface elements that give people a sense of perceived insecurity may allow us to design interactions that lower their perceived security in order to avoid a false sense of security that may lead to risky behaviors. Experience design can thus be used to purposefully design moments of doubt and reflection when it is in the interest of the user, but further research is needed to understand the nuances of such design interventions and how to best apply them. In addition, ethical implications of such design approaches need to be considered.

6.3. Ethical Implications and Potential for Misuse

When using experience design to either design for or against perceived security, malicious actors can use these insights go purposefully create a sense of security for unsafe websites. While we cannot prevent such misuse, we believe that a deeper understanding of how interface elements influence security perceptions is also valuable for benevolent actors. In particular, any design will impact user perceptions of the security of an interface, be it intentional or unintentional. Nevertheless, we believe that a further discussion of how experiential design aiming to change security perceptions can be considered a subtle

persuasive design technique [14] and should adhere to according ethical guidelines [5], similar to reflections in the field of warnings [7] would be of value to the community.

6.4. Limitations

This study has some limitations. We used a simulation of a smartphone application, rather than asking participants to download an application on their phone. This trade-off was carefully weighed in advance and allowed us to control the participants' exploration process of the app and to ensure that participants unwilling to download apps on their phones could still participate in the study. Participants also did not put any real personal information at risk, which allowed us to avoid any potential harm to the participants, but it might also have increased their perceived security. Lastly, we cannot be sure whether all participants knew the name of the medication used in the pharmacy context (a medication used to treat depression), which may have impacted their perception of the criticality. One might argue that some of the text samples were more familiar to participants than others, such as "securing" data. The word encryption, on the other hand, is a well established term in security research and one might thus assume that it results in higher perceived security for participants than more novel options (e.g., "translating to secret code"). While these are valid assumptions, no empirical evidence exists thus far, and it is compelling to deliver results to substantiate these intuitions.

We chose to use a simple ANOVA instead of a mixed model for repeated measures for reasons of parsimony. Given that all our significant results are highly significant, the tests can be considered powerful enough and the conclusions can be trusted to remain the same. We also conducted a mixed model analysis, which we provide [2].

6.5. Recommendations for the Design of Indicators for Perceived Security

Based on these results, we suggest the following recommendations for researchers and designers who have the objective of communicating encryption to users in way that enhances perceived security:

- When describing encryption with the intention to improve perceived security on an interface, text should be short and overly technical elements avoided for perceived security.
- When informing users of the result of encryption with the intent to improve perceived security, designers should be careful to avoid a strong focus on data transmission or third parties accessing data. Instead, the positive result of encryption seems to evoke a more positive response.
- Designers may choose to mention the threats a security measure protects users against with the purpose of creating moments of doubt and reflection when it is in the interest of the user. In this case, ethical concerns should be considered and misinforming the user must be avoided.

2. Link to mixed model analysis

7. Conclusion

This study addresses the timely question of how to describe encryption to users in a way that maximizes perceived security. It gives insights into the perceived security various textual samples evoke, demonstrating that text should be short and slightly technical for perceived security. While users overall did not feel more secure when knowing about the objective of encryption, framing the result of encryption in a positive way seems promising. We also discuss why using these results to design for perceived lack of security might be useful. We discuss ethical implications, and provide guidelines for describing encryption. We expect the results of this work to contribute to the design of secure systems by making a step towards more reassuring descriptions of encryption, and at a larger level, security systems that keep users in the loop in an experience-centred way.

Acknowledgment

We thank our shepherd Dr. Katharina Krombholz and the anonymous reviewers. We acknowledge support from the National Research Fund (FNR) under grant number PRIDE15/10621687. We also thank Etienne Le Bihan for his feedback.

References

[1] Ruba Abu-Salma, Kat Krol, Simon Parkin, Victoria Koh, Kevin Kwan, Jazib Mahboob, Zahra Traboulsi, and M. Angela Sasse. The security blanket of the chat world: An analytic evaluation and a user study of telegram. In *Proceedings 2nd European Workshop on Usable Security*. Internet Society.

[2] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the adoption of secure communication tools. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 137–153. IEEE.

[3] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Commun. ACM*, 42(12):40–46, December 1999.

[4] Wei Bai, Moses Namara, Yichen Qian, Patrick Gage Kelley, Michelle L. Mazurek, and Doowon Kim. An inconvenient trust: User attitudes toward security and usability tradeoffs for key-directory encryption systems. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 113–130. USENIX Association.

[5] Daniel Berdichevsky and Erik Neuenschwander. Toward an ethics of persuasive technology. 42(5):51–58.

[6] Xavier Bultel, Jannik Dreier, Pascal Lafourcade, and Malika More. How to explain modern security concepts to your children. 41(5):422–447.

[7] Kenzie A Cameron and David M DeJoy. The persuasive functions of warnings: Theory and models. In Michael S Wogalter, editor, *Handbook of Warnings*, pages 301–312. CRC Press.

[8] Alexander De Luca, Sauvik Das, Martin Ortlieb, Iulia Ion, and Ben Laurie. Expert and non-expert attitudes towards (secure) instant messaging. pages 147–157.

[9] Sergej Dechand, Alena Naiakshina, Anastasia Danilova, and Matthew Smith. In Encryption We Don't Trust: The Effect of End-to-End Encryption to the Masses on User Perception. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 401–415, Stockholm, Sweden, June 2019. IEEE.

[10] Albese Demjaha, Jonathan Spring, Ingolf Becker, Simon Parkin, and Angela Sasse. Metaphors considered harmful? An exploratory study of the effectiveness of functional metaphors for end-to-end encryption. In *Proceedings 2018 Workshop on Usable Security*, San Diego, CA, 2018. Internet Society.

[11] Verena Distler, Marie-Laure Zollinger, Carine Lallemand, Peter B. Roenne, Peter Y. A. Ryan, and Vincent Koenig. Security - visible, yet unseen? In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 605:1–605:13, New York, NY, USA, 2019. ACM.

[12] Paul Dourish, E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal Ubiquitous Comput.*, 8(6):391–401, November 2004.

[13] Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. Rethinking connection security indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 1–14. USENIX Association.

[14] Bj Fogg. Persuasive computers: perspectives and research directions. In *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '98*, pages 225–232. ACM Press.

[15] Nina Gerber, Verena Zimmermann, Birgit Henhapl, Sinem Emeröz, and Melanie Volkamer. Finally johnny can encrypt: But does this make him feel more secure? In *Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018*, pages 1–10. ACM Press.

[16] Adam Michael Houser. Mental models for cybersecurity: A formal methods approach.

[17] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. " if https were secure, i wouldn't need 2fa"-end user and administrator mental models of https. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 246–263. IEEE, 2019.

[18] Kenneth Laughery R and Smith Danielle Paige. Explicit information in warnings. In M Wogalter, editor, *Handbook of Warnings*, pages 605–615. CRC Press.

[19] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. Beyond the turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology*, 70:153–163, 2017.

[20] Emilee Rader and Janine Slaker. The importance of visibility for folk theories of sensor data. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 257–270. USENIX Association.

[21] Scott Ruoti, Nathan Kim, Ben Burgon, Timothy van der Horst, and Kent Seamons. Confused johnny: when automatic encryption leads to confusion and mistakes. In *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*, page 1. ACM Press.

[22] S.W. Smith. Humans in the loop: Human-computer interaction and security. 1(3):75–79.

[23] Borce Stojkovski, Itzel Vazquez Sandoval, and Gabriele Lenzini. Detecting misalignments between system security and user perceptions: a preliminary socio-technical analysis of an e2e email encryption system. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 172–181. IEEE, 2019.

[24] Distler Verena, Lallemand Carine, and Koenig Vincent. The power of visual indicators perceived security and interpretation of icons. under submission.

[25] Rick Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10*, page 1. ACM Press.

[26] Justin Wu and Daniel Zappala. When is a tree really a truck? exploring mental models of encryption. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 395–409, Baltimore, MD, August 2018. USENIX Association.

Appendix A. Link to full questionnaires

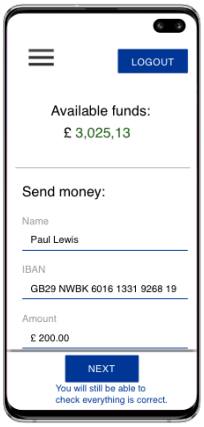
Online banking full questionnaire
e-voting full questionnaire
Online pharmacy full questionnaire

Appendix B. Security-critical action depending on context

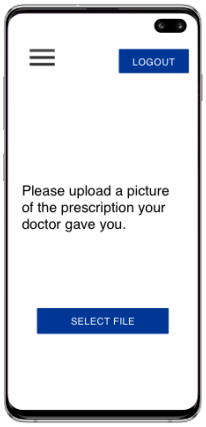
Step 4: Security-critical action

e-voting

online banking

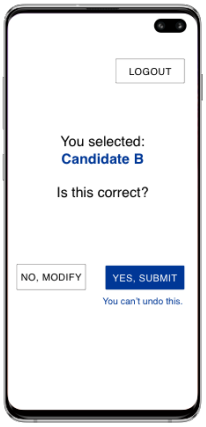


online pharmacy

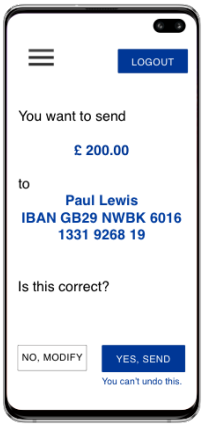


Step 5: Confirm choice

e-voting



online banking



online pharmacy

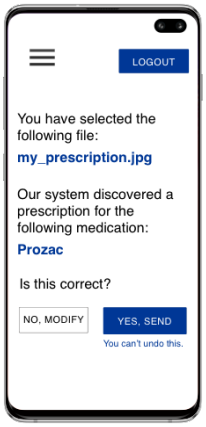


TABLE 7. DETAILED VIEW OF STEP 4 AND 5 IN FIGURE 2: DEPENDING ON CONTEXT, THE SECURITY-CRITICAL ACTION VARIED. THE TABLE SHOWS THE RESPECTIVE SECURITY-CRITICAL ACTION FOR EACH CONTEXT. (A SEPARATE PART ON ANOTHER TOPIC OF THE QUESTIONNAIRE WAS ANALYZED BY [24])