Voter, What Message Will Motivate You to Verify Your Vote?

M. Maina Olembo*, Karen Renaud†, Steffen Bartsch*, and Melanie Volkamer*
*CASED, TU Darmstadt
Hochschulstr. 10, 64289, Darmstadt, Germany
Email: firstname.lastname@cased.de
†School of Computing Science, University of Glasgow
18 Lilybank Gardens, Glasgow, G12 8RZ, UK
Email: karen.renaud@glasgow.ac.uk

***Abstract*—There is increasing interest in verifiable Internet voting systems that enable voters to verify the integrity of their vote on the voting platform prior to casting it, and any interested party to verify the integrity of the election results. The ease with which a vote can be verified plays a key role. Empowering individual voters to act as interested yet objective verifiers increases the probability of fraud detection. Verifying constitutes additional effort, something humans resist unless the benefits are compelling enough. Thus, what is the best way to provide such motivation? We report on a survey, distributed to 123 respondents, in which we explore the effects of three types of motivating messages on voters' intention to verify a vote, using a smartphone app. The motivating messages were intended to increase the intention to verify a vote. Our findings have persuaded us that further research on the use of motivating messages in the context of verifiable voting is warranted.**

I. Introduction

There is increasing interest in the deployment and use of Internet voting in legally-binding elections, for example, it has been used since 2007 in the Estonian parliamentary elections [22]. Voters are also interested in the use of Internet voting: a recent survey in Germany [1], where voting machines were rejected, reported that 51% of voters would vote over the Internet for federal elections.

Most of the Internet voting systems in use are so-called black box systems, i.e. voters are expected to trust that the voting system and indeed their own voting environment (e.g. their laptop) are neither deliberately malicious nor unwittingly compromised. To deal with some of these challenges, security researchers have proposed a number of verifiable voting protocols to enable voters to verify the integrity of their votes and the election results, while still providing vote secrecy due to the cryptographic primitives that are used. These protocols enable voters to verify that their votes are not modified prior to being sent from the voting platform to the voting server (cast as intended), stored unaltered in the electronic ballot box (stored as cast), and counted in the final tally, without modification (tallied as stored). With these provisions it is no longer necessary to blindly trust the Internet voting system.

Verifiable voting systems are in use both in academic and national contexts, for example, a verifiable voting system was used to elect the university president at the Universitê catholique de Louvain in March 2009 [2], while e-voting trials were carried out in 2011 and 2013 in Norway [59], [43]. Ideally, the verifying steps could be delegated to a trusted third party (such as a university, a political party, security agencies, or international election observer bodies, such as the Organization for Security and Co-operation in Europe (OSCE)). However, not all the verifiability steps can be delegated: specifically, the individual voter has to verify that his or her vote is cast as intended, in order to preserve vote secrecy. Further, two potential challenges could waylay the verifiability aspect. The first is that the voter may find the process too difficult, and the second is that he or she may not see the need to verify, especially since it requires them to expend extra effort.

While it is unfortunate that many of the proposed systems require additional (often cumbersome) steps for verifying, efforts to improve the usability of verifiability in the Helios voting protocol[1], demonstrate that it is indeed possible to iteratively improve the verifiability step, making it simpler for voters [3], [67], [29], [28].

Verifying a vote constitutes extra effort, no matter how easy it is to do. It is well known that users minimize effort wherever they can [68], [7]. Since voters often do not perceive a need to verify, due to their trust in the people and processes involved, and the overall election system [41], they are not likely to be motivated to do so. In this paper, we focus our attention on this challenge.

The question we wanted to answer was: 'Could a specially tailored message increase the intention to take up this verifiability opportunity?' At the outset, we acknowledge that our goal is to influence behavioural intention, but we know that such an intention does not always convert to actual behaviour. On the other hand, intention is definitely a necessary precursor to actual behaviour [34], and it is thus worth focusing attention

USEC '14, 23 February 2014, San Diego, CA, USA

http://dx.doi.org/10.14722/usec.2014.23038

[1] www.heliosvoting.org

and effort in this direction.

To this end, we identified a number of behaviour-changing theories and models. We summarized and grouped the findings into several categories, from which we deduced three types of motivating messages: those based on risk theories, those based on norm theories, and approaches utilizing analogies. The messages were tested in a survey with 123 German respondents, where we measured the effect on respondents' reported intention to verify and subsequent intention to vote online *(to ensure that we had not compromised this pre-existing intention.)* We found that the motivational messages did indeed influence German voters' intention to verify, without negatively affecting their pre-existing intention to vote online. As a result, we can recommend further investigation into the use of motivating messages in the context of verifiable voting, to increase the likelihood that vote manipulation will be detected. Further research is also necessary to investigate questions arising from this work.

The rest of this paper is structured as follows: first, we present related work in Section II, before discussing the literature review on behaviour change in information security, our findings, and how these were applied to design motivating messages. In Section III we present the survey developed to evaluate the designed messages, the results obtained in Section IV, and the implications for verifiable voting systems in Section V. We then conclude with open questions for future work in Section VI.

II. Related Work

In the literature, we find that the primary focus in usability evaluations of verifiable voting systems has been to instruct voters to check their votes. Studies of electronic voting machines revealed that instructions were not successful [13], neither were monetary incentives [53]. Hence, knowledge of how to verify and extrinsic rewards had little effect. In the context of electronic voting machines, emphasizing the verifying step in the context of review screens increased the number of participants who detected errors [20], [11]. User studies of verifiable voting systems have also concentrated on instructing participants on the steps to carry out, both in polling station based systems [38], [55], [51] and remote verifiable voting systems [67], [28].

A lot of research has also been carried out in the usable security field with respect to users acting securely. The efficacy of instructions is seen to vary depending on the application context, for example, users appreciate instructions how to create strong passwords [49], but where the instructions are complex, may suffer the discomfort [6] or opt out, for example, in [47]. The authors in [7], [24], and [30] point to the economic perspective in users' decision making as they evaluate whether to comply or not based on a cost benefit analysis, in cases where conflicts arise between their day-to-day tasks and security, or more effort is asked of them than they deem necessary.

Our work differs from existing research in that we seek to design motivating messages and to test their effect on voters' intention to verify. The messages are designed based on existing theories of behaviour change. A control group will act as a baseline, receiving straightforward instructions to verify, similar to current practice reported in the voting literature.

A. Behaviour-Change in Information Security

We report on the literature review carried out to identify behaviour-change theories and models, and the findings that were then used to develop motivating messages.

1) Literature Review: Using the methodology in [31], we searched for literature using the terms 'behaviour change' and 'information security'. From notable research repositories providing access to peer-reviewed literature [36], we identified papers published from the year 2000 to date. Those lacking empirical tests were excluded. Backward references [36] provided further publications. One of the authors of a recent literature review [34] provided an appendix of literature focused on motivating information security policy compliance in organizations. By cross-referencing papers in this appendix with the literature already identified, we included 20 new papers. The remaining papers had either already been identified, did not contain empirical work, or only had abstracts readily available.

A total of 135 papers were identified and reviewed. To extract data, we noted the theories and methodologies applied; the number of respondents recruited; how the approaches were applied: e.g. to develop a specific message; the context of use: e.g. home computer users or employees; and noteworthy findings applicable to our work.

2) Identified Categories: Twenty-eight identified theories and models were then categorized inductively into five groups. The theories and models generally have multiple individual constructs. A single construct can be operationalized as several variables for evaluation. In the literature, we found that either a single theory with multiple constructs, a single theory and individual constructs from other theories, or single constructs from a given theory, were applied. Where such cases were identified, the individual constructs were grouped along with the original theory or model, or categorized based on the element the authors concentrated on. As an example, while the Health Belief Model has been used to increase perception of threats and coping appraisal in order to change behaviour and is therefore classified under the Risk category, perceived susceptibility (a single construct from the model) was used in [18] to train respondents not to fall for phishing attacks. The final categories are listed below, along with descriptions and examples from literature.

- *Risk* — Change behaviour by providing information about existing risks or threats and how to cope, for example, the Protection Motivation Theory [4].
- *Training* — Change behaviour using training programs or security messages developed using learning theories [46].
- *Rewards/Penalties* — Change behaviour by rewarding "desired" behaviours [44] or penalizing "undesired" behaviours [23]. The rationale here is that users evaluate cost (effort) and benefit in deciding whether or not to carry out an action [7].
- *Norms* — Change behaviour by informing people of the behaviours of others, emphasizing the descriptive

norm and using human tendencies to imitate others' behaviours, to encourage particular behaviours [56].

We identified another potential theory, that of analogies. While this has not been used in security research before, it did seem to have potential in this context, therefore it was included.

- *Analogies* — Analogies exploit the direct personal experience of the person, and point out the links between a new idea and the existing experience, easing the instructional process [12]. In this case behaviour is changed by establishing links with previous knowledge and thereby improving understanding.

It is interesting to note the focus of these categories. Training attempts to address lack of knowledge about the process itself, analogies build on knowledge in a similar context. Norms impart knowledge about what other people do, and risk focuses on potential consequences of fraudulent behaviours of others. Rewards and penalties introduce additional artificial consequences into the equation.

B. Developing Behaviour-Change Messages

The first consideration in testing the message effects was how such messages should be delivered. A message utilizing images, sound or video would be very effective but would have to be delivered via a supporting platform. Unfortunately there is always the possibility that the voting platform has been compromised [50], thus delivering instructional messages this way seems insecure [2]. Hence we designed messages which could easily be delivered via a secure channel (e.g. postal mail). In this case they would have to be primarily textual. There is evidence that textual messages can be effective in motivating secure behaviour [4], [32], [64] so we considered this a reasonable compromise.

1) Excluded Categories: Our objective was to test a message belonging to each category identified in Section II-A. Some, however, were unsuitable. Here we explain why they were excluded.

Since verifying of votes cast via the Internet is a novel concept, the issue of knowledge has to be addressed. It seems impractical to contemplate implementing a training programme for an entire voting population. Instead we included, along with the messages that we did test, step-by-step instructions how to verify a vote using a smartphone app. Voter training, as a specific behaviour-change category, was thus excluded.

There is evidence in the psychological literature that suggests both rewards and penalties may be counter-productive [23], [9], [10]. The general view is that humans are not machines that can be easily controlled merely by a carrot or a stick. Pink [45] has shown, and replicated this finding in countries worldwide, that rewards usually lead to worse performance, not improved motivation, and have negligible impact in terms of behavioural change. Penalties are similarly flawed. Even in countries that use the severest possible penalty, i.e. the death penalty, there is no evidence that it reduces crime [35], thus we do not expect it to be efficacious in a voting context. In verifiable voting, understanding is seen to trump rewards and penalties. In a game-theoretic experiment reported in [38], participants were were offered monetary incentives in order to motivate them to post their vote receipt, and their earnings deducted as a penalty if any other participant correctly guessed their vote from the posted receipt. The financial incentives were shown to be insufficient motivation for those participants who did not understand that the receipt did not reveal their vote. Additionally, in this work we evaluated only the cast as intended verifiability step, which cannot be observed to determine whether or not a voter truly verified. Hence the use of rewards and penalties was excluded.

2) Included Messages: We iteratively designed messages using the remaining three behaviour-change categories: risk, norms and analogy. The messages were prepared in English and translated into German for the survey. As each message was based on a different theory, emphasizing different aspects, their lengths differed.

a) Risk: Communicating risk is potentially useful since risk has obvious threat connotations [32]. Overplaying the risks, however, can inhibit precautionary behaviour as people prefer to deny it, and do not engage in precautionary actions such as verifying [32], [69]. Huang et al. [25] report that awareness of threats was effective in motivating users to carry out necessary security steps in other contexts. Thus, we designed a risk message, emphasizing an existing threat and what the voter should do to avoid it. The risk message is shown below:

> *Studies by the Federal Office for Information Security show that most PCs or laptops with Internet access are infected with malicious software, e.g. viruses. This malicious software could change your vote before encrypting [3] and sending it to the election server, and you would not notice it. You can use the Election Verifying App to check if there is any malicious software on your PC or laptop that has changed your vote.*

We selected the threat of malicious software on the voter's PC [33]. The message included a coping strategy, since this is a necessary adjunct to a risk appeal [4], [27].

b) Norms: Norms have been shown to be effective in promoting desirable behaviour [52], as they give information about what is typically approved or disapproved of in a society [14]. Anderson and Agarwal [4] found a descriptive norm to be effective in motivating users to carry out security-related behaviours. Cialdani et al. [15] indicate that norms are more likely to influence behaviour when they are the main focus of a message. Consequently, we designed the brief descriptive norm message shown below:

> *Voters who want to protect democracy check if the voting system has correctly encrypted the selected candidates.*

c) Analogies: Curtis and Reigeluth [17] tested the use of analogies in written text. They argue that such analogies should consist of a concrete vehicle (in this case paper-based

[2]Thus we did not consider research on persuasion using technology e.g. [21].

[3]While we refer to 'encryption' the German term used for the study translates to 'coding'.

voting) and an abstract topic (in this case storage of a vote somewhere in cyberspace). They point out that this link will somehow force the reader to deploy their previously established cognitive strategy without further explanation. Shapiro [54] argues that analogies could make new information more concrete and understandable. Duit [19] references a number of studies to substantiate the constructivist perspective: that we learn because we build on previous knowledge. Using explicit analogies can therefore ease this process.

The analogy-based message establishes a link between a voter ensuring that their ballot is correct from when they select the candidates to when it is safely stowed in the sealed ballot box, and verifying the vote using the election verifying app.

> *You have previously voted in several elections. Whenever you participated in an election, you voted on a ballot paper that was counted manually. You could be sure that your ballot paper was correct because you were the one who put a cross next to your candidate's name, folded the ballot paper and placed it in the ballot box. In Internet voting, you put a cross next to your candidate's name by clicking on the candidate. Your vote is then encrypted on your PC or laptop and is sent to the election server. The Election Verifying App enables you to ensure that your vote was not modified before encryption.*

d) Summary: The rest of the paper will refer to the *Risk, Norm*, and *Analogy* messages as *motivating messages*, the instructions how to verify a vote as *instructions*, and the combination of both the messages and instructions as *voter communication*. In the survey, which we describe in Section III, the control group only received the instructions without any motivational message, while the three experimental groups received the instructions accompanied by a motivational message. Figure 1 summarizes the experiment.

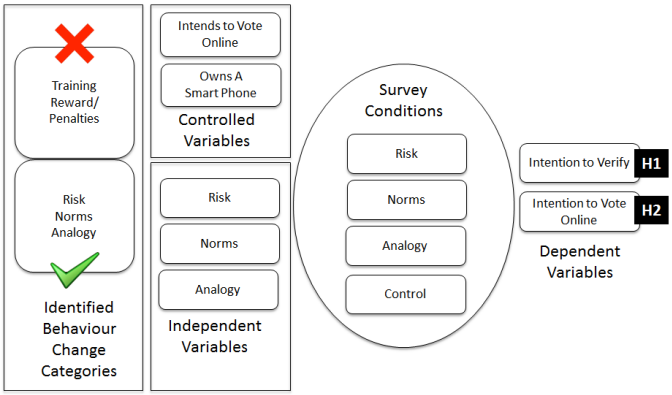

Fig. 1. Experiment

III. Testing the Behaviour-Change Messages

We first present the study hypotheses, and then give an overview of the survey carried out to evaluate the motivating messages.

A. Study Hypotheses

We anticipate that the motivating messages will have an effect such that respondents who receive them are likely to indicate an increased intention to verify than respondents in the control group, who only receive the instructions how to verify. Furthermore, the threat conveyed by the risk message, using norms to focus respondents' attention on "typical" behaviour, and using analogies and past experiences with voting to introduce new information on verifying, are each individually hypothesized to increase intention to verify as compared to the control group. The hypothesis is:

H_1: The motivating messages will increase intention to verify as compared to the control group.

This is divided into three sub-hypotheses:
H_{1r}, H_{1n}, H_{1a}: The Risk, Norm and Analogy messages will increase intention to verify as compared to the control group.

The behaviour-change literature indicates the potential negative effects of risk appeals – they can lead to denial or avoidance [37]. The risk message articulates the threats that face Internet voting. As a result, this message might reduce respondents' intention to vote online. The norm message, on the other hand, aims to motivate respondents to verify by stating that this action is somehow expected. To the extent that the norm message is perceived by respondents as limiting their freedom to act as they choose with respect to verifying, we hypothesize that it might reduce respondents' intention to vote online. The analogy message emphasizes to a greater extent than any of the other messages that the voter now has to take extra steps in comparison to paper-based voting. Thus, we hypothesize that the extra effort puts voters off online voting. The second hypothesis is:

H_2: The motivating messages will reduce intention to vote online as compared to the control group.

This is divided into three sub-hypotheses:
H_{2r}, H_{2n} and H_{2a}: The Risk, Norm and Analogy messages will reduce intention to vote online as compared to the control group.

B. Survey Overview

We discuss several considerations that informed our decision to use a survey for data collection, followed by the content and format of the survey, findings from pilot testing, and distribution of the survey for data collection.

1) Why We Used a Survey: Laboratory studies in the context of computer security pose several challenges. Participants sometimes feel safe in the study environment, and therefore exhibit less cautious behaviour, or give responses they think the experimenters would prefer [58]. Additionally, on being informed of the real purpose of a study, especially where there will be interaction with personal data, e.g. banking information, users may opt out even though this personal data may not necessarily be recorded in the course of the study [61].

The context of this research, voting, makes a laboratory study challenging as it would require observing a human who has a right to expect secrecy, since voting is similar to other security-related behaviours in this respect [66]. We therefore decided to collect data using a survey, which is an accepted tool in the security behaviour-change literature. Self-reports are less than perfect in indicating eventual behaviour, but

here satisficing seemed the wiser approach since observation would not be ethical, and given the existing challenges with laboratory user studies.

2) Format of the Survey: The scenario described to respondents was that they received a brochure from the election commission in preparation for a federal election. To increase credibility, we placed the German coat of arms as a logo on the page. The motivating messages were highlighted in red and the instructions in yellow, colors similar to those on the coat of arms. The colours were introduced to eliminate user errors that were observed during pilot tests and served to guide respondents on which sections were referred to in the questions. Correspondingly, questions specific to the different sections were highlighted in the appropriate color.

3) Content of the Survey: To ensure validity of the study instrument, we developed questions as recommended by [39] and adapted the question on intention to verify from [4]. Two other questions were used to gauge respondents' evaluation of the clarity of the voter communication [42], and their ability to verify a vote [27].

Five-point Likert scales, predominantly used in the literature, were used to collect responses. A single-item measure was considered appropriate since the questions asked respondents to describe their reaction to the scenario described immediately prior to the questions [57]. We collected qualitative data from respondents, to obtain feedback on their responses. The study questions are shown in Table I, while the instructions are displayed in Figure 2[4].

TABLE I. FINAL QUESTIONS IN THE SURVEY

Clarity of voter communication	The information in the voter communication is: (Very unclear - Very clear)
Intention to verify	I am going to use the steps (1 - 9) to check if the system has really encrypted the selected candidates (Strongly disagree - Strongly agree)
Ability to verify vote	I feel able to carry out the steps (1 - 9) to check if the system has really encrypted the selected candidates (Strongly disagree - Strongly agree)
Intention to vote online	After answering these questions would you still cast your vote over the Internet using your PC or laptop?: (Yes / No / I don't know)

4) Pilot Testing: We tested the reliability of the survey in a series of four pilot tests with nine respondents during the study design phase. Further, to validate the data collected, we asked the pilot testers to evaluate the clarity of the voter communication. Modifications were made from feedback obtained, centering around improving the wording and presentation of the information to enhance appearance, and to reduce confusion with the different sections and questions.

[4]For legibility of the image, we have not highlighted the instructions as in the actual survey.

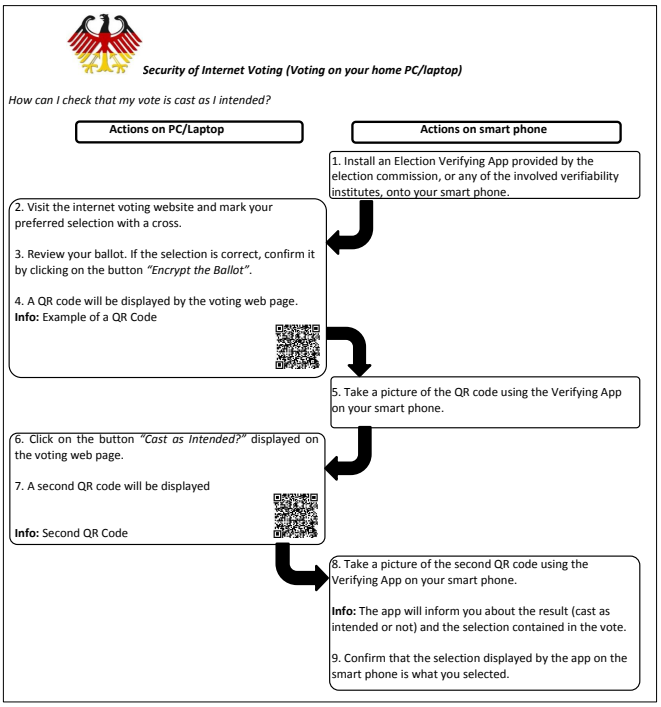

Fig. 2. Instructions how to verify

5) Distributing the Survey: The questionnaire was distributed on paper and online, via mailing lists, to staff[5] and students (both undergraduate and graduate) from two universities, a technical university and a university of applied sciences. They worked or studied in different departments including literature and languages, computer science, engineering and architecture. With this approach we drew a purposive sample [62] thus gaining insight into the possible verifying behaviour of smartphone owners who intend to vote over the Internet for federal elections.

Demographic questions were asked first as some were used to exclude ineligible respondents, ensuring that particular conditions were controlled. Only respondents who owned a smartphone, were German citizens and thus eligible to vote in federal elections, and who expressed an intention to vote over the Internet if the opportunity was provided, were recruited. The scenario in the survey described how voters would use a smartphone app to verify their votes in a federal election conducted over the Internet. The motivating message to verify an Internet vote is unlikely to influence voters who do not intend to cast an Internet vote.

Further demographic data was collected on respondents' gender, education level, and computer proficiency level (evaluated by whether they personally installed software on their computer or needed help to do so). Respondents read the scenario information, followed by the motivating message, and the instructions, before answering the final set of questions shown in Table I. Respondents in the control group only read the instructions before proceeding to the final questions.

[5]We were careful to contact and approach not only researchers at the universities, but administrative and support staff as well, for example secretaries and canteen staff.

6) Demographics: We collected data from 134 respondents, with approximately 30 respondents in each group. Similar research has shown robust results with fewer respondents (e.g. [18], [40]). Eleven respondents did not complete the questionnaire, leaving 123 respondents in total: 54 male (43.9%) and 69 female (56.1%). The majority of respondents were under the age of 30. Most were pursuing or had acquired university education, and had medium or high levels of expertise with computers, specifically, installing software on their own computers (medium), or helping others to do so (high). The demographic data is shown in Table II.

TABLE II. DEMOGRAPHIC DATA FOR RESPONDENTS IN THE FOUR GROUPS

	Risk (N=32)	Norm (N=30)	Analogy (N=31)	Control (N=30)
	(%)	(%)	(%)	(%)
Gender				
Male	56.3	50	38.7	30
Female	43.8	50	61.3	70
Age				
Average age	25.9	28.1	30.2	26.2
Education				
Non-college training	6.3	6.7	-	16.7
College training	34.4	23.3	38.7	53.3
University Education	59.4	70	61.3	30
Computer Proficiency				
Low	6.3	6.7	6.5	20
Medium	46.9	46.7	45.2	40
High	46.9	46.7	48.4	40

7) Data Analysis: Statistical tests were carried out using R version 3.0.1. Free-text responses were translated into English for analysis and reporting. A random sample was back- and forward-translated for consistency. Qualitative data analysis was carried out using the Grounded Theory Method [60] which has wide application in the analysis of qualitative data. We analyzed open responses to identify codes using spread sheets. Both descriptive codes (i.e. codes summarizing responses) and in-vivo codes (i.e. codes taken directly from responses) were used. Both approaches facilitated discussion among the authors, while in-vivo codes have the advantage of rooting the data in the respondents' language [48]. We coded responses to each question sequentially, that is, coding responses to the first question, before moving to the second question, and so on. We reviewed the data to identify emerging themes, and grouped the codes under relevant themes. The codes and themes were discussed iteratively by two of the authors.

8) Ethical Issues: Guidelines on ethical issues regarding research involving humans are provided by an ethics commission at the study university. The relevant requirements for this research relating to respondent consent and data privacy were satisfied. Respondents first read a pre-study sheet in which they were assured that their data would not be linked to their identity and that the responses would only be used for study purposes. Additionally, we designed a mild risk message which was not likely to induce any anxiety in the respondents.

IV. RESULTS

We first show that there is no significant difference in the clarity of the voter communication or the respondents' evaluation of their ability to verify based on the instructions. Moving to the main results, we report on the effect of the messages on respondents' intention to verify, and highlight insights from the qualitative data. We then turn to the effect of the messages on respondents' intention to vote online. As the data was not normally distributed (Shapiro-Wilk tests), we applied non-parametric statistical tests.

A. Clarity of the Voter Communication and Ability to Verify

The majority of respondents in all four groups indicated that the voter communication was clear. A Kruskal-Wallis test revealed that there were no significant differences between the groups ($p > 0.05$). Additionally, the majority of respondents felt that they were able to verify their votes. There were no significant differences between the groups ($p > 0.05$). Both these results are displayed in Table III. As expected, we observed a significant positive correlation between respondents' evaluation of their ability to verify the vote and their intention to verify (Pearson's R = 0.462, $p < 0.05$).

TABLE III. CLARITY OF COMMUNICATION AND ABILITY TO VERIFY

	Risk (%)	Norm (%)	Analogy (%)	Control (%)
Clarity: Clear/very clear	78	60	84	67
Ability to verify: Agree/strongly agree	94	93	94	83

B. The Effect on Intention to Verify

The risk, norm and analogy messages were all observed to increase respondents' intention to verify. We first examined whether, overall, the messages had an effect on intention to verify, comparing the treatment groups to the control group. There were significant differences between the treatment groups (N = 93) and the control group (N = 30), based on a Mann-Whitney's U test (H_1: U = 1280, $p < 0.05$, effect size r = 0.45). The differences are illustrated in Figure 3. **The hypothesis that the motivating messages will increase intention to verify as compared to the control group (H_1) is thus supported.**

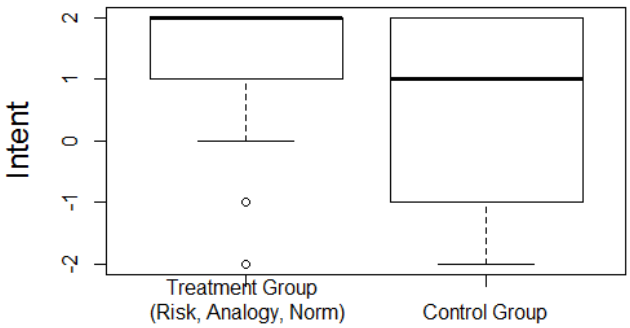

Fig. 3. Overall effect of messages compared to control group

We then tested for significant differences between the individual messages and the control group as shown in Figure 4. A Kruskal-Wallis test revealed no significant differences between the messages ($p > 0.05$). **Thus H_{1r}, H_{1n} and H_{1a} are not supported, that is, the Risk, Norm and Analogy messages did not increase intention to verify as compared to the control group.**

Respondents' open responses were evaluated for reasons why they would verify.

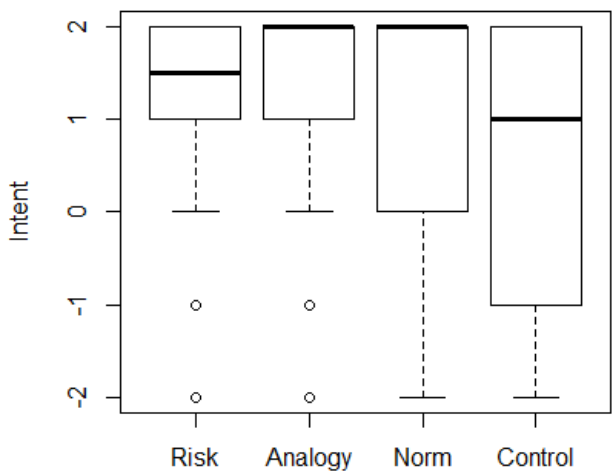

Fig. 4. Intent to verify the vote

1) Reasons for Verifying: The main themes that emerged were feelings of *security or insecurity*, verifying as a *precaution* and the *effort* involved in verifying. While these themes showed variation between the groups, we first report on the overarching reasons.

Within the first overarching theme, security and insecurity, we found numerous abstract comments that verifying gave a sense of security. The security of verifying was also doubted, particularly on technical grounds:

> *'If I don't trust the procedure I won't use it.'*

Respondents also stated that they would verify as a precautionary measure. This was particularly the case for the treatment groups where between 32% (risk and norm groups) and 29% (analogy group) of those intending to verify gave this reason, compared to only 8% in the control group.

The amount of effort respondents perceived to be required emerged as a reason why they would not verify. This was observed across the groups and respondents mostly evaluated the process as cumbersome or time consuming.

However, we also observed an accepting attitude, that if verifiability is provided one should simply use it:

> *'If there is a possibility to check your vote, you should use it.'*

One interesting point that came up across the groups was that respondents indicated they might only verify initially, out of curiosity. Some expected to trust over the long term.

> *'Perhaps at the first time. After some elections I will probably not check my vote so often.'*

2) Risk Group: In the risk group, we observed more responses that related to the (technical) risk aspects when respondents justified why they would verify:

> *'I want to be sure that my vote was transmitted correctly.'*

The technical precaution was even seen to offset the additional effort:

> *'It is a good safeguard that takes no more time than going to the polling station ...'*

Conversely, respondents who would not verify also related more often to security aspects – for example, regarding whether verifying is necessary or whether the procedure is actually secure:

> *'I trust that my PC is free from malware.'*
> *'... it remains to be seen whether the used encryption is secure enough.'*

While an evaluation of the respondents' computer proficiency levels and their intent to verify was not significant, we noted that two respondents in the risk group, who reported high computer proficiency levels, did not believe the message and indicated that they would not verify.

3) Norm Group: For the norm group, precaution was less focused on the technical safeguard, and more on the importance of the election:

> *'I want to have the certainty that everything is all right (with an important decision such as an election).'*

Interestingly, we also found that some respondents took offense at the norm message, with one commenting:

> *'It feels like an allegation if I don't do it.'*

4) Analogy Group: Respondents in the analogy group also often stated precaution as their reason to verify, but here more related to actual events:

> *'You can't be too careful. The incidents in the USA in the past show that control is better.'*

They also related to the act of voting itself:

> *'I want to make sure that I have voted for the right candidate and have not made any mistakes.'*

C. The Effect on Intention to Vote Online

A number of respondents in all four groups indicated that they would either not vote over the Internet, or they were not sure that they would do so. Chi-square tests revealed that these results were not significantly different between the groups. H_2 **is thus *not* supported, the same holds for H_{2r}, H_{2n} and H_{2a}, that is, the motivating messages did not reduce intention to vote online as compared to the control group, neither did the Risk, Norm and Analogy messages reduce intention to vote online as compared to the control group.**

V. Discussion

The goal of this work was to determine whether motivating messages would increase German voters' intention to verify the integrity of votes. We tested a specific scenario where verifying is done using a smartphone app. Our results show that motivating messages do significantly influence intention to verify. All three messages were observed to make a positive difference.

Importantly, our results also show that the interventions did not negatively affect voters' intention to vote online. These

findings are relevant in the context of verifiable voting, where currently verifiability is either not communicated [63], or voters are simply instructed to verify.

Our results do not identify one specific message as being more effective than the others. This could be as a result of the relatively small variation in the messages. For ethical reasons, we could only design a mild risk message, and while a stronger risk message may have led to greater variation, it cannot feasibly be used in practice.

Some observations were made on the effect of the messages based on the responses given. Most respondents reacted positively to the analogy message although it was somewhat contrived. There is really no close parallel between paper-based and electronic voting. Much that happens electronically is very difficult to make visible. The risk message, on the other hand, may have heightened respondents' awareness of possible threats but some respondents felt that it overstated the case. Interestingly, we noted from the open responses that it did not seem to motivate respondents who reported high levels of computer proficiency. Instead, they countered by saying that they trusted their PC or thought the described threat unlikely. Similar responses in the security context have been documented, e.g. [5] found that participants who were confident in their ability to carry out tasks on the computer showed low interest in carrying out recommended security actions. The norm message rather unexpectedly seemed to offend some respondents. This may be because they felt that it challenged their freedom to choose whether or not to verify the vote.

This study does face some limitations. The sample that was recruited is not representative of the entire German voting population. However, we do obtain insight on the effect of motivating messages on the verifying behaviour of smartphone owners who intend to vote over the Internet. Self-reported data on intention to verify was collected which may not indicate actual voter behaviour. While a link between intention and behaviour in the context of information security has been demonstrated [65], this is often not the case. Behavioural intention has been identified as an antecedent to actual behaviour [34]. Additionally, using a laboratory user study to observe actual behaviour faces related challenges: what is observed may not mirror the participant's genuine behaviour when unobserved. In remote voting, the voter expects to be in an environment of their choosing, to be unobserved, and for their vote to remain secret and their actions unobserved. Thus, any data collected by observation in a laboratory user study is unlikely to be natural behaviour.

VI. Conclusion

Internet voting continues to gain ground, with verifiable voting systems offering a mechanism for voters to verify the integrity of their votes on the voting platform. However, since extra effort is required from the voter, they do need to be motivated to carry out the necessary verifiability steps. Our study found that providing motivating messages, along with instructions on how to verify, is significantly effective in increasing intention to verify. Given that we identified a medium effect size [16], we consider the findings to be sufficiently compelling to justify further study in order to confirm the efficacy of motivational messages. This is planned for future work.

Since the survey was distributed in Germany, it would be necessary to test the impact of motivational messages in other countries. There is scope for extending this research using other message formulations which rely on different behaviour-change theories. As an example, messages can be designed for a long-term effect, as some respondents stated that they would only verify at the onset. Messages based on morality have been reported to have a long-term effect [64] and their use can be explored. Further, differently-worded norm messages can be explored.

While we only examined the potential negative effect of the motivating messages on voters' intention to vote online, other possible consequences, both negative and positive, can be explored. For example, the messages might well impact voters' trust in the voting system in general.

There may be a need to provide voters with information on how security in its entirety is catered for, not only about how integrity of the vote is assured. While voters, especially those with high technical expertise, may be interested in more security information, an open question is how this can best be presented to the general populace. The effectiveness of video and text in risk communication has been investigated by [8] who find that videos are more effective. Jenkins et al. [26] report that lean media (i.e. textual communication as developed in this work) are also appropriate. This will be explored further to determine the best approach for application.

Acknowledgment

This work was supported by CASED and Micromata. The authors would like to thank the respondents for their time. We acknowledge the support of Daniel Franke, Annika Hilt, Daniel Jones, Peter Mayer, and Robbie Simpson. Early versions of this work were discussed with Michaela Kauer and Heather Richter Lipford to whom we are grateful.

References

[1] "Forsa-Umfrage: Jeder zweite würde online wählen. Digitale Technologien stärken die Demokratie. Bürgerbeteiligung über das Internet fördert Vertrauen in die Politik," http://www.microsoft.com/germany/newsroom/pressemitteilung.mspx?id=533684., 2013, online; accessed on 4 December, 2013.

[2] B. Adida, O. De Marneffe, O. Pereira, and J. Quisquater, "Electing a University President Using Open-Audit Voting: Analysis of Real-World Use of Helios," in *Proceedings of the 2009 conference on Electronic voting technology/workshop on trustworthy elections*. USENIX Association, 2009.

[3] B. Adida, "Helios: Web-based open-audit voting," in *USENIX Security Symposium*, vol. 17, 2008, pp. 335–348.

[4] C. L. Anderson and R. Agarwal, "Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions," *MIS Quarterly*, vol. 34, no. 3, pp. 613–643, 2010.

[5] K. Aytes and T. Connolly, "Computer security and risky computing practices: A rational choice perspective," *Journal of Organizational and End User Computing (JOEUC)*, vol. 16, no. 3, pp. 22–40, 2004.

[6] D. Balfanz, G. Durfee, D. Smetters, and R. Grinter, "In search of usable security: five lessons from the field," *IEEE Security Privacy*, vol. 2, no. 5, pp. 19–24, 2004.

[7] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: managing security behaviour in organisations," in *Proceedings of the 2008 workshop on New security paradigms*, ser. NSPW '08. ACM, 2008, pp. 47–58.

[8] J. Blythe, J. Camp, and V. Garg, "Targeted risk communication for computer security," in *Proceedings of the 16th international conference on Intelligent user interfaces*. ACM, 2011, pp. 295–298.

[9] R. Brandt, "Punished by rewards," *Educational Leadership*, vol. 53, no. 1, pp. 13–16, 1995.

[10] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly*, vol. 34, no. 3, pp. 523–548, 2010.

[11] B. A. Campbell and M. D. Byrne, "Now do voters notice review screen anomalies? A look at voting system usability," in *Proceedings of the 2009 conference on Electronic voting technology/workshop on trustworthy elections, EVT/WOTE'09*. USENIX Association, 2009.

[12] J. B. Carroll, "The potentials and limitations of print as a medium of instruction," *Media and Symbols: The Forms of Expression, Communication and Education, 73rd Yearbook, Part*, vol. 1, 1974.

[13] Center for American Politics and Citizenship (CAPC), "A study of vote verification technology conducted for the maryland state board of elections. part ii: usability study," Tech. Rep., 2006, online accessed on 2nd December, 2013. [Online]. Available: http://www.cs.umd.edu/~bederson/voting/verification-study-jan-2006.pdf

[14] R. B. Cialdini, "Crafting normative messages to protect the environment," *Current directions in psychological science*, vol. 12, no. 4, pp. 105–109, 2003.

[15] R. B. Cialdini, L. J. Demaine, B. J. Sagarin, D. W. Barrett, K. Rhoads, and P. L. Winter, "Managing social norms for persuasive impact," *Social Influence*, vol. 1, no. 1, pp. 3–15, 2006.

[16] J. Cohen, "A power primer." *Psychological bulletin*, vol. 112, no. 1, p. 155, 1992.

[17] R. V. Curtis and C. M. Reigeluth, "The use of analogies in written text," *Instructional Science*, vol. 13, no. 2, pp. 99–117, 1984.

[18] N. Davinson and E. Sillence, "It won't happen to me: Promoting secure behaviour among internet users," *Computers in Human Behavior*, vol. 26, no. 6, pp. 1739–1747, 2010.

[19] R. Duit, "On the role of analogies and metaphors in learning science," *Science Education*, vol. 75, no. 6, pp. 649–672, 1991.

[20] S. P. Everett, "The usability of electronic voting machines and how votes can be changed without detection," Ph.D. dissertation, Rice University, 2007.

[21] B. J. Fogg, "Persuasive Technology: Using Computers To Change What We Think And Do," *Ubiquity*, vol. 2002, 2002.

[22] S. Heiberg, P. Laud, and J. Willemson, "The application of I-voting for Estonian parliamentary elections of 2011," in *E-Voting and Identity*. Springer, 2012, pp. 208–223.

[23] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems*, vol. 47, no. 2, pp. 154–165, 2009.

[24] C. Herley, "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*, ser. NSPW '09. ACM, 2009, pp. 133–144.

[25] D.-L. Huang, P.-L. Patrick Rau, G. Salvendy, F. Gao, and J. Zhou, "Factors affecting perception of information security and their impacts on IT adoption and security practices," *International Journal of Human-Computer Studies*, vol. 69, no. 12, pp. 870–883, 2011.

[26] J. L. Jenkins, A. Durcikova, and M. B. Burns, "Forget the fluff: Examining how media richness influences the impact of information security training on secure behavior," in *45th Hawaii International Conference on System Science (HICSS)*. IEEE, 2012, pp. 3288–3296.

[27] A. C. Johnston and M. Warkentin, "Fear appeals and information security behaviors: an empirical study," *MIS Quarterly*, vol. 34, no. 3, pp. 549–566, 2010.

[28] F. Karayumak, M. Kauer, M. M. Olembo, T. Volk, and M. Volkamer, "User study of the improved helios voting system interface," in *Socio-Technical Aspects in Security and Trust (STAST)*, 2011.

[29] F. Karayumak, M. Kauer, M. M. Olembo, and M. Volkamer, "Usability Analysis of Helios - An Open Source Verifiable Remote Electronic Voting System," in *Proceedings of the 2011 USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, 2011.

[30] I. Kirlappos, A. Beautement, and M. A. Sasse, ""Comply or Die" Is Dead: Long Live Security-Aware Principal Agents," in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science, A. A. Adams, M. Brenner, and M. Smith, Eds. Springer Berlin Heidelberg, 2013, vol. 7862, pp. 70–82.

[31] B. Kitchenham, "Procedures for performing systematic reviews," Keele, UK, Keele University, Tech. Rep. TR/SE-0401, 2004.

[32] R. LaRose, N. J. Rifon, and R. Enbody, "Promoting personal responsibility for Internet safety," *Communications of the ACM*, vol. 51, no. 3, pp. 71–76, 2008.

[33] T. W. Lauer, "The risk of e-voting," *Electronic Journal of E-government*, vol. 2, no. 3, pp. 177–186, 2004.

[34] B. Lebek, J. Uffen, M. H. Breitner, M. Neumann, and B. Hohler, "Employees' information security awareness and behavior: A literature review," in *46th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2013, pp. 2978–2987.

[35] S. D. Levitt, "Understanding why crime fell in the 1990s: Four factors that explain the decline and six that do not," *The Journal of Economic Perspectives*, vol. 18, no. 1, pp. 163–190, 2004.

[36] Y. Levy and T. J. Ellis, "A systems approach to conduct an effective literature review in support of information systems research," *Informing Science: International Journal of an Emerging Transdiscipline*, vol. 9, pp. 181–212, 2006.

[37] H. Liang and Y. Xue, "Avoidance of information technology threats: A theoretical perspective," *MIS Quarterly*, vol. 33, no. 1, pp. 71–90, 2009.

[38] M. Llewellyn, S. Schneider, Z. Xia, C. Culnane, J. Heather, P. Y. A. Ryan, and S. Srinivasan, "Testing voters' understanding of a security mechanism used in verifiable voting," *USENIX Journal of Election Technology and Systems (JETS) and Electronic Voting Technology Workshop/Workshop on Trustworthy Elections, EVT/WOTE'13*, vol. 1, 2013.

[39] G. Marshall, "The purpose, design and administration of a questionnaire for data collection," *Radiography*, vol. 11, no. 2, pp. 131–136, 2005.

[40] B.-Y. Ng, A. Kankanhalli, and Y. C. Xu, "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems*, vol. 46, no. 4, pp. 815–825, 2009.

[41] M. M. Olembo, S. Bartsch, and M. Volkamer, "Mental models of verifiability in voting," in *VOTEID 2013*. Springer, 2013, pp. 142–155.

[42] J. C. Otero and J. M. Campanario, "Comprehension evaluation and regulation in learning from science texts," *Journal of Research in Science Teaching*, vol. 27, no. 5, pp. 447–460, 1990.

[43] S. Øyvann, "Vote early, vote often: Inside Norway's pioneering open source e-voting trials," http://cacm.acm.org/news/167797-vote-early-vote-often-inside-norways-pioneering-open-source-e-voting-trials/fulltext, 2013, online; Accessed on 11th December, 2013.

[44] S. Pahnila, M. Siponen, and A. Mahmood, "Employees' behavior towards IS security policy compliance," in *40th Annual Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2007, pp. 156b–156b.

[45] D. H. Pink, *Drive: The surprising truth about what motivates us*. Canongate, 2010.

[46] P. Puhakainen and M. Siponen, "Improving employees' compliance through information systems security training: an action research study," *MIS Quarterly*, vol. 34, no. 4, pp. 757–778, 2010.

[47] F. Raja, K. Hawkey, P. Jaferian, K. Beznosov, and K. S. Booth, "It's Too Complicated, So I Turned It off!: Expectations, Perceptions, and Misconceptions of Personal Firewalls," in *Proceedings of the 3rd ACM Workshop on Assurable and Usable Security Configuration*, ser. SafeConfig '10. ACM, 2010, pp. 53–62.

[48] J. Saldaña, *The coding manual for qualitative researchers*, 2nd ed. London, UK: Sage Publications Ltd, 2012.

[49] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link' a human/computer interaction approach to usable and effective security," *BT Technology Journal*, vol. 19, no. 3, pp. 122–131, 2001.

[50] M. Schläpfer and M. Volkamer, "The secure platform problem taxonomy and analysis of existing proposals to address this problem," in *Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance*. ACM, 2012, pp. 410–418.

[51] S. Schneider, M. Llewellyn, C. Culnane, J. Heather, S. Srinivasan, and Z. Xia, "Focus group views on Prêt à Voter 1.0," in *International Workshop on Requirements Engineering for Electronic Voting Systems, REVOTE 2011*, 2011.

[52] P. W. Schultz, J. M. Nolan, R. B. Cialdini, N. J. Goldstein, and V. Griskevicius, "The constructive, destructive, and reconstructive power of social norms," *Psychological science*, vol. 18, no. 5, pp. 429–434, 2007.

[53] T. Selker, M. Hockenberry, J. Goler, and S. Sullivan, "Orienting graphical user interfaces reduce errors: The low error voting interface," Caltech/MIT Voting Technology Project, Tech. Rep., 2005.

[54] M. A. Shapiro, "Analogies, visualization and mental processing of science stories." 1985.

[55] A. T. Sherman, R. Carback, D. Chaum, J. Clark, A. Essex, P. S. Herrnson, T. Mayberry, P. Stefan, R. R. L., E. Shen, B. Sinha, and P. Vora, "Scantegrity Mock Election at Takoma Park," *Electronic Voting 2010 (EVOTE2010)*, pp. 45 – 61, 2010.

[56] M. Siponen, S. Pahnila, and A. Mahmood, "Factors influencing protection motivation and IS security policy compliance," in *Innovations in Information Technology, 2006*. IEEE, 2006, pp. 1–5.

[57] M. Siponen and A. Vance, "Neutralization: new insights into the problem of employee information systems security policy violations," *MIS Quarterly*, vol. 34, no. 3, p. 487, 2010.

[58] A. Sotirakopoulos, K. Hawkey, and K. Beznosov, ""I did it because I trusted you": Challenges with the study environment biasing participant behaviours," in *SOUPS Usable Security Experiment Reports (USER) Workshop*, Redmond, WA, 2010.

[59] I. S. G. Stenerud and C. Bull, "When reality comes knocking Norwegian experiences with verifiable electronic voting," in *Proceedings of the 5th International EVoting Conference*, vol. 205, 2012, pp. 21–33.

[60] A. Strauss and J. Corbin, *Basics of qualitative research*. Sage Publications, 1998.

[61] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor, "Crying Wolf: an empirical study of SSL warning effectiveness," in *USENIX Security Symposium*, San Diego, US, 2009, pp. 399–416.

[62] C. Teddlie and F. Yu, "Mixed methods sampling: A typology with examples," *Journal of Mixed Methods Research*, vol. 1, no. 1, pp. 77–100, 2007.

[63] G. Tsoukalas, K. Papadimitriou, and P. Louridas, "From Helios to Zeus," *USENIX Journal of Election Technology and Systems (JETS) and Electronic Voting Technology Workshop/Workshop on Trustworthy Elections, EVT/WOTE'13*, vol. 1, no. 1, 2013.

[64] D. Van Bruggen, S. Liu, M. Kajzer, A. Striegel, C. R. Crowell, and J. D'Arcy, "Modifying smartphone user locking behavior," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM, 2013, p. 10.

[65] A. Vance, D. Eargle, K. Ouimet, and D. Straub, "Enhancing password security through interactive fear appeals: A web-based field experiment," in *46th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2013, pp. 2988–2997.

[66] C. Vroom and R. Von Solms, "Towards information security behavioural compliance," *Computers & Security*, vol. 23, no. 3, pp. 191–198, 2004.

[67] J. Weber and U. Hengartner, "Usability study of the open audit voting system helios," 2009, online; accessed on 11 December, 2013. [Online]. Available: http://www.jannaweber.com/wp-content/uploads/2009/09/858Helios.pdf

[68] R. West, "The psychology of security," *Communications of the ACM*, vol. 51, no. 4, pp. 34–40, 2008.

[69] M. Workman, W. H. Bommer, and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior*, vol. 24, no. 6, pp. 2799–2816, 2008.