Voting Under Pressure: Perceptions of Counter-Strategies in Internet Voting

Christina Nissen[1](✉), Tobias Hilt[2], Jurlind Budurushi[3],
Melanie Volkamer[2], and Oksana Kulyk[1]

[1] IT University of Copenhagen, Copenhagen, Denmark
chfn@itu.dk
[2] Karlsruhe Institute of Technology, Karlsruhe, Germany
[3] Baden-Wuerttemberg Cooperative State University, Stuttgart, Germany

Abstract. While internet voting can enhance democratic participation, concerns about voter coercion have emerged due to the uncontrolled voting environment. To mitigate this, researchers have proposed different types of *counter-strategies*, allowing voters to cast their intended vote despite being coerced. We conduct semi-structured interviews ($N = 26$) to investigate voters' perceptions of six types of counter-strategies concerning their effectiveness. Our findings show that the voter's perception of the effectiveness of counter-strategies depends on both the technical and personal skills of voters, concrete risks, and ease of use. Overall, our findings pave the way for future research aimed at developing user-friendly solutions that are effective against voter coercion.

Keywords: Coercion resistance · Counter-strategies · User study · Internet voting

1 Introduction

Internet voting systems are an opportunity to make elections more accessible for disabled voters and for those abroad who have limited access to physical polling places. However, implementing internet voting introduces security risks due to the uncontrolled voting environment. One particular risk is voter coercion, where an adversary could force the voter to cast their vote in a particular manner, undermining the integrity of election results [20]. In order for the coercion to be successful, the adversary needs to have a possibility to confirm that the voter is complying; otherwise, the voter could lie to the coercer while still voting according to their own wishes.

To mitigate the problem of voter coercion, various counter-strategies have been proposed [6,20,25]. The main idea behind these counter-strategies is to provide a way for the voter to deceive the coercer. If successful, the voter is thus able to either vote according to their actual intention or, at least, to cancel the vote cast during coercion, while the coercer has no possibility of detecting it.

However, the effectiveness of these counter-strategies depends on whether the voters can execute them. Previous research, however, has identified a

D. Duenas-Cid et al. (Eds.): E-Vote-ID 2025, LNCS 16028, pp. 158–174, 2026.
https://doi.org/10.1007/978-3-032-05036-6_10

number of assumptions about the voters' behaviour and capabilities that the currently proposed counter-strategies rely on [22]. The empirical validation of these assumptions has been very limited so far. As such, while a few experiments investigate the usability of specific voting systems implementing a variant of proposed counter-strategies [8,27,28], no in-depth investigation has been conducted of how voters would perceive the feasibility of different types of counter-strategies and the risks connected to them in a real-world election. In this work, we address this gap by investigating the following research question:

RQ. How do voters perceive the feasibility of counter-strategies to ensure coercion-resistance in internet voting systems?

We conduct semi-structured interviews with a total of $N = 26$ participants from Denmark and Germany. While neither country uses Internet voting for political elections, Germany has used it in a nationwide election for the first time with the social elections 2023 [19], and the topic is regularly discussed in Denmark [21]. Thus, public interest exists in both nations. As Denmark and Germany are stable, high-trust democracies that have not implemented Internet voting broadly, they are ideal settings for studying how people perceive counter-strategies without direct exposure to Internet voting systems. This study helps identify potential barriers to adoption in countries that could implement online voting in the future but have not yet done so.

In this study, we introduce participants to six different types of counter-strategies. For each type of strategy, we ask our participants about their perceptions of these strategies' effectiveness in protecting against voter coercion, along with their assessments of the strategies' usability. We conduct a thematic analysis using an open coding approach to answer our research questions.

Our findings reveal key factors that determine the voters' perceptions of the feasibility of the counter-strategies, such as *memorability* of the counter-strategy (e.g., requiring the voter to remember secrets), personal characteristics of the voter (e.g., being able to lie convincingly to a coercer), their environment (e.g., having a trusted person), and technical skills. While some of the evaluated counter-strategies were perceived as usable, our participants were also aware of their limitations in being effective in protecting against voter coercion. Therefore, our findings highlight the need to consider the trade-offs between usability and security in voters' perceptions of the counter-strategies.

2 Related Work

A substantial number of counter-strategies have been offered to address the issue of voter coercion [3,4,6,7,9,11,15,17,18,23–25,34,38]. These solutions enable voters to deceive coercers by appearing to comply while ensuring that coerced votes are not counted in the final results. A classification of such counter-strategies divides them into three types – namely, *fake credentials*, *masking*, and *deniable vote updating* [22]. Furthermore, the analysis of these types has identified a number of assumptions about the voters' capabilities required to apply these counter-strategies successfully, such as being able to remember secret credentials without writing them down and to enter these credentials correctly without making a mistake. The study concludes that usability issues might prevent these counter-strategies from being effective; however, without conducting an empirical investigation to validate these conclusions. Further works have focused specifically on usability of coercion-resistant voting in proposing their own solutions [14,29,30], however, these solutions have not been empirically evaluated.

To the best of our knowledge, only a few user studies have evaluated the usability of counter-strategies in coercion-resistant voting, namely, investigating the counter-strategies based on *fake credentials* [8,27,28]. Cristiano et al. [8] report a mean system usability scale (SUS) score of 84.9, a measurement for assessing perceived usability, with all participants managing to complete their tasks within ten minutes. However, the study finds that the participants write down their credentials, reducing the offered protections against coercion resistance. Merino et al. [27] find a mean SUS score of 70.4, with 95% of the participants exposed to fake credentials understanding their use. However, they report that 10% of these participants mistakenly voted using a fake credential, which in a real-world election would result in these votes not being counted.

3 Counter-Strategies

To identify the full scope of available counter-strategies, we extend a systematic literature review conducted in 2020 that identified three types of counter-strategies: fake credentials, deniable vote updating, and masking [22] . We apply the same methodology to identify counter-strategies that have been proposed after the initial literature review has been conducted, i.e., covering papers published from 2020 to 2024. We identify three new counter-strategies: *decoy tokens*, *flexible vote updating*, and *signal-based nullification*. An overview of all six types of counter-strategies is provided below.

Fake Credentials [6,10,20]. During voter registration in a controlled environment, the voter receives a credential, which they use to authenticate when voting. Under coercion, the voter uses a fake credential, which is accepted by the system but results in a vote being excluded from the tally. This allows the voter to cast a true vote when unobserved.

Masking [37,38]. During voter registration in a controlled environment, the voter receives a masking value, which they use to mask their ballot when voting, allowing the system to later extract the vote. Under coercion, the voter provides a fake masking value, making the vote appear to follow the coercer's instructions.

Deniable Vote Updating [17,25]. Under coercion, the voter casts the vote according to the instructions. When unobserved, the voter returns to cast their true vote.

Decoy Tokens [24,34]. During voter registration in a controlled environment, the voter receives a set of tokens, one valid and the rest fake. Under coercion, the voter assigns a fake token according to the instructions, while the valid token is assigned according to their true preference, which is tallied.

Flexible Vote Updating [15]. In one scenario, the voter updates a coerced vote by adding the correct references to previous cast ballots together with the new ballot. In another, if the voter has cast a valid vote before coercion, the voter provides incorrect references together with the ballot, preventing the coerced vote from being tallied.

Signal-Based Nullification [7]. During voter registration in a controlled environment, the voter registers YES/NO public keys and keeps the corresponding private keys. They can share these with helpers and agree on a signal in case of coercion. Under coercion, the vote is cancelled via private key proof, either by the voter or a helper, following the voter's signal. This strategy only enables cancellation of a coerced vote.

4 Methodology

We describe the interview guide, recruitment, ethical considerations, and the data analysis in our study.

4.1 Interview Guide

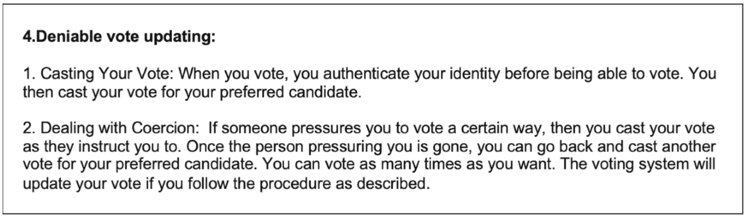
The interview guide was prepared in three languages: English, German, and Danish. The English version was prepared first and iterated in three pilot studies. The translations into the other two languages were done by the paper authors, who were fluent in these languages. To further validate the consistency among the translated versions, the translations were translated back to English using a large language model, and the output was compared with the original interview guide in English to detect any flaws with the translation.

The guide was structured as follows (see Appendix A)[1]. First, the participants were told about the purpose of the study and asked to read and sign a consent form (see Appendix A). The participants were furthermore provided with a one-sentence description of voter coercion, namely, 'Coercion in voting happens when someone pressures or forces you to vote in a way they want you to vote,' to guarantee a common understanding of the research topic we are investigating.

To address our research question, the participants were shown a description for each one of the six counter-strategies (see Sect. 3), prepared in lay terms (see Fig. 1 as an example for such a description).

The descriptions were presented to the participants one at a time in random order, and the participants were asked the following questions for each counter-strategy:

[1] The interview guide includes additional questions beyond the scope of this paper; here, we focus exclusively on questions related to counter-strategies.



4.Deniable vote updating:

1. Casting Your Vote: When you vote, you authenticate your identity before being able to vote. You then cast your vote for your preferred candidate.

2. Dealing with Coercion: If someone pressures you to vote a certain way, then you cast your vote as they instruct you to. Once the person pressuring you is gone, you can go back and cast another vote for your preferred candidate. You can vote as many times as you want. The voting system will update your vote if you follow the procedure as described.

Fig. 1. Description of deniable vote updating

- Do you believe this counter-strategy could work against voter coercion? Why/Why not?
- Do you think this is doable for a regular voter? Why/Why not?

Furthermore, we asked the participants to rank the six counter-strategies and justify their reasoning[2].

Finally, we included questions on socio-demographic information, such as gender, age, and level of education. Additionally, we included a scale-based question to assess participants' IT skills.

4.2 Recruitment and Ethics

For recruitment, we used a combination of purposive and convenience sampling [5]. The study was conducted between July and early September 2024, shortly after the EU election, which took place between June 6 and 9, 2024. Participants were purposively selected based on three criteria: (1) being between 18 and 30 years old, (2) either holding a university-level degree or being in the process of completing one, (3) being eligible to vote in EU elections, and (4) participants without specialised technical knowledge. The first two criteria were chosen since younger people with higher education are more likely to be first adopters of digital technologies; hence, in case Internet voting is introduced, this demographic is likely to be among the first ones using it [12,35]. This focus supports our study's motivation to investigate perceptions in countries like Denmark and Germany, where Internet voting has not yet been broadly implemented, helping to identify potential barriers to adoption in countries that may consider implementing online voting in the future. The third criterion was chosen given the time proximity to the EU election, reasoning that people who either voted or at least were eligible to vote in it would be more likely to pay attention to news and other media reports related to election processes; hence, they would be more likely to be aware of potential election integrity issues that might occur. Furthermore, we intentionally chose participants without any specialised technical knowledge, as Internet voting systems are intended for the general population, the majority of whom have no specialised technical knowledge.

[2] We do not include the rankings in the results section, as our primary interest is to find issues and perceptions concerning the counter-strategies rather than the rankings themselves.

Therefore, the participants' lack of technical expertise reflects the real-world user base of such systems, making their opinions relevant for evaluating the feasibility and usability of counter-strategies in practice. The recruitment for the study was conducted via flyers distributed at universities, social media, and snowball sampling [5]. We stopped recruiting new participants when data saturation was reached [16].

We coordinated the process alongside the ethical guidelines and received approval from the ethical committee of the German institution. At the Danish institution, ethical approval is not mandatory. However, we completed a privacy impact assessment for the project, which was approved by the institution's legal department. Participants from Germany received ten euros as reimbursement, aligning with the minimum wage. Denmark has no minimum wage, so the participants from Denmark received a gift card worth 13.41 euros (100 DKK) for an ice cream shop or a chocolate shop. For the Danish participants, the higher compensation is due to generally higher living costs, and the choice of providing gift cards instead of direct payment is due to institutional regulations. Prior to the interview, participants were asked to sign a consent form outlining the study's purpose, withdrawal options, and data handling procedures. Contact details for the researchers were also provided for any enquiries.

4.3 Data Analysis

All interviews were auto-recorded and transcribed using Amberscript and WhisperAI. Afterwards, the two interviewers reviewed the transcripts to ensure alignment with the original recordings. We used MAXQDA to support a coded thematic analysis of the interviews, employing an open coding approach to address the research question. We coded the interviews at the question level. The two researchers who conducted the interviews also carried out the coding in their respective languages. To develop the initial codebook, the two coders independently coded a randomly selected interview translated into English and discussed their findings. Subsequently, they each coded two interviews in their respective languages to identify additional codes, recognising that a single interview would not capture all potential codes. Based on these interviews, they discussed and revised the codebook. To ensure agreement between the coders, four interviews were translated into English and coded independently. An iterative process of discussion and refinement of the codebook followed, ultimately reaching a Cohen's Kappa of 0.76. Cohen's Kappa measures inter-coder reliability by assessing how much coders agree beyond what would be expected by chance, and a value of 0.76 indicates substantial agreement between the coders [31]. After the acceptable level of agreement was reached, the rest of the interviews were coded by each coder separately in their native language. To identify the themes, we grouped the codes using Post-its to visualise patterns and connections. We refer to Appendix A for the codebook.

5 Results

In this section, we present the results of our study. We recruited 26 participants in total, with 14 participants from Denmark and 12 from Germany. Our participants' ages ranged from 22 to 30, 14 of our participants were men, and 12 were women. We refer to Appendix A for more detailed demographics. In the following, we refer to the participants using the notation P# (e.g., P1 says: "quote").

We identified four key themes: system attributes, voter capabilities, risks, and security and privacy considerations.

5.1 System Attributes

The attributes of the counter-strategy (and, by extension, the voting system as a whole) that determine its feasibility are *convenience*, *closeness to established practices*, *flexibility*, *non-coercive cases*, and *general feasibility in practice*. Table 1 provides an overview of the identified attributes for each counter-strategy.

Table 1. System attributes for counter-strategies, as reported by participants. Green (+): attribute fulfilled; Red (–): not fulfilled; Yellow (+/–): mixed views. Empty cells: no mentions.

	Convenience	Flexibility	Practical limitations and pitfalls	Closeness to established practices	Non-coercive cases
Fake credentials	-/+	-		+	
Decoy tokens	-/+		-	-	-
Flexible vote updating	-/+	+	-	+	+
Deniable vote updating	+			+	+
Masking	-	-/+	-	-	-
Signal-based nullification	-/+	-	-		

Convenience has been mentioned by all of our participants, with a total of 230 mentions. The participants perceived strategies requiring physical visits (e.g., fake credentials) or multiple complex steps to complete them (e.g., masking) as inconvenient. P18 says: *"Well, because there are too many steps involved. It requires too much for people to bother voting, I would say."*

Closeness to established practices is an attribute that covers how close the strategy is to the established voting practices and digital platforms. Eight participants mentioned this attribute 17 times. P16 says: *"Because it seems like something you would normally do in connection with public authorities, that you log in with your ID. These are procedures that you have gone through before for something similar."*

Flexibility covers whether a counter-strategy is flexible to different scenarios of coercion. Seven participants mentioned this 14 times. The participants perceived flexible vote updating as flexible. P26 says: *"It gives you the flexibility to vote both before and after someone has blackmailed you into voting."* In contrast, fake credentials and signal-based nullification are perceived as less flexible.

The feasibility of a counter-strategy when the voter casts their ballot without being under any coercion is captured with **non-coercive cases**. Nine participants mentioned this 13 times and perceived some strategies negatively and others positively in non-coercive cases. P16 says: *"If you are not subjected to pressure, then you only need to vote once."*

Practical limitations and pitfalls is an attribute that covers how participants perceived the real-world viability of the counter-strategies. It encompasses factors such as the presence of significant gaps or pitfalls, as well as strategies that may appear effective in theory but fail to deliver in practice. Ten participants mentioned this 17 times, and they especially perceived signal-based nullification as incomplete, with 12 mentions. P24 says: *"So, it sounds like it was developed somewhat in an academic setting. It sounds great, but it doesn't work in practice."*

5.2 Voter's Capabilities

The feasibility of the counter-strategies is perceived to depend on voters' own capabilities, namely, their *memorisation skills*, *understanding skills*, and their *assertiveness* and *technical skills.*

Table 2. Voter capabilities required for counter-strategies, as reported by participants. Green (-): skill not required; Red (+): skill required; Yellow (+/-): mixed views. Empty cells: no mentions.

	Memory	Understanding	Assertiveness	Technical
Fake credentials	+	-/+	+	-
Decoy tokens	+	-/+	+	-/+
Flexible vote updating	+	-/+	+	-
Deniable vote updating	-	-	-	-
Masking	+	+	+	
Signal-based nullification	+	+		

The success of almost every counter-strategy relies on the voter's ability to remember specific elements such as credentials, tokens, or other components (Table 2). **Memory skills** were mentioned a total of 119 times by 25 participants. Moreover, they considered alphanumerical passwords harder to recall than visual symbols (e.g., coloured shapes). P13 says: *"Remembering symbols is easier for people; I think it is better than the password. It is easier for people to remember whether it was a triangle, an orange triangle, or a blue circle."*

Some strategies also require high skills in understanding complex procedures (e.g., masking). 14 participants mentioned **understanding skills** 35 times, 14 of which are about masking. P19 says: *"Well, I have a hard time fully understanding the addition of numbers; maybe others will too."*

The success of most counter-strategies relies on the voter's **assertiveness**, especially the ability of the voter to lie convincingly enough to deceive the coercer, which was mentioned by 20 participants 64 times. P14 says: *"But I also think it requires a bit of the person who votes. They also have to be good at lying."*

Finally, **technical skills** of the voters were mentioned as an important factor in counter-strategy feasibility (mentioned by 12 participants 23 times). Some counter-strategies (e.g., deniable vote updating) were seen as requiring fewer technical skills, while others raised mixed perceptions (e.g., decoy tokens). P23 says: *"Most people can manage drag-and-drop."*

5.3 Risks

The discussion of presented counter-strategies raised the risks of various mistakes disrupting one's vote, understood here as direct actions with clear negative consequences, namely, *typo mistakes*, *casting a wrong vote*, and *cancelling the vote*, as well as the risk of *last-minute coercion.*

The risk of a **typo mistake** is associated with fake credentials, which would lead to casting an invalid vote (mentioned by nine participants 13 times). P20 says: *"You think you voted, but you entered the information incorrectly, so you did not vote anyway."*

The risk of mistakenly **casting a wrong vote** (mentioned by 14 participants 34 times) is associated with decoy tokens (15 mentions), masking (15 mentions), and flexible vote updating (four mentions). P23 says: *"But it could be risky to have the possibility of voting incorrectly - even just by mistake."*

The risk of **cancelling a vote** covers several risks associated with the signal-based nullification strategy, which 15 participants mentioned 29 times. This includes the potential to cancel another person's vote by mistake because voters might fail to create a unique code or because a signal is misinterpreted. P14 says: *"There will definitely be situations where you consider something to be a signal without it being a signal."* Moreover, this code encompasses the participant dissatisfaction with the inability to recast a vote once revoked, leaving their choice unrepresented.

The risk of **last-minute coercion** (mentioned by 16 participants 26 times) is associated with deniable (19 mentions) and flexible (seven mentions) vote updating. P10 says: *"If the coercer stays with you until the end of the election and you can't change your vote, it is problematic."*

5.4 Security and Privacy Considerations

The security and privacy aspects of the discussed counter-strategies, reflecting perceptions of potential vulnerabilities or safeguards rather than direct consequences, include *coercer's capabilities and knowledge*, *security of knowledge-based secrets*, *writing down knowledge-based secrets*, *system feedback*, *depending on others*, and *voting several times.*

The **coercer's capabilities and knowledge** are security considerations associated with all counter-strategies, and 25 participants mentioned it a total of 122 times. The participants considered it to be public knowledge how the counter-strategies work, which they believed the coercer will use to their advantage. This could be by pressuring the voter to reveal their knowledge-based secret or waiting until the last minute to coerce. Additionally, they believed that the coercer is likely to suspect the voter of using a counter-strategy. P16 says: *"I think if this is known to everyone, it might not work as well because they would know that you are getting that code, and they would start trying to pressure you to give this code to them."*

The **security of knowledge-based secret** is an aspect associated with fake credentials, decoy tokens, and masking, and 18 participants mentioned this 37 times. The participants considered a strategy to be effective because the voter is the only one knowing their secret. P23 says: *"Well, again, here you have something that only you know. I think that has proven to be a reasonably secure solution."*

Writing down knowledge-based secrets is associated with several strategies, and the participants mentioned it 35 times (19 mentions for fake credentials, five for masking, four for decoy tokens, and two for flexible vote updating and signal-based nullification). The participants perceived a strategy to be less secure if the voter is writing down their knowledge-based secret. P8 says: *"You would write it down somewhere. When you are not prepared and someone comes in while you are voting and the password is there, the coercer could just vote for you directly."*

The importance of providing only limited **system feedback** was mentioned by 16 participants 29 times, in association with fake credentials, masking, and deniable and flexible vote updating. In particular, lack of feedback was deemed essential for successfully deceiving the attacker, as explained by P1: *"The attacker has to trust you because the system does not give any feedback."*

The security issues of being allowed to **vote several times** are associated with deniable and flexible vote updating, mentioned by 12 participants 105 times. The participants expressed concerns about overloading the server and the possibility of coercion happening over a longer time period. P24 says: *"If we say all five million Danes think it is super fun to vote all the time, it could overload the system, and then it collapses."* However, they noted positively that voting multiple times allows voters to cast their intended vote in a more secure situation.

Depending on others is considered to be a privacy and security concern related to signal-based nullification (mentioned by 23 participants 57 times), especially in the context of family coercion. The participants expressed concerns that not everyone trusts others, and the coercers could be family members. P26 says: *"I believe coercion often comes from people you know rather than strangers. And I think that would almost give people a free pass to have your vote cancelled, more than it would actually protect you from coercion."*

6 Discussion

Usability vs. Security. Our participants' opinions on the counter-strategies revealed a conflict between usability and security. As such, while they mention memorability as a potential issue for the success of almost every counter-strategy, they nonetheless emphasise the importance of keeping a **knowledge-based secret** (e.g., masking value) only known to the voter themselves for security reasons. This trade-off is a known issue in usable security and is exacerbated for coercion-resistant voting due to potential issues with storing the secret somewhere where the coercer can demand access. This issue has furthermore been noted by our participants: as such, while our participants suggested writing down or taking a picture of their knowledge-based secret to remember it, they also consider this a security issue if the attacker accesses the stored secret by finding or obtaining it through coercion. Previous research on the usability of **fake credentials** avoided this problem by letting the participants write down their credentials [8]. Hence, future work needs to focus on designing and evaluating other techniques either for the voters to remember their secrets without writing them down or for developers of the system to provide storage options not accessible to the attacker even in case of coercion. Such studies can furthermore be beneficial for all counter-strategies relying on memorability, which, according to our participants, applies to all except deniable vote updating.

A further example of the conflict between usability and security relates to **deniable vote updating**. Most of our participants find this strategy to be the easiest to apply, but note the risk of last-minute coercion. Since this risk would not be an issue for the other counter-strategies, the effectiveness of the deniable vote updating strategy in protecting against coercion can be seen as weaker. For real-world elections, decisions, therefore, need to be made on a case-by-case basis to determine whether the last-minute coercion risk outweighs the benefits of an overall simplicity of the counter-strategy. An open question that furthermore remains is how to communicate the relevant risks, in particular, the capacities of a potential coercer, to both voters and decision-makers, particularly in relation to the scalability of an attack. The risk of last-minute coercion is furthermore mentioned as an issue for **flexible vote updating**, despite this counter-strategy actually having mechanisms available to protect against this attack. Such a misconception highlights an issue with the strategy's understandability, and it remains an open question of how to explain the strategy without misrepresenting the risks. Previous research has shown that understandability directly influences how transparent an internet voting system is perceived to be [1]. Transparency, which is widely recognised by both researchers and policymakers as a key factor in building trust and fostering acceptance of internet voting systems [2,13,26,36]. Therefore, the understandability is not only important for their effectiveness but also for the broader acceptance of the voting system as a whole.

In addition to usability issues, our participants pointed to the **personal circumstances of the voter** regarding their environment and social circle. Participants are concerned about having to rely on others in **signal-based nullification** to be effective against coercion – either because the voters might be socially isolated and lack close trusted contacts or because the helpers themselves could potentially be the coercers. Consequently, they perceive signal-based nullification as ineffective against voter coercion in such situations. Deciding to use a particular counter-strategy should, therefore, take into account such personal circumstances, and studies need to be conducted to get a thorough understanding of the population that is of particularly high risk of coercion.

Participants further emphasise that voters need certain **resources and skills**, in particular the ability to lie to the coercer, which is required in most cases according to our participants. As such, when discussing using a **knowledge-based secret** in front of the coercer (e.g., by authenticating with fake credentials), the participants highlight that individuals who are not comfortable with deception might struggle in convincing the coercer that they are indeed using the right secret. This raises an important point about the psychological and social challenges of implementing such counter-strategies, suggesting that personal traits could influence the effectiveness of knowledge-based secrets in preventing coercion. Still, it remains an open question of how the voter's assertiveness impacts the effectiveness of counter-strategies in practice.

Role of Public Information. Applicable to all counter-strategies, the participants consider publicly available information about the procedures voters have to perform to apply these counter-strategies to be a problem for their effectiveness. As such, our participants note that for counter-strategies implementing a knowledge-based secret, the coercer might try to be present during the disclosure of the knowledge-based secret or use extreme threats to make the voter reveal it. For counter-strategies vulnerable to last-minute coercion, the coercer might attack right before the deadline, making it impossible to update the vote. In general, the coercer might suspect that the voter is trying to deceive them if they know that an Internet voting system has implemented a counter-strategy, making it harder for the voter to convincingly deceive a coercer. On the other hand, information about available counter-strategies might discourage the coercer from attempting coercion. Namely, as the coercer will have no way of knowing for sure whether the voter complied with the coercer's instructions, they might decide that the risks they face attempting coercion are not worth the uncertainty of the result. Furthermore, making information about the voting system publicly available aligns with recommendations from experts [2,13,26,36] and is perceived as improving election transparency and trust by the voters [1]. The specific trade-offs introduced by public information about counter-strategies therefore remain an open question, and an open challenge is how to design Internet voting systems that maintain transparency without making counter-strategies ineffective.

Design implications. Based on the identified challenges, we propose the following design implications, which we, as authors, have derived from our findings to help mitigate the concerns raised by our participants about the counter-strategies:

Visual Secrets (Fake Credentials, Decoy Tokens, Flexible Vote Updating, Signal-Based Nullification). To support memorability, voting systems should consider using visual secrets, such as images or icons, instead of complex passwords or long codes. Research shows that pictures are generally easier for users to recall than alphanumeric information, which can improve both usability and the effectiveness of the counter-strategies [32].

Multimodal Explanations (All Counter-Strategies). To enhance understandability, voting systems should support various media formats for explaining the counter-strategies, including text, audio, and video (e.g., demo videos). Providing explanations in multiple formats can help accommodate different learning styles and improve comprehension among non-expert voters [33].

Fallback to Physical Voting (All Counter-Strategies). To accommodate voters who may struggle with assertiveness, such as lying convincingly to a coercer, systems should allow users to override their online vote by casting a final vote at a physical polling station. This provides a secure, controlled environment for voters who feel unsafe or uncertain using coercion-resistant strategies online.

Private Browsing or Incognito Mode by Default (Fake Credentials, Deniable and Flexible Vote Updating). To prevent system feedback, such as browser history or cached data, from being used by a coercer to verify whether the voter has revisited the voting platform (and potentially changed their vote), the system should either prompt users to re-access the platform via private browsing mode after an initial vote, or automatically enforce this mode. This helps obscure traces of revisiting the system, thereby supporting plausible deniability and increasing coercion-resistance.

Restricting Copying of Secrets (Fake Credentials, Decoy Tokens, Masking, Flexible Vote Updating). To reduce the risk of voters easily copying and storing their knowledge-based secrets, the voting system should prevent simple extraction. For example, secrets (e.g., credentials) can be rendered as non-selectable images rather than text, which can be easily marked and copied using shortcuts. This subtle design choice can help by making it difficult for the voters to write down and store their secret, thus making it harder for the coercer to find or demand access to them.

Waiting Period to Prevent System Overload (Deniable and Flexible Vote Updating). To avoid overloading systems or potential abuse, the system should implement a waiting period after a certain number of rapid votes (e.g., five votes in quick succession).

Non-disclosing Prompts (All Counter-Strategies). To avoid user confusion and reduce the likelihood of errors (e.g., typos), the interface should include non-disclosing prompts such as: *"For your privacy, the system will not indicate whether your login was successful or not. Please double-check your entry before submitting."*

Limitations. Our findings may be subjected to bias due to the participants' lack of experience with Internet voting. To address this bias, future studies should explore how voters from countries such as Estonia, with an Internet voting system utilising deniable vote updating, perceive the counter-strategies. Another limitation is that all the participants are between 22 and 30 years old with a university-level degree or are in the process of completing one. This limits the generalisability of our findings, but since younger people with high education are more likely to be first adopters of digital technologies, hence, in case Internet voting is introduced, this demographic is likely to be among the first ones using it [12,35]. Still, future work should investigate perceptions among older voters and people with disabilities, as Internet voting often is proposed to enhance accessibility and participation for these groups. While the study provides valuable insights into voters' perceptions of the counter-strategies, its ecological validity is limited because the participants did not use them in an actual voting system. This may have affected their assessments of the strategies' feasibility and usability, so their responses might not fully reflect real-world reactions. Nonetheless, explanations of counter-strategies would likely be provided in any implemented internet voting system, suggesting the insights gathered here remain valuable.

7 Conclusion

We conducted 26 semi-structured interviews to explore how voters perceive the counter-strategies designed to resist coercion in Internet voting. From our findings, we conclude that voters prefer a counter-strategy that is easy to use, namely, the **deniable vote updating**, which further has the advantage of leaving the voting process unchanged in the absence of coercion. However, the counter-strategy also introduces the risk of last-minute coercion. Thus, for elections with a high risk for voter coercion, a more complex counter-strategy should be used. Furthermore, we conclude that regardless of how **signal-based nullification** is implemented, the voters are unlikely to accept the fundamental concept of having helpers cancel their coerced vote. Voters want to be able to cast an uncoerced vote rather than only cancelling a coerced vote, and they are generally reluctant to involve others in the inherently private act of voting. Future work should focus on improving and evaluating the usability of counter-strategies.

Acknowledgments. The work reported in this paper was supported by Independent Research Fund Denmark, grant number 10.46540/2101-00006B.

A Appendix

Due to the extensive length the interview guide, consent form, codebook, and demographics are provided in a single external link, accessible here: https://osf.io/3cd2r/?view_only=cfa43eae0e00457fb144c56e7ae6ca5c.

References

1. Agbesi, S., Budurushi, J., Dalela, A., Nissen, C., Kulyk, O.: How to increase transparency and trust in internet voting systems: an experimental study. In: Proceedings of the 13th Nordic Conference on Human-Computer Interaction. NordiCHI '24, Association for Computing Machinery, New York, NY, USA (2024)
2. Agbesi, S., Dalela, A., Budurushi, J., Kulyk, O.: "What will make me trust or not trust will depend upon how secure the technology is": factors influencing trust perceptions of the use of election technologies. E-Vote-ID **2022**, 1 (2022)
3. Aranha, D.F., Battagliola, M., Roy, L.: Faster coercion-resistant e-voting by encrypted sorting. Cryptology ePrint Archive, Paper 2023/837 (2023)
4. Araújo, R., Ben Rajeb, N., Robbana, R., Traoré, J., Youssfi, S.: Towards practical and secure coercion-resistant electronic elections. In: Heng, S.H., Wright, R.N., Goi, B.M. (eds.) Cryptology and Network Security, pp. 278–297. Springer, Berlin Heidelberg, Berlin, Heidelberg (2010)
5. Bjørner, T.: Why 'Qualitative Methods for Consumer Research'?, pp. 11–15. Hans Reitzels Forlag, Denmark (2015)
6. Chaieb, M., Yousfi, S.: LOKI vote: a blockchain-based coercion resistant E-voting protocol. In: Themistocleous, M., Papadaki, M., Kamal, M.M. (eds.) EMCIS 2020. LNBIP, vol. 402, pp. 151–168. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-63396-7_11
7. Chaum, D., et al.: VoteXX: a solution to improper influence in voter-verifiable elections. Cryptology ePrint Archive, Paper 2022/1212 (2022)
8. Christiano, L., Longo, R., Spadafora, C.: Click and cast: assessing the usability of vote app. In: Electronic Voting: 9th International Joint Conference, E-Vote-ID 2024, Tarragona, Spain, October 2–4, 2024, Proceedings (2024)
9. Clark, J., Hengartner, U.: Selections: internet voting with over-the-shoulder coercion-resistance. In: Danezis, G. (ed.) Financial Cryptography and Data Security, pp. 47–61. Springer, Berlin Heidelberg, Berlin, Heidelberg (2012)
10. Clarkson, M.R., Chong, S., Myers, A.C.: Civitas: toward a secure voting system. In: 2008 IEEE Symposium on Security and Privacy (SP 2008), pp. 354–368 (2008)
11. Cortier, V., Gaudry, P., Yang, Q.: Is the JCJ voting system really coercion-resistant? Cryptology ePrint Archive, Paper 2022/430 (2022)
12. Ehin, P., Solvak, M., Willemson, J., Vinkel, P.: Internet voting in Estonia 2005–2019: evidence from eleven elections. Gov. Inf. Q. **39**(4), 101718 (2022)
13. of Europe, C.: Recommendation cm/rec(2017)5[1] of the committee of ministers to member states on standards for e-voting
14. Feier, C., Neumann, S., Volkamer, M.: Coercion-resistant internet voting in practice. In: Informatik 2014, pp. 1401–1414. Gesellschaft für Informatik e.V., Bonn (2014)
15. Giustolisi, R., Garjan, M.S., Schuermann, C.: Thwarting last-minute voter coercion. Cryptology ePrint Archive, Paper 2023/1876 (2023)
16. Guest, G., Bunce, A., Johnson, L.: How many interviews are enough? An experiment with data saturation and variability. Field Meth. **18**, 59–82 (02 2006)
17. Haines, T., Mueller, J.: How not to VoteAgain: pitfalls of scalable coercion-resistant e-voting. Cryptology ePrint Archive, Paper 2020/1406 (2020)
18. Haines, T., Müller, J., Querejeta-Azurmendi, I.n.: Scalable coercion-resistant e-voting under weaker trust assumptions. In: Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing, pp. 1576–1584. SAC '23, Association for Computing Machinery, New York, NY, USA (2023)

19. Hilt, T., Kulyk, O., Volkamer, M.: German social elections 2023: An overview and first analysis. In: E-Vote-ID 2023. Lecture Notes in Informatics - Proceedings, Gesellschaft für Informatik (GI) (2023), 46.23.01; LK 01
20. Juels, A., Catalano, D., Jakobsson, M.: Coercion-Resistant Electronic Elections, pp. 37–63. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)
21. Kristensen, P.K., Pedersen, L.E.M.: Under corona har vi klaret alt online – derfor kan du ikke stemme digitalt (2021). https://www.dr.dk/nyheder/politik/kommunalvalg/under-corona-har-vi-klaret-alt-online-derfor-kan-du-ikke-stemme. Accessed 06 May 2025
22. Kulyk, O., Neumann, S.: Human factors in coercion resistant internet voting – a review of existing solutions and open challenges (2020)
23. Locher, P., Haenni, R., Koenig, R.E.: Coercion-resistant internet voting with everlasting privacy. In: Clark, J., Meiklejohn, S., Ryan, P.Y., Wallach, D., Brenner, M., Rohloff, K. (eds.) Financial Cryptography and Data Security, pp. 161–175. Springer, Berlin Heidelberg, Berlin, Heidelberg (2016)
24. Longo, R., Spadafora, C.: Amun: Securing e-voting against over-the-shoulder coercion. Cryptology ePrint Archive, Paper 2021/851 (2021)
25. Lueks, W., Querejeta-Azurmendi, I., Troncoso, C.: VoteAgain: a scalable coercion-resistant voting system. In: 29th USENIX Security Symposium (USENIX Security 20), pp. 1553–1570. USENIX Association (2020)
26. Marky, K., Gerber, P., Günther, S., Khamis, M., Fries, M., Mühlhäuser, M.: Investigating State-of-the-Art practices for fostering subjective trust in online voting through interviews. In: 31st USENIX Security Symposium (USENIX Security 22), pp. 4059–4076. USENIX Association, Boston, MA (2022)
27. Merino, L.H., et al.: E-vote your conscience: perceptions of coercion and vote buying, and the usability of fake credentials in online voting. In: 2024 IEEE Symposium on Security and Privacy (SP), pp. 3478–3496 (2024)
28. Neto, A.S., Leite, M., Araújo, R., Mota, M.P., Neto, N.C.S., Traoré, J.: Usability considerations for coercion-resistant election systems. In: Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems. IHC '18, Association for Computing Machinery, New York, NY, USA (2018). 10.1145/3274192.3274232, https://doi-org.ep.ituproxy.kb.dk/10.1145/3274192.3274232
29. Neumann, S., Feier, C., Volkamer, M., Koenig, R.: Towards a practical JCJ / civitas implementation. Cryptology ePrint Archive, Paper 2013/464 (2013)
30. Neumann, S., Volkamer, M.: Civitas and the real world: Problems and solutions from a practical point of view. In: 2012 Seventh International Conference on Availability, Reliability and Security, pp. 180–185 (2012)
31. O'Connor, C., Joffe, H.: Intercoder reliability in qualitative research: debates and practical guidelines. Int. J. Qual. Meth. **19**, 1609406919899220 (2020)
32. Paivio, A., Rogers, T.B., Smythe, P.C.: Why are pictures easier to recall than words? Psych. Sci. **11**(4), 137–138 (1968). https://doi.org/10.3758/BF03331011
33. Song, H., Healey, J., Siu, A.F., Wigington, C., Stasko, J.: Experts prefer text but videos help novices: an analysis of the utility of multi-media content. In: Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems, pp. 1–9. CHI '23, ACM (2023). https://doi.org/10.1145/3544549.3585900
34. Spadafora, C., Longo, R., Sala, M.: Coercion-resistant blockchain-based e-voting protocol. Cryptology ePrint Archive, Paper 2020/674 (2020)
35. Vassil, K., Solvak, M., Vinkel, P., Trechsel, A.H., Alvarez, R.M.: The diffusion of internet voting. usage patterns of internet voting in Estonia between 2005 and 2015. Govern. Info. Quart. **33**(3), 453–459 (2016)

36. Volkamer, M., Spycher, O., Dubuis, E.: Measures to establish trust in internet voting. In: Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance, pp. 1–10 (2011)
37. Wen, R., Buckland, R.: Masked ballot voting for receipt-free online elections. In: Ryan, P.Y.A., Schoenmakers, B. (eds.) E-Voting and Identity, pp. 18–36. Springer, Berlin Heidelberg, Berlin, Heidelberg (2009)
38. Zhaoju, Z., Hanbo, L., Hong, D.: Verifiable receipt-free electronic voting system based on mask ballot. In: 2021 IEEE 9th International Conference on Smart City and Informatization (iSCI), pp. 47–52 (2021)