E-Vote Your Conscience: Perceptions of Coercion and Vote Buying, and the Usability of Fake Credentials in Online Voting

EPFL Massachusetts Institute of Technology

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse
Federal Office for Defence Procurement

Online Voting

Increased Convenience

Increased Coercion Risk

Voters **cast** votes on an **unmanaged** device in an **unsupervised** environment

Coercion Examples

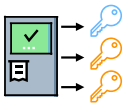
Forceful

Vote-Buying Selfie

"Dark" DAOs[1]

Unlike in-person voting, **online voting** is vulnerable to more **easily scalable** coercion threats

Coercion-Resistance[2,3]

Register	Real Vote	Fake Vote(s)
	Private Moment  Intended Vote	Under Coercion  Coerced Vote

Fake credentials cast votes that **do not** count **while** being **indistinguishable** from **real credentials** which cast votes that **do** count

Usability & Verifiability Concerns

Comprehension?

Real or Fake Credential?

Genuine?

Usability: Can voters **comprehend** and **use** fake credentials?
Verifiability: Is the **issued** "real" credential **genuinely** real?

User Study Results

Recruitment

150 Participants
Each Group: 30

Median Age: 36.5
Average Age: 44
Study Location: Boston, Massachusetts

Reported Coercion

26% report experiencing or knowing of someone who has experienced at least one form of voter coercion.

Success Rate

Create Credentials	Activate a Credential	Vote with Real Credential
		
95%	92%	90%

87%

83%

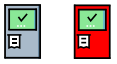
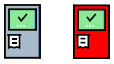
Fake Credentials

96% understood its use

76% create at least one **fake** credential

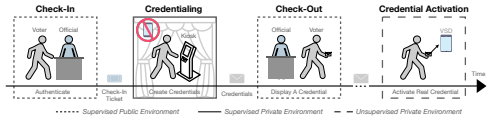
53% would create in **reality**

Kiosk Reporting Rate

Without Security Priming		With Security Priming	
			
0%	10%	0%	47%

User Study Design

TRIP: Trust-Limited In-Person Voter Registration[4]



5 Study Groups

	Honest Kiosk	Malicious Kiosk	Honest Kiosk + Security Priming	Malicious Kiosk + Security Priming
Real Cred. Only	Group C			
Fake Credentials	Group F	Group M	Group SF	Group SM

Intended Deployment

Malicious Kiosk aims to steal the voter's real credential, leaving the voter only with fake credentials.

Security Priming demonstrates to voters how in the unlikely event a kiosk may be malicious.

Conclusion

The Coercion Problem	Introduction to Fake Credentials	Usability of Fake Credentials
	**96%** Understood the use of fake credentials	STAR-Vote: 93%
26% faced coercion or know of someone who did	**53%** Willing to create fake credentials in reality	Online Voting { TRIP 83%; Helios: 60%; Prêt à Voter: 60%

References

1. Austgen, James, et al. *DAO Decentralization: Voting-Bloc Entropy, Bribery, and Dark DAOs*. arXiv:2311.03530, 2023.
2. Kulyk, Oksana, and Stephan Neumann. "Human Factors in Coercion Resistant Internet Voting–A Review of Existing Solutions and Open Challenges." International Joint Conference on Electronic Voting, 2020.
3. Juels, Ari, et al. "Coercion-Resistant Electronic Elections." *Towards Trustworthy Elections: New Directions in Electronic Voting*, 2010.
4. Merino, Louis-Henri, et al. *TRIP: Trust-Limited Coercion-Resistant In-Person Voter Registration*. arXiv:2202.06692, 17 Mar. 2024. *arXiv.org*, http://arxiv.org/abs/2202.06692.