

E-Vote Your Conscience



Institute of Technology Perceptions of Coercion and Vote Buying, and the Usability of Fake Credentials in Online Voting

Louis-Henri Merino, Alaleh Azhir, Haoqian Zhang, Simone Colombo, Bernhard Tellenbach, Vero Estrada-Galiñanes, Bryan Ford

Online Voting



Increased Convenience

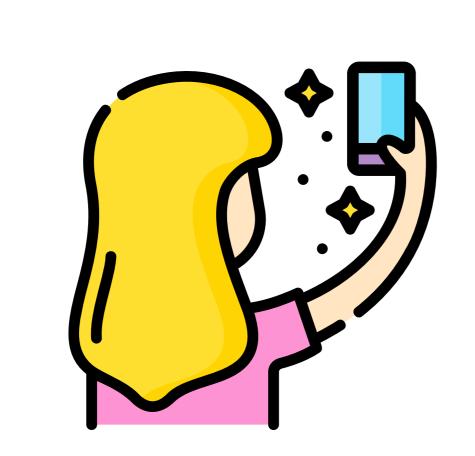


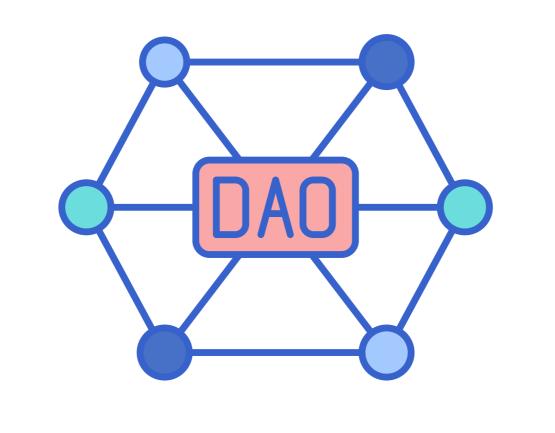
Increased Coercion Risk

Voters cast votes on an unmanaged device in an unsupervised environment

Coercion Examples







Forceful

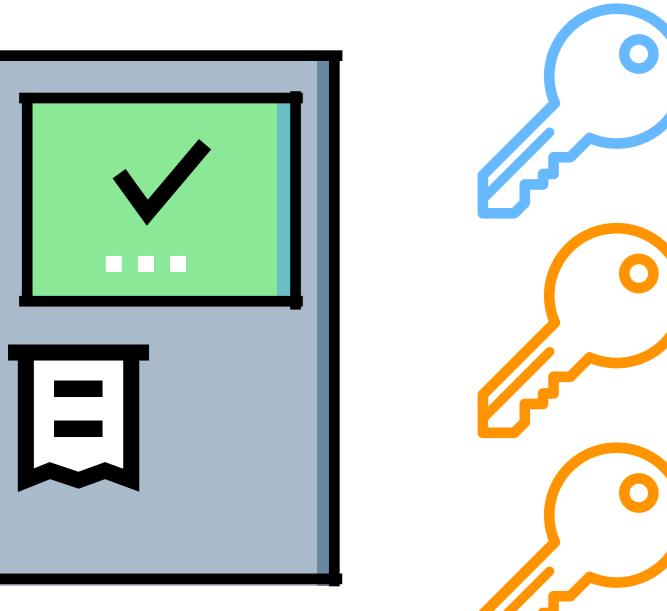
Vote-Buying "Dark" DAOs Selfie

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

Coercion-Resistance^{2,3}

Registration

Voting





Private Moment





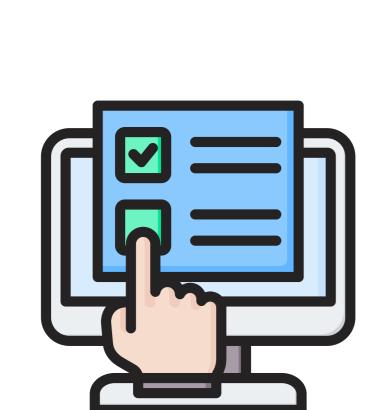
Under Coercion

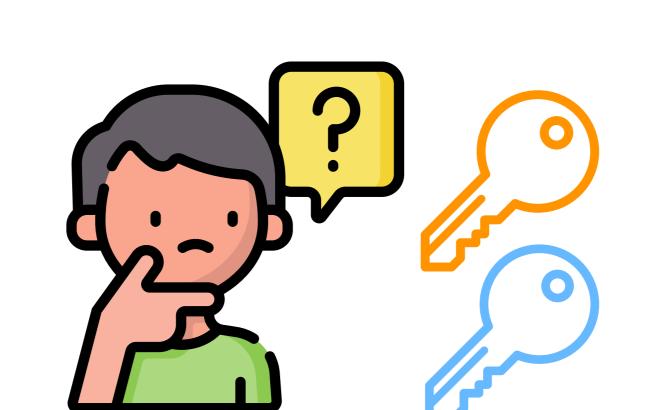
Coerced Vote

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

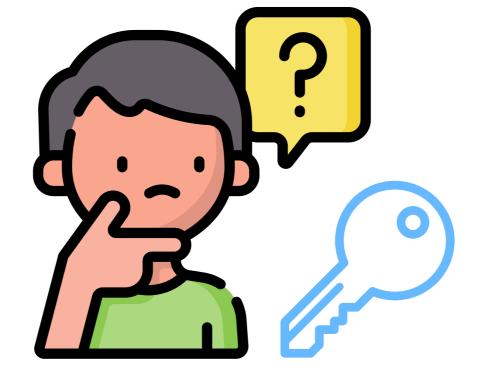
Concerns











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

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

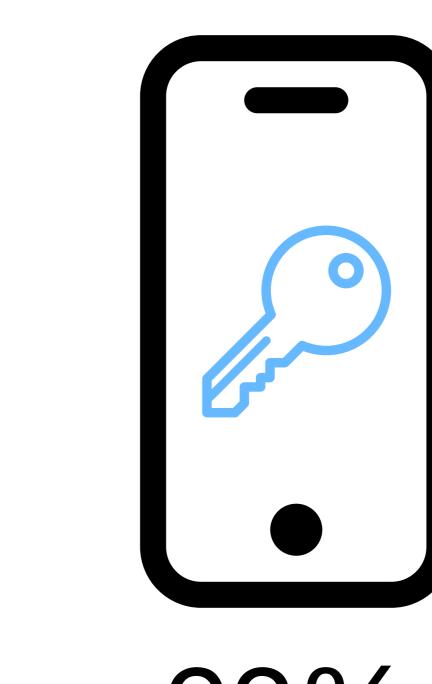
Reported Coercion



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

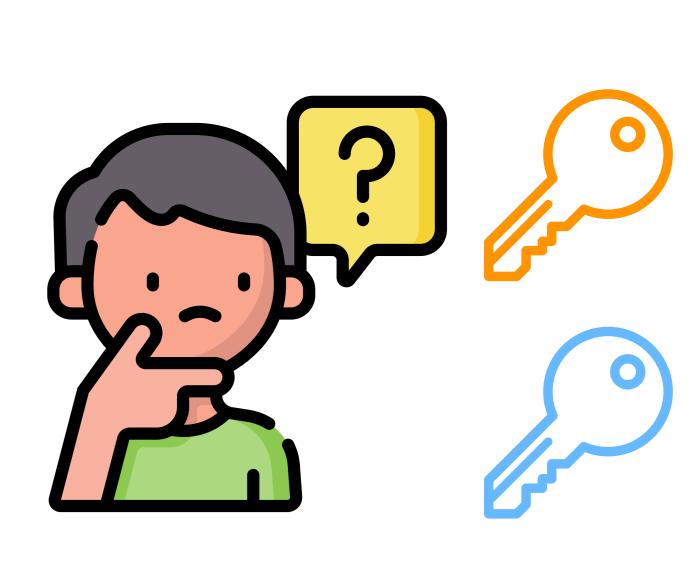
Success Rate

Create Credentials Activate a Credential



92%

Vote with Real Credential



90%

Fake Credentials



95%







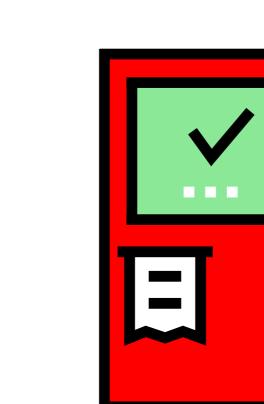
96% understood its use

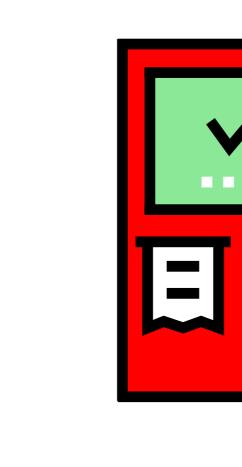
76% create at least one fake credential

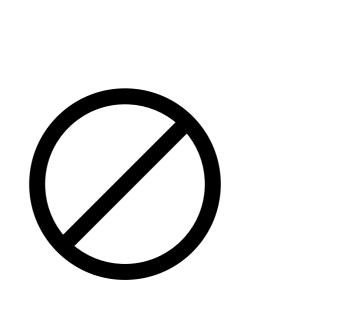
53% would create in reality

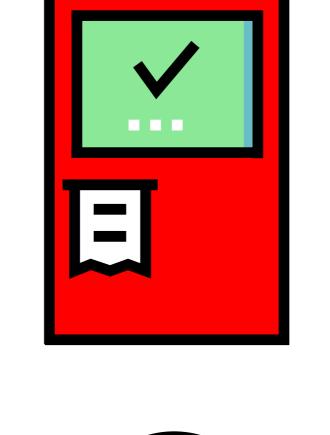
Kiosk Reporting Rate

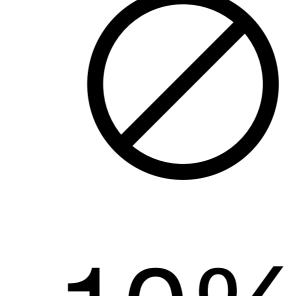
Without Security Priming

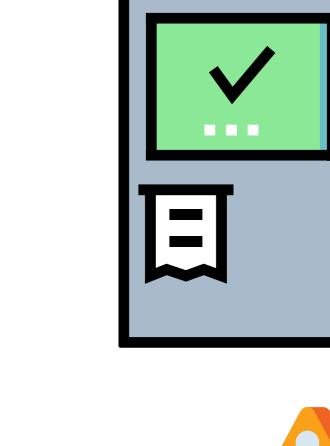


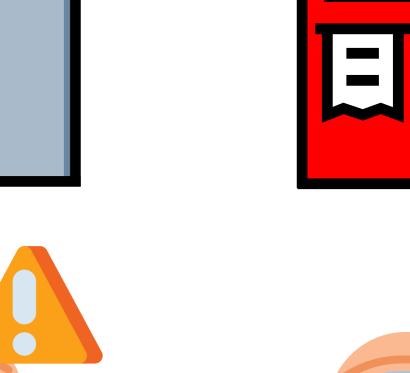










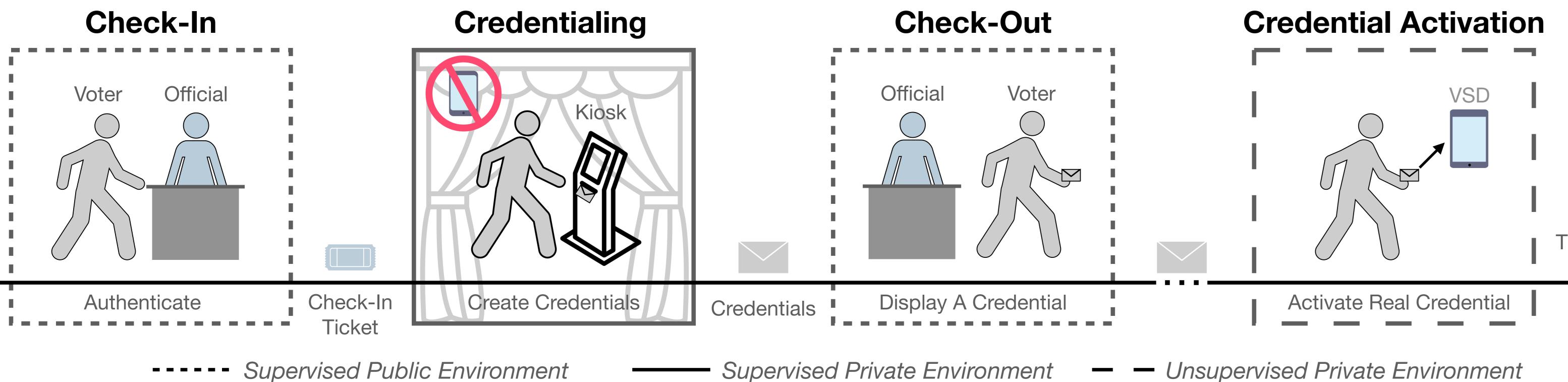


With Security Priming



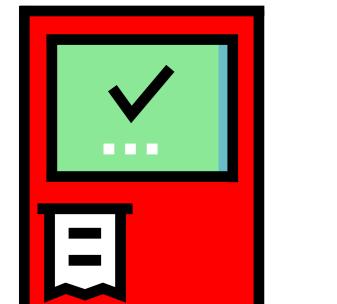
User Study Design

Trust-Limited In-Person Voter Registration³



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 <u>S</u> M



Intended Deployment

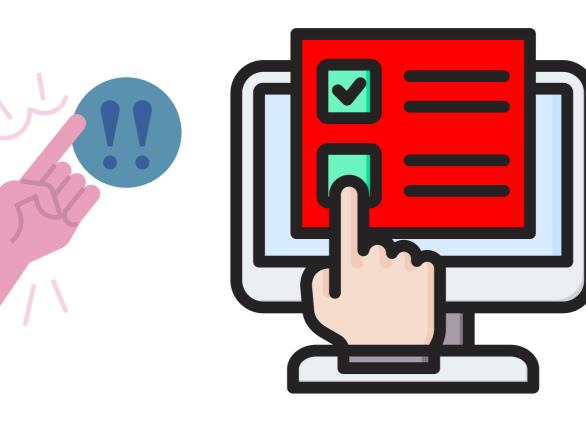
Malicious Kiosk aims to steal the voter's real credential, leaving the voter only with fake credentials.



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

Conclusion

The Coercion Problem



26%

faced coercion or know of someone who did

Fake Credentials

96%

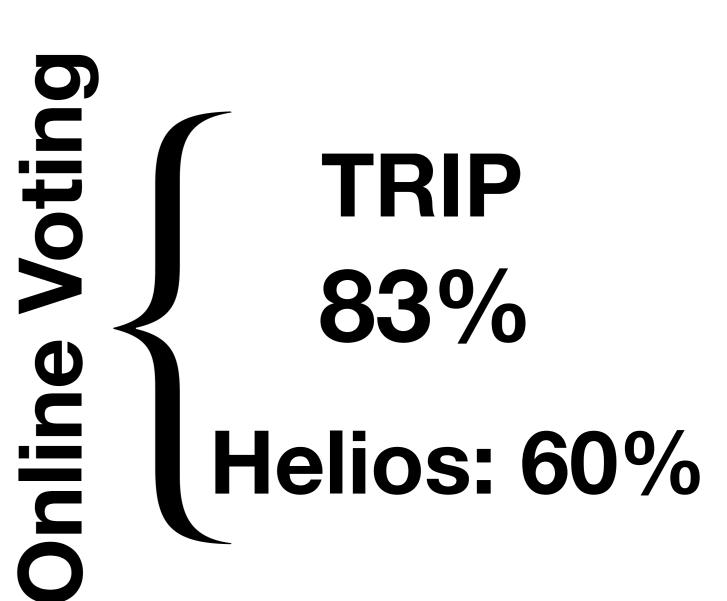
Understood the use of fake credentials

53%

Willing to create fake credentials in reality

Usability of Fake Credentials

STAR-Vote: 93%



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. Juels, Ari, et al. "Coercion-Resistant Electronic Elections." Towards Trustworthy Elections: New Directions in Electronic
- Voting, 2010. 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.