VerifiedVoting

Internet Voting is Not Secure for Any Voter

Multiple credible cybersecurity experts have concluded that internet voting is unsafe.

The National Academies of Science, Engineering and Medicine released a report in 2018 stating that the technology to return marked ballots securely and anonymously over the internet does not exist:

> *At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots. Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.*[1]

The National Institute of Standards and Technology report had similar findings. [2]

Internet voting is one of the most vulnerable forms of voting.

Internet voting is vulnerable to widespread attacks affecting multiple voters. The following types of attacks are credible threats and elevate the risk of voting via the internet:

- Voter authentication attacks (i.e. forged voter credentials)
- Malware on voters' devices (e.g., viruses, Trojan horses, malicious code embedded in software updates) that can modify votes undetectably
- Denial of service attacks (slowing a key part of the system to a crawl or crashing it by overwhelming it with traffic or taking advantage of a bug)
- Server penetration attacks (remote break-in and control of the election server)
- Spoofing attacks (directing voters to a fake voting website instead of the real one)
- Widespread privacy violations by any of several methods, taking advantage of the fact that online voters must transmit their names with their votes, which also violates a voter's constitutional right to a private ballot
- Voter coercion through automated vote buying and selling schemes (with cryptocurrency payments, e.g. Bitcoin, in exchange for votes)

In addition to concerns about the security of an internet-only voting system's technology, the security of the actual device that voters cast their votes on is unknown. The voter's device may already be corrupted with malware or viruses that could interfere with ballot transmission or even spread that malware to the computer at the elections office on the receiving end of the online ballot. Unlike other internet transactions, voting must simultaneously maintain ballot secrecy while still providing a verifiable record of the voter's intent. Internet voting lacks a voter verified record of the voter's choices and thus those votes are not auditable.

Blockchain does not solve the security issues inherent to internet voting.

The National Academies of Sciences report states that "blockchain technology does little to solve the fundamental security issues of elections, and indeed, blockchains introduce additional security vulnerabilities".[1] Blockchain technology is designed to keep information secure once it is received. It cannot defend against the multitude of threats to that information before it is entered in the blockchain, and voters cannot verify their votes are entered into the blockchain correctly without compromising ballot

secrecy. Recording ballots on a blockchain also risks ballot secrecy if encryption keys are not properly protected or software errors allow decryption of individual ballots.

Internet voting excludes voters from audits.

If we exclude voters from voting with a paper ballot, we are also excluding them from an authentic auditing process and taking away the ability to recover their votes in the event of a cyber-attack.

Safer alternatives exist for military and overseas voters

The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) requires a 45-day lead time for military ballots. Because of this, almost every overseas voter can receive, mark, and return a paper ballot in a timely manner. Unmarked ballots can also be sent electronically by the election board to overseas voters for faster receipt. Verified Voting supports secure options for overseas voters including extended deadlines for receipt of voted ballots.

1. National Academies of Science, Engineering, and Medicine, 2018. "Securing the Vote: Protecting American Democracy." Washington, DC: The National Academies Press. https://doi.org/10.17226/25120.

2. National Institute of Standards and Technology, Activities on UOCAVA Voting, February 2011. "Security Considerations for Remote Electronic UOCAVA Voting." http://www.nist.gov/itl/vote/uocava.cfmhttps://www.nist.gov/sites/default/files/documents/itl/vote/NISTIR-7700-feb2011.pdf