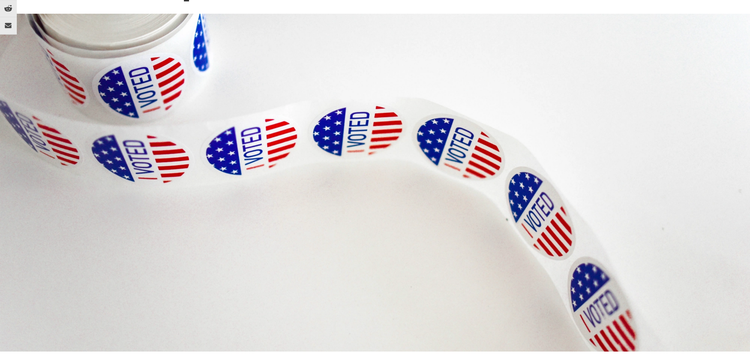
STATE

Researchers say OmniBallot online voting platform is vulnerable to manipulation



(Pexels)

Written by Benjamin Freed

JUN 8, 2020 | STATESCOOP

An online voting platform that a handful of states are using in limited capacities this year has been found to be vulnerable to hacking that could expose or manipulate how a person's ballot was cast without being detected either by voters or officials tallying results, according to a paper published Sunday by a pair of influential election-security experts.

The platform, OmniBallot, is scheduled to be offered by the states of Delaware and West Virginia as an option for active-duty military members, other overseas residents and voters with physical disabilities — and, in the case of Delaware, voters who are self-quarantining due to COVID-19. It was also used last month in local elections in New Jersey, though the Garden State does not plan to use the platform in its presidential primary next month.

According to the paper, by J. Alex Halderman, a computer scientist at the University of Michigan, and Michael Specter, a doctoral student at the Massachusetts Institute of Technology, OmniBallot "is vulnerable to vote manipulation by malware on the voter's device and by insiders or other attackers" who can compromise systems made by Amazon, Google, Cloudflare or OmniBallot's publisher, Democracy Live.

Halderman and Specter also wrote that OmniBallot "appears to have no privacy policy," a concern given that it collects several pieces of a voter's identity that could be sold to advertisers.

Unlike other mobile voting options, such as Voatz — a mobile app that was previously used in West Virginia — voters using OmniBallot can return their votes to their local election authorities several ways, including printing them out and mailing, emailing or faxing them.

Democracy Live's OmniBallot platform has long been used to collect votes from service members, who print out blank ballots, fill them out and return them through postal mail. But 2020 is the first year the platform will include an online ballot return — and will be opened to a wider universe of voters.

The paper cites a memo last month from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency that delivered a stern warning about the perils of online voting. Online voting, the memo read, "faces significant security risks to the confidentiality, integrity, and availability of voted ballots."

The CISA memo, which was also signed by the FBI, Election Assistance Commission and National Institute of Standards and Technology also said that even with the best cybersecurity practices in place, paper balloting is still far less risky than electronic voting.

"[W]e recommend paper ballot returns as electronic ballot return technologies are high-risk even with controls in place," the agencies said at the time.

Halderman, a longtime skeptic of online voting, and Specter, who co-authored a February report that revealed several major vulnerabilities with Voatz, wrote that while OmniBallot's ability to deliver ballots to hard-to-reach voters is laudable, the platform should be avoided if possible.

"Your safest option is to avoid using OmniBallot," they write. "Either vote in person or request a mail-in absentee ballot, if you can."

If a voter's only option is OmniBallot, they recommend printing out the empty ballot, completing it by hand, and returning it in the mail. Using the platform's on-screen ballot-marking option, they write, "will send your identity and secret ballot selections over the Internet to Democracy Live's servers even if you return your ballot through the mail."

Halderman and Specter's most explicit warning came against returning a completed ballot by any means other than postal mail: "If at all possible, do not return your ballot through OmniBallot's website or by email or fax. These return modes cause your vote to be transmitted over the Internet, or via networks attached to the Internet, exposing the election to a critical risk that votes will be changed, at wide scale, without detection."

In an interview with the New York Times, Democracy Live's chief executive, Brian Finney, defended OmniBallot.

"No technology is bulletproof," he said. "But we need to be able to enfranchise the disenfranchised."

Finney also told the Times OmniBallot has been vetted by security researchers and that it does not share or sell its data to advertisers.

In this Story

Democracy Live, election security, OmniBallot, online voting

RELATED NEWS

EMERGING TECH

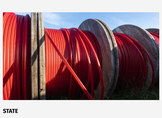
Tennessee's Medicaid program is going in on process automation

by Colin Wood • 1 week ago

DIGITAL SERVICES

Code for America's 'Safety Net Innovation Lab' names first 4 states

by Benjamin Freed • 1 week ago



STATE

Biden administration sets guidelines for $45B in new 'BEAD' broadband program

by Benjamin Freed • 2 weeks ago