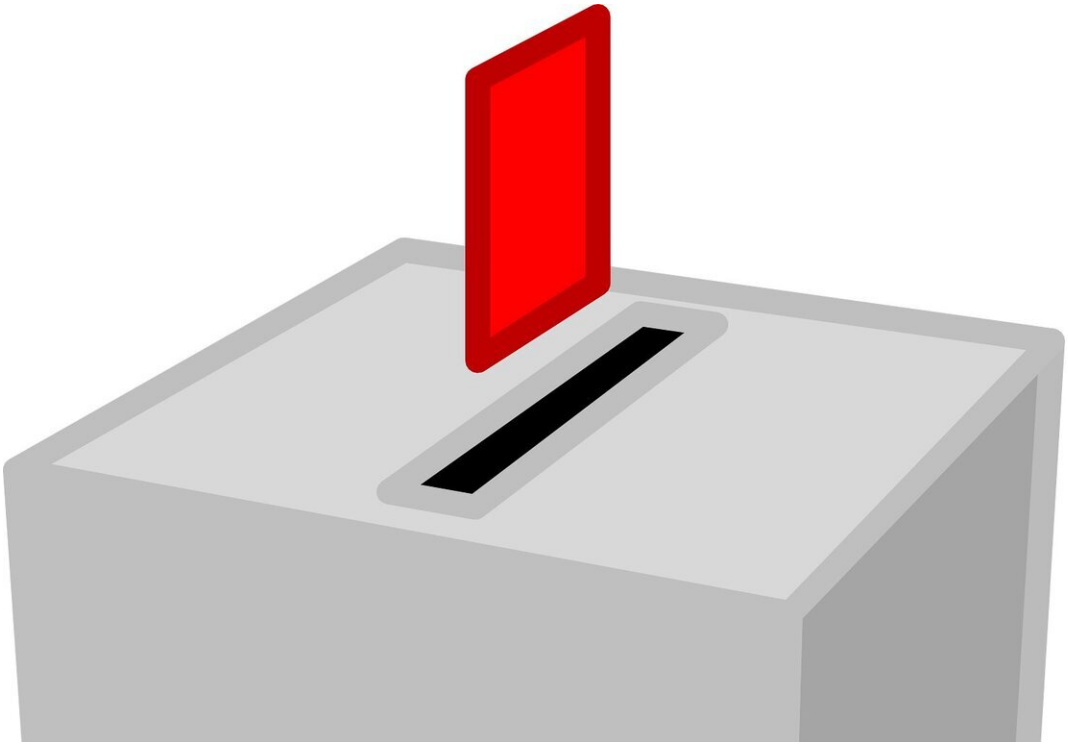
New remote voting risks and solutions identified

June 10 2020, by Nicole Casal Moore



Credit: CC0 Public Domain

The upcoming presidential election in the middle of a pandemic has jurisdictions exploring new technologies. They're not secure.

Election security researchers at the University of Michigan and MIT have found vulnerabilities in an internet voting and ballot delivery

system being used in 14 states.

Their work is the first public, independent analysis of the security and privacy risks of Democracy Live's OmniBallot system. In a recently released report, they outline security holes and offer recommendations for both election officials and voters.

Delaware, West Virginia, and New Jersey have either deployed OmniBallot or plan to do so for fully online voting, also referred to as "electronic ballot return." Other states including Colorado, Florida, Oregon, Ohio and Washington, the *New York Times* reports, use it to deliver blank ballots to registered voters who can mark them and return them by fax, email or mail. Neither of these uses are adequately secure, the researchers found.

"OmniBallot's design is overly simple, and ignores 30 years of research about building E2E-verifiable online voting. The voter's identity and ballot choice are just sent to a server in Amazon's cloud, which generates a ballot that officials can download. As a result, there's no way for voters, officials, or Democracy Live to be sure votes aren't modified," J. Alex Halderman, professor of computer science and engineering at U-M and an author of the report, said in a Twitter thread.

"There are important risks even when OmniBallot is used only for delivering blank ballots, including the risk that ballots could be misdirected or subtly manipulated in ways that cause them to be counted incorrectly."

Michael Specter, a doctoral student at MIT who worked on the report with Halderman, says the team's goal is "to provide election officials and citizens the information they need to ensure that elections are conducted securely."

For individual voters, the researchers recommend these steps, as outlined by MIT CSAIL:

- Avoid using OmniBallot if possible. Either vote in person or request a mail-in absentee ballot. Mail-in ballots are a reasonably safe option, provided you check them for accuracy and adhere to all relevant deadlines.
- If you can't do that, your next-safest option is to use OmniBallot to download a blank ballot and print it, mark it by hand, and mail it back or drop it off. Always double-check that you've marked your ballot correctly, and confirm the mailing address with your local jurisdiction.
- If you are unable to mark your ballot by hand, OmniBallot can let you mark it on-screen. However, this option (as used in Delaware and West Virginia) 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. This increases the risk that your choices may be exposed or manipulated, so the researchers recommend that voters only use online marking as a last resort. If you do mark your ballot online, be sure to print it, carefully check that the printout is marked the way you intended, and physically return it.
- 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. Recent recommendations from the Department of Homeland Security, the bipartisan findings of the Senate Intelligence Committee, and the consensus of the National Academies of Science, Engineering, and Medicine accord with the researchers' assessment that returning ballots online constitutes a severe security risk.

For election officials, they recommend these steps, as tweeted by Halderman:

- Discontinue online voting. No readily available defense can adequately mitigate the risks of OmniBallot's electronic return mechanism.
- Reserve online marking for voters who need it. Although online marking is critical for some disabled voters, it carries higher risks and becomes an attractive target when widely used. Marked ballots should always be printed and physically returned. To reduce security and privacy risks for voters who do need online marking, ballots should be generated locally in the browser, using client-side code. Democracy Live already offers this option in California and some other localities.
- However ballots are returned, states should require that Democracy Live adopt an enforceable privacy policy that prohibits using voters' information for any purpose unrelated to servicing their ballots.
- States should also require public, independent security analysis before considering online voting systems. Without such analysis, voters and officials will be unable to accurately weigh the tradeoffs between risk and access.

"States are adopting OmniBallot for laudable reasons: to help overseas voters, voters with disabilities, and those who can't safely go to the polls due to COVID-19," Halderman says. "But, as we learned in 2016, elections face serious security threats. That's especially true for online voting."

OmniBallot's ballot delivery and marking modes have the potential to be valuable tools for helping voters participate, if used with specific security precautions and changes recommended in the study, the researchers say. Some of those recommendations can be followed

directly by individual voters but many will also require action by election officials.

"On the other hand," the researchers added, "as online ballot return represents a severe danger to election integrity and voter privacy that no available technology can adequately mitigate, we recommend that Democracy Live and jurisdictions discontinue this feature."

Provided by University of Michigan