Local U.S. Election Officials' Emails Vulnerable to Cyberattacks, Report Warns

Email privacy controls-or a lack thereof-could put state and local election administrators at risk of phishing.

July 27, 2020 2 min read

This story originally appeared on PC Mag

In just 99 days, US citizens will pile into polling places to cast their vote in the 2020 presidential election. Which means the 10,000-plus state and local administrators whose email privacy controls makes them susceptible to online attacks have little more than three months to tighten security. A new report from Area 1 Security, in partnership with Americans for Cybersecurity, reveals troubling statistics about digital defense tactics—or lack thereof.

"The administration of elections in the United States is complicated," Area 1 CEO Oren J. Falkowitz wrote in the report. "The federal government has immense resources and capabilities, but little authority. Local officials who, with the most limited resources, find themselves in the crosshairs of nation-state cyber warfare without the knowledge or tools to fight back. A political theorist would deem the intertwined roles and responsibilities elegant by design. But from a cybersecurity perspective this complex system is a cluster[f**k] of vulnerability."

According to the findings, a mere 18 percent of election administrators have implemented advanced anti-

phishing cybersecurity controls, while 5 percent were caught using personal email addresses or technologies designed for non-standard email. The map included in the report shows Area 1 Security's rating system applied to every county in the US. The agency also discovered a number of officials who independently manage their own custom email infrastructure—including one known to be targeted by Russian cyber actors linked to previous election interference.

The good news is, the dispersed nature of US elections makes it impossible to hack voting nationwide. Attackers can, however, infiltrate local events that, even if statistically insignificant, can create a negative ripple effect across the country. "We hope that this [report] may serve as a catalyst for an optimistic all-out assault," Falkowitz said. One that "ensures elections in the United States are free, fair, and full of cybersecurity."

https://www.entrepreneur.com/article/353839