David Singleton Outlines Cybersecurity Risks during Elections

David A. Singleton of Minnesota is on the frontline of the election results. As the nation processes new risks to election tampering, we review protection steps


David Singleton MN

MAPLEWOOD, MINNESOTA, UNITED STATES, January 21, 2021 /EINPresswire.com/ --
Minnesota Civilian Public Safety Commission Founder and Executive Chairman, David A. Singleton outlines Cybersecurity risks during elections.

David Singleton of Maplewood, Minnesota talks about the security risks prevalent during elections. David ran for Secretary of State as an independent candidate in Minnesota, in 2014.

He has experience as a local government and chairman of council boards. For over two decades, he's also run a small business in Maplewood, MN that has been very successful.

David's interest in politics has driven him to bring to light the prevalent security risks during elections.

As someone who believes in democracy and the rule of law, his concerns are a huge aspect of his personality. He understands the importance of a free and fair election to ensuring democracy and allowing the people to choose who must represent them.

According to David Singleton, one of the biggest cybersecurity risks during elections the world is facing is ransomware. Hackers seem to have developed the capacity to infiltrate servers and computers used for election and taking them over. When this happens the data is either retrieved or the hacker holds the system hostage for money.

Voter data manipulation done in advance of an election is another challenging issue that David Singleton feels election officials and technicians are going to face. In this scenario, hackers get access to voter data and then change information like names, addresses, and locations. Such a change can lead to frustration and confusion during an election period and can disenfranchise

people that have been targeted.

Instead of relying on crowd-sourcing or vulnerable technology, county clerks and other local officials are responsible for reporting vote tallies on their website after the election.

David Singleton believes that America's centralized voting systems may be exposed to reporting errors. Hackers could attack the systems reporting on vote totals on election nights by attempting to manipulate results on the websites. This could lead to confusion and distrust in the electoral system that can cause even more severe havoc to election integrity.

To plan against the possibilities of these attacks and reduce election manipulation risks, David Singleton suggests that the American voting system infrastructure increases protection via top cybersecurity firms. One of the best ways to do this is to upgrade or change outdated voting machines which election supervisors are quick to point out. Any vulnerabilities found under these conditions aren't indicative of problems that actually could be exploited during an election.

David Singleton of Maplewood, MN also advises the establishment of cybersecurity standards to protect election infrastructure against possible attacks. Elections officials need to know these standards and ensure they try their best to abide by them.

Theresa Brandley
SquareOne Digital, LLC
+1 347-508-0434
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
