Website Security Shortcomings Could Render U.S. Elections Susceptible to Digital Disinformation

Election Website Research Frequently Asked Questions

This document briefly summarizes the key takeaways from McAfee's research into election website security and provides other answers to frequently asked questions about this research and McAfee's perspectives on threats to the 2020 U.S. elections overall.

Q: What did McAfee find?

A: McAfee's January survey of 13 projected 2020 battleground states found that their county websites and county election administration websites lacked the necessary ".GOV" website validation and "HTTPS" website encryption to prevent malicious actors from launching fake web domains posing as legitimate county government sites.

- The survey finds 83.3% of 2020 election battleground state counties use websites lacking U.S. government .GOV certification.
- 88.9% of Iowa county websites lack .GOV validation.
- Nine of ten New Hampshire county websites lack .GOV validation.
- Minnesota ranked lowest in .GOV validation with 95.4% of counties lacking certification
- 46.6% of battleground state counties fail to protect voters visiting their websites with HTTPS encryption
- Inconsistent standards, easy-to-remember naming formats are likely a security liability versus an advantage

McAfee asserts that these shortcomings could make it possible for malicious actors to spread false and misleading election information through mass bulk email campaigns and website promotions.

These fake communications could suppress, misdirect, or otherwise disrupt election proceedings in such a way that they could impact the number of votes cast and, ultimately, perhaps impact the results of the 2020 U.S. elections.

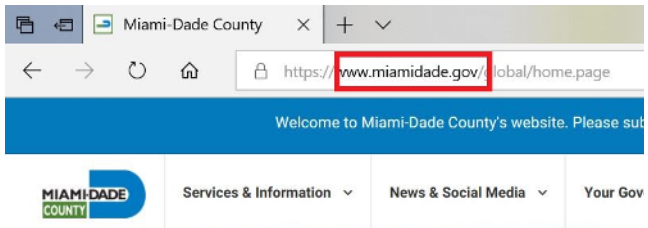
FAQ

Q: What is .GOV validation and why is it so important?

A: Acquiring a .GOV website name requires that governments submit evidence that they truly are buying these names on behalf of legitimate local, county, or state government entities.

Websites using .com, .net, .org, and .us in their names are easily accessible to anyone with a credit card from website domain vendors such as GoDaddy.com.

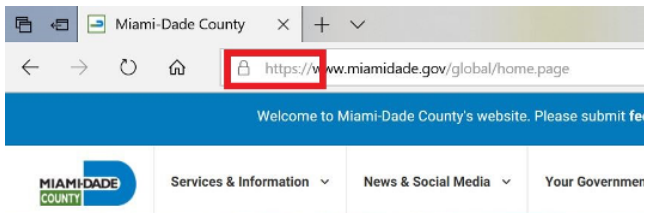
Example of county website using both HTTPS encryption and .GOV:



The lack of U.S. government validation means that malicious actors could spoof legitimate government election sites with fake websites.

Q: What is HTTPS encryption and why is it so important?

A: When website visitors see the HTTPS in the web address of a website they are visiting, that means that their browser has made a secure, encrypted connection with that website through a technology called Secure Sockets Layer (SSL). Websites bearing the HTTPS in their name may also see a "lock" icon in their web browser address window.



While the SSL name of this security measure may sound technical, the security the technology delivers is not difficult to understand. When website visitors see the HTTPS in a web address it means:

- Any personal information that they share with those websites is encrypted and cannot be intercepted and stolen by hackers while they are visiting the website.
- Visitors cannot be re-routed against their will from legitimate government websites to disinformation websites pretending to be government websites.

FAQ

Q: Why does the lack of .GOV usage in website names pose such a threat to our elections?

A: Without a government body validating whether websites truly belong to the government entities they claim, it's possible to spoof legitimate government sites with fraudulent websites.

If a malicious foreign actor can spoof government websites, he can send hundreds of thousands of emails to voters and use both those emails and the websites to which they are tied to send voters information on the wrong polling places, phony voter registration processes or requirements (barriers), or other incorrect voting instructions that confuse, misdirect, or suppress a key county's electorate from voting and/or voting with confidence.

Example of disinformation email:

From: noreply@votebrowardcountynow.net
Sent: Tuesday, October 23, 2018 11:48 AM
To: molly_thomas@yahoo.com

Subject: PLEASE READ: URGENT BROWARD COUNTY VOTER INFO UPDATE

Importance: High

Broward COUNTY RegistertoVoteFlorida.gov

YOUR VOTING LOCATIONS IN BROWARD COUNTY, FL

Because every vote must count, we thank you for registering to participate in this year's important midterm elections.

Please take note of your Pompano Beach voting locations in Coral Springs, Pembroke Pines, Miramar, Hallandale, Plantation, and Dania Beach. For voting location addresses, please visit the official Broward County website: www.votebrowardcountynow.net.

IMPORTANT: WHAT YOU NEED TO VOTE

To register online you will need to provide the following:

- Florida driver's license or Florida identification card number
- Two documents proof of county address
- Social Security card
- Voter registration card

If you do not have any portion of the required information, follow this link to provide your voting address using our paper form (PDF). Once you complete this form, you must sign and send it to your county board of elections.

We thank you for performing your important civic duty as a citizen of Broward County!

Best regards,

Broward County Elections Board

www.votebrowardcountynow.net

EXAMPLE OF WHAT A MIS-INFORMATION EMAIL COULD LOOK LIKE - FOR EDUCATION PURPOSE ONLY

If the actor can launch such a digital disinformation campaign close enough to election day, he could reach a significant number of voters. If he does so before county and state officials become aware of the campaign, it could be very difficult for the officials to counter the disinformation before voter behavior is influenced.

If the actor can successfully disrupt, suppress and/or confuse the voting behavior of just tens of thousands of citizens in key battleground states, their votes may not be counted or their confidence in the validity of election results and even legitimacy of the democratic process overall could be badly shaken.

Ultimately, if a malicious actor is seeking to undermine confidence in government, he can succeed in damaging confidence in the electoral process, even if he cannot succeed in impacting votes.

FAQ

Q: Is an election disinformation campaign influencing voter turnout a greater threat that election system hacking campaign that seeks to change votes that have already been cast?

A: These threats pose the same level of risk. Malicious actors such as nation-state and cybercriminal hackers always seek to achieve their objectives with the least efforts and resources.

While it is possible that such actors could hack into local voting systems and change vote counts in the battleground states, such a hacking campaign would require a herculean effort of orchestration across 1,117 counties and thousands of voting precincts.

Alternatively, a digital disinformation campaign seeking to suppress or otherwise disrupt voting behavior would be less complicated to execute and therefore more likely to be attempted than efforts to change vote counts.

If executed successfully at scale in critical counties and states, this disruption could accomplish the same goals of a hacking campaign at a fraction of the resources.

Q: Why would county websites be such a key target for these digital disinformation campaigns?

A: Unlike state-level websites, county websites are more obviously accessible to local citizens seeking election information, and less likely to have government validation and encryption to ensure that they are genuine, safe websites for citizens to visit.

Yet, Election 2020 prognosticators have identified key counties in states where the 2016 presidential election was decided by as few as tens of thousands of votes. For 2020, these prognosticators argue that counties such as Arizona's Maricopa County, Florida's Miami Dade County, Georgia's Cobb and Gwinnett Counties, Pennsylvania's Philadelphia and Beaver County, and counties in other key battleground states could decide which party wins the states.

Therefore, any manipulation of voter turnout in these counties' different precincts could impact the election results there. The weak validation and security of the website domains in these counties is a weak link and presents target for any malicious actors seeking to shape the election results in their favor.

FAQ

Q: Which website feature—.GOV government validation or HTTPS encryption—are more important in preventing election disinformation campaigns?

A: The .GOV validation is most important because an official government authority is guaranteeing that a website is genuine, legitimate, and can be trusted. Alternatively, anyone with a credit card can purchase HTTPS encryption for any website they own, validated or not, legitimate or not.

But McAfee advises that governments provide both .GOV and HTTPS encryption given the importance of protecting voters and maintaining their trust. Voters already receive encryption when they visit corporate websites to share sensitive information, and when they visit ecommerce websites to make purchases. They should receive the same or better protection when they visit websites related to something as important as our electoral process.

McAfee™

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847 8766
www.mcafee.com