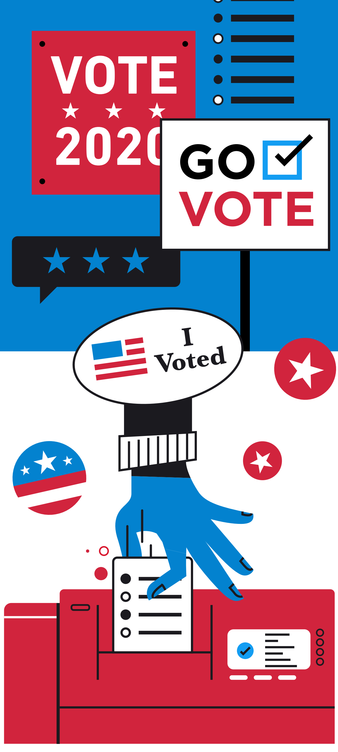
Are the 2020 US Elections Vulnerable to Cyberattacks?

Exploring security weaknesses and solutions



Americans want secure elections — but with the foreign interference into the 2016 elections and the rise of large-scale cyberattacks, we're realizing our vulnerabilities. The reality is that there are potential security pitfalls throughout the election process from campaign offices and voter databases to primaries, caucuses, and voting places. And solving for these weaknesses is of national importance.

Disinformation goes viral

Before any votes are cast, opinions and attitudes are shaped. Outside groups have become experts at leveraging available personal data — locations, preferences, Facebook groups — to direct false information at voters based on their online personas.[1]

Facebook and Twitter have recently attempted to combat fake news and tighten restrictions on political ads, but in 2016 social media platforms found that:[2]

470
fake Russian accounts produced 80,000 Facebook posts

120,000
Instagram posts were generated from Russian troll farms

2,752
Russian-linked Twitter accounts were suspended

Breaches on the campaign trail

Candidates and campaigns usually rely on flocks of volunteers and canvassers spreading their message — often via a worker's personal (and easy-to-hack) device. This can potentially compromise vital information such as voter databases or even internal campaign strategy.

Ransomware attacks, like those that have recently hit city government networks in Atlanta and Baltimore, pose a threat of holding voter data hostage.[2]

90,000
personal voter records in Illinois were compromised due to a targeted phishing email attack on staffers.[3]

Outdated voting equipment

After the 2000 election recount drama, ease-of-use took priority over cybersecurity when manufacturing voting machines, and that push and pull remains to this day. As voting equipment ages, vulnerabilities will continue to appear.[4]

16 Million
Number of Americans projected to use paperless voting machines in the 2020 election[5]

45
Number of states using voting equipment so old it's no longer manufactured[6]

So, what can be done?

Modern security technology can help shore up election safety in many ways.

Advanced analytics can help detect unusual behavior in user practices and flag data exfiltration.

New software is being piloted to spot disinformation like fake news stories or doctored photos and videos.

Cybersecurity best practices include training staff, implementing two-factor authentication, and putting in solutions to help identify voting machine vulnerabilities during the primaries and all the way to November 3rd.

If you're concerned about security in elections or the integrity of your local polling location, one of the best things to do is get involved! Sign up to be an election worker, contact your local board of elections, and speak to the staff about how they are ensuring security.

Sources:
1 U.S. Unleashes Military to Fight Fake News, Disinformation, 2019, Bloomberg
2 U.S. officials fear ransomware attack against 2020 election, 2019, Reuters
3 How Russia meddling became social media's problem, 2017, Bloomberg
4 Russian Hacks on U.S. Voting System Wider Than Previously Known, 2017, Bloomberg
5 Voting Machine Security, 2019, Brennan Center
6 Every state was giving funding for election security, 2019, Fortune
7 Understanding the challenges of frontline security, 2019, Exabeam

exabeam®