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.

Modern security technology can help shore up election safety in many ways. So, what can be done?

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.

Candidates and campaigns usually rely on flocks of volunteers and canvassers spreading their messages — 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.

Outdated voting equipment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.

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:
2. U.S. officials fear ransomware attack against 2020 election, 2019, Reuters
3. How Russia meddling became social media’s problem, 2017, Bloomberg
6. Every state was giving funding for election security, 2019, Fortune
7. Understanding the challenges of frontline security, 2019, Exabeam

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, implement- ing two-factor authentication, and putting in solutions to help identify voting machine vulnerabilities during the primaries and all the way to November 3rd.

So, what can be done?

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

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

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.

Candidates and campaigns usually rely on flocks of volunteers and canvassers spreading their messages — 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.

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.

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:
2. U.S. officials fear ransomware attack against 2020 election, 2019, Reuters
3. How Russia meddling became social media’s problem, 2017, Bloomberg
6. Every state was giving funding for election security, 2019, Fortune
7. Understanding the challenges of frontline security, 2019, Exabeam