Top Tips to Protect the Integrity of Elections

For voters, poll workers, and election officials

Top Tips to Protect the Integrity of Elections

Our democracy is meant to reflect the will of the people. We expect our vote to count, and we place our trust in the system that elects our leaders. If that trust is shaken, our democracy itself is shaken. Simply put, the system must work. We must be able to trust it.

There are currently over 9,000 election jurisdictions across the U.S., and in every election cycle more and more of our elections are conducted electronically. Unfortunately, that means more of our elections are vulnerable to cyber attack.

Despite the glare of recent headlines and the fact that computers and the internet now are part of elections infrastructure, this is nothing new. Attacks on the voting process are as old as democracy itself. There is no way around the fact that protecting our democracy means protecting our elections.

The call is clear. But what can **you** do? Whether you are a voter, poll worker, or part of an election organization, here are 15 essential tips to improve the integrity of our elections.

Top Five Security Tips for Voters

First, fear not. There are concrete steps you can take, as well as numerous resources available, to ensure your vote is cast—and counts—on Election Day. **Here are the top five actions to take:**

If you are a voter ...

Validate your voting registration status. The key first step. You must be 18 and a U.S. citizen to be able to vote, and nearly all states require voters to be registered. Most states have registration deadlines ahead of Election Day, with the actual lead time varying. One way to register? Submit a National Mail Voter Registration Form (although North Dakota and Wyoming do not accept these), available at the U.S. Election Assistance Commission's website. You can also find voter registration forms at most state and local government offices, as well as the DMV or your local library. If you know you will be unable to get to your polling place on Election Day, apply for an absentee ballot. That too can be done on the EAC website, where there is even a portal to validate an existing registration if you are already on the voting rolls. Whatever way you make yourself eligible, whether online or on paper, exercise your right to vote!

Identify your correct polling place. Polling locations sometimes change from election to election, so if even you have voted before, do not assume it will be in the same place. You can look up your polling place on the very helpful U.S. Election Assistance Commission website. You can also find out what time the polls open and close, so you may plan your Election Day voting with confidence. Also, it's a good idea to familiarize yourself with the candidates and issues on the ballot ahead of Election Day. For some people, going into a voting booth can feel a bit momentous, even be slightly nerve wracking. **It's best to be prepared.**

Exercise normal caution. Once Election Day arrives and you are at your local polling station with proper identification, remember that voting is a transaction much like any other. You should treat using a voting machine like using an ATM or buying gas with a credit card. Protect your personal details the same as with any other day-to-day electronic interaction. If the equipment seems to be malfunctioning or behaving oddly, alert your poll worker. Sometimes equipment fails, or has been tampered with. **If you see something, say something.**

Make sure your ballot is accurate. Verify that your touch screen or scan card ballot looks exactly like the one in your voters' guide. Make sure your preferred candidates' names appear and are spelled correctly. There should be no errors with your ballot. **If anything seems at all incorrect, say something to a poll worker.**

Finish strong: confirm your vote. Follow through to the end of the process, meaning: return all voting materials to the polling station workers; watch the number counter advance when you scan your ballot; and use the step-by-step voting guide resources so you know your electronic vote has been counted. If you experience a problem at a polling place or with voting procedures in your jurisdiction, report the problem at your polling place and/or file a complaint. The website for the U.S. Election Assistance Commission has information on **how to contact your state's election office and report any problems or irregularities.**

Additional Resources for Voters

* U.S. Election Assistance Commission—

The National Mail Voter Registration Form:

https://www.eac.gov/voters/national-mail-voter-registration-form/

Information on voter registration in your state:

https://www.eac.gov/voters/register-and-vote-in-your-state/

Election Day Contact Information, including polling place location lookup:

https://www.eac.gov/voters/election-day-contact-information/

* Voting Information Project—Helps voters find information about their elections with simple tools:

https://votinginfoproject.org/

* Ballotpedia—A non-partisan site providing accurate, objective, and up-to-date political info:

https://ballotpedia.org/Main_Page

* VerifiedVoting.org—Interactive map that identifies the types of voting equipment in use:

https://www.verifiedvoting.org/verifier/

* ProCon.org—Instructions for using various electronic voting machines:

https://votingmachines.procon.org/view.resource.php?resourceID=000276

* National Conference of State Legislatures—Information on Provisional Ballots:

http://www.ncsl.org/research/elections-and-campaigns/provisional-ballots.aspx

Provisional Ballots

There are all kinds of reasons why you might need a provisional ballot, sometimes called a 'challenge ballot' or an 'affidavit ballot', depending on your state. Your name might not be on the registration list, or you requested an absentee ballot but did not receive it, or your name or address have changed but your registration information doesn't reflect that. No matter what the reason you are denied a regular ballot, all voters have the right to cast a provisional ballot.

To do this you will need to provide a written affirmation stating that you are genuinely eligible to vote in that election. Once that is completed, you will be issued a provisional ballot to fill.

After you're done, federal law requires election officials to give you information on how you can check whether your vote was counted and, if not, the reason why.

Remember: no matter why you might need a provisional ballot, it is your right to have one!

The National Conference of State Legislatures has published an exhaustive guide on how to enforce your right to cast a provisional ballot on Election Day, including the particulars in your state or territory.

http://www.ncsl.org/research/elections-and-campaigns/provisional-ballots.aspx

Top Five Security Tips for Election Poll Workers

Whether you're a paid worker or volunteer, you are the front line of defense in election security. The actions you take are critical in making sure everybody's vote counts.

If you are a Poll Worker ...

The same as with a voter, if you see something, say something. If something appears suspicious or malfunctioning, chances are it is. Speak up to your supervisor or someone in authority until the issue is resolved. If a tamper-resistant seal looks tampered with, call attention to it. If a voter complains a machine is not working right, don't just reset it, get someone in charge to take a look. Don't worry about raising an alarm–after all, that's your role in protecting the integrity of our elections. It's what being 'the front line of defense' means. **Wear it proudly.**

Make sure there's enough paper on hand. As a worker at the start of Election Day, make sure you have enough optical scan paper ballots or provisional paper ballots should something should go wrong at your direct recording electronic (DRE) system polling place. Double check you have enough physical ballots to cover all registered voters on your roll. Remember, the goal is for every voting machine is to have an individual, voter-verified paper trail that can be cross-checked against the electronic results. **Voters have to be able to trust that their vote was for the candidate they actually voted for, and that it was counted.**

Be a good worker. Of course, we appreciate that you take your work as a poll worker seriously. You show up on time. That's great. Now, take the next step and make sure you're properly trained and well-practiced on opening and closing procedures, voting equipment operation for your particular machines, and voter check-in scenarios. Make sure Election Day supplies are available in ample quantities. **And do NOT use e-poll book equipment to go on the internet to check websites or your email, or for anything other than specifically what they are intended for—the voting process.**

Monitor voting time in the booth. This belongs in the 'if you see something, say something' category, but it bears its own heading because it's often overlooked. With simple training and observation, you should be able to gauge the typical time it takes to vote. There are even tools to help you learn to make this calculation. The bottom line? **If somebody is taking way too long, check in with them to assess the situation.**

Watch out for physical devices. There are items that simply don't belong in a voting booth. These may include laptops, USB or thumb drives, tools (screwdrivers and wire cutters), even cell phones in some jurisdictions. If you see something suspicious, report it to your polling supervisor. **Also, anyone showing up claiming to repair or inspect the voting equipment should be confirmed with your supervisor, and not allowed near the voting machines until they have been cleared.**

Being the first line of defense in protecting the integrity of our elections is a serious responsibility. We thank you for your time and effort. And please, while you are proudly helping the rest of us execute our civic duties, don't forget to exercise your own right to vote!

Additional Resources for Poll Workers

* Voting Time Estimator—Easy-to-use tool estimates the time needed to vote a ballot:

https://electiontools.org/tool/voting-time-estimator/

Top Five Security Tips for Election Systems

Our elections, whether local, state, or federal, are managed day-of and on-the-ground by clerks and volunteers who may not have a familiarity with professional cyber security. Sometimes even the officials in charge do not have a full awareness of cyber threats to our voting systems. If it's your responsibility to administer and safeguard our elections, know that our adversaries are playing a long game. They are smart, well-funded, and dedicated. Still, there are a host of best practices and workable steps to protect our basic democratic right to vote.

If you are an Election Official ...

Update the firmware and software on your voting and tallying machines. The majority of voting machines are more than ten years old. Many have not been patched or updated, so be sure to check that your machines are using the latest software or firmware. Familiarize yourself with how the machine should properly operate, and limit the number of people with administrative access to the system. Of course, you can learn more about the specific workings of your precinct's voting machines from the manufacturer-issued manuals, but also from websites such as VerifiedVoting.org. **Check to make sure your machines are fully up to date.**

Physically secure your voting machines and e-pollbooks, from storage to polling place. Visual security—making sure the machines have not been tampered with—is a simple way to limit vulnerability. When voting machines are transported, make sure they never go out of sight, and that they are always under the control of an individual, preferably two individuals. When the machines are stored, make sure they are locked away securely. Use tamper-evident seals on all external ports not required for regular use and deactivate any other ports not regularly used. When voting is done, collected, and brought back to the central tabulation point, those devices should be under the same control of two individuals. Solid voting system security flows almost entirely from people simply following proper procedures. **Safeguard your hardware as if everything depends on it, because it does.**

Limit your attack surface—no Bluetooth or unsecured Wi-Fi. Even though some voting machines are Wi-Fi-enabled, keep them off line. If a connection between networked devices is required, use hardwired cables instead of Wi-Fi. If you are obligated to connect polling machines or e-pollbooks to the internet, be sure to use secured networks, a VPN, and two-factor authentication. Two-factor authentication ensures that, even if your passwords are sniffed or stolen, the attackers won't be able to use them without that second factor. It's actually good cyber hygiene for all circumstances, professional or personal. **And be sure to change the passwords between elections.**

Back up with paper, both voting e-roll books and provisional ballots. Establish paper trails to ensure that, even if the electronic vote count is maliciously altered, a true voter-verified record exists on paper to be audited after the fact. Also, consider printing enough paper ballots to cover all registered voters in case of equipment failure, as well as sending printed-paper pollbooks to polling stations so that, in case of e-pollbook failure, poll workers can quickly and easily continue the voting process. Keep in mind recovery procedures should be simple and not introduce new obstacles to voters who are simply there to cast their ballots. And the instructions for provisional ballots should be clear, and clearly labeled, so that if a provisional ballot is needed, both the poll worker and voter know exactly how to use them. **Be prepared.**

Back up digital voter rolls. Voter registration databases (VRDBs) are digital records of registered voters and face the same security vulnerabilities as any other critical data. Back up the VRDB daily and store it offline as part of your solid recovery plan. Separately, make full post-election audits standard practice. Not only do they prove out the methods and equipment your organization has used, but they demonstrate transparency, which is infinitely valuable in maintaining the public trust. **And trust in our voting system is key to maintaining the trust in our very democracy.**

Additional Resources for Election Officials

* National Conference of State Legislatures—Information on the use of E-Poll Books:

http://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx

* Belfer Center—Their D3P Cyber Security Playbook offers a solid approach to election security:

https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf

* Brennan Center—A closer look at best practices for a variety of voting machines:

https://www.brennancenter.org/analysis/overview-voting-equipment

Why We Care

As our nation's voting is more and more conducted electronically, it becomes more and more important that we remain vigilant about how our vote is actually counted.

"Symantec is heavily focused on two major parts of society. One is cyber defense for governments and companies around the world, and the other is digital safety for individuals and citizens around the world. If we look at the place those two intersect, it's often in major events like elections. And so, our mission is to make sure the bond of trust and relationship, both on the government and business side as well as the individual side, is upheld so that the integrity of the system we live and operate in as a society is allowed to move forward and thrive." — **Samir Kapuria**
EVP & GM, Cyber Security Services, Corporate Vision, Symantec

Never forget, **you** serve a vital role in protecting our voting system. By following these tips, you will do your part to ensure our elections are secure, safe, and counted.

Most important, make your own voice heard and vote!

Authors

Brian Varner, Eric Chien

Contributors

Colin Gibbens, Samir Kapuria

Editor

Joshua Abramson

About the Authors

Brian Varner is the Special Projects Researcher aka 'Tinkerer-in-Chief' in Symantec's Cyber Security Services.

Eric Chien is a Distinguished Engineer and Technical Director of Symantec's Security Technology and Response (STAR) Division.

Colin Gibbens is Symantec's Director of Product Management, Endpoint Detection Response & Integrated Cyber Defense Exchange

Samir Kapuria is Symantec's EVP & GM, Cyber Security Services, Corporate Vision

About Symantec

Symantec is the world's leading cyber security firm and has been involved in election security. Protecting critical infrastructure—including elections—is what Symantec does every single day.

Election Integrity Resources

Ballotpedia

https://www.ballotpedia.org/Main_Page

Nonpartisan online encyclopedia provides accurate, objective, and up-to-date political information.

Belfer Center for Science and International Affairs

https://www.belfercenter.org/

Harvard Kennedy School's think tank advances policy-relevant information about international security and more.

Belfer Center Resources

- State and Local Election Cybersecurity Playbook

  https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

  Guides election officials in choosing election security strategies and how to work with technical specialists.

- Election Cyber Incident Communications Coordination Guide

  https://www.belfercenter.org/publication/election-cyber-incident-communications-coordination-guide

  Guides election officials in coordinating and aligning communications across jurisdictional boundaries following an election-related cyber security incident.

Brennan Center for Justice

http://www.brennancenter.org/

Law and public policy institute, at New York University Law School, advocates for progressive public policies.

Brennan Center Resources

- Better Safe Than Sorry: How Election Officials Can Plan Ahead to Protect the Vote in the Face of a Cyberattack

  https://www.brennancenter.org/publication/better-safe-sorry#report

  Offers concrete proposals for avoiding, mitigating, and recovering from election-related cyber attacks.

- Securing Elections from Foreign Interference

  https://www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference.pdf

  Offers concrete policy proposals for—you guessed it—securing elections from foreign interference.

- Brennan Center's Voting Machines at Risk: An Update

  www.brennancenter.org/analysis/americas-voting-machines-risk-an-update

  Describes unresolved cyber security vulnerabilities in today's voting machines.

Center for Civic Design

https://civicdesign.org/

Nonprofit educational research organization emphasizes design as a way to ensure voter intent is captured.

Center for Civic Design Resources

- Center for Civic Design Field Guides

  https://civicdesign.org/fieldguides

  The series guides election officials and poll workers on communications with voters and more.

Center for Internet Security

https://www.cisecurity.org/

Nonpartisan nonprofit develops and disseminates cyber security best practices.

Center for Internet Security Resources

- A Handbook for Elections Infrastructure Security

  www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

  Details election infrastructure security risks and the ways to mitigate those risks.

Department of Homeland Security

https://www.dhs.gov/publication/election-security-resources

Third-largest U.S. cabinet department oversees antiterrorism, cyber security, disaster prevention, and other activities nationwide.

US Election Assistance Commission (EAC)

https://www.eac.gov/voters/register-and-vote-in-your-state/

Independent U.S. government agency creates voting guidelines, tests voting systems, administers funds, and more.

EAC Resources

- Election Security Preparedness

  https://www.eac.gov/election-officials/election-security-preparedness/

  Prepares election officials and poll workers for election day with checklists, best practices, and more.

- EAC Standards for Poll Workers

  www.eac.gov/research-and-data/provisional-voting/

  Describes best practices for facilitating provisional voting on election day.

- Ten Things Election Officials Can Do to Help Secure and Inspire Confidence in This Fall's Elections

  https://www.eac.gov/assets/1/28/EVN%20Top%20Ten%20v7.pdf

  Describes ten ways election officials can secure, and inspire confidence in, the November 2018 mid-term elections.

Election Verification Network

https://electionverification.org/askanexpert/

Nonpartisan network of election integrity experts shares information, strategy, and coordinated work.

Election Verification Network Resources

- Ask an Elections Expert

  https://electionverification.org/askanexpert/aee-advocacy/

  Provides elections experts via email to address your pressing concerns.

National Association of State Election Directors

https://www.nased.org/

Nonpartisan professional group disseminates best practices and information regarding U.S. election administration.

National Conference of State Legislatures (NCSL)

http://www.ncsl.org/research/elections-and-campaigns/election-security-state-policies.aspx

Bipartisan NGO summarizes state election processes and procedures, especially regarding security.

NCSL Resources

- Electronic Pollbooks

  www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx

  Details states' use of, and requirements for, e-pollbooks.

ProCon.org

https://www.procon.org/

Nonprofit researches, and presents its findings on, controversial (including political) issues.

ProCon.org Resources

- ProCon.org: How to Vote on an Electronic Voting Machine

  https://votingmachines.procon.org/view.resource.php?resourceID=000276

  Describes step-by-step process for using various electronic voting machines.

Secure Our Vote

https://secureourvote.us/

Activist coalition of organizations working to ensure every vote has a paper trail and can be audited.

Secure Our Vote Resources

- Securing Election Offices and Data

  https://secureourvote.us/securing-voter-rolls-offices/

Verified Voting

https://www.verifiedvoting.org/

Nonpartisan nonprofit works to establish electronic voting systems that concerned citizens can trust.

Verified Voting Resources

- Verified Voting Verifier

  www.verifiedvoting.org/verifier/

  Identifies, by county and by state, the types of voting equipment
  in use.

- State Audit Laws Searchable Database

  https://www.verifiedvoting.org/state-audit-laws/

  Searchable resource describes state laws, regulations, and procedures for post-election audits.

Voting Time Estimator

https://electiontools.org/tool/voting-time-estimator/

Easy-to-use tool estimates the time needed to vote a ballot.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | **www.symantec.com**