The following information is provided by:

ITRC | IDENTITY THEFT RESOURCE CENTER

Don’t Vote for Fraud this Election Year

Election season is here, and there just might be unprecedented interest in various states’ midterm elections. Pride and patriotism are leading more and more people to take an interest in the political system. Unfortunately, this civic interest can also cause scammers to take advantage of the public, targeting voters for identity theft, access to their financial accounts and more.

To be a civic-minded citizen while still protecting yourself, it’s important to know how to spot a possible scam and take action:

1. Voter surveys

One of the many ways that political candidates gauge the concerns of their constituents is to ask questions about the issues. Unfortunately, this approach can also allow scammers to seek personally identifiable information. Be careful not to overshare your name, address, email address, birthdate and certainly not your Social Security number or driver’s license number. It’s also important to avoid the “confirm your status as a registered voter” phone or email scams.

2. Voter registration drives

All over the country, dedicated volunteers are helping citizens register to vote. You may see tables at outdoor festivals or farmers’ markets, on college campuses or other widely populated events. If you’re concerned about your data security—such

as the filled-out forms are left where anyone can see them—take the offered form, fill it out and mail it or deliver it to your local officials instead.

3. Petitions

This is another excellent way to express concern about critical issues, but it can also lead to identity theft if the person handling the petition does not properly administer it. You might have signed a petition in high school to get more pizza on the cafeteria menu, and that didn't require much more than your signature. A political petition, on the other hand, can request things like names, addresses or phone numbers. However, there's no reason for more sensitive information, and you are not required to submit your entire identity. Walk away if you get the impression that too much information is required.

4. Voting "support"

Believe it or not, someone may try to make a fast buck off your desire to vote. With so much news lately about names dropping from the voter rolls, scammers can easily send out phishing messages that playoff your fear of not getting to vote. However, there is absolutely no reason to pay someone to tell you if you're still registered to vote! That information is available for free from your local voter registration office.

5. Hoaxes on Social Media

Yes, there have been reports about some shady political ads on social media, unauthorized access to voter information via Facebook and more. Don't let that cause you to become anyone's victim. If you see posts online that you aren't sure are accurate, don't hit like or share. Check them out for yourself from reliable sources before engaging with them on social media. Remember, even if they're not out to steal your account access or your identity, engaging with a post—even to point out that it contains false or misleading information—gives that post greater visibility and traction.