



The security of our elections is a top priority for the State of Texas.

The State continues to employ effective and forward-thinking cybersecurity measures to further strengthen elections systems and safeguard our elections infrastructure against malicious cyber activity. Now more than ever, it is important for Texas voters to be aware of cybersecurity risks around elections, and how to stay educated and protected.

CONNECT WITH CARE, BE CYBER AWARE



What We Are Seeing



Cybercriminals have targeted non-government websites that support elections and provide election information across the state. These cyberattacks strive to cause widespread voter confusion and infect victims with malware.

Cybercriminals are rapidly creating hundreds of malicious websites every day and manipulating search engine results to present those malicious sites in the search results when citizens search for local election support organizations.

When members of the public search for a particular organization or for information about elections, they are presented with one of the infected websites and with descriptions that appear to match their search.

New websites continue to be added daily to the operation while older websites are cleaned up or removed. While the operation is occurring nationally, it has been confirmed that many Texas counties have non-governmental support organizations that have been included.

What You Can Do



Texans should take great care in their interactions with the others on the internet and take the following measures:

- ✓ **Click Carefully:** If you receive emails from individuals you do not personally know, do not click directly on any links. Instead, use your internet browser to go directly to the website of the organization that sent the email.
- ✓ **Trusted Texas Sites:** When you are gathering information in preparation to vote, confirm that

you are obtaining all information about the voting process from VoteTexas.gov or your county website. Most Texas counties use websites that end in .gov or .tx.us.

- ✓ **Consider the Source:** Carefully consider and verify the source of information. Use the official websites of trusted non-profits, communities, campaigns, and media outlets for your information sources, and check multiple trusted sources to validate information that is shared through social media.

Contact Your County



Elections create the discourse that is essential to the democratic process but also provide an opportunity for those with malicious intent to mislead voters, compromise systems, and affect election outcomes.

The State of Texas is doing its part to ensure the reliability and security of election systems.

Texas voters must also be vigilant online and connect with care.

Voters should contact their county if they need to ensure that information related to the election process is valid and accurate.



More Tips to Stay Cyber Aware



Update

- Best defense against viruses and other online threats.
- Keep your devices, security software, and web browsers updated with the latest patches.



Clicking

- Be wary of email and online advertising links.
- This is a common way criminals can gain access to your computer.
- Remember if it sounds too good to be true, it probably is.



WiFi

- Be extra vigilant when using unfamiliar WiFi hotspots.
- Do not conduct sensitive work on public WiFi.
- Adjust your device security settings to limit who can access your device.



Deleting

- When in doubt, throw it out.
- If a link, email, tweet, post, online ad looks suspicious, even if you know the source, it's best to delete or, if appropriate, mark as junk email.