Recommendations for Minimizing Cyber Risk

Political campaigns and organizations share the responsibility for defending democracy against cyber threats. Our actions are critical in maintaining public trust in our elections and reducing the risk of cyber incidents.

As a crucial component in safeguarding our democracy, I want to remind you to take precautions to protect yourself and your organization from a cyber incident.

Recognized best cybersecurity practices for minimizing risk:

1) Implement a cybersecurity user awareness and training program that includes guidance on identifying and reporting suspicious activity or incidents.

2) Enable automatic updates for your antivirus and anti-malware software.

3) Maintain offline, encrypted backups of critical data, and regularly test the availability and integrity of the backups.

4) Monitor social media platforms for false or misleading election information.

5) Implement phishing-resistant Multi-Factor Authentication (MFA) for all services that access critical systems.

6) Implement password policies that require unique passwords of at least 15 characters.

7) Separate administration accounts from user accounts.

8) Create, maintain, and exercise a basic incident response plan and associated communications plans, including response and notification procedures.

9) Subscribe to credentials monitoring services to monitor the dark web for compromised credentials.

10) Apply the principle of least privilege to all systems and services so that the users only have the access to what they need to perform their jobs.

Other Resources:

- Cybersecurity and Infrastructure Security Agency (CISA) provides a comprehensive guide on best practices to detect, respond, and recover from a phishing attack. https://www.cisa.gov/sites/default/files/2023-06/StopRansomware_Guide_508c.pdf

- The Global Cyber Alliance (GCA) offers several free toolkits to help mitigate cyber risks. https://gcatoolkit.org/elections/

- Harvard Kennedy School's Belfer Center for Science and International Affairs published The Cybersecurity Campaign Playbook in 2018, which provides information and strategies for keeping campaigns secure.

If you detect suspicious activity:

In the event you observe or detect any suspicious activity, please alert law enforcement officials immediately and please contact my office with any important information. As a reminder, state law requires any entity that has access to voter data from the California Secretary of State's Office to report a breach of this information to our office immediately.

Should you have any questions or desire additional information, please contact my Office of Election Cybersecurity at electioncybersecurity@sos.ca.gov.

Sincerely,

California Secretary of State