





Securing Elections from Cyber Attacks

2

- ✓ Understand your online presence
- ✓ Establish lines of communication
- ✓ Secure your technology
- ✓ Ensure incident handling protocols are in place
- ✓ Inform your users to the threat





Securing Elections from Cyber Attacks

3

Understand your online presence

- Inventory social media accounts
- Review social media account security
- Monitor social media account activity
- Control access to social media (password management)
- Establish means for reporting misinformation





Securing Elections from Cyber Attacks

4

Establish lines of communication

- The FBI are a resource for reporting and actioning on incidents
- The Department of Homeland Security (DHS-CISA) offers many election-centric security services at no cost
- Your state fusion center is a hub for intelligence and action regarding cyber actors
- Elections is a shared responsibility, partnering with other election districts will help create a shared defense





Securing Elections from Cyber Attacks

5

Secure your technology

- Know what your critical systems are
- Know where your critical systems are
- Patch your systems
- Protect your passwords
- Pentest your internet facing applications





Securing Elections from Cyber Attacks

6

Ensure incident handling protocols are in place

- Have a strategy for dealing with phishing attacks
- Establish an Incident Responses Plan
- Establish a Continuity of Operations Plan
- Create an emergency contact list





Securing Elections from Cyber Attacks

7

Inform your users to the threat

- Organizational awareness announcements
- User security awareness training
- Sponsored phishing assessment
- FBI/DHS election security brief





Securing Elections from Cyber Attacks

8

Contact:

Michael Moore

Information Security Officer

Maricopa County

mmoore@risc.maricopa.gov