Elections Infrastructure ISAC®

Protecting Against Potential Russian Cyber-Attacks

Protecting Against Potential Russian Cyber-Attacks

Guidance for Election Officials

WHAT YOU SHOULD DO TODAY

- Join the EI-ISAC and/or MS-ISAC
- Join online at www.cisecurity.org
- No charge to join

Protecting Against Potential Russian Cyber-Attacks

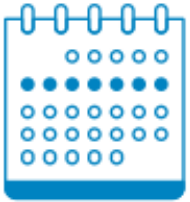
Guidance for Election Officials

WHAT YOU SHOULD DO TOMORROW

- Stop malicious internet activity with Malicious Domain Blocking and Reporting (MDBR)
- MDBR is provided at ***no charge*** to election offices
- Prevents users from connecting to known or suspected malicious sites
- Takes about 15 minutes to redirect domain name system resolution
- No other configuration or maintenance required

Protecting Against Potential Russian Cyber-Attacks

Guidance for Election Officials

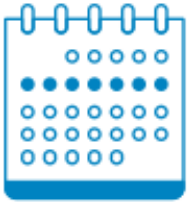


WHAT YOU SHOULD DO IN THE NEXT WEEK

- Turn on multi-factor authentication (MFA) for any system that offers it.
- MFA is a feature that comes with many systems.
- Level of effort: as little as 10 minutes.

Protecting Against Potential Russian Cyber-Attacks

Guidance for Election Officials

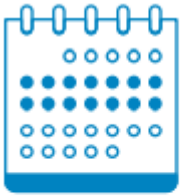


WHAT YOU SHOULD DO IN THE NEXT WEEK

- Make sure you have a recent vulnerability scan of externally facing IT assets.
- Install all possible patches and updates.
- Level of effort: minimal.

Protecting Against Potential Russian Cyber-Attacks

Guidance for Election Officials



WHAT YOU SHOULD DO IN THE NEXT TWO WEEKS

- Enable logging on any device that is capable
- Configure a log collection system
- Helps put the puzzle together:
  - Who the adversary was
  - How they got in
  - How long were they in the system
  - What did they do while in the system

Protecting Against Potential Russian Cyber-Attacks

Guidance for Election Officials

- Develop or update an incident response (IR) plan.
- Ensure systems are properly backed up and backups are protected from ransomware attacks.
  - Endpoint security