

Ransomware

Quick Reference Guide for Election Office Cyber Attacks



SPOT THE SIGNS

Know what a ransomware attack looks like so you know where to begin. This is not a full incident response plan, but a set of best-practice steps for those critical first minutes—or for when every second counts.



WARNING SIGNS



A screen displays a ransom note, a lock screen, or a countdown timer



Files suddenly have new extensions or won't open



Unusual pop-ups demanding payment or claiming your files are "encrypted"



A device is behaving erratically, is unusually slow, or restarts unexpectedly



Printers or shared systems suddenly stop working across multiple stations

1 Do not panic, do not pay, do not delete anything

Do not attempt to pay a ransom, follow on-screen instructions, or try to fix it yourself.

2 Disconnect, do not power off

If you can safely do so, unplug the network cable/turn off Wi-Fi on the affected device. Leave the device powered ON. Turning it off can destroy needed evidence.

3 Do not use the same network to communicate

Don't email or message coworkers about the incident from a possibly-compromised network or device. Use a phone or a device that is unaffected.

4 Notify your designated contacts immediately

See the back of this card for your contact list. If you cannot reach your state or local contacts, call CISA at 1-844-SAY-CISA (1-844-729-2472).

5 Contain and preserve (IT staff only, if applicable)

Identify next steps with your office's ransomware response plan. Isolate systems on the same network. Do not wipe, reformat, or reinstall anything. Photograph any evidence, and note the time it started.

6 Wait for guidance

Do not resume normal use of the affected system until the appropriate authorities advise it is safe.

Key Contacts & Resources

JURISDICTION:

ROLE	NAME	PHONE	NOTES
IT Support/ Security Team			
Election Office Supervisor			
County/State Election Official			
State Election Security Lead			
Local Law Enforcement <i>Non-Emergency</i>			
State Fusion Center			
Managed Service Provider <i>(if applicable)</i>			
Cyber Insurance Carrier <i>(Add policy # in notes)</i>			
Legal Counsel			

JURISDICTION NOTES & LOCAL PROTOCOL

ADDITIONAL RESOURCES:

*StopRansomware.gov: Government
ransomware resources and alerts*

CISA Report: 1-844-SAY-CISA

CISA Central: central@cisa.gov

*EI-ISAC/MS-ISAC: soc@msisac.org or
1-866-787-4722*

*FBI Internet Crime
Complaint Center: ic3.gov*

Access these
resources
and more:



Last updated:

Distributed by:

Poll worker and election staff use—Not for public distribution

