OHIO AUDITOR OF STATE
KEITH FABER

Cyber Incident Response

What to do if infected with Ransomware

1. If you believe you are the victim of a ransomware attack, immediately remove the infected computer from your network and/or the Internet. This can be done by removing your network cable or turning off the computer's WiFi connection. This will prevent the ransomware from attacking your network or share drives.
2. If you suspect other devices have been affected, you should isolate or power-off them as well. This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.
3. Immediately secure backup data or systems by taking them offline. Ensure backups are free of malware.
4. We strongly encourage you to contact a local field office of the Federal Bureau of Investigation (FBI) immediately to report a ransomware event and request assistance.

   Ohio FBI Field offices

   Cincinnati Office for Southern counties
   2012 Ronald Reagan Drive
   Cincinnati, OH 45236
   cincinnati.fbi.gov
   (513) 421-4310

   Cleveland Office for Northern counties
   1501 Lakeside Avenue
   Cleveland, OH 44114
   (216) 522-1400

   If a non-infected system is available, a cyber incident can be reported at the following FBI website: http://www.ic3.gov

5. Contact local law enforcement. Inform them that you have reported an incident to the FBI.
6. Contact your IT provider. Technical assistance will be needed to repair and restore your system.
7. Implement your business continuity plan while your system is being restored.

References:
https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view
https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise
https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf