

WISCONSIN ELECTIONS COMMISSION

212 EAST WASHINGTON AVENUE, 3RD FLOOR
POST OFFICE BOX 7984
MADISON, WI 53707-7984
(608) 261-2028
ELECTIONS@WI.GOV
ELECTIONS.WI.GOV



COMMISSIONERS

BEVERLY R. GILL
JULIE M. GLANCEY
ANN S. JACOBS
JODI JENSEN
DEAN KNUDSON

MARK L. THOMSEN, CHAIR

ADMINISTRATOR MICHAEL HAAS

DATE: December 8, 2017

TO: Wisconsin Municipal Clerks
City of Milwaukee Election Commission
Wisconsin County Clerks
Milwaukee County Election Commission

FROM: Michael Haas, Administrator
Tony Bridges, WisVote Specialist

SUBJECT: Ransomware Cyber Security Threat

Cyber security is a growing concern in not only elections, but in all aspects of local and state government. The Elections Commission is aware that many municipalities throughout the state may not have access to cyber security information through a municipal IT department. Therefore, the WEC is developing additional training and guidance regarding cybersecurity and the vital role it plays in elections administration, which will include cyber security updates and resources to municipal clerks. It has come to our attention that a municipal clerk has been the victim of a cyber security threat known as “ransomware.” More information on this threat and steps you can take to avoid it are available below. **Given the recent ransomware incident, and the immediate risks that potential ransomware attacks pose to all governmental agencies and the data they secure, please give this information your prompt attention.**

One of the challenges of cybersecurity is that malicious people regularly come up with new ways to attack systems and users. The past few years have seen a rise in a particularly insidious threat called ransomware. Ransomware is a piece of software that, once on your computer, encrypts all your files so that you can't access them. Everything on your drive and any connected drives you might have are immediately lost. Then the program displays a message informing you that all your data has been encrypted, and that to decrypt it you must first pay some amount of money to an anonymous account. This notice will be deliberately frightening, and often includes a timer to try and push you into an emotional decision.



If you do pay the ransom, the attacker may or may not decrypt your data so that you can access it again. Sometimes they take your money and do nothing. In some cases, they never had the means to decrypt your data in the first place. They will almost certainly spread the word to other hackers that you paid, making you more likely to be a target in the future.

Ransomware attacks have managed to bring down a wide variety of targets, from Great Britain's National Health Services to police departments and municipal clerks. If it should happen to you, the best thing you can do is to stay calm. Contact your local law enforcement. Using ransomware to attack other computers is a federal crime and the FBI will investigate and, if possible, prosecute the perpetrator. If the affected computer or computers contains election or voter-related data, or is used to access WEC systems, you should also notify the WEC so that we can take steps to protect our systems and other users.

Fortunately, the best practices for avoiding ransomware are the same as for most other cybersecurity threats. The attacker must first get the program on your computer. You can prevent this by keeping your software, especially your browser and email client, patched and up to date. Do not open suspicious emails or click on suspicious links. If you receive an attachment that you were not expecting from a colleague or other trusted source, contact that source through another means such as calling them to verify that they sent the attachment. If you have questions about an email or a link, contact your IT department. If you do not have an IT department, you can contact the Elections Help Desk at elections@wi.gov or 608-261-2028.

Software like anti-virus programs or firewalls can also help keep you safe. Anti-virus programs scan files on your computer to determine if they contain any known threats. Firewalls make it harder for attackers to directly access your computer. If you have the resources, you might also consider internet proxies or email security appliances. These will investigate emails and links before you click on them, and prevent known threats from ever reaching your computer.

It is also strongly recommended that you keep regular backups that are not connected to your computer. There are many online backup services that can be used for this, or you can copy files to a thumb drive or external hard drive that you do not keep connected to

your computer. That way if you do get infected by ransomware, you will not have to worry about losing your data.

If you have any questions regarding this process, please contact the Elections Help Desk at **elections@wi.gov**.