Wisconsin Elections Commission

212 East Washington Avenue | Third Floor | P.O. Box 7984 | Madison, WI 53707-7984
(608) 266-8005 | elections@wi.gov | elections.wi.gov

DATE: October 22, 2020

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

FROM: Meagan Wolfe
Administrator

SUBJECT: Election Cybersecurity Reminders

1. **Purpose**. As we proceed through the 2020 election cycle, we continue to stay alert on the impact cybersecurity has with keeping our elections secure. Following basic cyber security practices will help protect you from potential threats. These are just reminders and resources we want to bring to your attention as we enter the final weeks before the 2020 General Election.

2. **Required Action**. Ensure you and your organization are following these best practices:

A. E-Mail Safety. E-mail is the most common entry point for cyber-threats.

1) Use caution opening emails from people you do not recognize, or emails with suspicious subject lines, links or attachments. Human nature is generally trusting so being skeptical may mean going against your first instinct.
2) Avoid clicking on links or attachments that come from sources you do not recognize or are not expecting. If someone responds to your three-month-old email by sending a link or an attachment, call them before clicking.
3) Check with your email provider to see if you can use Multi Factor Authentication (MFA) to protect your email account.

B. Passwords Use complex passwords (i.e. use a long phrase, instead of a word), and implement Multi Factor Authentication if possible. Do not reuse the same password in multiple places. Consider using a password manager, but do not store passwords in a browser or any other application not specifically designed for it. For instructional videos on these topics, please see the resources section of this memo.

C. Regular Backups. Backing up your computer is the best defense against ransomware. Backup or copy any data/documents onto a separate drive that is then disconnected from your computer and stored in a safe place. For Windows users, type “backup” in the bottom left corner of your screen’s search box or see the additional resources page for a collection of how-to resources. You may want to work with your IT provider for assistance.

D. Update Software & Restart Frequently. Software updates protect you from known vulnerabilities.

1) Protect your computer by turning on automatic updates. Since some updates are not applied until your computer restarts, it is a good idea to shut your computer down when you are done using it for the day or restart it regularly. Leaving a running computer unattended for days or weeks hampers your ability to contain or notice an incident. Restarting your computer also protects it by clearing certain items such as typed usernames and passwords that remain in memory until a restart.
2) Update any and all software that is on your computer. Outdated software such as internet browsers (even programs you don't use) are entry points for attackers to compromise your system. A link to Microsoft's guidance on updating software is on the following page.

E. Upgrade to Windows 10. As of January 14, 2020, Microsoft no longer provides free security updates and support for the Windows 7 operating system. If you continue to use Windows 7 your device is at serious risk for security threats and viruses. Systems using Windows 7 or other operating systems no longer supported by their developers are not authorized to access WisVote. There is additional information about this change in the clerk communication dated August 28, 2019.

F. Research services provided by DHS. The Department of Homeland Security (DHS) provides several free cybersecurity services to local governments. The division of DHS responsible for this support is called the Cybersecurity and Infrastructure Security Agency (CISA). A description of three popular services can be found in Attachment 1.

G. Consider Free DDOS Protection. In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim's website originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source. There are anti-DDoS services out there and you can find additional information about that on attachment 2.

H. Enroll in RAVE. RAVE is a mass notification system maintained by the WEC that can be used to send calls, emails, and/or texts to clerk's offices and to any other contact information volunteered by the clerk. Once enrolled in the program, clerks can update their contact information, preferences, and opt out of alerts at any time. WEC will be able to provide targeted alerts regarding security threats, Election Day emergencies, WisVote outages, and other emergency situations

3. **Resources**. For additional information on the actions above, you may wish to visit these links from Microsoft and the Global Cyber Alliance. As well, there are attachments about Distributed Denial-of-Service and acquiring services from the Department of Homeland Security (DHS).

Microsoft's instructions on how to enable automatic updates for your computer:
https://support.microsoft.com/en-us/help/17154/windows-10-keep-your-pc-up-to-date

Wisconsin Elections Training video on password complexity: (requires login)
https://electiontraining.wi.gov/mod/scorm/view.php?id=367

The Global Cyber Alliance’s toolkit for password complexity, password managers and Multi Factor Authentication: https://gcatoolkit.org/smallbusiness/beyond-simple-passwords/

The Global Cyber Alliance’s toolkit for how to back up your computer: https://gcatoolkit.org/smallbusiness/defend-against-ransomware/

4. **Questions**. If you have any questions, please contact the WEC Help Desk. Call 608-261-2028 or e-mail elections@wi.gov.

Attachment 1

How to Request DHS Services

I. Background. The Department of Homeland Security (DHS) provides several free cybersecurity services to local governments. The division of DHS responsible for this support is called the Cybersecurity and Infrastructure Security Agency (CISA). A description of several popular services follows. NOTE: THESE SERVICES ARE UNLIKELY TO BE AVAILABLE BEFORE THE NOVEMBER GENERAL ELECTION BUT REMAIN HIGHLY RECOMMENDED FOR MEDIUM AND LARGE JURISDICTIONS.

II. Remote Vulnerability Assessments. This service scans internet accessible systems for known vulnerabilities on a continual basis. As vulnerabilities are identified, DHS notifies the locality so they may address the risk. This service is fully automated, and generates a weekly assessment delivered as a password-protected e-mail attachment. Because these reports are technical in nature, the WEC recommends they be reviewed with an IT professional. To request this service, clerks should e-mail vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services" to get started.

III. Phishing Campaign Assessment. The Phishing Campaign Assessment helps to train an organization's staff while measuring their susceptibility to social engineering attacks. Over a six-week period, the program will attempt increasingly sophisticated methods to gain access to local systems. At the conclusion of the assessment, localities are provided a detailed report that provides guidance and justifies resources needed to defend against phishing attacks. To request this service, clerks should e-mail vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services" to get started.

IV. Remote Penetration Testing. This is a six-week program that simulates the tactics and techniques of real-world threats. A dedicated team of professionals will perform a customized assessment and provide a detailed written report with recommendations. Note that there is a waiting list for this service. To request this service, clerks should e-mail vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services" to get started.

V. Regional Resiliency Assessment Program (RRAP). Each RRAP project typically involves a year-long process to collect and analyze data on the critical infrastructure within the designated area, followed by continued technical assistance to enhance the infrastructure's resilience. Projects can incorporate opportunities for valuable information and data exchanges, including: voluntary facility and security surveys; first responder capability assessments; targeted studies and modeling; subject matter expert workshops. For more information, please send an e-mail to Resilience@hq.dhs.gov.

Attachment 2

Anti-DDoS Services (CloudFlare Athenian and Google Shield)

I. Background. Jurisdictions with larger networks should obtain protection from Distributed Denial-of-Service (DDoS) attacks. In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim's website originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source. A DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, thus disrupting business.

II. Solutions. Several companies provide anti-DDoS services. Two of the most popular are CloudFlare and Google.

A. Cloudflare Athenian. Cloudflare launched the Athenian Project to provide free Enterprise-level service to election and voter registration websites run by state and local governments in the United States. To sign up for the Athenian Project, visit their website at: https://www.cloudflare.com/athenian/

B. Google Shield. Google's service was designed to protect news, human rights, and elections sites with protection from DDoS attacks. This service is free. Jurisdictions must apply on line through the project's homepage. Ensure you identify as providing official election information. Their homepage is https://projectshield.withgoogle.com.