MIIA Cyber News - September 2023

September 8, 2023

Dear Members,

In this newsletter:
- 2023 Municipal Cybersecurity Summit
- New Alert from KnowBe4 - Threads
- Why are municipalities so vulnerable to cyberattacks?
- Municipal resources to enhance your cybersecurity

SAVE THE DATE!
The MassCyberCenter will hold its third annual Massachusetts Municipal Cybersecurity Summit on October 5 in Worcester.
The free day-long event features cybersecurity experts from state and federal agencies and the private sector, who will give municipal officials and employees a better understanding of pressing cybersecurity issues, the current threat landscape, and state and federal initiatives. It will also provide practical ideas, information and resources for improving cybersecurity.
REGISTER HERE

New Alert from KnowBe4 - Threads
Recently, Meta launched a text-based social networking app called Threads. Deemed the "Twitter killer", since it functions almost identical to X formerly known as Twitter, it's becoming the perfect phishing opportunity for cybercriminals. **KnowBe4 warns spoofed domains are posing a cyber risk.**

Why are municipalities so vulnerable to cyber attacks?

Municipalities have become the third largest industry target for ransomware attacks. IT experts have identified some of the common threads contributing to this alarming statistic.

Exploitation of RMM Platforms
- According to CISA, the continued exploitation of RMM platforms by ransomware actors presents a growing risk to small and medium-sized organizations that support national critical functions. To combat this threat, on August 16, 2023, CISA released the **JCD** (Joint Cyber Defense) Remote Monitoring and Management (RMM) Cyber Defense Plan which provides cyber defense leaders in government and industry a collective plan for mitigating threats to the RMM ecosystem. **Read More**

Three municipal trends
Recently, a cyberattack forced Prospect Medical Holdings, to shut down its computer network causing sixteen hospitals and over 165 facilities to go offline. As attacks such as this continue to increase, three trends are leaving towns and cities increasingly more vulnerable.

- Under investing in cyber security
- Relying on outdated software
- Not switching to a .gov account

KnowBe4 offers the following tips on how to avoid ransomware scams

- Only download apps from trusted publishers. Anyone can publish an app on official app stores or sites - including cybercriminals.
- Before you click a link, always hover your mouse over it. Watch out for spelling mistakes or suspiciously long URLs that can hide a website's true domain.
- Keep your devices up to date. Software updates often include security patches to protect you against known vulnerabilities.

Municipal Resources to Enhance Your Cybersecurity

CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience.

CISA Tabletop Exercise Packages (CTEPs) are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios.

Read More

MasscyberCenter- The Center leads two working groups Cyber Resilient Massachusetts and Cybersecurity Training & Education to facilitate better cybersecurity planning and collaboration and promote resiliency and workforce development for the Commonwealth.
- Minimum Baseline of Cybersecurity for Municipalities
- Cybersecurity Toolkit

Zywave- Ransomware Survival Guide
Contact Mary Ann Marino at mmarino@mma.org to register for Zywave, MIIA's content platform to access this guide and other related content.

MIIA CyberNet. MIIA's online member cyber resource and training platform. To register for the platform contact Mary Ann Marino at mmarino@mma.org

VC3 is the IT partner that focuses on municipalities.

Municipalities Expert IT and Cybersecurity Insights

MS-ISAC The mission of the Multi-State Information Sharing and Analysis Center® (MS-ISAC®) is to improve the overall cybersecurity posture of U.S. State, Local, Tribal, and Territorial (SLTT) government organizations.

MIIA
Risk Management
Work Safe. Be Safe.