Beware of Phishing Emails and Suspicious Links

Colleges,

As part of my ongoing efforts to maintain cybersecurity within the Municipal League, I would like to take a moment to remind everyone about the importance of staying vigilant when it comes to email security.

Unfortunately, phishing attacks and other forms of cyber threats continue to pose significant risks to organizations worldwide. One of the most common methods used by cybercriminals is to send deceptive emails containing malicious links or attachments. Clicking on these links or downloading these attachments can result in serious consequences, including data breaches, malware infections, and financial losses.

To protect ourselves and the Municipal League from these threats, it's crucial that we all remain cautious and exercise good judgment when interacting with emails. Here are some important tips to keep in mind:

1. **Be Skeptical:** If you receive an email from an unfamiliar sender or one that seems suspicious in any way, exercise caution. Look for telltale signs of phishing, such as generic greetings, spelling or grammatical errors, urgent requests for personal information, or unexpected attachments or links.

2. **Verify the Sender:** Before clicking on any links or downloading attachments, take a moment to verify the authenticity of the sender. Check the email address carefully to ensure it matches the official email addresses used by our organization. If you're unsure, reach out to the supposed sender through a separate communication channel like a phone call, to confirm the legitimacy of the email. (ex: **Shari Veazey <govstaff06@gmail.com>**) That is not Shari's email address, but you may not look at the username or the domain so make sure you always watch out for that.

3. **Hover Before You Click:** Before clicking on any links within an email, hover your mouse cursor over them to preview the destination URL. Pay attention to whether the URL looks legitimate and matches the expected website. If it looks suspicious or unfamiliar, refrain from clicking on it. (ex: https://www.mmlonline-phishing.com - that is fake It will take you to a phishing website. https://www.mmlonline.com - that is real.)

4. **Think Before You Act:** Never provide sensitive information, such as passwords, account numbers, or personal details, in response to an email request. Legitimate organizations will never ask you to disclose such information via email. If you're unsure about the authenticity of a request, contact the relevant department or individual directly using verified contact information.

5. **Report Suspicious Emails:** If you receive an email that you believe to be a phishing attempt or otherwise suspicious, report it immediately to our IT department. They can investigate further and take appropriate action to mitigate any potential risks.

By incorporating these practices into our everyday exercises, we will better guard ourselves and our virtual belongings from cyber threats. Remember that cybersecurity is a shared responsibility, and each one of us performs a role in retaining secure online surroundings. If you are ever unsure about anything, please ask!

Thanks,
Austin