Colleagues,

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 identifying spoof emails and protecting our data from potential threats.

Spoof emails, also known as phishing emails, are deceptive messages designed to trick recipients into revealing sensitive information or performing actions that could compromise our security. These emails often impersonate legitimate sources such as trusted organizations, colleagues, or even our own institution.

To help you recognize spoof emails and minimize the risk of falling victim to such scams, here are some key indicators to look out for:

1. **Sender's Email Address:** Check the sender's email address carefully. Spoof emails often use email addresses that resemble legitimate ones but may contain slight variations or misspellings.
2. **Urgency or Threats:** Beware of emails that create a sense of urgency or pressure you to act quickly. Threats of negative consequences or warnings about account closures are common tactics used by spoofers to manipulate recipients.
3. **Requests for Personal Information:** Be cautious of emails requesting sensitive information such as passwords, account numbers, or login credentials. Legitimate organizations typically do not ask for such information via email.
4. **Unusual Links or Attachments:** Avoid clicking on links or downloading attachments from unfamiliar or suspicious emails. Hover your mouse over links to preview the URL and verify that it matches the purported destination.
5. **Poor Grammar or Spelling Errors:** Pay attention to the language used in the email. Many spoof emails contain grammatical errors, spelling mistakes, or awkward phrasing that can indicate fraudulent activity.

If you receive an email that raises suspicion or appears to be a spoof, please follow these recommended steps:

1. Do not click on any links or download any attachments.
2. Do not reply to the email or provide any personal information.
3. Report the email to me by clicking the “Phish Alert” icon from within the message immediately for further investigation.
4. If you are not sure if an email is legitimate, please do not hesitate to ask me if it is real or not.

By remaining vigilant and staying informed about common spoofing tactics, we can work together to protect our organization's sensitive data and prevent cybersecurity breaches.

Thanks,

Austin