Importance of Good Cybersecurity Practices

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 good cybersecurity practices not just within the Municipal League but also outside the Municipal League.

As our reliance on digital technologies continues to grow, it's essential to remain vigilant about cybersecurity. I know it's boring, but I would like to take a second to emphasize some desirable cybersecurity practices which could help protect the Municipal Leagues data:

1. **Strong Passwords**: Ensure that your passwords are complex, have special characters, and are not effortlessly guessable. Consider using a passphrase or a password supervisor to keep track of your credentials **SECURELY**.

2. **Two-Factor Authentication (2FA)**: Enable 2FA on any account that contains personal information, even if you do not think it would be compromised. This usually includes receiving a one-time code through a text message or Microsoft Authenticator app.

3. **Regular Updates**: Keep your operating device, software program, and antivirus programs up to date. Software updates regularly incorporate patches for security vulnerabilities that hackers take advantage of. Your IT admin should keep all office devices up to date, which I do, but if they are personal devices, please keep them up to date.

4. **Beware of Phishing**: Be careful of emails, texts, or messages from unknown assets inquiring about personal or financial data. Phishing scams are a common tactic used by cybercriminals to gain access to personal information. **NEVER SEND THEM MONEY** no matter how good the "deal" sounds.

5. **Public Wi-Fi**: Avoid accessing touchy records or conducting economic transactions over public Wi-Fi networks, as they may be often unsecure and liable to interception. **If you ae out on a business trip, use your hotspot when accessing the VPN in the office.**

6. **Data Backup**: Regularly backup your important files and information to an outside tough pressure or a cloud-primarily based carrier. This guarantees that you may recover your information in case of a cyberattack or hardware failure.

Importance of Good Cybersecurity Practices

7. **Privacy Settings**: Review the privateness settings in your social media money owed and other online systems to govern who can get the right of entry to your statistics. Make sure you do not allow apps to track as shown in the attached picture.

8. **Cyber Hygiene**: Practice appropriate cyber hygiene with the aid of logging out of apps when not in use, not clicking on suspicious links or attachments, and being conscious of the facts you share on-line.

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