In Your Inbox

Insights, Advisories and Alerts

Vol. 2, Issue 4 | April 2026

Reduce Your Risks by Enabling Multifactor Authentication

Cyberattacks against local governments are increasing. Such attacks often begin when a cybercriminal gains unauthorized access to systems and data by obtaining an employee's password through methods such as phishing, malware, or automated guessing tools.

An easy and effective way to prevent attacks against your municipality is to enable **multifactor authentication (MFA)**, which adds a log-in security control to email, financial, and other operational systems. Simply put, MFA requires users of your systems to have a password plus a second identifier.

MFA can confirm a user's identity in several ways, including through:

- A fingerprint, facial recognition, or other biometric check
- A phone call asking for login approval
- A one-time code from an authentication app
- A one-time code sent to the user's phone

Why MFA Matters

Cities and towns rely on email and other online systems to conduct daily business, including systems that manage finance, payroll, and document storage. If a cybercriminal gains access to one of these systems, they may be able to read sensitive data, send fraudulent emails, or use your municipality's information for nefarious purposes.

If your municipal systems only require a password, an attacker can more easily gain unauthorized access.

MFA is a strong tool to defend against many of these incidents because **the attacker needs the second verification step**, such as a code sent to the employee's phone or authentication app. Without this second factor, the attacker's login attempt fails.

Remember:

- **Password only**: If a password is stolen, an attacker can gain unauthorized access to your systems.
- **Password + MFA**: The attacker needs a second piece of information to gain access to your systems.

Many commonly used applications already offer MFA. Nearly all major banks and financial institutions, as well as platforms such as Microsoft Office 365, Google, and Amazon include MFA options. Many other municipal software systems support it as well. In many cases, enabling MFA is a **low-cost or no-cost security improvement** that can significantly reduce the risk of unauthorized access to your municipality's sensitive data.

MFA Tips

MFA is very effective, but users should follow a few basic rules:

- Never share your MFA code with anyone.
- Do not approve login requests you did not initiate.
- Report suspicious login prompts or emails to your IT department or vendor.

Other Cybersecurity Recommendations

You can take additional steps to improve your data security.

- Conduct a cybersecurity risk assessment to determine security gaps in systems and networks.
- Implement prevention strategies such as strong passwords, multifactor authentication, encryption for laptops, thumb drives, and mobile device policies.
- Keep software updated.
- Train employees on ways to minimize risks.
- Back up data.
- Update IT/computer/cybersecurity policies and procedures.
- Obtain cyber liability insurance and keep the policy up to date.
- Develop a cyber incident response plan in case of a breach.
- Administer an effective offboarding plan that immediately disables an employee's access to email accounts and systems upon that employee's departure.

Learn More

For more information on multifactor authentication:

Microsoft Multi-Factor Authentication

Commonwealth of Massachusetts Multi-Factor Authentication

For more information on municipal cybersecurity:

Both the MassCyberCenter and the Executive Office of Technology Services and Security offer resources on municipal cybersecurity, including grants and technical assistance to help municipalities implement cybersecurity strategies.

MassCyberCenter - Municipal Cybersecurity

EOTSS - Office of Municipal and School Technology

*The OIG periodically issues **OIG In Your Inbox: Insights, Advisories and Alerts** as a way to succinctly share timely topics with key stakeholders, most notably the leaders within the Commonwealth's 351 local communities. The OIG hopes that **OIG In Your Inbox: Insights, Advisories and Alerts** will prompt dialogue and needed action on matters important to public entities.*