

# Why Municipalities Need a .gov Domain and Professional Email Provider

When you interact with a business, would it comfort you more if they had a professional email address (such as john.doe@professionalbusiness.com) instead of a consumer-grade email address (such as jdoe400@yahoo.com). While a legitimate business can certainly use a consumer-grade email address, a professional email address and domain just looks more reputable and professional.

This need for professionalism becomes more important when people deal with government.

For many, an important mark of legitimacy is the .gov email address, which has become expected and standard for government. .gov should be part of a professional email domain (such as john.doe@cityofexample.gov) that lends your city a stamp of legitimacy.

Where do you store your email data? Are you using a professional enterprise platform such as Microsoft 365? Or a consumer-grade email such as Yahoo or AOL? Such a decision can affect email delivery, records retention, and compliance.

In this article, we look at each email issue separately and offer you some ways to resolve them.

## Email Domain Issues When You Lack a .gov Domain

Several issues arise when you don't use a .gov email domain.

### 1. Loss of credibility and professionalism

It looks a little embarrassing for a municipality to use an aol.com or yahoo.com email address. After all, you're a municipality. The government of your city or town. Many one-person businesses have professional email addresses. You need to step up and do the same.

In addition to issues with professionalism, you also lack credibility when communicating with the outside world. With everyone's cybersecurity anxiety heightened today, it looks suspicious when an email comes from a city that says mayor204@aol.com rather than mayorjohndoe@professionalcitydomain.gov.

A .gov domain is recognized as an official government domain, which immediately signals to the public that communications are legitimate and trustworthy. Having a standardized .gov domain across all departments presents a unified and professional image. Residents are more likely to trust communications from a .gov address, especially in situations where they need to provide personal information or when responding to public notices or alerts.

### 2. Risk of spam filters trapping emails you send

Spam filters are more triggered by emails that are likelier to be malicious. For example, an email coming from an aol.com-type of email address will more likely trigger a spam filter to block it versus a professional email with a legitimate domain. You want to make sure your emails actually arrive in a person's inbox—and a .gov email domain decreases the chance of getting caught by antis spam tools.

## Steps to Acquire a .gov Email Domain

Here are some steps you can take to acquire a .gov email domain

### 1. Follow the registration process

You can apply for a .gov domain by visiting the official .gov domain registration website. The application process involves filling out a form with relevant details including your desired domain name, contact information, and verification of government status.

You must provide the official names and titles of those responsible for the domain, such as IT directors or municipal leaders. The General Services Administration (GSA) reviews the application and may request additional documentation or clarification. Once the application is approved, your municipality will receive instructions on how to configure and activate the domain.

### 2. Implement the domain

Implementation should be handled by IT professionals. Steps will include:

- **DNS Configuration:** Configure your Domain Name System (DNS) settings to point to the correct mail servers. This process usually involves working with your email service provider or IT vendor to ensure that email routing is properly set up.
- **Email Migration:** If your municipality is migrating email to use a .gov domain, existing email accounts may need adjustments. The ownership of the .gov domain must be verified and configured within the email provider's system (e.g. Microsoft 365). This process involves ensuring that your new .gov domain points to the correct mailboxes. It may also include exporting current email data and importing this data to existing or newly set up mailboxes to ensure a seamless transition. (While .gov is simply the new domain, it is separate from the mailbox itself, which can be accessed through multiple domains if needed.)
- **Testing and Rollout:** Before fully launching the .gov

domain, you should conduct thorough testing to ensure that all email functionalities are working correctly, including sending, receiving, and spam filtering. After successful testing, you can begin using the .gov domain for all official communications.

- **Security:** GSA guidelines exist about implementing security measures to protect your domain. IT professionals can handle this technical implementation.

Once your .gov domain is live, it's important to inform residents and stakeholders about the change. This can be done through public notices, website updates, and social media announcements.

Remember, your .gov domain needs to be renewed periodically. Keep your contact information up to date with the GSA to avoid any disruption in service.

## Email Platform Issues

The email platform you use has a huge impact on your municipality—for better and for worse. Let's look at some issues that result when you use a consumer-grade platform rather than an enterprise-grade professional platform.

### 1. Inability to follow laws and regulations

Without an enterprise-grade email platform, you may be limited in your ability to enforce records retention policies and comply with open records laws. For example, think about the following scenarios:

- You receive an open records request that involves retrieving information from a disorganized employee's personal aol.com email account.
- You are required by law to retain records related to city business, but the ex-mayor and various former elected officials have personal email accounts with critical information that you must access.
- Litigation requires you to produce specific city records, and employees must submit to an audit of their personal email accounts.

While it's not impossible to follow records retention laws using personal email accounts, the process is incredibly messy and fraught with risk. There is no centralized way to manage records retention policies around emails and enforce archiving or deletion rules.

Using a reputable email service provider makes following records retention laws easier and more likely ensures compliance with cybersecurity standards.

### 2. Lack of email security

It's important for IT professionals to enforce password policies, detect suspicious user activity, and delete or deactivate email accounts if an employee leaves. Some security measures that are easier to oversee with an enterprise grade email platform include:

- Password best practices and multi-factor authentication

- Access and authorization to sensitive and confidential information
- Encryption
- Antispam and phishing protection
- Data backup and disaster recovery
- Protection against viruses, malware, and ransomware

### 3. Lack of control over email information

This is a huge risk related to personal email accounts. When a mayor, councilmember, or employee leaves, they take their email with them. So what happens if you need to produce one of their emails or search that account for a piece of information? It walks out the door.

Also, you cannot control data privacy around that email information, easily transfer that information over to a new email account or database, or deactivate a user when they leave. With a reputable email service provider, you can retain all email despite an employee leaving, deactivate their account, and control how that email information is stored and transferred.

It's highly inadvisable to use a Yahoo, AOL, or other free consumer-grade email service as your email service provider. Work with a municipal-experienced managed service provider or IT professional to help you pick an email service provider that can provide you with the features and security required of a municipality.

**Enhanced Security:** Reputable email service providers employ advanced filters to detect and block spam and phishing emails, protecting municipal employees from malicious attacks.

**Reliable Performance:** Reputable email service providers guarantee high uptime percentages (often 99.9% or higher), ensuring that email services are consistently available.

**Compliance and Data Privacy:** Your email service provider should provide you the tools to comply with laws and regulations such as open records requests.

**Robust Support and Maintenance:** A robust email service provider makes it easy to keep your email system up to date with the latest security patches and features, reducing vulnerabilities.

**Large Storage Capacities:** A reputable email service provider gives you ample storage space for emails and attachments, reducing the need for frequent archiving.

**Automated Backups:** A reputable email service provider will regularly back up your email data, ensuring that information is not lost in case of hardware failure or other disasters.

By partnering with a reputable email service provider, municipalities can enhance their security, ensure reliable communication, and comply with regulatory requirements. These benefits collectively contribute to more efficient and effective municipal operations, ultimately improving service delivery to citizens.