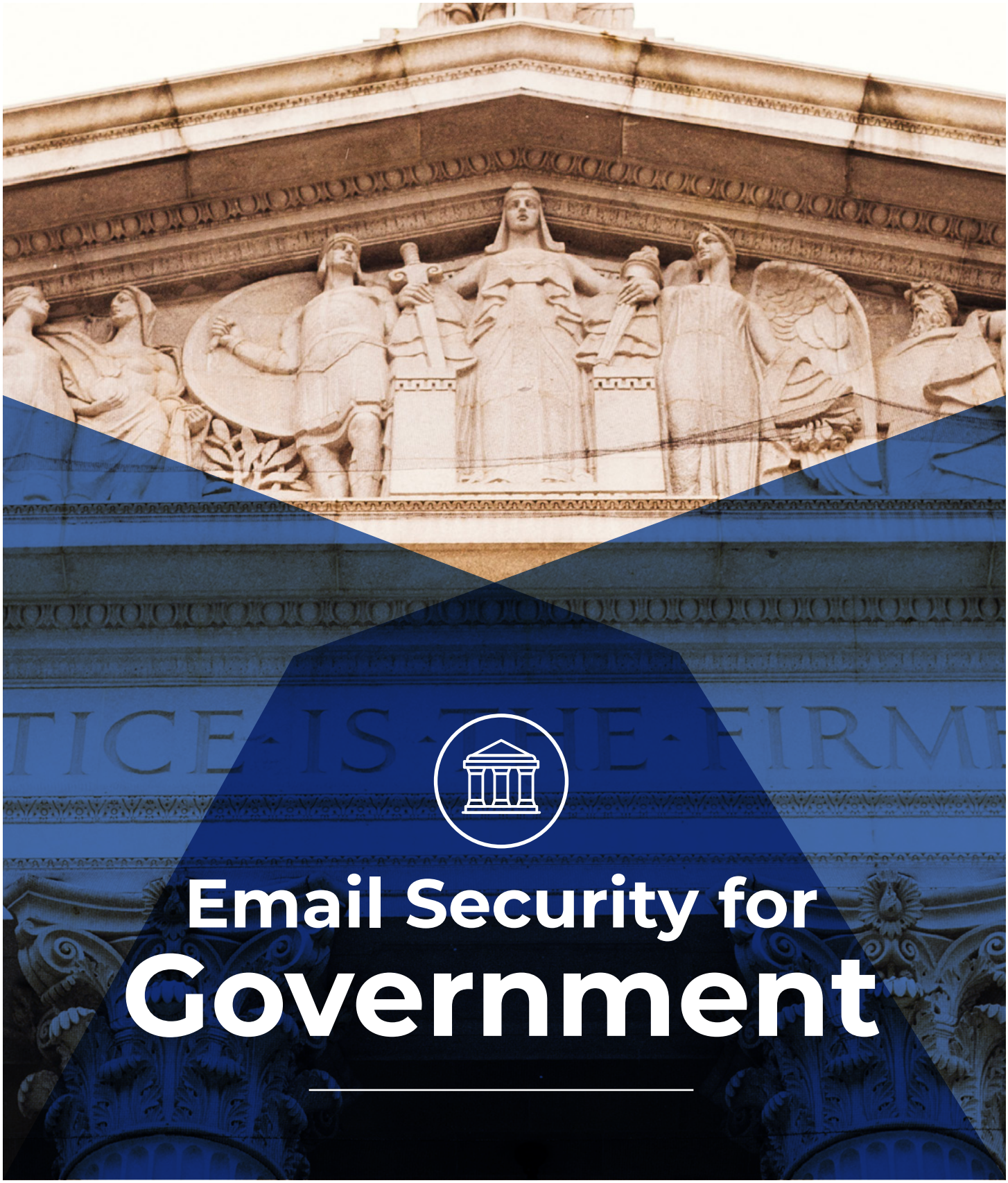


Email Security for Government

Trustifi

Governments all over the world are often uninformed in their cybersecurity knowledge and prowess. Many lack cybersecurity training in systems that prevent hackers from stealing their valuable information and data. Hackers are all too happy to ransack government agencies who may be unaware they are under attack.

With their outdated websites and antiquated systems, local governments are a prime target for hackers. Of all the possible attack vectors out there, the most commonly utilized one is email; as reported by **Verizon**, 92% of all malware is delivered via email. Many local governments believe they cannot afford most email security solutions, however that could not be further from the truth. Modern email security solutions can be scaled to meet the needs of a government agency with 5 or 50,000 employees.

Not only do governments have important citizen information, they also have highly classified information that could endanger the safety of an entire nation. Undercover agents could be exposed if an intelligence officer mistakenly emails a wrong party and could result in the deaths of those agents.

Many government agencies may believe that phishing schemes are a product of the past. We all remember the most famous phishing scheme, where a 'Nigerian Prince' would send you an email asking for help. He promised great rewards if help was delivered, but most people recognized this as a scam. Phishing schemes have only become more complex since those days.

Even large federal governments fall for phishing schemes. In January 2020, the Puerto Rican government sent $2.6 million to a fraudulent bank account. That is a substantial sum for a territory that has been in recession for the past 13 years. The governmental agency was fooled by a phishing email that told them to change a bank account for remittance payments. The U.S. military has also been the victim of successful phishing schemes as well.

Phishing for Government Information

The U.S. Federal Government uses anti-phishing software on its emails at a rate higher than any other industry. That should help you sleep at night, however more than 15% of federal agencies are not using any anti-phishing software. These agencies are easy targets for hackers to exploit.

> *How can government agencies hope to avoid the painful attacks from malicious actors?*

Trustifi has developed a comprehensive email security solution to help agencies defeat government phishers. The first part of the solution is an advanced rating detection system. When a user receives an email, an associated trustworthiness rating will be shown to help users identify if the email is a threat. The ratings can range from

‘Authenticated’ for a safe and legitimate email to ‘Spoofing Attack’ for emails where the attacker pretends to be someone else. Users will then be able to tell if the email sender can be trusted.

The second part of the solution is an inbound-protection system that works behind the scenes to protect your users. An easy way to think of this system is a water filter; it keeps all of the junk out, without the user having to do anything. Administrators can develop a comprehensive set of rules for that particular government agency, so you can decide which emails reach your users and which are removed before causing any potential harm. Once those rules are set up, any suspicious emails will be quarantined and will not reach the intended inbox.

Phishing is not the only issue that government agencies have to worry about. Employees accidentally forgetting to encrypt emails and attachments is another potential pathway for hackers.

Prevent Your Employees From Making Mistakes

Trustifi takes the guesswork out of encrypting emails by ensuring that every email that needs to be encrypted is. People are forgetful; there have been times when all of us have forgotten to send an attachment along with an email. That same kind of forgetfulness may cause an employee to not encrypt an email.

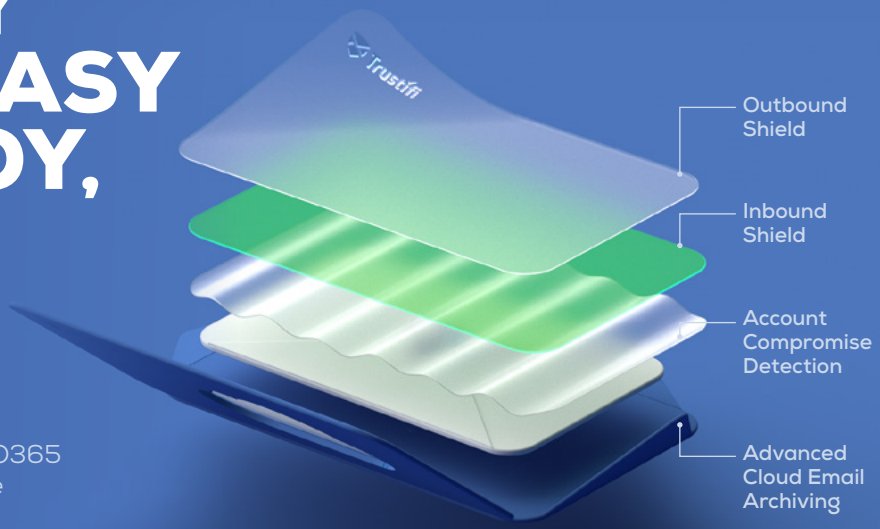
This is precisely why Trustifi developed an AI system to ensure that all emails with sensitive data are encrypted. Trustifi uses AI powered technology to scan all outgoing emails, identify sensitive information and data, and then automatically encrypt and lock the email. Administrators can decide exactly which type of sensitive information to look for, so you can make sure the data that is most relevant to your agency is protected. You can rest easy at night knowing that all of your sensitive government data will not fall into the wrong hands.

Trustifi also monitors emails in real time. When potentially sensitive information is entered, the user will be alerted to choose an encryption option. Administrators can also be alerted whenever an email is encrypted with sensitive information. This feature can help management understand who could use additional cybersecurity training. Trustifi uses a multi-factor authentication system to ensure that only the correct recipient opens the email. All of these solutions work in tandem to ensure your government does not fall victim to hackers.

www.**trustifi**.com

Trustifi

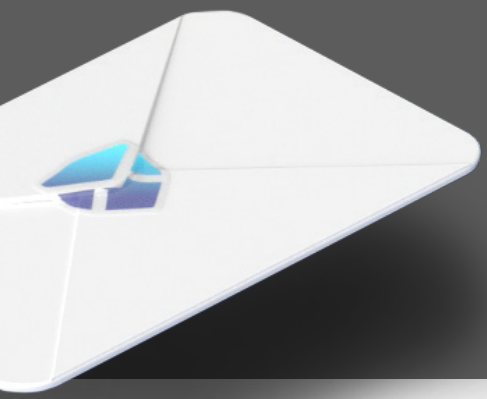
EMAIL SECURITY THAT IS EASY TO DEPLOY, MANAGE, AND USE



Easy integration with O365 and Google workspace

- Office 365
- Google Workspace

Customize a complete email security and compliance solution for your whole organization in minutes.



Outbound Shield

- Email Encryption and Recipient Multi Factor Authentication
- Data Loss Prevention and Email Data Exfiltration
- One-Click Compliance™

Inbound Shield

- AI engines to keep inbox clean
- Advanced Threat Protection
- Phishing and BEC Protection
- Stop SPAM and Gray Mail

Account Compromise Detection

- Instantaneously Identify Accounts that Have Been Compromised
- Automatically Block Access to Compromised Accounts

Advanced Cloud Email Archiving

- A cloud-based secure and convenient way to access emails
- Define controls and permissions to monitor and record user's activities
- Easily share data, cases and queries

Expert Insights ★★★★½ 4.8/5

Gartner peerinsights ★★★★★ 5/5

G2 ★★★★½ 4.8/5

Sales@trustificorp.com | +1 844-235-0084 | www.trustifi.com