Zoho eProtect

An admin's guide to setting up an organization's email security

ZOHO

Table of contents

Introduction

Email is the most commonly used medium for modern communication. Every important business transaction, new product idea, or partnership request leaves behind an email trail. With this in mind, threat actors across the globe are exploiting email to penetrate organizational defenses and gain access to sensitive data. This makes email the number 1 threat vector for advanced threats because it's the easiest path into a company's network.

An organization's admins need to be extra cautious when they're configuring their company's email security policies and settings. A single misconfigured policy or overlooked setting can open the door to data breaches, financial loss, and reputational damage.

This guide is designed to help IT administrators take control of their email ecosystem with a structured, security-first approach. Whether you're building protections from scratch or strengthening an existing setup, you'll find practical steps, key considerations, and proven configurations to safeguard your users and data. Use it as a blueprint to create an email environment that's protected from evolving threats and meets compliance requirements.

Email is the number 1 threat vector for advanced threats.

Why is email security important?

With email being the backbone of most business communications, it's crucial that all sensitive data is guarded with top-notch security measures. With the amount of importance placed on data, it's evident that data is the new currency and cybercriminals are looking for increasingly innovative ways to breach into an organization. A lack of focus on email security can affect organizations in many ways.

1 Data breach

Threat actors may gain access to email accounts and systems, leading to exposure of sensitive data. Because patented designs and business-critical information may reside in emails, cybercriminals may sell this data on the dark web for financial gains.

2 Loss of sensitive data

In a move to extract money or cause chaos among your employees, threat actors may even delete data from email accounts. When important files go missing, it can have far-reaching repercussions, leading to gaps in communication and confusion.

3 Huge financial losses

When threat actors penetrate your operation's defenses under the pretext of a legitimate entity, they reach out to finance teams to initiate payment transfers. When the recipient falls prey, the financial implications may cause huge losses for the company.

4 Legal repercussions

When customers' data or the operations of a company is affected due to a security incident, it could lead to failure of compliance with regulatory bodies. Companies may face legal repercussions or even class action suits, if such situations arise.

5 Lack of customer trust

Your customers place a certain level of trust when they decide to use your services. When they see that your defenses aren't strong enough, they lose trust in your company, leading to poor customer retention and severe reputational damage.

Factors to consider before setting up your email security

While setting up your company's email security, it's important to consider a few essential factors. This will ensure that you choose the right solution, set up the right configurations, and pick the best policies to suit your organization's needs.

The email environment

Your organization's email provider has certain built-in security controls. The new email security configurations you pick should work in tandem with the existing controls. To ensure that these configurations don't conflict with one another, carefully consider the policies you set up in both and test them to see that none of the configurations can be overridden.

You must also consider whether your email is hosted on the cloud or on premises. The security solution that you pick must work with your email provider and offer full-fledged support, irrespective of the mode of email hosting.

High-risk targets

Not all of your employees require the same level of security controls. The policies and restrictions for certain employees should be more stringent, based on the nature of their role. For employees working in the HR or finance teams, a higher level of protection may be required because they have the power to authorize transactions or send out organization-wide policy documents or announcements.

Similarly, C-suite employees also must have stricter security controls. These employees usually have the highest level of control. Protecting their accounts prevents any misuse or impersonation to perform or approve any sensitive operations.

Key security risks

Before you set up your security, it's wise to take stock of what your organization needs protection from. Go through your employees' reports, the existing quarantine reports, or the user-reported threats to get an idea of the different types of threats that your organization faces. This will also shed light on the commonly targeted users, and the common tactics used.

This uncovers specific areas of security that your organization needs to focus on. Based on the gathered data, you can configure policies and set up finer controls for commonly occurring security risks.

Compliance and regulatory requirements

Every organization has to comply with certain regional and industrial requirements, based on the nature of their work. Identifying the laws that you need to comply with, and listing the email and security mandates of these laws, can help with drafting the right policy. Based on the number of years the emails need to be retained and the steps to be taken in case a security incident occurs, you can configure the level of control your company needs.

User roles and access levels

In companies with hundreds or thousands of employees, it's not practical to have just one admin managing the security controls. Pick trustworthy, responsible employees to manage sensitive operations, such as policy changes, quarantine management, and others. Similarly, based on the role and access given to each employee, the security and access controls set for their account should also be enhanced.

Following the principle of least privilege ensures that your employees only have access to what they absolutely need. This way, information leaks can be avoided and users will deal with the data that's in their reach with the required level of caution.

Security awareness and user training

While setting up policies and security controls can help keep threats out of mailboxes, it's also important for users to be aware of emerging threats. Evaluate your employees' prevailing cybersecurity knowledge and give them adequate training to improve your security posture.

In addition to structured workshops, conduct periodic simulation exercises to test the efficacy of your trainings. If you find employees are still falling prey to phishing emails, conduct additional training. It's good practice to consider these factors before setting up or enhancing your security because it gives you an idea about the high-risk users. This will help you establish finer controls for such users.

Important configurations for your email security

Once you've assessed all of these factors, you can start setting up the security configurations for your employees.

1 MFA

Although MFA is well-known as the most simple and basic security measure that organizations can take, many businesses fail to understand the importance of adding an extra layer of security to their email accounts. In fact, 54% of SMBs fail to implement MFA for their businesses. When MFA is added as part of the login process, businesses can prevent unauthorized entries into their employees' mailboxes, even if their account credentials are leaked through other phishing or malware attacks. It's good practice to mandate this across the board.

54% of SMBs fail to implement MFA for their businesses.

2 Configure a strict password policy

With the prevalence of cyber incidents, most internet users are aware of the common password practices to follow. In spite of this, many users still believe that they won't be targeted in attacks and continue to use weak passwords or reuse passwords. A testament to this is the fact that 12345 is still the most commonly used password. Set up strict password policies in your email provider, making accommodations for password, age, reuse, mix of characters, and other provisions available.

> **"123456" was the most commonly used password globally, appearing over 4.5 million times .**

3 Set up SPF, DKIM, and DMARC protocols

Several email authentication protocols, such as SPF, DKIM, and DMARC, are common today. Configuring an action for emails that fail these checks adds extra security for your users' mailboxes. Sometimes, threat actors tamper with emails in transit, and the resultant email at the recipient end could be a spoofed email. Having strict policy controls to identify these authentication measures spots these emails before they can do any damage.

Beyond configuring policies for incoming emails, you also have the responsibility to ensure that all of the emails sent using your domain are authenticated. Configure SPF, DKIM, and DMARC policies for your organization's domains. Take time to go through the DMARC reports to take stock of who's sending emails on behalf of your domain. This helps you identify whether your organization's identity is being spoofed.

> **A DMARC report provides a daily summary of every email claiming to come from your domain and shows whether each message passed SPF and DKIM checks.**

4 Set up spam and phishing protection

Spam and phishing emails make up the bulk of email threats that an organization faces regularly. Setting up policies to handle them the right way is crucial. Configure the allowed lists, blocked lists, and the action to be taken on blocked emails. If your security solution allows finer controls, such as language and geo-location based allowed or blocked lists, configure them carefully as well. Email recipients often tend to click on links or engage with emails sent in foreign languages.

To spot and prevent phishing or spoofing, configure username and domain name impersonation protection. This ensures that your employees' identities aren't impersonated and misused by external entities. Because it happens while perpetrating CEO fraud or business email compromise attacks, it's vital to ensure essential protection measures are in place.

> Email recipients often tend to click on links or engage with emails sent in foreign languages.

Define actions for suspicious emails: While configuring anti-spam and anti-phishing policies, pay attention to the action settings. For highly sensitive configurations, set the quarantine or reject action. If users find these emails in their spam, there's still a chance that they engage with them.

Configure quarantine policies: The quarantine policies need to be monitored and handled regularly. For security-conscious users, you can permit self-moderation of quarantine emails. You can also configure quarantine reports so users are aware of any legitimate emails identified as suspicious.

Handle user-reported phishing: Take phishing or spam reports by users seriously. Take time to review them regularly and modify or iterate them based on the reports. These actions need to be taken immediately because cybercriminals target multiple employees at a time, and some of them may fall prey to the threat.

5 Configure alert banners

Use the alerts configuration option in your email security provider to set up alerts for attack types that you commonly come across in your email environment. This is particularly useful when not all emails of a certain type are malicious. Setting up a banner to display these alerts will ensure that your employees are cautious when they open such emails. Based on further inspection of any other malicious markers in the email, they can choose to engage with the email or report it as malicious.

6 Set up granular policies and rules

Granular email policies let you control message flow with precision, reducing both spam exposure and data loss risks. Define distinct inbound and outbound rules to manage external threats and prevent confidential data from leaving the organization.

Configure connection filtering rules to block or allow messages based on IP reputation, domain, or authentication results before they enter your network. Implement content filtering rules to inspect subject lines, body text, and attachments for sensitive keywords, file types, or malware signatures. By layering these policies, you create a flexible yet tightly governed email environment that adapts to evolving security needs.

7 Enable encryption for your emails

Email encryption ensures that sensitive messages remain private and unreadable to unauthorized parties while they're in transit or at rest. By enabling protocols such as TLS (Transport Layer Security) for message transmission and S/MIME or PGP for end-to-end encryption, you can protect confidential data from interception or tampering. Enforcing encryption across all mail servers and client applications safeguards against eavesdropping and also supports compliance with data protection regulations like GDPR or HIPAA, reducing the risk of data breaches and reputational damage.

Protocols such as TLS for message transmission and S/MIME or PGP for end-to-end encryption can protect confidential data from interception or tampering.

8 Monitor threat activity regularly

Once you've set up all of the policies and rules, continuous monitoring is critical to detecting suspicious patterns before they escalate into full-scale attacks. Administrators should track email traffic logs, authentication failures, spam filter results, and unusual sending behaviors to identify anomalies such as sudden spikes in outbound messages, repeated login attempts, or policy violations.

Leveraging built-in dashboards, SIEM integrations, or threat intelligence feeds provides real-time visibility into phishing attempts, malware delivery, and compromised accounts. Regular reviews of these insights enable quick remediation, fine-tuning of security rules, and proactive responses to emerging threats.

Leveraging built-in dashboards, SIEM integrations, or threat intelligence feeds provides real-time visibility into threats.

9 Mandate timely software updates

Keeping security tools, email clients, and your other software up to date is one of the simplest yet most effective defenses against cyberattacks. Regular patching closes known vulnerabilities and fixes configuration flaws. Establish a clear update policy that includes automated patch management and routine audits to verify compliance, reducing the window of opportunity for attackers to exploit outdated software.

Incident response and recovery planning

Even the most secure email environment can face breaches, phishing incidents, or account compromises, which is why a well-defined incident response and recovery plan is essential. Administrators should establish clear procedures for detecting, reporting, and containing email-related threats, assign roles and responsibilities for quick action, and maintain

communication protocols to keep stakeholders informed. Equally important is restoring affected accounts and learning from the incident to prevent recurrence. By formalizing these steps in advance, organizations can minimize downtime and build resilience against future attacks.

How can Zoho eProtect help?

Zoho eProtect is an email security solution that's built to provide enterprise-grade threat protection for all organizations, irrespective of the email provider that you've hosted your email with.

With eProtect, you get:

Advanced threat protection against phishing, spoofing, malware, and zero-day attacks.

Multi-layered filtering to block malicious attachments, links, and spam before they reach the inbox.

Real-time monitoring and threat intelligence to identify and stop evolving attack patterns.

User behavior analysis to detect account compromise, insider misuse, and negligent activity.

Detailed threat reports and insights that help IT teams understand attack trends, spot vulnerabilities, and make informed security decisions.

Easy integration with your existing email infrastructure for seamless deployment.

Conclusion

Securing your organization's email environment is an ongoing commitment. From defining user roles and enforcing authentication protocols to monitoring threats and planning for incident response, each layer of protection strengthens your defenses against an ever-evolving threat landscape. By implementing the configurations and best practices outlined in this guide and reviewing them regularly, you create a resilient email ecosystem that protects sensitive data.

This guide was released by Zoho eProtect as part of Cybersecurity Awareness Month 2025. eProtect is a cloud-based email security and archiving solution that provides advanced threat protection for all on-premise and cloud email accounts. eProtect is the security solution powering Zoho Mail, a platform trusted by millions of users.

Knowledge is the first step.
Protection is the next.

Discover how Zoho eProtect secures your email →