White Paper

INTRODUCTION

Since the commercialization of the Internet in the mid ’90s, email has been one of the most trusted business communication tools.

However, email has also become the most common cyber-attack vector in recent years. Attackers are constantly improving their attack mechanisms to deliver spam, inject malware, and launch phishing attacks or other email based threats undetected, with an intent to steal, alter, or destroy critical data and information systems.

In fact, according to SpamLaws, about 14.5 billion spam emails are sent every single day. That makes it about 45% of the world’s daily email traffic. While this figure is a general consensus, there are some spam traffic statistics that suggest as many as 73% of all emails are unwanted promotions, or malicious in nature. For a small-to-medium-sized business, this means receiving thousands of spam emails yearly, each with varying potential for financial and reputation loss.

With this white paper, Zoho intends to create awareness about the most common email-based threats that businesses face today and helps explore in depth the defense mechanisms that Zoho Mail's spam engine employs to ensure secure email communication and business continuity for its customers.

UNDERSTANDING EMAIL-BASED THREATS

According to the FBI’s Internet Crime Complaint Center (IC3), cybercrime costs $3.5 billion in losses in 2019 alone, with business email compromise (BEC) causing the most damage. To safeguard business as well as personal and business data, it is imperative to know the common email-based threat types. This can help avoid vulnerabilities and associated risks by taking necessary preventative measures.

The 8 typical email-based threats you need to know about

Spam: Unsolicited commercial email, or spam, is unwanted junk email sent out in bulk. Typically, spam is for commercial or advertising purposes, although some attackers use it for distributing malware and viruses. Targeted companies can expect to see a large influx of spam, leading to hampered productivity, security breaches, added bandwidth and storage expenses, disaster recovery expenses, and other issues.

Phishing: Phishing is a practice of sending fraudulent communications, most often targeted to hundreds or thousands of recipients, by someone posing as a legitimate institution, usually through email. The goal is to obtain sensitive information, such as usernames, passwords, and credit card details, often for malicious reasons. An advanced level of this tactic is called “spear-phishing”.

Spear-Phishing: This is a highly targeted to individuals in order to steal sensitive information such as passwords, account numbers, user IDs, access codes, PINs, or financial information from a specific victim, often for malicious reasons. To acquire these details, the attackers disguise themselves as a trusted entity, individual, friend, or acquaintance, typically through email or other online messaging.

Malware: Malicious software, commonly referred to as malware, is software developed & distributed as a script, usually, to exploit the normal functioning of any electronic device. Malware typically acquires a hold on the device, then starts deleting, corrupting, or encrypting files to demand a ransom .

Viruses: Viruses are a type of malware program that piggybacks onto a legitimate application code, then spreads itself from there. Software viruses are loaded onto a user’s computer without the user’s knowledge and perform malicious actions, destroy data, and slow down the system resources.

Ransomware: Ransom malware, or ransomware, is a type of malware with only one aim: to extort money from its victims. It prevents users from accessing their system or personal files and holds it for ransom before allowing the user to regain access.

Social Engineering: Social Engineering is an art of manipulating people to make them give up confidential information. This attack happens in one or more steps, although it begins by gaining the trust of the victim by phone, email, or even in person. Criminals use social engineering tactics because it's usually easier to take advantage of your natural inclination to trust than to find ways to hack your software.

Business Email Compromise: In BEC attacks, scammers impersonate an employee in the organization in order to defraud the company, its employees, customers, or partners. Attackers target employees who have access to the company’s finances or sensitive data, tricking them into performing wire transfers or disclosing sensitive information. These begin with an email, usually following social-engineering tactics and compromised accounts, which don't involve viruses or malicious links and attachments, making it hard to detect.

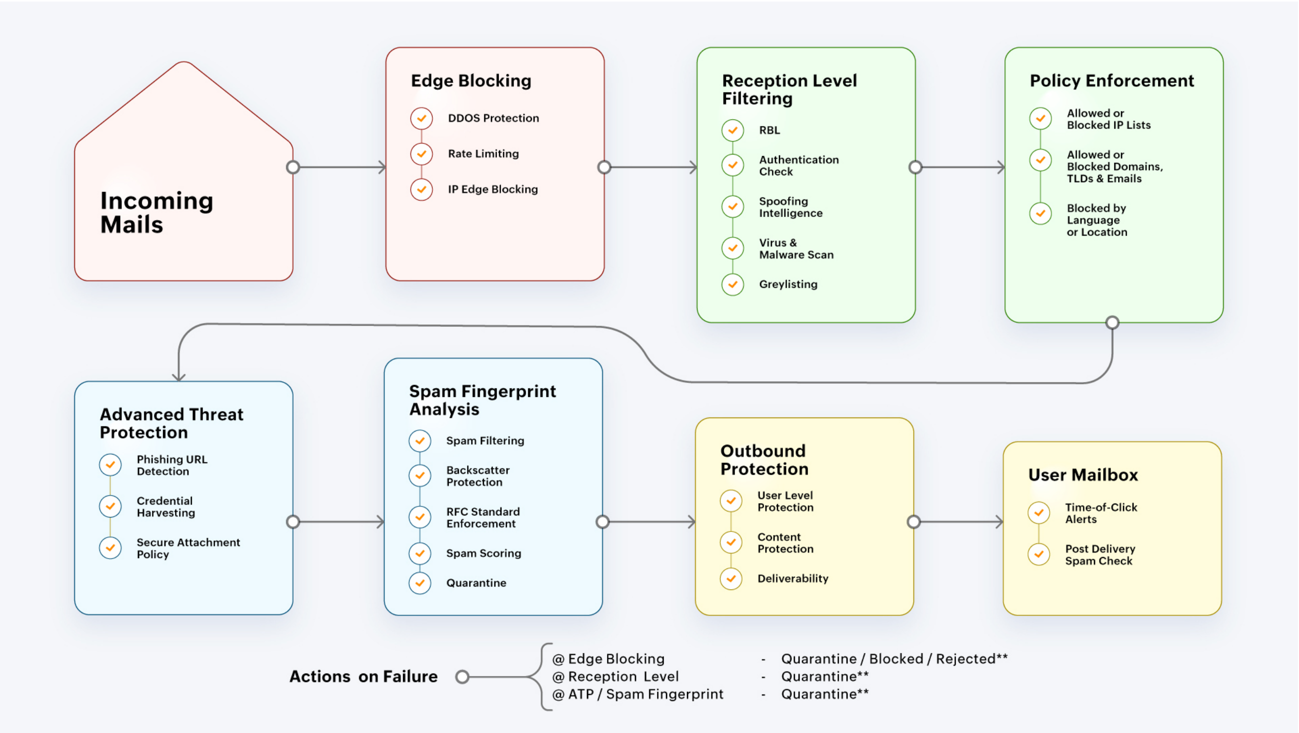
The growing variety of threats and the dynamics of today's cyberattacks demand a sophisticated and adaptable first line of defense to safeguard your organization from such email-based threats.

ZOHO MAIL'S COMPREHENSIVE EMAIL DEFENSE

Zoho Mail has a multi-layered anti-spam and email protection engine designed to detect unwanted and unsolicited emails and defend networks against email-based threats. Our approach to spam protection begins with *perimeter/edge protection* and goes all the way to *time of click spam protection* in the user's inbox, ensuring that your organization not only stays productive, but also protected from email-borne threats.

Cyber Resilience for Email - Zoho Mail’s approach to Email Security

Zoho Mail provides a robust, yet simple to manage protection from spam by combining the most effective spam elimination technologies into one cohesive, easy to-manage system. It combines connection analysis, local and global reputation, and advanced statistical and content analysis techniques that inspect all incoming and outgoing emails to protect users from diverse cyber-threats.



CONNECTION LEVEL FILTERING

A. Edge Blocking

- **Distributed Denial of Service (DDOS) Protection**

A DDoS attack is a type of DoS attack in which multiple hijacked systems are used to overload system resources or network bandwidths. These threats may render the email service unavailable, causing disruption in email accessibility. Zoho Mail acts as your first layer of defense against such threats by receiving all inbound emails, assuring that these threats never reach your network perimeter.

- **Rate Limiting**

Automated spam software is often used to send bulk emails to a single mail server. To protect the email infrastructure from email flooding, our spam engine throttles inbound emails for a period of time after the rate limiting threshold is exceeded. It will also block any further connection attempts from repeated offenders.

Rate limiting, ensures service availability while ensuring your user inbox is not flooded with spam.

- **IP Edge Blocking**

Next, the defense mechanism compares IP addresses of inbound mails against known offender lists, such as:

- Dynamic IP Block
  The dynamic IP block list is a public block list of malicious IP addresses or address ranges. Instead of blocking the user account, the spam engine blocks the originator IP address for their malicious email or failed login attempt using a different username and commonly used passwords for a specific period.
- Third-Party Reputation Check
  Third-party reputation services compile and manage lists of desirable or undesirable IP addresses. The spam engine uses these block lists and third-party reputation services as part of its protection system.

B. Reception Level Filtering

Once the emails are received for further processing, the following reception level checks are done to reject, quarantine, or tag spurious emails.

i. **Real-time Block List**

SMTP Real-Time Block List (RBL) is a mechanism for publishing the IP addresses of SMTP spammers. You can configure Zoho Mail's spam engine to utilize RBL servers to check the IP addresses of incoming requests against known or suspected spam-originating IP addresses.

Note: While SMTP RBL is an aggressive spam filtering technique and may show false-positive results as it is complied from the reported spam activity. To avoid emails from trusted sources being blocked by RBLs, add them to an Allowed List.

ii. Authentication Check

The Sender Authentication layer uses many frameworks, such as SPF and DKIM, while also analyzing emails based on DMARC policy to validate the authenticity of the sender with standard protocol checks and checks for domain name spoofing or other camouflaging techniques. Emails that fail these checks are classified as spam or spoofed emails, and the appropriate action is triggered to isolate them.

iii. Spoofing Intelligence

- Spoofing

  When someone or something pretends to be something else in an attempt to gain our confidence, get access to our systems, steal data or money, or spread malware, it is called Spoofing.

  Cousin Domain (look-alike domain) Spoofing and Display Name spoofing are other methodologies used by phishing tools to make a message look like it comes from a trusted source.

iv. Virus & Malware Scanning

The spam engine utilizes multiple layers for virus scanning and automatically decompresses archives for comprehensive protection. Virus scanning precedes over any other available scanning techniques and is applied even if the email passes through any other Connection Layers. This means even if an email comes from a “allowed” or “trusted” IP addresses or domains, emails are still scanned for viruses, and are blocked if a virus is detected.

v. Greylisting

If spam emails are received from IPs with very poor reputation, the system will automatically greylist the IP address, thereby reducing the amount of spam received.

C. Policy Enforcement

i. Based on IPs

Zoho Mail's spam engine lets administrators define a list of trusted mail servers by the IP address, thus, avoiding spam scanning for legitimate emails. Likewise, administrators can also segregate and organize a list of fraudulent email senders to block them further. In some cases, administrators may also prefer to utilize IP block range to limit specific email servers as a matter of policy instead of as a matter of spam protection.

ii. Based on Domains, TLDs and Emails

- Blocked List
  This lets you filter out sender addresses and domains from which you never want to receive email.

- Allowed List
  By approving senders, you can automatically allow messages from trusted mail servers or email addresses. Messages from approved senders or domains are not checked for spam or source reputation. However, messages from this list are still scanned for viruses.

- Trusted Lists
  Emails from email addresses that are added in the Trusted Emails List are delivered to the mailbox without any spam check. These emails will not be validated for SPF/ DKIM/ block list checks.

iii. Based on Location and Language

Some organizations expect never to communicate with particular countries or languages from which they receive a great deal of spam. Therefore, they use country-based or language-based filtering (or both) – a technique that blocks email from certain countries or languages. This allows you to identify and block spam emails based on the country of origin.

D. Advanced Threat Protection

i. Phishing URL Detection

This detection module scans incoming emails for known malicious hyperlinks. It enables real-time scanning of links, including links in email messages that point to downloadable content.

ii. Credential Harvesting

Malicious email campaigns use harvested credentials (username & password combination) to exploit the user’s email account or other accounts for additional malicious purposes.

iii. Secure Attachment Policy

The Secure Attachment Policy intends to protect the users from malicious files and attachments. Certain attachments containing executable/ program files may have destructive programs or malicious functions which perform phishing, spamming, or other malicious activities in the user system. To avoid such security threats, emails with certain types of files as attachments are blocked in Zoho Mail.

E. Spam Fingerprint Analysis

i. Spam Identification

- **Intent Analysis**
  Every spam email is sent with an 'intent' of receiving a reply, a call, or a website visit. With intent analysis, we identify the intention behind the string of emails received, and detect if it is spam. Typically, intent analysis acts as a defense layer that catches phishing attacks.

- **Content Analysis**
  The Zoho Mail's spam engine enables administrators to set custom content filters based on the subject line, message headers, message body and attachment file content. In general, administrators do not need to set their own filters for the purposes of blocking spam, as comprehensive analysis mechanisms are preconfigured and are constantly upgraded in Zoho Mail's spam engine to tackle evolving spam scenarios intelligently. This allowing DLP to maintain complete visibility and control, especially in the case of outbound emails.

- **Other Analysis**
  HTML Tag Based: Emails with a potentially harmful form, embed, iframe, or object tag can also land under the spam category if marked.
  Attachment Filters: The Attachment filter facility can reject or quarantine mails based on the attached file's extension. If any of it matches, the email will be directly rejected or marked as spam.
  Blocking attachments with macros: Certain malicious macros in attachments can be executed when opened. You can choose to block attachments that include macros.

ii. Back-scatter Protection

Back-scatter occurs when a spammer sends out spam or virus emails using a forged email address in the "From:" line or as the return path of their messages. This leads to thousands of bounce notifications or autoresponder emails, ending up in your mailbox. To combat back-scatter, Zoho ensures that only legitimate Delivery Status Notifications and Auto-responders get delivered to your accounts.

iii. Enforcement of RFC Standards

Many spammers use poorly written software or are unable to comply with the standards because they do not have legitimate control of the computer they are using to send spam. By setting tight limits on the deviation from RFC standards, Zoho allows you to reduce spam significantly.

iv. Spam Scoring

Once an inbound message has passed the initial Zoho Mail's spam engine block/accept filters, it receives a score for its spam probability. Based on this score, the Zoho Mail's spam engine can take one of the following actions:

- Block
- Quarantine
- Allow (inbound mail only)

v. Quarantine

The spam engine automatically quarantines spam emails, ensuring your inbox is free from any sort of threat. Such quarantined emails are held for 60 days, then dumped. Admins can view the message header of the email to check and recover any legitimate email that may have been quarantined.

F. Outbound Protection

i. User Level Protection

- **User authentication**

  To eliminate the risk of suspicious logins or spoofing, Zoho Mail's spam engine can be configured to perform SMTP authentication, building trust between the customer's email exchange and itself. This prevents spammers from sending mails as a user.

- **Reputation & Block List Checks**

  While IP reputation is important, domain reputation and email sender reputation are significant factors when it comes to deliverability. The higher the score, the more likely an Email Service Provider (ESP) will deliver emails to the inboxes of recipients on their network. If the score falls below a certain threshold, the ESP may send messages to recipients' spam folders or even reject them outright. Hence, various mechanisms to validate sender reputation are incorporated.

- **Rate Limiting**
  In order to prevent bulk spam emails getting through, smart rate limiting is enforced on the outbound emails. For instance, if a user hits the outbound sending limit within a time frame, they will automatically be prevented from sending out any more email until rolling count below the limit.

ii. Content Protection

- **Content & Intent Analysis**
  Custom content filtering based on the subject, headers, mail body, and attachment file type can be applied to outbound mail, just as it can be done for inbound mail. This further includes URL validation, virus scanning, phishing scan, detecting spam emails and emails soliciting sensitive information and pattern matching, and more, in order to prevent data leakage and ensure compliance.

- **Spam Scoring**
  Just like inbound emails, outbound emails are also assigned a score based on which the outbound email will be sent or blocked.

- **Outbound Quarantine**
  Quarantining the outbound message means that the message is suspected to be spam or in violation of the policy, and will be stored for the administrator to review and act upon.

iii. Deliverability

- **Increased Deliverability** (based on sender' IP reputation)
  Email delivery goes hand-in-hand with the sender's IP reputation. If you have multiple dedicated IP addresses or send multiple types of emails, it is advisable to separate your IPs into IP groups to better manage your sending reputation. Consistent volume of emails, fewer bounces and complaints, preventing spam traps, user interactions, and subscribing rates are some other factors that positively influence the reputation and deliverability.

- **Rate Limiting & Throttling**
  While rate limiting is applied to ensure that your email servers are not misused for spamming, throttling intelligently spools emails based on recipient email server deliverability, ensuring optimal deliverability.

G. Time of Click Alerts

The time of Click Alerts is an automatic email notifications sent based on a certain category of senders, such as unauthenticated senders or senders outside the contact list and senders external to the organization, as set by the administrator. It also alerts users about link-based malware and phishing attacks by analyzing the reputation of a URL at the time of click by users on their endpoints.

H. Post Delivery Filtering

While most of the secure email gateway providers tend to concentrate on preventing phishing, spear phishing, and malware from reaching end users, Zoho Mail's spam engine is effective in providing post-delivery protection as well, extending the defense even to the time of click and beyond.

CONCLUSION

Zoho Mail's comprehensive spam protection is your best defense against email-based threats. Bundled with its elegant web and native email clients, it offers the best-in-class cloud email experience, with enterprise grade mail security.

Our software is extraordinarily simple to set up and manage and provides many features, including 99.97% spam detection, virus and malware blocking, authentication control, outbound scanning, and robust reporting structures.