



Emailing in China

Email works in China, but it behaves differently: popular overseas services may be blocked, delivery can be delayed, and end-to-end encrypted email is not supported on Chinese networks.

If you travel to China or operate an office there, your goal is simple: keep business email reliable, professional, and predictable — while assuming messages can be read by third parties.



Foundation Being seen in China articles

Discovery Being found in China article

Execution Start trading in China articles

Focus: reliability + security

Audience: overseas businesses

Last modified: v5.1 – 16 October 2026

Why this matters

If you trade with China, email is still used for quotes, invoices, formal documents, and business introductions. However, email delivery and access in China can be disrupted by network controls, service blocking, and slower international connectivity.

Practical takeaway: Build an email plan for China that assumes delays, avoids blocked services, and keeps communications professional even when staff are using mixed email providers.

The basics of email delivery

To understand how email processing in China works, it helps to understand how email is sent in general. Below are the key “hops” where emails can be stored, scanned, delayed, or blocked.

Email between two people on a company email server

- The email is created on a local device (PC, mobile, etc.). When sent, a copy is kept locally and a copy is sent to the company email server.
- The recipient downloads the email using local software (IMAP/POP/ActiveSync). A copy is usually stored on the local device.
- Alternatively, the user reads and writes email directly in a browser (webmail). In this case, the email remains on the server rather than being stored locally.
- Company email servers normally use SSL/TLS, so emails cannot be read *in transit* between the user and the company server.

In this closed scenario, the business has strong control over security — but only if users follow the rules and avoid forwarding sensitive content to public services.

Sending emails outside the company server

When email leaves your company server, it can pass through multiple third-party systems.

- Your server forwards the email using TLS encryption between mail servers (“server-to-server TLS”).
- Mail may be routed through relay servers: datacentres, national gateways, cloud relays, or anti-spam filtering services.
- Even if TLS is used, emails can be stored and read on intermediate servers if those servers are accessed by third parties.

China reality: Assume third parties can store, open, and read email that travels on the public internet.

Email security options

1) An enclosed email service

This is a closed system where staff can only send and receive within the enclosed network. Remote users connect back to the central system over secure connections (VPN/SSL/TLS).



Quick checklist

Use this checklist when you travel to China or open an office.

- Is your email service accessible from mainland China networks?
- Do staff use company email for official communications?
- Are SPF, DKIM, and DMARC configured correctly?
- Do you avoid large attachments and heavy HTML emails?
- Do you have a local fallback (QQ/163/Aliyun) for travel?
- Do you assume emails can be read by third parties (no ETEE)?
- Have you tested delivery to/from Chinese domains (QQ, 163, etc.)?

Note: SSL/TLS protects email in transit, but it is not end-to-end encryption. Plan accordingly.

Need help?

If you want help testing email access from China and improving deliverability, contact support@accesstochina.com

Large companies and governments use this because it is very secure — but it is expensive and depends on correct staff behaviour.

2) End-to-End Email Encryption (ETEE)

ETEE tools such as PGP and S/MIME can ensure that only sender and recipient can read email content.

However, ETEE must be supported and allowed on the networks where you send and receive email.

Important: China's networks and email services do not support ETEE.

How email is used in China

- Many people use personal email and messaging accounts for business, not company email addresses.
- Free Chinese email services can be configured to use your own domain name (for example, QQ mail with a custom domain setup).
- Because staff may use mixed providers, verifying who works for which company can be confusing.

Service blocking and the Great Firewall

The Great Firewall controls internet access and blocks or restricts certain services. This can directly impact email access — especially if you depend on blocked public services.

- Most overseas public email services (for example Gmail) are blocked in China.
- If your business operates a dedicated email service on your own domain, it may not be blocked — but you should test from within China.
- If you travel to China or open an office, check with local contacts whether your email service is available.

Local providers used in China

Local providers are commonly used because they are generally more reliable inside China's network environment.

- **QQ Mail** (Tencent)
- **163 Mail** (NetEase)
- **Aliyun Mail** (Alibaba)

A practical option for travel is to create a QQ email account and forward email while you are in China.

VPNs and workarounds

A VPN can allow access to overseas services from China, but VPN use is heavily regulated.

- VPN providers must be government-approved.
- Unapproved VPN services may not work reliably and could lead to penalties.

Performance and delays

Even if email is not blocked, delivery can be delayed due to international connectivity.

- Large attachments and embedded media can be very slow to download from overseas services.
- Time-sensitive messages should be planned with delays in mind.

Best practices for emailing to and from China

- **Keep it professional:** if you operate an office in China, instruct staff to use the company email system for all published information.
- **Avoid sensitive topics:** especially political or Chinese government-related topics.
- **Use plain text:** avoid heavy HTML and large attachments to reduce delays and filtering.
- **Configure mail authentication:** SPF, DKIM, and DMARC reduce “spam” flagging and improve deliverability.
- **Test access from China:** do not assume your mail service works — verify from real networks.

Website testing tools: Test from inside China

Using your own company email server with SSL/TLS

Using your company email server with an SSL/TLS certificate can offer advantages — but it is not a guaranteed way to avoid Great Firewall issues.

Benefits

- **Increased control:** you control how email is sent, received, and stored.
- **SSL/TLS encryption in transit:** protects data between clients and your server.
- **Avoiding service blocks:** you are not relying on blocked public services like Gmail or Outlook.
- **International security standards:** easier to meet partner and compliance expectations.

Challenges

- **IP throttling/blocking:** your server IP can still be throttled or blocked if flagged.
- **SSL alone is not enough:** SSL protects in transit but does not hide metadata (sender, recipient, time) and does not guarantee privacy against interception.
- **Server location matters:** hosting outside China can still be slow; hosting inside China introduces compliance and localisation obligations.
- **Operational risk:** reliable email requires anti-spam hygiene, monitoring, and correct DNS configuration.

Recommended setup

- Use a trusted SSL/TLS certificate authority (Let's Encrypt is widely used and available).
- Configure DNS properly: SPF, DKIM, DMARC.
- Consider hosting close to China (e.g., Hong Kong or Singapore) to reduce latency while avoiding mainland hosting complexity.
- Monitor deliverability and whether Chinese ISPs are blocking or delaying your server.

Related: [Translate your website?](#)

Related: [How Name Servers \(NS\) and DNS operate in China](#)

 [Test a web page from China](#)

 [Download "Emailing in China" paper \(PDF\)](#)

Access to China — emailing to and from China: deliverability, reliability, and practical security.

Last modified: v5.1 – 16 October 2026

Written by Peter Heather

Hits: 18,622