Best Practice Checklist Series - Issue 4

Email Security and Solutions

Understanding the basics: A layperson's guide and checklist for overseeing IT.

Best Practice Checklist Series
An exclusive publication of Sandbox Technologies, Inc.

3868 W Carson St, Suite 316
Torrance, CA 90503
Tel. (424) 207-5130
www.sandboxtech.com

SANDBOX TECHNOLOGIES

Small Business Solutions
Enterprise GrowthPath®
EGP Secure®
EGP Cloud™
ConstructIT®

Table of Contents

Email Security & Solutions....3
When it goes wrong....4
- The Spoofed Domain....4
- The Password That Skipped MFA....4
- The Unapproved Phone....4
- The Exposed On-Premises Server....4
- Regulated Data by Email....4
- The common thread....4

What to Ask Your IT Manager or Provider....5
- Spam and Malware Pre-Filtering....5
- Content Scanning to Limit Legal Exposure....5
- Certificate and Transport Security....5
- DMZ Reverse Proxy....6
- SPF Published....6
- DKIM Enabled....6
- DMARC Configured....6
- Mobile Device Approval....7
- Legacy Protocols Disabled....7

Terminology....7
- What a DMZ reverse proxy does....7
- Why this earned its own section....7
- On-premises or the cloud....8
- SPF, the guest list....8
- DKIM, the tamper-evident seal....8
- DMARC, the instructions....8

© 2026 Sandbox Technologies, Inc.

Email Security & Solutions

An everyday doorway into your organization deserves careful protection

Email is a common route for attacks because it reaches employees and carries the organization's identity. Protection depends on authentication records, filtering, access controls and maintained services. Missing controls can enable fraud or data loss. The following situations are illustrative examples of gaps to review, not guarantees that any single setting will prevent an incident.

© 2026 Sandbox Technologies, Inc.

When it goes wrong

No single control stops every email threat, and that is expected. Email security works in layers, and each layer closes a specific gap. The point here is not to alarm. It is to show what a missing layer actually looks like in practice, so you can decide which gaps you are comfortable leaving open.

The Spoofed Domain

A vendor, or an executive, appears to email accounts payable with new wire instructions. The address looks right, because the domain publishes no rules telling receiving servers which systems may send on its behalf. The request is convincing, and the payment goes out.

The Password That Skipped MFA

An employee's password is phished. Multi-factor authentication is enabled, so the account should be safe. But an older mail protocol that does not enforce that second factor is still switched on, and the attacker signs in through it.

The Unapproved Phone

An organization has not applied appropriate authentication and device-access policies to its mobile mail clients. An attacker uses stolen credentials through an allowed weak access path. Modern mobile clients can enforce MFA and Conditional Access; verify the actual configuration.

The Exposed On-Premises Server

An organization runs its own Exchange server, published directly to the internet so staff can reach mail from anywhere. A new vulnerability is discovered, and automated scans reach the server directly, before a patch is available to install.

Regulated Data by Email

Under time pressure, a staff member emails a spreadsheet of Social Security or account numbers to keep a deal moving. There is no scanning layer to catch sensitive content on the way out, so nothing intervenes.

The common thread

None of these required a sophisticated attack. Each one exploited a specific setting that was never turned on, or a server left exposed when it did not need to be. Email security is not one product. It is a set of individual, checkable controls.

These risks call for tested controls and ongoing maintenance. Some improvements require licensing, equipment or specialist support. This issue helps identify missing or assumed protections.

© 2026 Sandbox Technologies, Inc.

What to Ask Your IT Manager or Provider

and how to know if the answers are good ones

You do not need to administer a mail system to oversee one. You need to know what to ask. A fuller primer on the on-premises mail gateway and DMZ reverse proxy, and on how the email authentication records work, is provided at the end for those who want the detail. First, the part that matters: run the checklist below with your IT professional. If any item is not marked green, it may warrant a closer look.

Spam and Malware Pre-Filtering

Is inbound email filtered for spam and malware before it reaches the mail server or cloud mailbox? Reducing clutter is the visible benefit, but the more important job is to strip malicious attachments and intercept the social-engineering messages designed to trick users into surrendering credentials, before those messages ever reach an inbox.

Compliant	NOTES:
Needs Attention	
N/A	

Content Scanning to Limit Legal Exposure

Are inbound and outbound messages scanned for restricted or sensitive content? Email was never designed as a secure channel for data such as Social Security numbers, card numbers, or account details, yet convenience tends to win when nothing enforces the policy. Content scanning can mask sensitive data, or reject a message and prompt the sender to route it securely, which reduces both exposure and legal risk.

Compliant	NOTES:
Needs Attention	
N/A	

Certificate and Transport Security

For on-premises mail, are certificates valid and supported TLS versions securely configured? A certificate binds an identity to a public key; the TLS protocol and negotiated keys protect traffic. Disable SSL and deprecated TLS 1.0/1.1. Use supported TLS 1.2/1.3 configurations appropriate to the platform. Transport encryption is not necessarily end-to-end message encryption.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

DMZ Reverse Proxy

For on-premises mail, has the exposed-service architecture been assessed? A properly configured reverse proxy can mediate supported web access and restrict direct backend connections. SMTP mail flow may use a separate gateway. Neither device guarantees that forwarded requests are safe; patching, monitoring and incident response remain essential.

Compliant	NOTES:
Needs Attention	
N/A	

SPF Published

Is an accurate SPF record published for legitimate sending services? SPF authorizes hosts for the SMTP envelope domain, which can differ from the visible From address. SPF alone does not authenticate that visible address; DMARC checks domain alignment.

Compliant	NOTES:
Needs Attention	
N/A	

DKIM Enabled

Is DKIM signing configured for legitimate senders? A valid signature associates a signing domain with selected message content and verifies its integrity. It does not establish the human author or guarantee safe content. Test signing and domain alignment for each sending service.

Compliant	NOTES:
Needs Attention	
N/A	

DMARC Configured

Is DMARC configured and monitored? Either SPF or DKIM passing with alignment to the visible From domain is sufficient. DMARC fails when neither aligned method passes. The domain requests monitoring, quarantine or rejection; receivers apply their own handling rules. Review legitimate senders before enforcing policy.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Mobile Device Approval

Do approved mobile mail clients enforce MFA and appropriate device or application policies? Modern authentication can support these controls. Exchange ActiveSync allow/block/quarantine rules can restrict supported clients, but are not a substitute for MFA or a complete control over every mobile app. Test actual access paths, licensing and exceptions.

Compliant	NOTES:
Needs Attention	
N/A	

Legacy Protocols Disabled

Are unnecessary mail protocols disabled and weak Basic authentication blocked? POP and IMAP can use modern OAuth authentication; the protocol name alone does not mean MFA is bypassed. Confirm each application's authentication, permissions and access policies, including service accounts and SMTP. Remove unused access paths and test required integrations.

Compliant	NOTES:
Needs Attention	
N/A	

Organizations that run their own internal mail server, rather than using a cloud service, take on the job of protecting a system that must be reachable from the internet. Best practice for that situation is to place a mail gateway between the outside world and the mail server, so inbound connections are inspected and filtered before they ever reach the server itself.

Terminology

What a DMZ reverse proxy does

A DMZ is a network segment separated from internal systems by controlled boundaries. A reverse proxy can receive supported web requests and forward them to a mail service while limiting direct backend access. SMTP may need a separate mail gateway. A proxy can forward malicious requests too: it does not replace secure configuration, prompt updates or monitoring. Design each exposed service and restrict paths between the DMZ and internal network.

Why this earned its own section

In March 2021, Microsoft disclosed the Exchange vulnerabilities commonly called ProxyLogon and urged immediate updates. Sandbox patched affected client systems and investigated for signs of compromise. The historical observation below does not establish that a reverse proxy blocks every exploit.

© 2026 Sandbox Technologies, Inc.

In Sandbox's review at the time, client Exchange servers behind a DMZ reverse proxy showed no evidence of successful tampering. That observation does not establish that the proxy alone prevented compromise or that a different proxy design would do so. The enduring lesson is to reduce unnecessary exposure while patching, investigating and monitoring all supported systems.

On-premises or the cloud

Choose a supported mail platform based on security, workflow, licensing and recovery needs. For on-premises systems, assess proxy and gateway controls as part of the design rather than as a guarantee. Microsoft 365 shifts infrastructure operation to Microsoft, but the organization still manages identities, access, configuration and data protection. Costs and responsibilities vary.

SPF, the guest list

SPF authorizes sending hosts for an SMTP envelope or HELO domain through DNS. It does not by itself authenticate the visible From address; DMARC checks alignment.

DKIM, the tamper-evident seal

DKIM signs selected message content. A receiver verifies the signature using the signing domain's public key in DNS. This protects signed content and associates the domain with the message, but does not prove its human author or safety.

DMARC, the instructions

DMARC connects authentication to the visible From domain. Either aligned SPF or aligned DKIM passing is sufficient; failure means neither aligned method passes. The domain can request monitoring, quarantine or rejection and receive reports. Receivers still apply their own policies, and legitimate forwarding can complicate authentication.

All three are published in DNS and apply whether email is hosted on-premises or with a cloud provider such as Microsoft 365.

© 2026 Sandbox Technologies, Inc.

This document is protected by US and International copyright laws. Reproduction or distribution of this document for commercial advantage and without written permission from Sandbox Technologies, Inc. is strictly prohibited. Any distribution must retain attributions and this notice.

© 2026 Sandbox Technologies, Inc.