Email Security & 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....5
- 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

The most attacked door into your organization is the one everyone uses all day

Email is the channel attackers probe first, because it reaches every employee and carries the organization's identity with it. Most of what protects it is invisible: a handful of authentication records, a filtering layer, and a few server settings that decide whether a stolen password, a spoofed domain, or an exposed server turns into a real loss. When one of those layers is missing, the failure is usually silent until money or data has already moved. The situations below are ordinary, not exotic.

© 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

With nothing more than a stolen username and password, an attacker connects a personal mobile device to the mail system. By default, little stands in the way, and mobile connections often sit outside the multi-factor rules that protect a browser login.

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.

Every one of these outcomes is addressed by configuration you can verify, not by a larger budget. The purpose of this issue is to help you confirm that each layer is actually in place, rather than assumed.

© 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

If email is hosted on-premises on an Exchange or similar server, is a current certificate installed, and is the transport protocol up to date? Certificates encrypt the traffic to and from web-facing mail servers. The older SSL protocols, along with TLS 1.0 and 1.1, are now deprecated; TLS 1.2 should be treated as the minimum, with TLS 1.3 preferred where the environment supports it.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

DMZ Reverse Proxy

If email is hosted on-premises, does a DMZ reverse proxy sit in front of the mail server, so inbound traffic from the internet never reaches it directly? A DMZ is a buffer network between the public internet and the systems that hold confidential data. Placing a reverse proxy there, and directing all outside traffic to the proxy rather than the mail server, adds a layer of separation against direct inbound exploits. The primer below explains this in more detail.

Compliant	NOTES:
Needs Attention	
N/A	

SPF Published

Is SPF (Sender Policy Framework) published for the domain? SPF is a public DNS record listing the servers authorized to send mail for a domain. It is one of the main defenses against spammers and fraudsters spoofing an address, and it applies whether email is hosted on-premises or in the cloud.

Compliant	NOTES:
Needs Attention	
N/A	

DKIM Enabled

Is DKIM (DomainKeys Identified Mail) enabled for the domain? DKIM adds a cryptographic signature to outbound mail, allowing receiving servers to confirm a message genuinely came from an authorized source and was not altered in transit. Like SPF, it applies to both on-premises and cloud-hosted email.

Compliant	NOTES:
Needs Attention	
N/A	

DMARC Configured

Is DMARC (Domain-based Message Authentication, Reporting and Conformance) configured? DMARC tells receiving servers what to do with mail that fails SPF or DKIM, whether to reject it, quarantine it, or let it through, and it can report on messages sent using the domain. Without it, SPF and DKIM results are advisory rather than enforced.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Mobile Device Approval

Are new mobile devices blocked from connecting until an administrator approves them? By default, ActiveSync, the mechanism Exchange and Microsoft 365 use to sync mobile devices, lets anyone with a valid username and password connect a device, and those connections often fall outside multi-factor protection. Enabling the feature commonly called ActiveSync Quarantine, in both on-premises Exchange and Microsoft 365, requires an administrator to approve each new device first.

Compliant	NOTES:
Needs Attention	
N/A	

Legacy Protocols Disabled

Are the legacy POP and IMAP protocols, and legacy (basic) authentication, disabled where they are not needed? POP and IMAP are older, rarely required protocols that attackers use to sidestep multi-factor authentication. Microsoft has been retiring basic authentication across Exchange Online for this reason, but the setting still warrants confirmation, particularly on on-premises systems and for any mailbox where these protocols were once enabled.

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 (demilitarized zone) is a buffer network that sits between the public internet and the internal network where confidential data lives. Systems that must be reachable from outside are placed in the DMZ, and traffic between the DMZ and the internal network is tightly restricted. A reverse proxy in that DMZ receives inbound mail traffic on the server's behalf and forwards only what is legitimate, so the Exchange server is never exposed directly to the internet. It is recommended that a reverse proxy be used in a DMZ for on-premises Exchange and mail servers, with all externally originated traffic directed to the proxy.

Why this earned its own section

In early 2021, a set of Microsoft Exchange Server vulnerabilities, later known collectively as ProxyLogon, was disclosed and widely exploited. As soon as the exploits became known, our organization applied the associated patches to active Exchange clients, and then went further, scanning each environment for signs that a backdoor had been installed during the weeks the

© 2026 Sandbox Technologies, Inc.

vulnerabilities were believed to have been exploited before disclosure. Industry reporting at the time indicated that a substantial share of internet-facing Exchange servers had been probed or compromised. In our review, the clients whose Exchange servers sat behind a DMZ reverse proxy showed no evidence of successful tampering. Those specific vulnerabilities are long patched and now historical, but the lesson they illustrate is durable: a server that is not directly reachable is a far smaller target.

On-premises or the cloud

Where security or workflow requirements make an on-premises Exchange server the preferred option, adding a DMZ reverse proxy is strongly encouraged, and the cost can be modest for organizations already using virtualization. In many cases, however, migrating email to Microsoft 365 removes much of this exposure by shifting the internet-facing infrastructure to Microsoft. No two environments are identical, and the right choice depends on the organization's particular needs.

SPF, the guest list

Sender Policy Framework is a DNS record that publicly lists which servers are allowed to send email for a domain. A receiving server can check that list and treat mail from anywhere else with suspicion.

DKIM, the tamper-evident seal

DomainKeys Identified Mail adds a cryptographic signature to each outbound message. The receiving server verifies the signature against a public key in the sender's DNS, confirming the message came from an authorized sender and was not altered along the way.

DMARC, the instructions

Domain-based Message Authentication, Reporting and Conformance ties the two together. It tells receiving servers what to do when a message fails SPF or DKIM, whether to reject, quarantine, or allow it, and it can send back reports on who is sending mail using the domain. Without DMARC, SPF and DKIM produce a verdict that no one is obligated to act on.

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.