M365 Email Security

Starter Kit

DEMO

Practical Email Security Framework for SMEs

Ireland • UK • EU

Version 1.3 | February 2026

iterik.ie | iterik.eu

Contents

Executive Summary

Email is the most common path into SMEs because it touches identity, finance, suppliers and daily operations. Most incidents are not caused by advanced malware: they are caused by repeatable, fixable weaknesses.

💸 The Cost of One Incident

Invoice fraud losses for SMEs typically range from 5 to 6 figures.
Many are never recovered. Banks rarely bear liability when standard controls were absent.
This guide costs €49. One prevented incident covers it thousands of times over.

Current SME Email Threat Patterns (2026)

These are the attack patterns most commonly seen in SME environments right now. Understanding them is the first step to closing the gaps.

Threat Pattern	How It Works	Primary Defence
Invoice Redirection Fraud	Attacker spoofs or compromises supplier email; requests bank detail change before payment	DMARC enforcement + out-of-band verification policy
CEO / Executive Impersonation	Display-name spoofing or lookalike domain tricks staff into urgent wire transfers	Impersonation protection in Defender + training
Fake Microsoft Login Pages	Phishing email links to convincing Microsoft login clone to harvest credentials	MFA + Conditional Access + Safe Links
MFA Fatigue Attacks	Repeated MFA push notifications until exhausted user approves	Number matching MFA + anomaly alerts
Compromised Supplier Mailbox	Attacker controls a supplier account; sends legitimate-looking invoice from real address	Out-of-band verification for all payment changes
Silent Forwarding Persistence	Post-compromise: attacker sets silent forwarding rule to monitor finance emails undetected	Forwarding disabled by default + mailbox rule audits

Core Outcomes

- A verified baseline score and a documented mail flow diagram.
- A safe DMARC rollout plan with clear ownership and review cadence.
- Reduced bypass risk when using a secure email gateway.
- A Defender baseline focused on impersonation, high-risk users, and quarantine workflows.
- A first-hour incident checklist plus communication templates for staff, finance and suppliers.

What This Guide Does NOT Cover

ℹ️ INFO	This guide is focused specifically on M365 email security for SMEs. The following topics are out of scope and require separate specialist guidance.

- Endpoint Detection & Response (EDR): device-level security and antivirus strategy.
- Backup, recovery and business continuity planning.
- Full Azure Active Directory / Entra ID governance and Conditional Access design.
- Advanced threat hunting, SIEM, or Security Operations Centre (SOC) functions.
- Legal reporting obligations under GDPR, NIS2 or sector-specific regulations.
- Data protection compliance, DLP policy design, or classification frameworks.

Most Common SME Traps

⚠ WARNING	Treating p=none DMARC as protection: it is monitoring only, not enforcement.
⚠ WARNING	Assuming MX pointing to a gateway means the gateway cannot be bypassed.
⚠ WARNING	Fixing false positives by creating broad allowlists — this undermines filtering.
⚠ WARNING	Buying awareness training but leaving external forwarding and admin hygiene unmanaged.
⚠ WARNING	Ignoring mailbox-rule persistence — attackers use silent rules to monitor finance emails undetected.
DISCLAIMER	This guide provides practical guidance for improving email security in Microsoft 365 environments. It does not replace professional security assessment, legal advice, or incident response services. Apply all changes through change management and test carefully.

How to Use This Guide

- Start with Section 0 (Change Management) before touching any configuration.
- Then Section 1 for your baseline exposure check and Appendix A scorecard.
- If you use a gateway: read Section 3 before changing connectors, bypass rules or allowlists.
- If you handle invoices: adopt Appendix I (finance verification policy) and run an annual tabletop exercise.
- Use Section 9 (Troubleshooting) when something breaks or looks inconsistent.

1 The 30-Minute Exposure Check

This section gives you a structured baseline. You are not trying to perfect configuration in 30 minutes. You are trying to answer one question: do we have verified control over identity, authentication, and mail flow?

1.1 Quick Triage Questions

Mark each item: ✔ Verified | ⚠ Configured but not reviewed | ✖ Not configured | ? Unsure

Area	Check	Status
DMARC	Record for every sending domain; policy none/quarantine/reject known.	✔/⚠/✖/?
DKIM	Enabled for every domain sending through M365 or a gateway.	✔/⚠/✖/?
SPF	Exactly one record per domain; within lookup limits; not ending +all.	✔/⚠/✖/?
Mail Flow	Gateway cannot be bypassed; M365 restricted from direct delivery.	✔/⚠/✖/?
Forwarding	Automatic external forwarding disabled or tightly controlled.	✔/⚠/✖/?
Rules	Inbox rules reviewed for high-risk users (finance/executives).	✔/⚠/✖/?
Defender	Anti-phishing policy and impersonation protection configured.	✔/⚠/✖/?
Identity	Separate admin accounts, MFA enforced, legacy auth disabled.	✔/⚠/✖/?
Process	First-hour incident checklist exists with a named owner.	✔/⚠/✖/?

1.2 Interpreting Your Results

💡 TIP

Lots of '?' means you do not have verified assurance. Lots of '⚠' means drift risk. Drift is normal; unmanaged drift is the problem. Use the appendices to document current state and make ownership explicit.

1.3 High-Risk Findings

- SPF ends with +all or multiple SPF records exist.
- No DMARC record exists for an active sending domain.
- DMARC remains at p=none with no reporting owner.
- Gateway deployed but Microsoft 365 can still accept direct delivery.
- External forwarding broadly enabled.
- Global Admin accounts used for daily email and browsing.

5 M365 Email Security Maturity Model

Use this model to understand where your organisation currently sits and what the next level looks like. Share it with your leadership team to build the case for investment.

Level 1 — Basic — Minimal Controls
✔ SPF record exists but may not be validated or within lookup limits
✔ DKIM not enabled or only for some domains
✔ No DMARC record, or DMARC is p=none with no report owner
✔ Default Defender configuration only — no tuning
✔ No documented mail flow or sender inventory
✔ No formal incident process

Level 2 — Controlled — Core Controls Active
✔ SPF validated, within limits, enforced with -all
✔ DKIM enabled for all sending domains
✔ DMARC progressed to p=quarantine with an assigned report owner
✔ Gateway bypass path closed — M365 connector restricted to gateway IPs
✔ External forwarding disabled by default
✔ Basic incident checklist exists

Level 3 — Hardened — Active Defence
✔ DMARC at p=reject for all sending domains
✔ Impersonation protection tuned for priority users
✔ Mailbox rules and forwarding reviewed quarterly for high-risk accounts
✔ Quarantine workflow owned with defined SLA
✔ Awareness training running with click-rate and report-rate tracking
✔ Incident plan tested at least annually

Level 4 — Mature — Governance & Resilience
✔ Quarterly review rhythm documented and consistently followed
✔ Mail flow fully documented; no-bypass confirmed quarterly
✔ Exceptions log maintained with review dates
✔ Annual tabletop exercise completed across finance, IT, and leadership
✔ DMARC reports reviewed monthly; sender inventory kept current
✔ Change management process followed for all configuration changes

Quick Reference Card: Print and Keep

Five things to check first on any M365 tenant:

#	Check	Tool
1	SPF: one record per domain, ends with -all, within 10-lookup limit	MXToolbox → SPF Check
2	DKIM: enabled in Defender portal for all sending domains	MXToolbox → DKIM Lookup
3	DMARC: published and progressed to quarantine or reject	MXToolbox → DMARC Check
4	Gateway bypass: M365 inbound connector restricted to gateway IPs only	Send direct external test email
5	External forwarding: disabled in outbound spam policy	M365 Defender Admin Portal

Key tools: mxtoolbox.com | mail-tester.com | dmarcian.com | urlscan.io | haveibeenpwned.com

Your Maturity Level target: Level 1 → Level 2 immediately | Level 3 within 90 days | Level 4 ongoing