CLOUDSWITCHED

FREE RESOURCE — BEST PRACTICES GUIDE

Email Security Best Practices

SPF, DKIM, DMARC, phishing protection, and email hygiene for UK businesses. Protect your organisation from the number one attack vector with the essential email security measures that catch the vast majority of inbound threats.

91%	£50m	3	4
ATTACKS START WITH EMAIL	UK BEC LOSSES IN 2024	DNS RECORDS TO CONFIGURE	GUIDE SECTIONS

SPF / DKIM / DMARC · MICROSOFT 365 · ANTI-PHISHING · UK SME

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Read-only PDF

01

Understanding email threats

Email remains the primary attack vector for cybercriminals targeting UK businesses. Over 91% of successful cyber attacks begin with a phishing email, and Business Email Compromise (BEC) cost UK organisations over £50 million in 2024 alone. Email security is not optional — it is a critical business control that must combine technical defences with staff awareness.

91%
CYBER ATTACKS START BY EMAIL

£50m+
UK BEC LOSSES IN 2024

£25k
AVERAGE LOSS PER BEC INCIDENT

The five threat categories every inbox faces

THREAT TYPE	HOW IT WORKS	LIKELY IMPACT
Phishing	Fraudulent emails impersonating trusted brands to steal credentials	Account compromise, data breach
Spear phishing	Targeted attacks aimed at specific individuals with personalised content	Executive compromise, financial fraud
Business Email Compromise	Attackers impersonate executives to authorise payments or data transfers	Financial loss (avg. £25,000+)
Malware & ransomware	Malicious attachments or links that install code on the endpoint	System encryption, data loss, ransom demand
Domain spoofing	Attackers send emails that appear to come from your own domain	Reputation damage, recipient trust loss

CEO FRAUD IS INCREASING

Business Email Compromise attacks impersonating CEOs or Finance Directors are increasingly sophisticated. They often contain **no malware and no link** — just a convincing request to transfer money or change banking details. Technical controls alone cannot stop them; they must be combined with staff awareness training and a verify-by-phone payment policy.

02

SPF, DKIM & DMARC configuration

These three DNS records work together to authenticate your outbound email and prevent attackers from spoofing your domain. Configuring all three is the single highest-leverage email-security action a UK SME can take — it is free, it takes a couple of hours, and it stops most domain-impersonation attacks dead.

SPF — Sender Policy Framework

What it does. Specifies which mail servers are authorised to send email on behalf of your domain. Receiving servers check the SPF record to verify the sender is legitimate.

Example record: `v=spf1 include:spf.protection.outlook.com include:_spf.google.com -all`

- **Use `-all` (hard fail)** rather than `~all` (soft fail) once you are confident every legitimate sending source is included.
- **Include all sending sources:** email provider, CRM, marketing platform, helpdesk, invoicing tool — anything that sends mail from your domain.
- **Stay under 10 DNS lookups** to avoid exceeding the SPF lookup limit, which silently breaks authentication.

DKIM — DomainKeys Identified Mail

What it does. Adds a cryptographic signature to outbound emails so recipients can verify the message was not modified in transit and genuinely came from your domain.

- **Enable DKIM signing** in your email provider settings (Microsoft 365 Defender, Google Workspace Admin Console).
- **Publish the DKIM public key** as a CNAME or TXT record at the selector your provider gives you (e.g. `selector1._domainkey`).
- **Use 2048-bit keys minimum** — 1024-bit keys are deprecated and increasingly rejected by major receivers.

02

SPF, DKIM & DMARC (continued)

DMARC — Domain-based Message Authentication

What it does. Tells receiving servers what to do when SPF or DKIM checks fail, and provides aggregate reports so you can monitor authentication results across the internet. Without DMARC, SPF and DKIM are advisory; with DMARC, they become enforceable.

Why it matters. A DMARC `p=reject` policy is the only configuration that fully stops attackers from sending mail that appears to come from your domain to your customers, partners, and staff. It is increasingly a requirement for UK Cyber Essentials, ISO 27001, and large supplier-due-diligence questionnaires.

Recommended DMARC rollout

Weeks 1–6 — monitor. Publish `p=none` with a `rua=` reporting address. Read the aggregate reports to identify every legitimate sending source and any gaps in SPF/DKIM coverage.

Weeks 7–10 — quarantine. Move to `p=quarantine` so failing messages land in the recipient's spam folder. Continue reading reports for unexpected failures.

Week 11+ — reject. Move to `p=reject` once reports show only legitimate senders passing. Spoofed mail is now blocked at the receiver before delivery.

CHECK YOUR CURRENT RECORDS

Use free tools like **MXToolbox** or **DMARC Analyser** to inspect your current SPF, DKIM, and DMARC configuration. Many UK businesses still have incomplete, soft-fail, or missing records — leaving them open to domain spoofing and increasingly failing Cyber Essentials and supplier-due-diligence checks.

03

Microsoft 365 configuration checklist

Microsoft 365 ships with strong email-security features, but many of them are off or set to weak defaults out of the box. Work through this checklist with your administrator to bring every tenant up to the level expected by Cyber Essentials, ISO 27001, and most cyber-insurance underwriters. Tick each item once it has been verified in the Microsoft Defender portal.

- ☐ **Safe Attachments** — enable in Microsoft Defender to scan every attachment in a sandbox before delivery (Standard or Strict preset).
- ☐ **Safe Links** — rewrite all inbound URLs so they are re-checked at time-of-click, including links inside Teams and Office documents.
- ☐ **Anti-phishing policy** — configure with mailbox intelligence, spoof intelligence, and impersonation protection enabled.
- ☐ **Impersonation protection** — explicitly list your CEO, CFO, finance team, and any other high-risk users so spoofed display names are blocked.
- ☐ **Block high-risk attachments** — `.exe`, `.js`, `.vbs`, `.ps1`, `.bat`, `.scr`, `.cmd`, and macro-enabled Office formats.
- ☐ **External sender tagging** — enable the “External” tag in Outlook so messages from outside the tenant are visually flagged in every client.
- ☐ **Quarantine policy** — let users review suspected phishing with admin override and daily digest, so legitimate mail is recovered quickly.
- ☐ **Outbound encryption** — configure Microsoft Purview Message Encryption for finance, HR, and legal communications carrying sensitive data.
- ☐ **Multi-Factor Authentication** — enforced for every mailbox using Conditional Access (no exceptions, including shared and service mailboxes).
- ☐ **Audit logging** — unified audit log enabled with at least 180-day retention so post-incident investigation is possible.

04

Staff awareness & best practices

Technical controls stop the vast majority of malicious email, but the inbox is where the last line of defence lives. These six habits are what separates a near-miss from a 72-hour ICO breach notification. Build them into induction, refresher training, and the quarterly all-staff comms.

Phishing simulations. Run at least quarterly using KnowBe4, Proofpoint Security Awareness, or Microsoft Attack Simulator (included in M365 Defender for Office P2).

Report, don't delete. Train staff to use the *Report Phishing* button in Outlook so suspicious mail goes to IT for triage, not the bin.

Verify payment changes. Always confirm bank-detail changes or new payment requests by phone using a previously-known number — never the number in the email.

Hover before clicking. Train staff to hover over every link to preview the real destination URL before clicking, on mobile as well as desktop.

Check the sender. Display names can be spoofed at will — always check the actual email address, not just the friendly name.

Challenge urgency. Phishing emails manufacture false urgency. When pressured to act fast, slow down and verify through a second channel.

UK-SPECIFIC LURES TO HIGHLIGHT IN TRAINING

HMRC tax refunds, **NHS appointment messages**, **Royal Mail delivery notifications**, **TV Licensing threats**, **energy company billing scams**, and **parking-fine notices** are the lures UK attackers reach for most often. Use real recent examples in every awareness session — they hit harder than generic illustrations.

04

Review & sign-off worksheet

Use this worksheet after running through the SPF/DKIM/DMARC configuration and the Microsoft 365 checklist. Record tenant-specific notes — selector names, SPF includes you needed, exclusions agreed with the business — so the next review picks up where this one finished.

NOTES — TENANT-SPECIFIC CONFIGURATION

PREPARED BY	DATE	APPROVED BY

CLOUDSWITCHED

CYBERSECURITY & EMAIL PROTECTION

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom