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 these essential email security measures.

91%	SPF+DKIM	DMARC	Free
CYBER ATTACKS START BY EMAIL	ESSENTIAL DNS RECORDS	DOMAIN SPOOFING PROTECTION	SECURITY GUIDE

1 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. Business Email Compromise (BEC) cost UK organisations over £50 million in 2024 alone. Email security is not optional — it is a critical business control.

THREAT TYPE	DESCRIPTION	IMPACT
Phishing	Fraudulent emails impersonating trusted brands to steal credentials	Account compromise, data breach
Spear Phishing	Targeted phishing 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 malware	System encryption, data loss, ransom demands
Domain Spoofing	Attackers send emails that appear to come from your domain	Reputation damage, recipient trust loss

CEO Fraud Is Increasing

Business Email Compromise attacks impersonating CEOs or Finance Directors are increasingly sophisticated. They often do not contain malware or links — just a convincing request to transfer money. Technical controls must be combined with staff awareness training.

2 SPF, DKIM & DMARC Configuration

These three DNS records work together to prevent domain spoofing and authenticate your email.

SPF (Sender Policy Framework)

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

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 all legitimate sources are included
- → Include **all legitimate sending sources**: email provider, CRM, marketing platform, helpdesk
- → Keep the record **under 10 DNS lookups** to avoid exceeding the SPF lookup limit

DKIM (DomainKeys Identified Mail)

What it does: Adds a digital signature to outbound emails, allowing recipients to verify the email was not modified in transit and genuinely came from your domain.

- → Enable DKIM signing in your **email provider settings** (Microsoft 365, Google Workspace)
- → Publish the **DKIM public key** as a CNAME or TXT record in your DNS
- → Use **2048-bit keys** minimum for security strength

DMARC (Domain-based Message Authentication)

What it does: Tells receiving servers what to do when SPF or DKIM checks fail. Provides reporting so you can monitor authentication results.

Recommended rollout:
1. Start with `p=none` (monitor only) for 4–6 weeks
2. Move to `p=quarantine` (send failures to spam) for 4 weeks
3. Move to `p=reject` (block failures) once clean

Check Your Records

Use free tools like MXToolbox or DMARC Analyser to check your current SPF, DKIM, and DMARC configuration. Many UK businesses have incomplete or missing records, leaving them vulnerable to domain spoofing.

3 Microsoft 365 Email Security Configuration

Configure the built-in security features of Microsoft 365 to their strongest settings.

- [ ] Enable **Safe Attachments** in Microsoft Defender — scans attachments in a sandbox before delivery
- [ ] Enable **Safe Links** — rewrites URLs to check for malicious content at time of click
- [ ] Configure **anti-phishing policies** with mailbox intelligence and impersonation protection
- [ ] Enable **impersonation protection** for your CEO, CFO, and Finance team specifically
- [ ] Block **high-risk attachment types** (.exe, .js, .vbs, .ps1, .bat, .scr, .cmd)
- [ ] Enable **external sender tagging** to visually flag emails from outside your organisation
- [ ] Configure **quarantine policies** so users can review suspected phishing (with admin override)
- [ ] Set up **email encryption** for sensitive outbound communications

4 Staff Awareness & Best Practices

Technical controls are essential but must be complemented by user awareness.

- → **Conduct phishing simulations** at least quarterly using tools like KnowBe4 or Microsoft Attack Simulator
- → **Report, don't delete:** Train staff to report suspicious emails using the 'Report Phishing' button in Outlook
- → **Verify payment changes:** Always confirm bank detail changes or payment requests by phone using a known number
- → **Hover before clicking:** Train staff to hover over links to preview the destination URL before clicking
- → **Check the sender:** Display names can be spoofed — always check the actual email address
- → **Challenge urgency:** Phishing emails create false urgency. If pressured to act fast, slow down and verify

Notes

Need Email Security Implemented?

Our team configures comprehensive email security for Microsoft 365 including SPF, DKIM, DMARC, and advanced threat protection.

info@cloudswitched.com
New London House, 6 London St, London EC3R

Prepared by: Date: Approved by:

© 2026 CloudSwitched Limited. All rights reserved. This resource is provided for informational purposes and does not constitute professional IT advice.