Email Security Best Practices for UK Firms

Why email is the top threat vector

- Email is the largest cybersecurity threat for UK businesses in 2026.
- 85% of all breaches via cyber methods start with an email attack.
- Cyber criminals use phishing emails, bogus invoices, and fake 'CEO' emails to trick victims into breaching their organisation's security.
- A single Business Email Compromise (BEC) attack can have massive costs to an organisation.
- Breaching the UK GDPR by sending an email to the wrong recipient can result in reports of the breach and associated fines.
- The evolving model of hybrid and remote working has increased risks to email security.
- Microsoft 365 and Google Workspace are used by most UK small- to medium-sized enterprises (SMEs.) They also have robust email security built in as part of their service.
- When an organisation ensures their email is set up correctly and that they train their employees properly, they can reduce email exposure by 90% or more without spending large amounts of money.

How email attacks typically happen

The most common types of email attacks proceed according to a standard set of operations:

- **Reconnaissance:** The attacker will research your company through various sources (e.g., LinkedIn, your company web site, Companies House) to identify who handles the finances, the name of the CEO, and suppliers etc.
- **Initial compromise:** The attacker will send a phishing email containing a malicious link/attachment or use stolen credentials from a previous breach in performing credential stuffing.
- **Account take-over:** Attacker is able to login (if there is no MFA, the process is easy), read your emails, and set rules to conceal their activities.
- **Theft of money or data:** The attacker is able to change your payment details or request an urgent transfer of funds, download sensitive data, or send malware to your contacts.
- **Cover-up:** The attacker will delete evidence or create delays in order to go undetected.

The most damaging of these attacks (BEC and payment redirection) will typically take place after a period of days or weeks where the attacker is quietly monitoring your activities before actually committing fraud. This is one of the reasons that early detection and strong authentication are so crucial.

The most common email threats facing UK firms

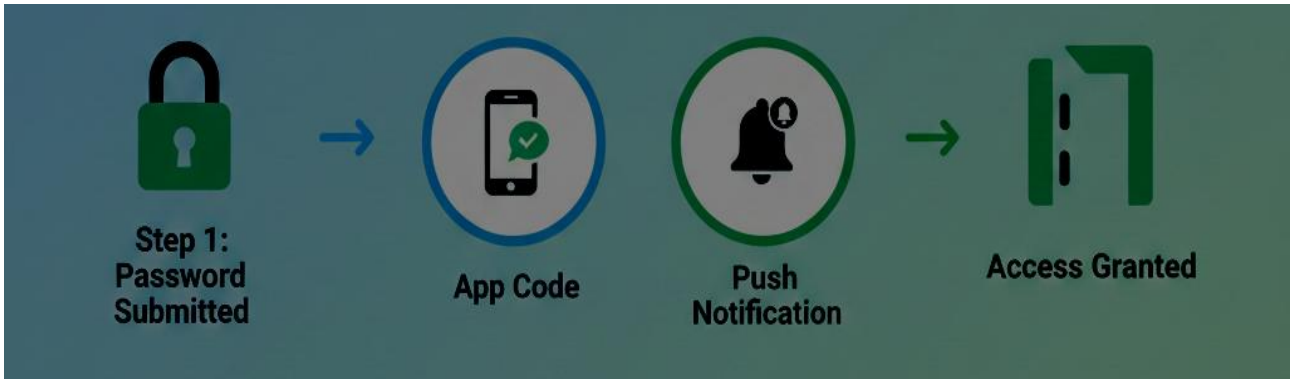
- Phishing and spear phishing
- Business Email Compromise (BEC)
- Invoice/payment redirection fraud

- Account takeover
- CEO impersonation
- Malware attachments
- Mis-sent emails
- Shared mailbox exposure
- Weak password reuse

Core email security controls every firm should implement

1. Multi-Factor Authentication (MFA)

- **What:** A second layer of verification (from app code or push notification) that happens after a password is submitted.
- **Why:** According to Microsoft, MFA blocks 99.9% of credential attacks that use automated methods.
- **Minimum:** Implement MFA across all email & cloud service accounts.
- **Better:** Use pseudo-physical MFA (such as a push notification from the Microsoft Authenticator app) rather than SMS-based MFA.
- **Quick win:** Set up MFA for MS 365 / Google Workspace Admin Center accounts (15-30 minutes) using IT Admin account.



2. Strong Password Policies & Password Managers

- **What:** Require a minimum of a 14 character password that is useable once. Reuse is prohibited.
- **Why:** Use of weak/reused passwords continue to be the second most common means of gaining unauthorised access.
- **Minimum:** Require minimum of 14 characters as well as no imposed required changes every month (NCSC standard).
- **Better:** Require all passwords to be stored in a company owned password manager e.g., Bit-warden Teams or similar ($3-$5/user/month).

- **Quick win:** Require the use of pass-phrases as opposed to passwords and disallow reuse for the last 10 passwords.

3. Email Filtering & Anti-Spam Solutions

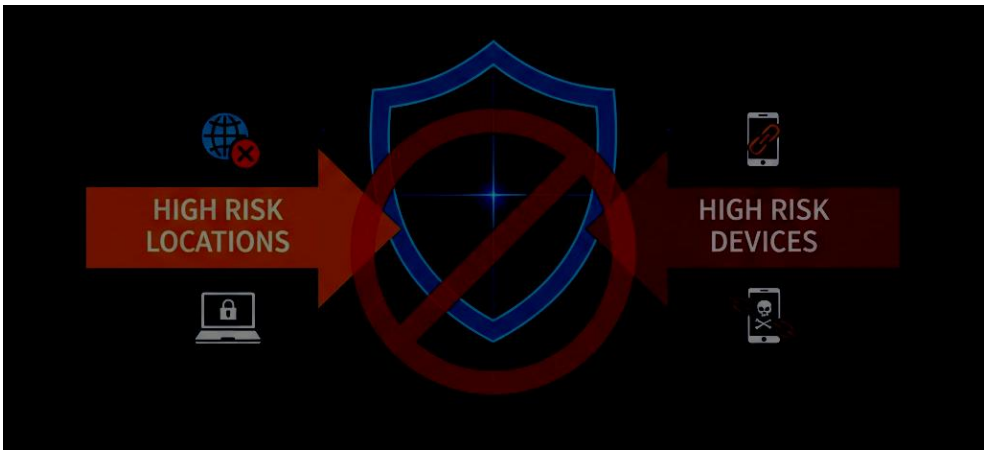
- **What:** Filters for blocking phishing and malware and fraudulent impersonation emails before they are delivered to the respective user inboxes.
- **Why:** Filters for 95%+ of all malicious emails sent.
- **Minimum:** Use Windows Defender or Gmail default filtering.
- **Better:** Purchase Advanced Threat Protection (ATP) from Microsoft ($2-$5/user/month).
- **Quick win:** Add “External” tags in subject line for external senders in the Administrator’s email account settings.

4. DMARC, SPF and DKIM (explained simply)

- **What:** Industry standard for validating that the message received is as it claims to be.
- **Why:** To eliminate the ability for a hacker to “spoof” your organisation.
- **Minimum:** Use an SPF record to allow the sending domain to be verified.
- **Better:** Set up a DMARC policy to “reject” any email attempting to spoof your organisation.
- **Quick win:** Use the free dmarcian.com wizard to set up a working SPF/DKIM/DMARC email compliant setup.

5. Conditional Access Policies

- **What:** Prevents logins from high risk locations/devices
- **Why:** Protects against attackers using stolen credentials in other countries
- **Minimum:** Block logins from users that are outside the UK (unless travelling internationally)
- **Better:** Enforce compliant devices
- **Quick Win:** Can be enabled in Microsoft 365 Admin Center approximate 10 mins to implement.



6. Account Lockout Controls

- **What:** Locks account after multiple failed login attempts
- W**hy:** Prevent brute-force login attempts
- **Minimum:** Lock account after 5 to 10 failed logins (for 30 minutes)
- **Better:** Progressive lockout combined with Admin alerting
- **Quick Win:** Set in your Directory Settings.

7. Secure Email Gateways

- **What:** Additional security layer that scans all incoming and outgoing email messages
- **Why:** Catched Advanced Threats that built-in Email Filters do not
- **Minimum:** Your current Email service provider (Google or Microsoft) will provide the base protection
- **Better:** Acquire a third-party Email Secure Gateway (e.g., Mimecast or Proof point at £3-8/month/user)
- **Quick Win**: Enable Advanced Attachment/Link Scanning.

8. Data Loss Prevention (DLP)

- **What:** Blocks sensitive data (e.g., bank account information and National Identity numbers) leaving your organisation via email
- **Why:** Reduces the possibility of either accidental or maliciously sending the information
- **Minimum:** Use the built-in Microsoft 365 DLP Policy (e.g., block credit card numbers)
- **Better:** Create DLP policies based on client data
- **Quick Win:** Enable the Default DLP Policy Templates.

Email Fraud and Payment Redirection Explained

- How do thieves get into conversations?
- Modifying invoices
- Changing on bank account details
- Verification controls
- Finance team processes

Include detailed scenario.

Protecting Sensitive Data via Email

- UK GDPR relevance
- Risk to personal information

- Encryption
- DLP
- Access control
- Secure alternatives for file sharing

Staff Training and Awareness

- Frequency
- Simulation
- Report format
- Example from management

Email Security Checklist for Directors

☐ Email and Cloud Accounts Have MFA

☐ 14+ Character Passwords Cannot Be Reused

☐ External Sender Tags Are On

☐ SPF, DKIM, DMARC Are All Configured

☐ Conditional Access Policies Are Blocking Risky Access

☐ Users Will Be Locked Out Of Access To Their Email Account After 5 Failed Logon Attempts

☐ Advanced Email Filtering Is Turned On

☐ DLP Rules Are Created For Sensitive Data

☐ Run Defender For Endpoint Protection

☐ Back Up To The Cloud Daily, With The Ability To Restore From Previous Versions

☐ All Staff Receive A Phishing Brief Quarterly

☐ Policy Required Procedure For Verifying Payment Method

☐ Email Access Checklists For Joiners/Leavers

☐ Process Established For Reporting Incidents Of Breaches

☐ ICO Data Protection Fee Has Been Paid

FAQs

1. **Is antivirus protection sufficient?**

Not at all; the majority (70%) of email breaches are caused by stolen credentials rather than malware.

2. **Does Microsoft 365 provide automatic protection?**

While Microsoft 365 offers many robust features, proper configuration is essential to providing adequate protection.

3. **Do small businesses get targeted by cyber criminals?**

Absolutely; all automated attacks are not based on the size of your business.

4. **How often should your employees undergo phishing training?**

At least annually, and your organisation should continue to provide periodic phishing training refreshers.

5. **What is the minimum acceptable configuration for an email service?**

Multi-Factor Authentication (MFA), strong password policies, and implementing SPF/DKIM/DMARC policies in addition to employing email filtering and backups.

6. **Is Cyber Essentials certification required?**

A certification for Cyber Essentials demonstrates your organisation is operating with a minimum security baseline; in many cases it is a requirement to obtain public sector contracts.

About This Guide

The **Computer Support Centre** is an IT and Cyber Security Provider based in the UK that supports small and medium-sized companies.

This guide is to provide decision-makers with a simple, practical, non-technical guidance on how to reduce the risk of email fraud and phishing attacks as well as reducing the risk of data losses in the UK through appropriate, realistic, controls.

The **Computer Support Centre** can provide an email security review of your business if required, and present you with practical recommendations that are in line with UK best practices and the Cyber Essentials Framework.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:
 https://computersupportcentre.com

Conclusion

Email continues to be the major way that cyber attacks happen to UK companies. This is not necessarily because the companies don’t use good security practices; it is simply a function of where email is used to do business, and therefore, where bad actors can target access to their businesses’ finances and operations and communications with their clients.

The good news is that a significant proportion of all email-related Fraud, Phishing Attacks and Data Breaches can be prevented. If a company implements a multi-factor authentication program, uses strong passwords, properly verifies changes in payment methods, configures their SPF/DKIM/DMARC correctly and trains their employees regularly, they can greatly reduce the chance of suffering from email security incidents.

Email Security is not about expensive tools or complicated technology; it is about implement strong controls consistently, develop clear processes and have a reasonable system of oversight from the company’s Board of Directors.