PROTECTING AGAINST EMAIL ATTACKS

What SMEs Should Do Now

A Practical Approach Designed for SMEs That Need Stronger Controls and Workable Day-to-day Experience

1 CLOSE THE DMARC ENFORCEMENT GAP (PROPERLY)

- Move from 'p=none' to 'quarantine'/'reject' with monitoring and staged rollout
- Ensure all legitimate senders are aligned (your CRM, marketing platform, ticketing system, etc.)
- Tighten SPF (avoid "include everything forever") and enable DKIM wherever possible

This won't stop every attack (especially compromised accounts), but it removes a huge amount of low-effort spoofing.

2 TREAT TRUSTED PLATFORM MESSAGES AS HIGH-RISK BY DEFAULT

If your business heavily relies on DocuSign/Adobe Sign, SharePoint, OneDrive, Dropbox/Google Drive, or calendar invites from external parties... then those categories deserve additional scrutiny:

- Link scanning/detonation
- Banner warnings for external senders
- Tighter rules around newly seen senders/ domains
- Monitoring for lookalike domains and suspicious reply-to behaviour

3 HARDEN MICROSOFT 365 FOR MODERN PHISHING

A lot of "successful" attacks don't use malware - they use stolen logins and convincing pages. Key improvements usually include:

- Conditional access and sign-in risk policies (where licensing allows)
- Disabling legacy auth and controlling external forwarding
- Improving MFA approach (avoid "approve spam" fatigue; use stronger methods where possible)
- Tighter controls around OAuth app consent (a common persistence tactic)

4 BUILD A REPORTING CULTURE (FAST WINS)

When phishing volume is high, speed matters.

- Make reporting one-click (or at least simple)
- Acknowledge reports ("thanks, good catch!") to help behaviours stick
- Run short, regular training refreshers (5 minutes beats 50)

Remember: only around 1 in 5 businesses reported staff cyber security training in the prior 12 months in the UK survey. That's a huge gap attackers exploit.

5 ADD SUPPLIER AND FINANCE VARIATION RULES

Because so many real attacks are "please pay this" or "bank details changed", build a non-negotiable process:

- Bank detail changes: Verify via a known phone number (not the email thread)
- Urgent payment requests: Second approver + out-of-band confirmation
- New suppliers/invoices: Additional checks when the email involves links to "shared documents"