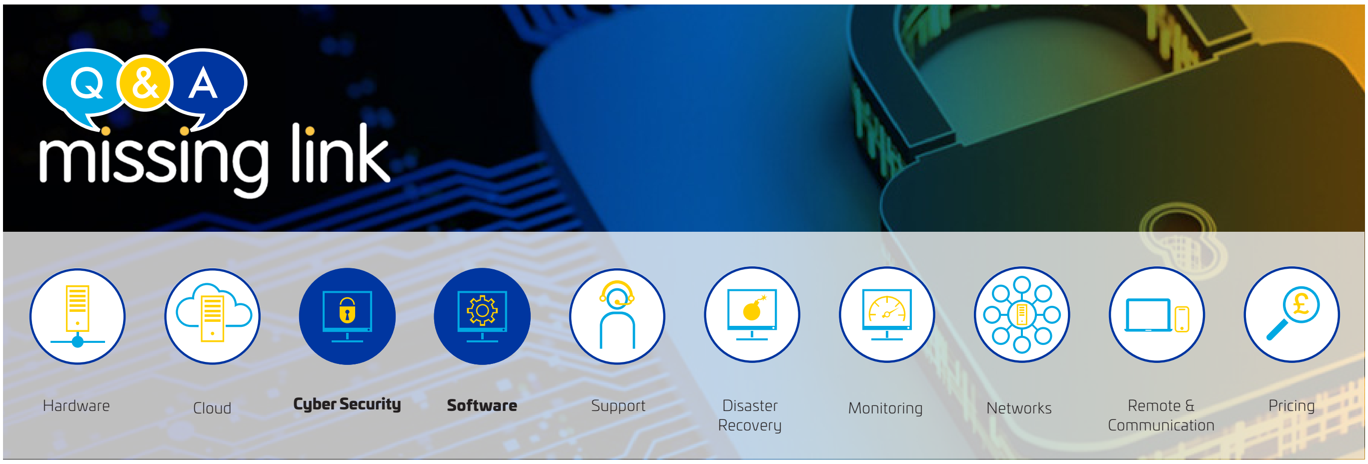

What are Microsoft's best practices for securing email?

Microsoft provides a comprehensive set of best practices and recommendations for securing email, especially when using their Office 365 and Microsoft 365 platforms.

Here are some of the key best practices for securing email:

Enable Multi-Factor Authentication (MFA):
This adds an additional layer of security by requiring two or more verification methods: something you know (password), something you have (a trusted device), or something you are (fingerprint or facial recognition).

Use Strong Passwords:
Encourage users to set strong, unique passwords and consider implementing a password policy that requires complexity and regular changes.

Educate Users About Phishing:
Regularly train and educate users about the dangers of phishing emails and how to recognize them.

Advanced Threat Protection (ATP):
Use Microsoft's ATP to protect against sophisticated threats hidden in email attachments and links, and get cutting-edge defenses against zero-day threats, ransomware, and other advanced malware attempts.

Mailbox Auditing:
Turn on mailbox auditing to log mailbox access by mailbox owners, delegates, and administrators.

Message Encryption:
Use Office 365 Message Encryption to encrypt emails that contain sensitive information. This ensures that only the intended recipient can read the email.

Data Loss Prevention (DLP):
Implement DLP policies to monitor the actions that are being taken on items you've determined to be sensitive and to help prevent the unintentional sharing of those items.

Mobile Device Management (MDM):
Use MDM to control which devices have access to email, enforce device security policies, and perform remote wipes of lost devices.

Anti-Spam and Anti-Malware Policies:
Ensure that Office 365's anti-spam and anti-malware filters are configured and kept up-to-date.

Safe Attachments and Safe Links:
With ATP, you can check email attachments and web links for malicious content.

Configure SPF, DKIM, and DMARC:
These are email authentication methods designed to detect email spoofing and protect users from phishing attacks.

SPF (Sender Policy Framework):
Helps prevent spoofing by verifying that the email is sent from a domain that is authorized to send it.

DKIM (DomainKeys Identified Mail):
Adds a digital signature to emails, allowing the recipient to verify that the email was sent from an authorized system and hasn't been altered.

DMARC (Domain-based Message Authentication, Reporting, and Conformance):
Builds on SPF and DKIM and provides a way for recipients to report back to senders about emails that fail authentication checks.

Regularly Review Security & Compliance Center Reports:
Microsoft provides various reports that can help you identify potential security issues, so it's a good practice to review these regularly.

Limit Mail Forwarding:
Disable automatic mail forwarding to external addresses to prevent data leaks or theft.

Implement Role-Based Access Control (RBAC):
Ensure that only necessary personnel have access to specific features in the Exchange admin center.

Regularly Update and Patch:
Ensure that all systems, including email servers and clients, are regularly updated and patched to protect against known vulnerabilities.

Backup:
Regularly backup emails and ensure that backups are secure and can be restored quickly in case of data loss.

Conclusion

Remember, while these best practices can significantly enhance email security, no system is entirely immune to threats. Continuous monitoring, user education, and staying updated with the latest security recommendations are crucial.
If you want advise on securing your email then Missing Link have a range of security solutions and MFA technologies, so depending on your requirements or risk tolerance we have a solution to suit your needs. If you would like to discuss this or any other related topic, then please contact myself or one of the Missing Link team on info@mlinkuk.com or call 01257 473445 and we will happily guide you through all the pros and cons associated to such a technology.

Contact Information

Phil Heyworth
Commercial Director

E: phil@mlinkuk.com
T: 01257 473445
DDI: 01257 478278
M: 07768 330703
W: mlinkuk.com