SCG®
Midlands

Key Factors to Consider when Protecting your Business Emails

How to protect your business email from cyberattack

Key factors to consider when protecting your business email

In today's digital landscape, email remains one of the primary modes of communication for many businesses. However, it also poses significant security risks, including phishing attacks, malware infections, and data breaches.

At SCG, we understand the criticality of email security and provide comprehensive solutions to protect your organisation from evolving cyberthreats. The following guide highlights the key factors to consider when protecting your business email from cyberattack.

Read on to learn what the key factors are when protecting your business email from malicious attacks.

The key factors...

Achieving total email protection requires a comprehensive approach that considers various aspects of email security. Here are some key factors that a business should consider:

Strong authentication

Implement robust authentication mechanisms such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) to verify the legitimacy of incoming and outgoing emails.

Anti-spam filters

Utilise effective anti-spam filters to identify and block unsolicited or malicious emails. These filters should use advanced techniques like machine learning to continually improve their accuracy.

Anti-malware and anti-virus protection

Deploy reliable anti-malware and anti-virus solutions to scan email attachments and detect any malicious code or malware. Regularly update these solutions to ensure they can identify the latest threats.

Email encryption

Use encryption technologies like Transport Layer Security (TLS) to secure email communication between servers. Additionally, consider implementing end-to-end encryption for sensitive information to protect it from unauthorised access.

Phishing protection

Educate employees about phishing attacks and encourage them to exercise caution when interacting with email attachments, links, or requests for sensitive information. Implement tools and systems that can detect and block phishing attempts. Want to know more about phishing and other email threats?

Email archiving and retention

Establish policies and systems to archive and retain emails for a specific duration. This can help with compliance, legal requirements, and retrieval of important communications when necessary.

Employee training and awareness

Conduct regular training sessions to educate employees about email security best practices, such as recognising phishing emails, avoiding suspicious links, and reporting any suspicious activity. Encourage a culture of cybersecurity awareness.

Conduct simulated phishing campaigns to assess the effectiveness of training efforts and identify areas for improvement.

Strong password policies

Enforce strong password policies for email accounts, including the use of complex passwords and regular password changes. Consider implementing multi-factor authentication (MFA) for an additional layer of security.

Regular software updates

Keep email server software, email clients, and security solutions up-to-date with the latest patches and security updates. Regular updates help address vulnerabilities and protect against emerging threats.

Incident response plan

Develop an incident response plan that outlines procedures for handling security incidents related to email, such as a data breach or email compromise. This plan should include steps for containment, investigation, communication, and recovery.

Monitoring and auditing

Implement email monitoring and auditing mechanisms to track and analyse email traffic, detect anomalies, and identify potential security breaches or policy violations.

Ongoing effort

Remember that achieving total email protection is an ongoing effort, and it requires a combination of technical solutions, user awareness, and proactive security measures. Regular evaluation, testing, and updates are essential to maintain a strong defence against evolving threats.

SCG®
Midlands

About SCG

Founded in 1965, SCG has been supporting SME and corporate businesses, along with healthcare and education clients for over 60 years. We provide end-to-end IT, cybersecurity, voice and data communication solutions.

As part of our end-to-end cybersecurity portfolio, our email protection Solutions provide SMEs with Next Generation anti-virus, endpoint detection and response patch management, data loss prevention, mobile device security and endpoint encryption solutions. This allows our customers to focus on their core business functions. Our cost-effective solutions offer peace of mind and help safeguard the business's critical assets in the increasingly complex digital landscape.

Our specialist team helps you find the right mix of products and services for your needs and optimises them with ongoing and unrivalled support.

To find out more about how we could help protect your business against cyberattacks, book a discovery session with one of our cybersecurity specialists.

Get in touch

0330 333 0001
www.scgmidlands.co.uk