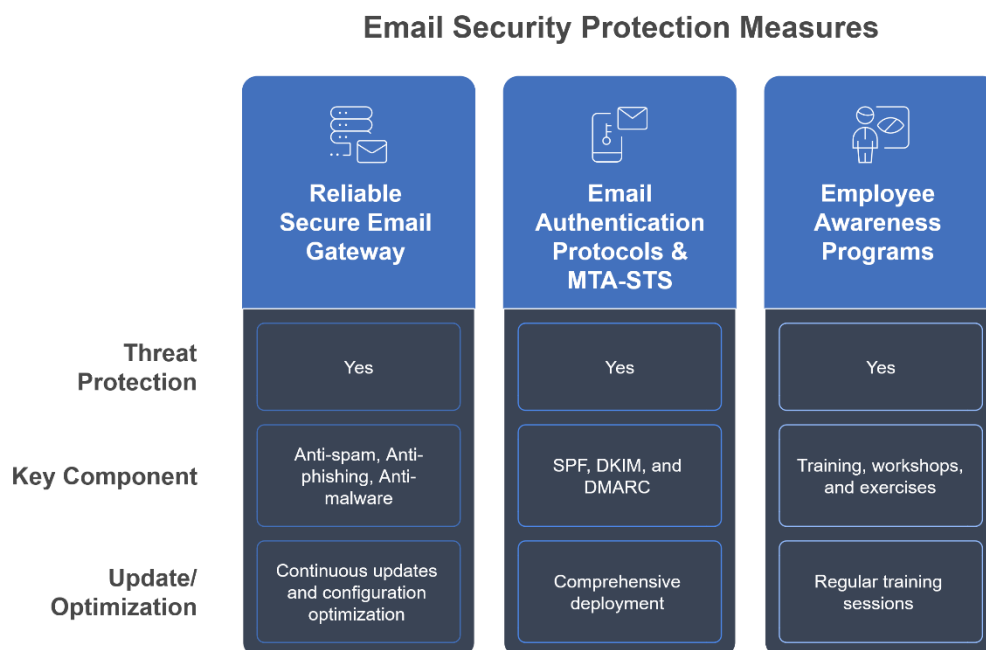


<https://www.thestar.com.my/news/nation/2025/03/14/kitchenware-company-loses-rm258400-in-bec-scam>

It is not the first case reported locally and this is not an isolated threat. Certainly, it's never be the last...

The issue raised an essential yet critical for the businesses (domain owner) of having comprehensive Email Security protection.

1. **Reliable Secure Email Gateway (SEG):** Anti-spam, Anti-phishing, Anti-malware protection through email communication channel. A Secure Email Gateway (SEG) acts as the frontline defense against phishing emails, malware, and other malicious email-based threats. Continuous updates and configuration optimization are essential to address emerging cyber threats effectively.
2. **Email Authentication Protocols & MTA-STS** deployed correctly and comprehensively. Email authentication protocols such as SPF, DKIM, and DMARC are vital for verifying the authenticity of email senders. These protocols work together to prevent email spoofing, one of the common techniques used in BEC scams. Additionally, MTA-STS (Mail Transfer Agent Strict Transport Security) enhances email security by ensuring that email communication is encrypted during transit, mitigating risks of interception and tampering. Implementing these technologies fortifies the organization's defenses against sophisticated email-based attacks.
3. **Employee Awareness Programs:** Employees play a pivotal role in identifying and preventing email-related threats. Awareness programs should educate employees on recognizing phishing tactics, verifying suspicious email requests, and reporting potential scams promptly. Regular training sessions, practical workshops, and simulated phishing exercises are effective in reinforcing vigilance and ensuring a high level of security awareness across the organization.



4. **Conclusion:** A ***multi-layered email security strategy is essential yet it is critical*** to safeguard organizations from threats like BEC scams. By combining reliable SEG solutions, robust email authentication protocols, and empowered employees through awareness programs, companies can significantly reduce their vulnerability to cyber threats. Proactive measures not only protect financial assets but also enhance trust and resilience in today's complex digital landscape.