Complete Email Security for Microsoft 365

Email is a core component of everyday working life within organisations and there is no doubt that it is a great way to communicate with anyone from around the globe. However, it is reported that between 75% and 90% of targeted cyber-attacks start with an email. Email attachments that contain malware and suspicious links are all common threats to SMEs and attackers are using ever more sophisticated techniques, automation and phishing to socially engineer their way into a network.

Technology to Protect your Email Environment

For many years, businesses have used anti-spam technology to help protect against large amounts of unwanted spam email and these are still commonplace today. Microsoft 365 has a built-in level of anti-spam technology, providing a base layer of protection for users.

Complete Email Security for Microsoft 365 will help to further protect against unwanted emails. Built around Barracuda Sentinel software, which detects threats that traditional email security solutions can't. Integrating with Microsoft 365 it will detect attacks coming from both internal and external sources using artificial intelligence (AI) to recognise signs of malicious intent and deception within every email.

cit
Complete I.T.

Core features:

Spear Phishing Prevention

Automatically detecting and preventing spear phishing attacks, the AI engine learns each organisation’s unique communication patterns and leverages these patterns to identify anomalies and quarantine spear phishing attacks in real-time.

Detection of Employee Impersonation

Detecting any type of employee impersonation, including impersonation of executives. It can detect spoofed emails, typo-squatted domains, and impersonation emails sent from free or personal email accounts.

Stop Zero Day Phishing

Discovers anomalous in communication patterns, within the body of the email, the link or the email header to stop zero-day phishing attacks.

Detection of Web Impersonation

Emails impersonating web services such as DocuSign and Dropbox, which are a very successful method of attack and can be very realistic in their look, feel and language are stopped.

Investigate Inbox Rules

Changes to users’ email inbox rules can potentially indicate an account takeover. Alerts can be created to allow for investigation when recent changes to inbox rules are detected.

Detect Compromised Email

Automatically identifies malicious emails sent from compromised accounts and will flag them to administrators.

Complete I.T.