Security Check List for Microsoft 365 Email

backuptechnology
an iomart company

Organizations migrating to Microsoft 365 discover a new way to work and with it, IT Departments discover a new array of challenges.

You have many details to consider before and after moving to a cloud solution, and security should be on the top of the list.

Productivity, collaboration, and email applications are quickly moving to the cloud. Cloud services and, more specifically, email is a favorite entry point for malware, hackers, scammers, and security breaches. In fact, according to a 2019 Verizon Data Breach Investigations Report, **email delivered 94% of malware.**

It is true M365 has some basic security features, but most companies need more advanced security capabilities. Many of which are either beyond those available at Microsoft or expense add on services.

There is a reason companies choose to upgrade from the free and included security provided by Microsoft. The free or included measures are often good enough for consumer protection but simply do not cut it for today's compliance, security, and enterprise requirements.

This checklist should give you a good start towards protecting your Microsoft 365 environment and users. We've split it into two groups.

- ☐ The First checklist has settings for the basic M365 email plan and requires no licensing beyond that. These are the minimum baseline settings that EVERYONE should adopt.
- ☐ The Second checklist has specific advanced and best practice security settings that require additional licensing upgrades from M365.

Security starts with a well-documented plan followed by consistent and robust implementation. We hope this email security checklist helps you secure your data and users.

Are you waiting for the right time to migrate email to M365?

Contact us today and learn more about our M365 Migration Service and see if you qualify for FREE Migration. Reach our email **us.sales@iomart.com** or backup-tech.com.

Checklist: Security Settings and Required Options

This first section requires no further licensing beyond the conventional M365 email programs and includes the recommended baseline that EVERYONE ought to adopt.

- ☐ Enable mailbox auditing log search
- ☐ Configure mobile device policies (ActiveSync or Office 365 MDM)
- ☐ Eliminate legacy protocols
- ☐ Email authentication: SPF, DKIM, and DMARC
- ☐ Disable mailbox auto-forwarding to remote domains
- ☐ Empower multi-factor authentication (admins and users alike)
- ☐ Disable "basic" authentication
- ☐ Block sign-in for all shared mailboxes
- ☐ Adjust anti-spam, anti-virus, and outbound spam policies
- ☐ Configure the default option Alert policies
- ☐ Configure mobile device policies (ActiveSync or Office 365 MDM)

Email Security Facts

- 33% of breaches included social attacks
- 15% of breaches were misuse by authorized users
- 43% of breaches involved small business victims
- 32% of breaches involved phishing
- 71% of breaches were financially motivated
- 29% of breaches involved use of stolen credentials
- 94% of malware was delivered via email (Verizon Data Breach Investigations Report 2019)

The following security measures require licensing beyond the basic mailbox plan. They are highly recommended for all companies and required by regulations for many companies. Although Microsoft's Exchange Online Protection (EOP) covers some of these, they are expensive upgrades and rely on a less effective "traditional" approach.

Security Check List for Microsoft 365 Email

backuptechnology
an iomart company

Backup Technology bundles a "User-Centric" security approach into three simple security tiers. Our monthly price for advanced security is often 54% less than similar options from Microsoft. Please find more information today at backup-tech.com or email us directly at us.sales@iomart.com. Remember, more than 90 percent of targeted attacks start with email, and 99 percent of threats rely on USERS to run malicious code.

Advanced security setting and 24/7 monitoring with alerts to identify threats to prevent and respond to potential future issues. Including notifications for:

- ☐ Any change to security policies
- ☐ Sign-in from unusual locations, unknown devices, or IP
- ☐ Suspicious mailbox activities
- ☐ Administrator abuse
- ☐ Any deleted accounts from hackers
- ☐ Emails sent to external sources
- ☐ Public sharing of company data
- ☐ Management impersonation via email by hackers
- ☐ Newly created accounts by hackers
- ☐ The creation of SharePoint sites
- ☐ Audit Logs Always On
- ☐ Mailbox Audit Logs Always On
- ☐ Multi-factor authentication
- ☐ Spam notifications
- ☐ Block harmful email attachments
- ☐ Prevent users from making their personal info public through their calendar
- ☐ Block mass exfiltration of company email to an external destination
- ☐ Alert you if users are spamming
- ☐ Improve users' password habits
- ☐ Email Continuity in case M365 has an outage
- ☐ Secure email Communications that contain sensitive data
- ☐ Email Archiving for legal holds and regulatory requirements

Internet Security Threats

- 65 percent of attacker groups used spear phishing as the primary infection vector.
- 1 in 36 mobile devices has high-risk apps installed.
- The email phishing rate is the highest for organizations less than 250 employees at 1 in 2,696.
- The rate of employees target by phishing is highest at smaller organizations at 1 in 52.
- The malicious email rate, 1 in 323, is the highest at smaller organizations.
- Scripts are the most common malicious file attachment at 47.5 percent.
- Office files account for 48 percent of malicious email attachments.
(Symantec Internet Security Threat Report 2019)

Our Microsoft 365 (M365) plans are the same as those directly offered by Microsoft. That means the same great features and apps and the same excellent uptime of 99.9%. However, we add more effective and less expensive security services and a personalized approach to ensure you remain fully productive.

"We've discovered M365 clients choosing to be unprotected because Microsoft's "advanced security packages" are cost-prohibitive. Please don't overpay and settle for less. Our comprehensive security packages are up to 54% less than similar options from Microsoft"

Whether you are already using M365 or waiting for the right time to migrate your email, contact us today and learn more about our M365 Migration Service and see if you qualify for FREE Migration via email us.sales@iomart.com or backup-tech.com.

For most business migrations are a one-time activity At Backup Technology, cloud services and migrations are our daily business. We migrate clients from in-house servers, exchange, Gmail, and other mail products to the cloud and M365 every day, all day.

Backup Technology | 800-220-7013 | us.sales@iomart.com | www.backup-tech.com
4801 Woodway Dr Suite 300E Houston, TX 77056