# Microsoft 365 Security Fundamentals

Microsoft 365 (formerly Microsoft Office 365) has grown into an extensive collaboration and communication platform which is used the world over, and by most businesses that we work with. As a subscription-based product there are various increments available depending on whether the basic, standard, or premium package is taken.

Many organisations rely on it for hosted emails, video conferencing, authentication, file sharing and the various cloud hosted applications, and it has become an integral part of the "business as usual" functionality of the workplace.

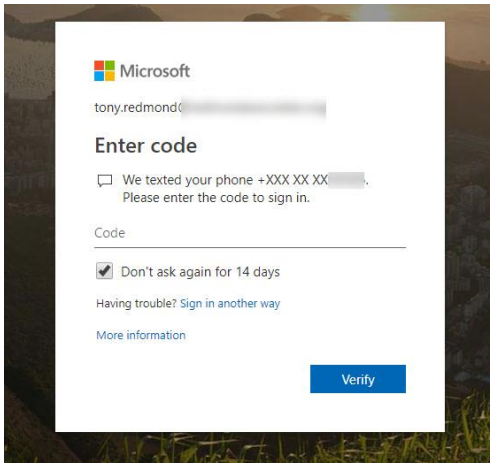
As such, protecting the data, finances and reputation of a business has become an important consideration regarding Microsoft 365.

Therefore, we have prepared a list of **fundamental security controls** that all Microsoft 365 business users should have in place to protect the data that they process in Microsoft 365.

Microsoft Silver Partner

Labyrinth Technology are Microsoft Silver Partners and can review your Microsoft 365 security, implement any necessary controls, and then support them.

## 1. Multifactor Authentication




Multifactor Authentication, also known as MFA, is possibly the most important and effective security control you can implement for Microsoft 365. It is also free and easy to deploy. MFA involves adding a secondary method of authentication which users must input when they sign into a new device or use the 365 web portal. This is in the form of a one-time code sent to an app on the user's mobile phone. With this in place, it is almost impossible for a cyber attacker to access your account.

## 2. Email Security Solution for Phishing, Malware and Spam

You must implement an email security solution which checks emails for phishing, malware, and spam content before delivering them to users' mailboxes. Some of these systems can also scans links in emails when users click on them and block access if they are malicious.

There are many platforms available which provide these features such as Microsoft Defender for Office 365, Vade Email Secure and Mimecast.

## 3. Dedicated Third Party Backup System

**This is important to remember!** Microsoft's terms and conditions are clear; they are not responsible for your data and recommend that you implement your own backups. Labyrinth use Datto's SaaS (Software-as-a-Service) protection system for backing up Microsoft 365 mailboxes, groups, and SharePoint sites.

## 4. Access Management

Granular access should be in place throughout Microsoft 365. Users must only be given access to the minimum data and systems required for their job role. Microsoft 365 groups are generally the best way to achieve this, alongside strict access management processes such as a formal approval process and starters/leavers checklists.

**Access should be periodically audited without fail.**

## 5. User Cyber Security Awareness

Inevitably some phishing emails will slip through the net, so it is important that users understand how to spot them. You should be constantly providing regular guidance to your users, or even take it a step further and implement an ongoing user cyber security awareness platform. Labyrinth Technology have introduced the Cyber-Assure security awareness product, which features **gap analysis, targeted training videos, simulated phishing attacks, policy management and dark web monitoring** (proactive alerts if your user credentials have been leaked as part of a third party data breach).

Labyrinth Cyber-Assure
Protecting your business in the maze of modern technology

## 6. Disable Unused Apps and Features

Most Microsoft 365 subscriptions have many apps bundled in with them. Identify which apps and features your users require and turn of everything that is not being used to minimise risk.

## 7. Mobile Device Management (MDM)

Microsoft 365 has a built-in MDM system available to all exchange (hosted email) users, and also a more advanced MDM platform as part of Microsoft Intune.

Both tools allow you to set conditional access policies which prevent users from signing into Microsoft 365 on their mobile phones and tablets unless they meet the minimum requirements (such as password protection and encryption).

## 8. Notifications for Forwarding Rules

Often when a cyber attacker manages to get into a Microsoft 365 mailbox, they turn on a forwarding rule so they can receive copies of your emails without you knowing even if you change the password. Alerts can be configured to notify your IT team when forwarding and other rules are put in place so they can investigate and confirm they are legitimate. Labyrinth Technology puts this in place as standard for all our clients and contact users to validate such rules.


Article by Matthew Dunn

Director of Support at Labyrinth Technology Ltd


With over a decade of IT service management experience, Matthew heads up our support department. Matthew joined the company in 2015 and ensures that every single one of our clients receives a first-class service from us and are using the best technologies to run their business. He is an expert in cloud services, information security and IT project management, regularly contributing articles on these topics. Prior to joining Labyrinth Matthew was an IT Manager in the financial sector for 5 years.