Microsoft 365 Security Check

Secure your business data and protect users from common cyberattacks

In 2019 the UK Government reported that 32% of large UK Businesses suffered a cyber attack or data breach in the last 12 months. The average cost of a breach to a large business was £22,700.

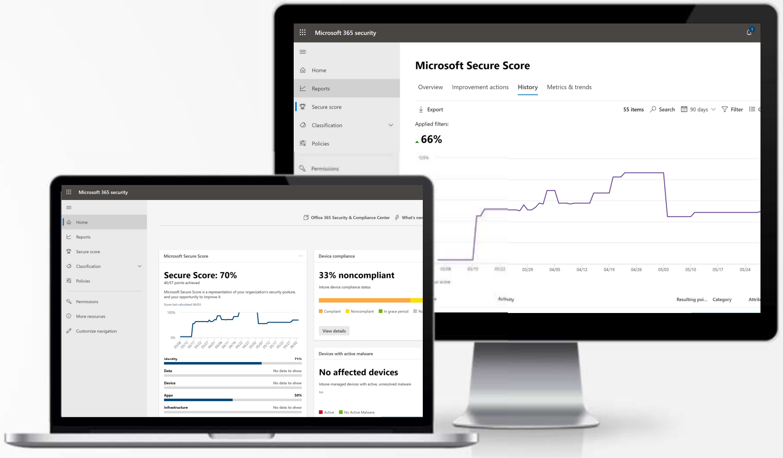
Out of the box, Office 365 has a fantastic array of tools to mitigate many of these common threats and cyberattacks however **they are not enabled by default**. Whilst some features do require specific licences, there are a large number of security settings which can be enabled on any Office 365 subscription.

Recommendations for all Office 365 subscriptions
Regardless of which subscription you have with Microsoft, there are a number of key security features which can be enabled. By configuring these settings, you can dramatically increase your security posture and reduce the risk to your team and your business data.

There are over 50 built-in controls available to;

- Protect your Users from identity impersonation
  - *28% of UK businesses have suffered identity impersonation attacks in 2019*[1]
- Safeguard your business Emails from internal and external threats
  - *80% of UK businesses have suffered phishing email attacks in 2019*[1]
- Set internal and external sharing policies for your business files
- Configure Office 365 global security settings
- Enable Backup for files on local machines into OneDrive for Business

This list is by no-means exhaustive but simply to highlight a number of features which are available to Office 365 subscribers but not enabled by default.



61% of all UK companies suffered some form of cyberattack in 2019

Source: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019

Microsoft 365 Security Check

Security Best Practice from an experienced team

Built from our experience and also using guidelines from the UK Government National Cyber Security Centre, we have developed a 50 point health-check to assess the security of your Office 365 configuration

The security assessment reviews of configurable security settings across;

- Azure Active Directory; the hub for identity and password control in Office 365
- Exchange Online; responsible for email messaging and calendars
- Sharepoint and Onedrive; the home of your business data in the Office 365
- Global System configurations; security policies applied to the wider tenant

We'll produce a 50 point check-list report which will show you;

1. The Severity Level
How serious is the risk of not having this element configured properly?
Colour coded from

Critical or Recommended , to Optional

2. The Attack Kill Chain
i.e. where does this risk and the appropriate protection applies;

- Is it **Pre-Breach** i.e. before an attacker gets in

or

- **Post-Breach**, alerting you that something has happened which needs investigation or Immediate action to be taken.

Outcomes
With our report and guidance in hand, you'll have a full view of the current risks and what actions need to be taken to secure your Office 365 configuration