SECURITY CHECKLIST

How to secure Microsoft 365 across your organisation

Microsoft 365 is now one of the critical foundations of SMEs: email, files, Teams, collaboration, customer data and access to line-of-business applications. When it's poorly configured, it can become a major point of vulnerability, with immediate consequences: business disruption, loss of trust, exposure of sensitive data and high remediation costs.

Microsoft 365 already includes many built-in security features, but their effectiveness depends on how well they're configured, monitored and adopted by users. This checklist helps business leaders and IT managers identify the priorities to address, reduce blind spots and progressively secure their environment.

AN OPERATIONAL RISK, NOT JUST A TECHNICAL ONE

Moving to the cloud brings flexibility, mobility and efficiency. But it also opens up new access points that need protecting: remote connections, personal devices, external sharing, guest accounts and third-party applications. This is therefore not purely an IT matter; it directly affects the organisation's ability to operate, serve its customers and protect its sensitive information.

For an attacker, compromising a Microsoft 365 account can provide access to emails, confidential documents, contracts, customer data, Teams conversations and business tools. In most cases, attacks exploit not the Microsoft platform itself, but insufficiently protected accounts, overly permissive configurations or risky user habits.

DEFAULT SETTINGS AREN'T ENOUGH FOR AN EXPOSED SME

Having the right Microsoft licences doesn't automatically guarantee a good level of security. An organisation can remain exposed if MFA isn't enforced everywhere, if external access is too open, if devices aren't managed, or if users don't know how to recognise a phishing attempt.

Microsoft 365 security needs to be managed as an ongoing process: setting priorities, fixing weaknesses, measuring progress and supporting teams. The goal isn't to add complexity, but to reduce risk while keeping a simple, smooth working experience.

DECISION CHECKLIST: THE MEASURES TO PRIORITISE

01

Turn on multi-factor authentication for every user

Multi-factor authentication adds a verification step at sign-in, for example via the Microsoft Authenticator app or a passwordless method. It's one of the most effective measures for limiting account compromise.

02

Set up Conditional Access policies

Conditional Access policies let you adapt security to context: user, device, location, risk level or application used. They help block suspicious sign-ins while keeping a smooth experience for legitimate use.

03

Block legacy authentication protocols

Older protocols such as POP, IMAP or SMTP Auth can bypass modern protections like MFA. Disabling them significantly reduces the scope for credential-theft attacks.

04

Protect sensitive information

Microsoft Purview and information protection features let you identify, classify and protect sensitive data across documents and emails. This step matters most for organisations handling customer, financial, HR or regulated data.

05

Manage devices with Microsoft Intune or an MDM solution

Device management lets you apply security policies to the computers, smartphones and tablets used to access Microsoft 365. It also makes it possible to selectively wipe corporate data if a device is lost or stolen, or when an employee leaves.

06

Strengthen email security

Email remains one of the main attack vectors. It's recommended to enable anti-phishing protection, attachment and link scanning, as well as SPF, DKIM and DMARC to limit identity spoofing.

07

Keep external sharing under control

SharePoint, OneDrive and Teams make it easy to share files with partners or clients. This needs to be governed so sensitive documents don't stay accessible too widely or for too long.

08

Track your Microsoft Secure Score regularly

Secure Score gives an indication of your Microsoft 365 environment's security level. It helps identify weaknesses, prioritise actions and track improvements to your security posture over time.

09

Keep raising user awareness

Technology alone isn't enough. Staff need to be able to recognise a suspicious email, respond to an unusual request, report an incident and adopt good habits day to day. Training and awareness remain essential pillars of cybersecurity.

AN ESSENTIAL STEP FOR EVERY ORGANISATION

Securing Microsoft 365 isn't just IT best practice. It's a governance measure that protects business continuity, customer data, the organisation's reputation and compliance with data protection requirements.

A properly adapted configuration reduces the risk of compromise, limits the impact of an incident, and demonstrates to both customers and partners that security is being managed seriously and proactively.

NEED TO ASSESS YOUR MICROSOFT 365 ENVIRONMENT?

A Microsoft 365 security audit provides a clear, actionable view of the priority risks: at-risk accounts, overly open access, absence of MFA, poorly controlled sharing rules, insufficient email protection or incomplete compliance settings. The challenge isn't just spotting the weaknesses, but knowing which actions to take first.

At AWSMTECH, we help SMEs move from a Microsoft 365 configuration that simply works to a secure, transparent and manageable environment. Our approach combines technical analysis, risk reporting for leadership, and a prioritised action plan, strengthening protection without complicating teams' day-to-day work.

Want to know if your Microsoft 365 environment is really protecting your organisation?

AWSMTECH can run a clear diagnostic of your configuration and provide you with a prioritised, easy-to-read, actionable plan.

REQUEST A DIAGNOSTIC