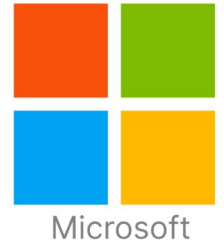


Top 5 Critical Business Premium Security Gaps

Are you really protected, or is your **Business Premium** license leaving you exposed?

Even with Business Premium, many businesses leave gaps that attackers can exploit. Here are the top 5 you must check today.



1

Multi-Factor Authentication Not Fully Enforced

Risk: Accounts are easier to hack if MFA isn't turned on.

Check: Is everyone using MFA every time they log in?

Tip: Use MFA apps, block risky logins, and require it for all users.

2

Conditional Access Policies Missing or Weak

Risk: Hackers could log in from unknown devices or locations if rules aren't set.

Check: Are logins limited by device, location, or risk level?

Tip: Apply strict rules for sensitive users, test regularly, and block risky access.

3

External Sharing Controls Are Too Loose

Risk: Sensitive files could get shared outside your company by mistake.

Check: Can employees share files with anyone outside without approval?

Tip: Require approvals, set expiration on links, and review shared files weekly.

4

Data Loss & Information Protection Not Configured

Risk: Important or confidential info could be sent accidentally or stolen.

Check: Are rules in place to protect sensitive data and emails?

Tip: Label sensitive files, encrypt automatically, and alert on external sharing.

5

Microsoft Defender for Office 365 Not Fully Active

Risk: Harmful emails, links, or attachments could reach inboxes.

Check: Are Safe Links, Safe Attachments, and alerts switched on?

Tip: Enable full Defender, review alerts daily, and train employees on phishing.

Even with Business Premium already set up, it's worth checking these settings regularly to stay fully protected.

If you spot anything or need advice, call **1800 911 000**.

