ALL I.T
data | voice | cloud

8 STEPS TO SECURE YOUR BUSINESS DATA

Is your business data really safe? Implementing these 8 easy steps will help to keep your business data safe.
If you need help to implement these steps and keep your data safe,

contact the All I.T team: 1300 425 548 or security@allitservices.com.au

1. MULTI FACTOR AUTHENTICATION

Multi Factor Authentication (MFA) should be tuned on be default across all platforms and for all users – do not rely on passwords alone!
Without MFA it is not IF you get breached but WHEN!

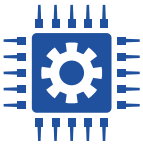
2. EMAIL SETTINGS

Have you had your Microsoft 365 Domain analysed and set for Security?
Microsoft DO NOT have these setups turned on by default:

- Flagging of External Emails
- Phishing Protection – setup of DKIM & DMARC
- Microsoft Security Defaults turned on
- Old Authentication methods such as POP3 disabled

3. ANTI-MALWARE & VIRUS

Whilst a last line of defence Anti-Virus is still important –
Is your protection being managed from a central location in the cloud by your I.T Provider?



4. UPDATES & UPDATE POLICIES

Do you have all your computers configured with the correct update policies to be automatically protected by new releases?
i.e. Microsoft released a warning for a zero day flaw and an update released immediately - **are you automatically protected by these releases?**

5. MICROSOFT OFFICE SECURITY

The Australian Government's Essential Eight Security Model includes recommendations for restricting Macro's within Microsoft Office – this can easily be configured and provides protection against commonly used vectors using macro's

6. USER TRAINING

The largest companies in the world spend millions a year on cyber protection with the very latest in technology deployed - and still get hacked!
The primary reason for this is end users not educated on basic cyber training.
We highly recommend yearly online training that only takes 20 mins per employee

7. BACK UP STRUCTURE

When was the last time you reviewed your back up structure? Do you have:

- Computer data backup
- Microsoft 365 backup: Microsoft DO NOT backup your email and cloud data by default, leaving you exposed from Microsoft error or malicious external or internal activity.
- External Cloud backup of your data: do you have separate 'air-gapped' cloud stored backups to protect your form crypto virus that can potentially lock all your data

8. BANKING SECURITY

We recommend all businesses have in place a process for changing of bank details and employment information that includes verification by outbound phone call –
DO NOT rely solely on email communication