Questions to Ask Your IT Team

1. Online Backup

Do you have offsite backups of ALL your data? This means you won't have to pay a ransom.

2. Email 2FA

Do you have 2FA on your email? This can stop your account from being the attacker of others.

3. AV Protection

Do you have AV that has ransomware protection? This can stop ransomware spreading.

4. Patching

Are all your PC's and Servers patched - ransomware exploits known vulnerabilities in systems. Patching prevents this.

5. Remote Desktop Protection

Have you got a Remote Desktop Server exposed to the internet? (Very high risk). Common way in for hackers.

6. Firewalls

Have you got a good firewall with IPS/IDS that is patched and up to date? This can prevent ransomware communicating with attackers.

7. VLANs

Have you got Virtual LANs in your office? This stops the spread of ransomware internally.

8. Penetration Testing

Have you had a network penetration test? This can show you where you are at risk so you can mitigate it.

9. Anti-Spam

Have you got anti-spam protection to prevent malicious emails hitting your team? -This helps prevent attacks.

10. Cyber Awareness Training

Have your team had cyber awareness training so they can spot risks?

11. M365 Backup

Backup your office365/Gmail - it does not have it as standard.

12. Password Protection Manager

A Password Management Tool alerts you to password breaches & other security problems. Weak or

reused passwords cause 81% of data breaches.

13. Web Filtering

This controls the content an Internet user can access. It can prevent users from accessing sites that execute malicious code on the user's computer.