nostra

Simplify Your I.T.

Questions to Ask Your I.T Team ?

1. Do you have **Cyber Insurance**?

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

3. Do you have **2FA** on your email? This can stop your account from being the attacker of others and is free. You just need to switch it on.

4. Do you have **Anti-Virus** that has **Ransomware Protection**? This can stop ransomware spreading.

5. Are all your PC's and Servers **patched** - ransomware exploits known vulnerabilities in systems. Patching can prevent this.

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

7. Have you got a good **Firewall** that is patched and up to date? This can prevent ransomware communicating with attackers.

8. Have you got **Virtual LAN's** in your office? This stops the spread of ransomware internally.

9. Have you had a **Network Penetration Test**? This can show you where you are at risk so you can mitigate it.

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

11. Have your team had **Cyber Awareness Training** so they can spot risks?

12. Have you enabled all the security functionality available in **Microsoft 365**?

13. Do you have a **Password Management Tool**? This alerts you to password breaches & other security problems. Weak or reused passwords cause 81% of data breaches.