

8 CYBERSECURITY MYTHS

DEBUNKED

Myth

Reality

✗ Your business is too small to be targeted by hackers.



Small businesses made up over half of last year's breach victims.



✗ Strong passwords are enough to keep your data safe.



Two-factor authentication and data monitoring is also needed.



✗ Anti-virus software will keep your business completely safe.



Software can't protect against all cyber attacks.



✗ If WiFi has a password, it's secure.



Any public WiFi can be compromised, even with a password.



✗ Cybersecurity threats are only external.



Insider threats are just as likely, whether from human error or malign intent.



✗ Annual employee security awareness training is sufficient.



Regular phishing exams and training prepares employees to recognize attacks.



✗ You'll know right away if you are hacked.



Modern malware is stealthy and hard to detect.



✗ Cybersecurity is solely the IT Department's responsibility.



Every staff member should be familiar with good cybersecurity practices.



Reality by the Numbers

81%

of hacking-related breaches leveraged either stolen and/or weak passwords.

62%

of SMBs don't have an up-to-date or active cybersecurity strategy in place.

60%

of SMBs will go out of business within 6 months of a cyber incident.