Cybersecurity Myths vs. Facts

What Every Business Needs to Know

AwareSecureCo

Don't let misconceptions put your business at risk.

Here are 8 dangerous cybersecurity myths – and the real facts every business should know.

Myth #1: "Cybersecurity is only an IT issue."

- **Fact:** Cybersecurity is a business-wide responsibility; employees, leadership, and IT all play a role in protecting data and systems.

Myth #2: "Small businesses aren't targeted by hackers."

- **Fact:** 43% of cyberattacks target small businesses because they often lack strong security measures.

Myth #3: "Strong passwords are enough to keep accounts safe."

- **Fact:** Passwords can be compromised, Multi-Factor Authentication (MFA) significantly strengthens security.

Myth #4: "Antivirus software is all I need to be secure."

- **Fact:** Antivirus helps, but true cybersecurity includes updates, training, access **controls, and phishing protection.**

Myth #5: "If I get hacked, I'll know right away."

- **Fact**: Most breaches go undetected for weeks or months; regular monitoring and alerts help detect threats early.

Myth #6: "Public Wi-Fi is safe if I don't enter passwords."

- **Fact**: Hackers can intercept data even if you're just browsing. A VPN encrypts traffic and protects sensitive information.

Myth #7: "I don't need backups, my data is in the cloud."

- **Fact**: Cloud storage can still be attacked; regular secure offline backups ensure recovery from cyber incidents like ransomware.

Myth #8: "Employees automatically know how to spot cyber threats."

- **Fact**: Phishing and scams are more sophisticated than ever; regular training is crucial to keep employees cyber aware.