Why SMBs must prioritize cybersecurity in 2025

The 5 main cyberthreats

SMBs faced last year include ransomware attacks, phishing and malicious emails, exploitation of vulnerabilities, compromised IT companies and AI-enabled attacks.[4]

43%
of cyberattacks target small businesses.[1]

45%
of SMBs reported losing revenue to a cyberattack.[2]

83%
of SMBs are not prepared to recover from the financial damages of a cyberattack.[3]

Why cybersecurity matters

Growing threats:

As technology advances, so do the methods of cybercriminals. SMBs are increasingly vulnerable.

Financial impact:

Data breaches can lead to significant financial losses, legal fees and reputational damage.

Operational disruption:

A major breach can disrupt business operations, leading to downtime and lost productivity.

Essential cybersecurity measures

Regular data backups

Why Ensure you never lose critical information.

How Schedule automated backups and store data in secure, offsite locations.

Employee phishing training

Why Help employees recognize and thwart potential threats.

How Conduct regular training sessions and simulate phishing attacks to test readiness.

Multi-factor authentication (MFA)

Why Add an extra layer of security.

How Implement MFA for all user accounts and sensitive systems.

Robust disaster recovery plan

Why Get back to business quickly after a breach.

How Develop and regularly update a comprehensive disaster recovery plan.

Contact us

to schedule a free cybersecurity consultation.

Technology Warehouse
+26461416303 support@tw.na
https://www.tw.na

Sources: 1. Accenture's Cost of Cybercrime Study. 2. Identity Theft Resource Center. 3. Cybersecurity Magazine. 4. Acronis H1-24 Cyberthreats Report.