

How Secure is Your Business?

Cyber threats are no longer just a risk—they're a certainty. Canadian Small and Medium Enterprises (SME) are being targeted at an alarming rate, yet most still lack the essential defences needed to prevent financial losses, operational disruption, and reputational damage.

The good news? With the right steps, you can strengthen your cyber resilience and protect your business.

1. Key Findings from the F12 Cyber Health Risk Report

54% of SMEs still believe they are too small to be targeted.1



43%

of cyberattacks are aimed at SMEs-because attackers know they are easier targets.2



Less 20% have dedicated cybersecurity resources in place.3

Only 8 % of small businesses have a dedicated cybersecurity budget, and nearly have no cybersecurity budget at all.4



2. F12 conducted thousands of cyber assessments with SMEs across Canada. The data reveals:

94% of SMEs are not following baseline cybersecurity best practices, making them highly vulnerable to phishing and ransomware.5





Average Initial

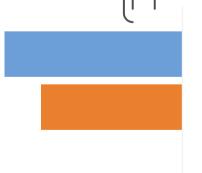
Cyber Health Risk Score:

(Think of it like a credit score—but for cyber security).

Average Improvement with F12's Best Practices: 96% in just 30 days.

The F12 Cyber Health Risk Score is based on industry-leading frameworks like SOC 2 Type 2 and NIST, providing SMEs with a clear, actionable roadmap to strengthen their cybersecurity posture.

3. Measuring Cyber Risk & Resilience



of cyberattacks stem from human error. Yet of SMEs lack structured

cybersecurity awareness training.7

Process



of SMEs do not have a formal incident response plan.8

Tools







Security, 2024. 9. "55% of SMEs Never Perform Vulnerability Scans," IACIS Report, 2024.

provide password management tools to their employees.

Cyber Resilience Starts Here. Stay Secure, Stay Ahead.

Get Your Free Cyber Health Risk Assessment

and see where your business stands.