Protecting your business from cybercrime

MADE EASY WITH CYBOTS

CYBOTS

CYBER THREATS DON'T SLEEP. **NEITHER DO WE.**

Cybercrime — a sophisticated enemy

"TODAY, CYBERATTACKS FROM INCREASINGLY SOPHISTICATED ACTORS THREATEN ORGANISATIONS ACROSS EVERY SECTOR AND WHETHER A LARGE ASX100 COMPANY OR A LOCAL BAKERY, ORGANISATIONS OF ALL SIZES NEED TO TAKE STEPS TO LIMIT THE DANGERS POSED BY THESE THREATS."

Microsoft

Source: Australia's Cyber Security Strategy 2020

With cybercrime on the rise across Australia and New Zealand more than ever, protecting your business from its impact has never been more essential.

The coronavirus pandemic has highlighted how cybercriminals can take advantage of national and global crises to conduct data breaches, mass phishing scams and targeted attacks against vulnerable businesses. Malicious online actors are infiltrating systems from anywhere in the world, targeting critical infrastructure and stealing intellectual property, and rely on common lapses in cybersecurity to maximise their chances of success.

To help protect people and businesses from cybercrime, the Australian Government is investing $1.67 billion in cybersecurity regulations and bold initiatives, along with policy changes to set a strong foundation for active defence. This also means there will be stronger incentives for Australian businesses to invest in cybersecurity.

This guide outlines the evolution of cybercrime in Australia, how it affects small to medium businesses, which industries are being targeted and what actions you can take to advance your protection against the damage of cybercrime.

Cybots is Australia and New Zealand's first AI-powered cybersecurity solutions specialist, and helps every business advance its protection against cybercrime.

We're on a mission to make cybersecurity easier, flexible and more affordable for every Australian business as the influx of cybercrime continues to grow. Our unique systems are expertly built to the specific needs of all small to medium enterprises with up to 200 employees, and comprehensively support the Australian Government Cybersecurity strategy.

Cybercrime in Australia

"SMES ARE ESPECIALLY VULNERABLE TO CYBER SECURITY THREATS...SMES OFTEN LACK THE RESOURCES OR EXPERTISE TO DEFEND THEMSELVES AND THAT THERE CAN BE A LARGE IMPACT ON REGIONAL COMMUNITIES WHEN CYBER CRIMINALS TARGET SMES."

Commonwealth Bank of Australia

Source: Australia's Cyber Security Strategy 2020

Pandemic-driven cybercrime drove incidents to a new high in 2020-21

- 67,500 cybercrime reports, a nearly 13% increase from the previous financial year
- $33billion lost by businesses that reported cybercrime
- 87% of SMEs believe antivirus software alone can protect their business from cyberattacks, yet 64% have experienced disruption from cybercrime
- Medium businesses lost $33,442 on average due to cybercrime in 2020/21
- Small businesses lost $8,899 on average due to cybercrime in 2020/21
- Approximately one quarter of reported incidents affected entities associated with Australia's critical infrastructure
- Nearly 500 ransomware cybercrime reports, a nearly 15% increase from the previous financial year

Source: ACSC Annual Cyber Threat Report 2020-2021

TOP 5 REPORTING SECTORS FOR RANSOMWARE-RELATED CYBERSECURITY INCIDENTS

1. Professional, scientific and technical services
2. Health care and social assistance
3. Manufacturing
4. Education and Training
5. State, Territory and Local Government

Cybercrime in Australia

How cybercrime can impact SMEs

- Sustained disruption of essential systems and associated services
- Exfiltration or deletion/damage of key sensitive data or intellectual property
- Malware, beaconing or other active network intrusion
- Low level malicious attack – targeted reconnaissance, phishing, non-sensitive data loss
- Scanning or reconnaissance

What you can do as a SME

- Report all cybercrime and cybersecurity
- Know your networks
- Patch within 48 hours where an exploit exists
- Prepare for a cybersecurity incident by having an incident response, business continuity and disaster recovery plans in place and test

Source: ACSC Annual Cyber Threat Report 2020-2021

HOW YOU AND YOUR EMPLOYEES CAN STAY SECURE ONLINE

Privacy Be wary of what is shared and with whom

Passwords Create strong passwords to be secure

Suspicious messaging Treat any unexpected messages with caution

Surfing safely Avoid malware – keep to trusted websites

Online finance and payment Keep financial details from prying eyes

Tablets and mobiles Be mindful when using free Wi-Fi

Backups and protection Backup and update for safety

Reporting Keep everyone safe by reporting scams

Get back to business faster with Cybots' advanced AI-powered protection

Proactively protect your business from costly impact and disruption of cybercrime with Cybots unique AI-powered cybersecurity solutions. Our first of its kind technology delivers advanced protection, fast detection and zero downtime in the event of a threat.

- ✓ Instant threat detection
- ✓ 15 minute response
- ✓ Simple, affordable & flexible plans
- ✓ Peace of mind
- ✓ Future proof potential risk

As a leader in cybersecurity across Asia Pacific, Cybots provides effective, efficient and affordable cyber defence solutions, using cutting-edge and focussed cyber military defence-standard protocols with zero network interruptions to rapidly deliver actionable insights.

READY TO PROTECT YOUR BUSINESS?

CONTACT CYBOTS AUSTRALIA / NEW ZEALAND
contactus@cybotsai.com
Level 5, 111 Cecil St, South Melbourne

Read the latest on Cybersecurity from the Australian Government

Small Business Cyber Security Guide
Cyber Security Strategy 2020
Annual Cyber Threat Report 2020-2021