Microsoft

CYBER CRIME IN NEW ZEALAND

WHAT YOU NEED TO KNOW

Cyber crime is the term used to describe a range of online criminal activities ('cyber attacks') carried out against individuals, businesses and other organisations. It's on the rise and here are the key threats all businesses should know about and how to protect against them.

Increase in cyber security incidents recorded by the NZ National Cyber Security Centre

2015 → 2016

78%

200,000+

New Zealand businesses targeted by cyber attacks in the last year

$19,000

Average cost of cyber attacks to New Zealand businesses

THE IMPACT OF CYBER CRIME

Effects of cyber crime reported by small and medium businesses

- DOWNTIME 45%
- PSYCHOLOGICAL STRESS 41%
- EXPENSE 29%
- PRIVACY BREACH 16%
- FINANCIAL LOSS 15%
- DATA LOSS 12%

THREE TYPES OF CYBER ATTACKS YOU SHOULD KNOW ABOUT

PHISHING ATTACK

Attacks are usually conducted through emails and websites which have been disguised to appear legitimate and attempt to trick recipients into providing sensitive information like passwords and bank account numbers.

RANSOMWARE ATTACK

Ransomware attacks encrypt victims' data or computers unless they pay a ransom. It is a type of malware, the collective term used for a range of "malicious software" including computer viruses, Trojan horses, spyware, adware and any software designed to facilitate unauthorised access to a computer.

DDoS ATTACK

DDoS stands for 'Distributed Denial of Service'. These attacks involve cyber criminals targeting a specific website or network, and overwhelming it with web traffic or data until it 'crashes' and becomes inaccessible for its intended users.

NEW ZEALAND BUSINESSES UNPREPARED FOR GROWING THREAT

x3

Ransomware events around the world tripled between the first and third quarters of 2016 - a 200% increase in just six months.

55%

of New Zealand organisations either don't have an incident response plan for cyber crime, or have one but it's not yet operational.

50%

Only half of board members request information about their organisation's state of cyber readiness.

10 WAYS TO PROTECT YOUR BUSINESS FROM CYBER ATTACKS

EDUCATION is the first line of defence - ask employees to read basic guidance and/or complete training that details common methods of malware attacks.

REVOKE ACCESS privileges when an employee changes roles, leaves the company, or no longer requires access to certain data.

Consider implementing **EMAIL PROTECTION SOLUTIONS** that can help prevent malware and phishing attempts from reaching employees' inboxes.

Have a clear **BRING YOUR OWN DEVICE** ('BYOD') policy in place.

Enforce **STRONG PASSWORD AND IDENTITY MANAGEMENT** ideally with multi step identity verification.

Consider **MIGRATING** your apps and services to a public cloud service provider to leverage advanced security capabilities.

KEEP YOUR SOFTWARE UP TO DATE - including websites - be vigilant with updates and patches.

RESTRICT ACCESS and administrative privileges only to staff who require them to perform their jobs.

Use a **REAL TIME INTERNET PROTECTION & ANTIVIRUS PROGRAM** on all devices used for business.

Use **APPLICATION WHITELISTING** to help prevent malicious software and unapproved programs from running.

SOLUTIONS

PREVENT IDENTITY COMPROMISE
Help protect against compromise while uncovering potential breaches

SECURE APPS & DATA
Boost productivity with cloud access while helping keep information protected

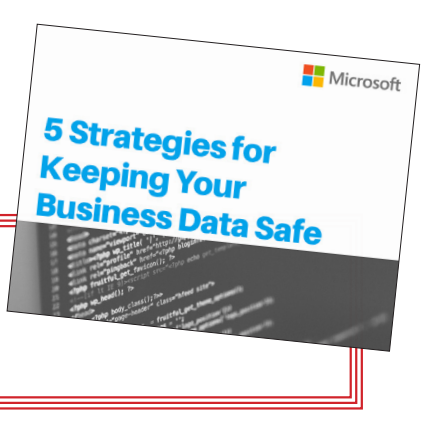
EXPAND DEVICE CONTROLS
Deliver enhanced security across both company and personal devices

WE BUILD SECURITY INTO MICROSOFT PRODUCTS AND SERVICES FROM THE START.
Find out about Microsoft solutions at http://aka.ms/keepsafe

WHAT TO DO IF YOU EXPERIENCE A CYBER ATTACK

1. Refer to your cyber crime incident response plan outlining company procedure in the event of various cyber attacks.
2. Contact your IT support partner
3. Microsoft — If you don't have an IT support partner, find one through us at http://aka.ms/findapartner
4. Notify the NZ Computer Emergency Response Team (CERT) at cert.govt.nz
5. Notify any affected parties (customers, partners or internal staff)

LEARN MORE



Learn more about strategies for protecting your business against cyber crime and data loss with our free ebook **'5 Strategies for Keeping Your Business Data Safe'** which you can download at **https://aka.ms/securityebook**