CYBERCRIME: THE RISK IS REAL

DON'T LET YOUR BUSINESS BECOME THE NEXT CYBERCRIME STATISTIC.

netcare

THE NETCARE CYBER CHECKLIST

1. INSTALL SOFTWARE UPDATES

One of the most effective things you can do to keep your system safe.

2. IMPLEMENT TWO-FACTOR AUTHENTICATION:

When someone logs in with a username and password, they need to provide something else to verify their identity.

3. ENSURE DATA IS SAFELY BACKED UP.

If data is lost, leaked or stolen — you'll have a backup, or copy, so you can restore it.

4. SET UP LOGS.

Logs alert you to any unusual or unexpected events that you need to know about – for example multiple failed log ins.

5. CREATE A RESPONSE PLAN.

No cybersecurity is 100% safe, but if you have a response plan in place, damage and stress can be kept to a minimum.

6. SECURE YOUR DEVICES

Enable anti-malware software on any device that accesses your business data or systems - even more important with staff working at home.

7. SECURE YOUR NETWORK

Configure network devices to secure and control connections in and out of your business network.

GET YOUR CYBERSECURITY SORTED TODAY

0800 378 888 | NETCARE.NZ

netcare

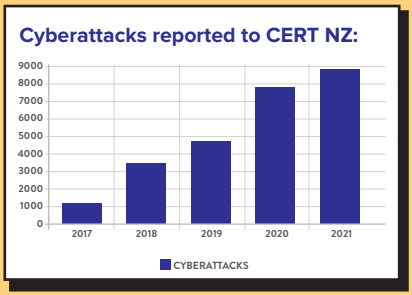
HOW TO PROTECT YOUR BUSINESS AGAINST THE GROWING THREAT OF CYBERATTACKS.

Cyberattacks are becoming more and more regular in New Zealand.

Think Waikato DHB, where sensitive patient information was held captive by hackers. Or the New Zealand Stock Exchange which was brought to a standstill by a cyberattack. Or where hackers infiltrated the I.T. system of Pinnacle Health and accessed personal data from 450,000 patients.

Unfortunately, these publicised attacks are just the tip of a growing iceberg.

In 2021 there were over 8,831 cyberattacks reported to CERT NZ, costing companies around $16.8m.



WHAT TO LOOK OUT FOR:

PHISHING
A scam that tricks employees into clicking links that appear legitimate but are malicious. The link infects your device with malware allowing criminals to access your I.T. system and steal sensitive information.

VIRUSES / RANSOMWARE
Hackers capture sensitive data or take down your network and demand payment for restored access (hold you to ransom).

LACK OF STAFF TRAINING
Human error always provides cybercriminals with opportunities - especially when employees are not trained in basic cybersecurity practices, for example, password security or how to recognise fake emails.

POOR DATA MANAGEMENT
When massive amounts of unnecessary data are kept, it's easier to lose and expose essential information. A vulnerable data storage setup can also leave companies exposed.

HOW NETCARE CAN HELP YOUR BUSINESS BE CYBERSAFE

1 WE GET THE 'TECH' SIDE RIGHT

We understand that each business has different cybersecurity needs, so we'll start by conducting a Cybersecurity Audit that allows us to see where the gaps are.

We then put the technical 'nuts and bolts' in place - to make sure your operating systems and data storage are secure - and provide reliable defence against ransomware, viruses, malware and other threats.

2 WE GET THE 'PEOPLE' SIDE RIGHT

The most robust technical measures can be worthless if your staff don't follow basic cybersecurity procedures.

Netcare train, audit and support businesses to adopt stronger cybersecurity practices and protocols. Ensuring a safe digital environment for staff and providing peace of mind for customers and clients.

HOW DOES YOUR CYBERSECURITY RATE?

TAKE OUR FREE 1-MINUTE CYBER HEALTH CHECK. GO TO: NETCARE.NZ/CYBER-HEALTHCHECK