SECURITY FOR YOUR SMALL BUSINESS

New Zealand

A guide to help keep your small business secure.

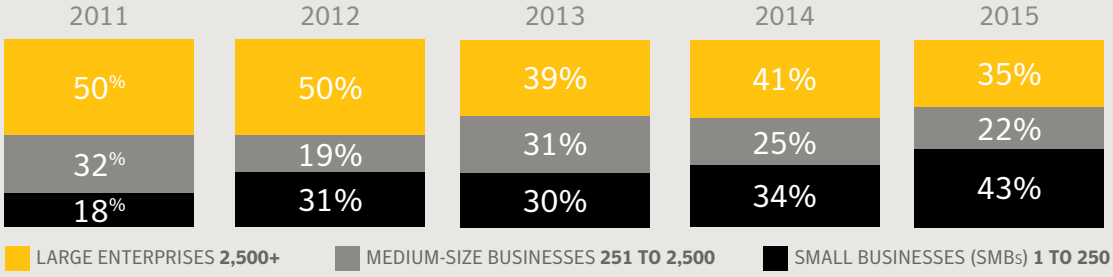
Norton by Symantec

RUNNING A BUSINESS IS NO SMALL FEAT

In today's evolving digital landscape, security is key. Whether you're a one person business working from home, a team in a shared office space, or have a flexible travelling setup, it is important to ensure the safety and security of your company's network, client information and vendor details.

Small to medium businesses (SMBs) have increasingly become victims to cyberattacks. The below graph shows the steady increase in targeted attacks on small businesses since 2011.[1]

SPEAR-PHISHING ATTACKS BY SIZE OF TARGETED ORGANISATION



New Zealand SMBs are not exempt from targeted cyberattacks as highlighted in the recent Norton SMB Cybersecurity Survey.

ALMOST 1 IN 5 SMALL BUSINESSES HAVE BEEN TARGETED BY A CYBERATTACK

THE TYPES OF CYBERTHREATS THAT HAVE IMPACTED THESE SMBs?

Email or phishing scam (an attempt to acquire sensitive information such as user names, passwords and credit card details)	**70%**
Hacking attempt	**47%**
Ransomware scam (a virus that encrypts your files and then requests a ransom payment to recover them)	**17%**
Online identity fraud (obtaining the personal or financial information of another person for the sole purpose of assuming that person's name or identity to make transactions or purchases)	**11%**
An accidental loss of a laptop or mobile device or well-meaning employee distributing confidential data unintentionally	**9%**
Privacy or data breach (unauthorised access to, or collection, use or disclosure of personal information either by an organisation or individual)	**7%**
An internal threat such as employee stealing data on USB key or leaking information to competitors	**2%**
An employee posting confidential information on a social networking site	**1%**

OF THE BUSINESSES WHO HAD EXPERIENCED A CYBERATTACK: ALMOST THREE QUARTERS HAD FALLEN TO AN EMAIL OR PHISHING SCAM[1]

Source
1. Symantec Internet Security Threat Report 22, 2016
2. Norton SMB Cyber Security Survey - New Zealand, 2016

Norton by Symantec

TOP ONLINE THREATS TO AVOID

It's important to know what you're up against.

While many business owners may know they need to protect themselves from viruses, there is more to digital security than just antivirus. The world of cybercrime has evolved to adapt to changing online habits, and there are a whole host of cyberattacks and threats that could put your devices and business-critical data at risk.

MALWARE

"Malicious Software" is a category of malicious code that includes viruses, worms, and Trojan horses. They seek to exploit existing vulnerabilities on systems making for an easy entry.[3] It also includes apps for mobile devices, such as those running Android and iOS operating systems.

PHISHING

Essentially an online con artist, phishers are nothing more than tech-savvy con artists and identity thieves. They use SPAM, malicious Web sites, email messages and instant messages to trick people into divulging sensitive information, such as bank and credit card accounts, or perform an activity such as transfer funds or make payment on a fake or fraudulent invoice.[4]

RANSOMWARE / CRYPTO-RANSOMWARE

Another form of Malware, the scam works by disabling the victim's device until a ransom is paid to restore access or decrypt your files. They're most commonly found on suspicious websites, and emails. Even if a victim pays the ransom, it doesn't guarantee functionality is restored. The only way to completely restore access is to remove the malware.[5] Ransomware can be particularly crippling for a small business that can't afford downtime without access to business-critical data.

SOCIAL MEDIA SCAMS

Facebook and Twitter have collectively over 1 billion active monthly users - a haven for scammers. Often fake news, sensationalised click-bait type links are designed to lure users to download special plugins to view the story, and thus the user has downloaded spyware on to their device, collecting personal or confidential information.[6] It's important that all employees in a small business are aware of these risks and what is considered acceptable social media usage when at work or on work devices.

MOBILE DATA LOSS

As mobile devices have become indispensable to SMBs for day to day activity, they become a more attractive target for criminals. There is often a huge amount of confidential data that is stored on, or able to be accessed from work mobile devices such as email messages, customer contacts and accounting or taxation apps. Data on these devices can be intercepted or lost in many ways - from mobile malware downloaded from seemingly innocent-looking apps, to device theft or loss. It's important that small business operators think of their mobile devices as an extension of their office computers and secure them appropriately.

PUBLIC WI-FI

Hackers exploit unsecured public Wi-Fi networks to intercept email messages, passwords, login credentials, or any other unencrypted information. Some hackers even create rogue hotspots that have seemingly legitimate names, such as "Official Airport Wi-Fi," so they can eavesdrop on all of your online activities and steal your confidential information.

3. https://nz.norton.com/security_response/malware.jsp
4. https://nz.norton.com/security_response/phishing.jsp
5. https://nz.norton.com/ransomware/article
6. https://community.norton.com/en/blogs/norton-protection-blog/top-ten-cyber-security-predictions-2017

Norton™ by Symantec

RANSOMWARE ATTACKS ON THE RISE

Ransomware was one of the most significant threats facing both individuals and organisations in 2016. Symantec's Internet Security Threat Report 22, 2016 revealed an alarming 36% increase in global ransomware detections.[7]

Ransomware infections occurring in enterprise and other organisations accounted for roughly 31% of infections (as opposed to consumer based) for most of 2016, until December 2016 with enterprise and other organisations increasing to close to 50%.

GLOBAL RANSOMWARE DETECTIONS

5% OF SMBs AFFECTED BY A **RANSOMWARE ATTACK**[8]

AVERAGE RANSOM PAID BY NZ SMBs
USD $1,340[8]

67%
OF BUSINESS OPERATORS WERE **LIKELY TO REPORT A RANSOMWARE ATTACK TO THE POLICE**

68%
OF BUSINESS OPERATORS **DON'T THINK THEY WOULD LAST A WEEK** WITHOUT CRITICAL BUSINESS INFORMATION

31%
OF BUSINESS OPERATORS **DON'T THINK THEY WOULD PAY A RANSOM**

7. Symantec Internet Security Threat Report 22, 2016
8. Norton SMB Cyber Security Survey - New Zealand, 2016

Norton by Symantec

TURN UNCERTAINTY...

Here are our best practices to help keep your business safe from cybercriminals:

- **Don't wait until it's too late to know your business:** It's tough running a small business at the best of times and sometimes businesses overlook things and then it's too late. Businesses shouldn't wait until they've been hit by a cyberattack to think about what they should have done to secure their information. Not only is downtime costly from a financial perspective, but it could mean the complete demise of a business. SMBs need to begin understanding the risks and the security gaps within their business before it's too late.
- **Invest in security and backup:** To reduce the risk of being hit by a cyberattack, SMBs must implement comprehensive security software solutions such as Norton Small Business for all their devices. Businesses should also use backup solutions to protect important files, such as customer records and financial information, and should consider encryption to add further protection in case devices are ever lost or stolen.
- **Keep up-to-date:** Ensure all your company devices, operating systems, software and applications are always up to date with the latest versions and patches. It's a common pitfall for many small businesses to delay software updates but outdated software, operating systems and applications can have security vulnerabilities that can be exploited, leaving many small businesses open to cyberattacks.
- **Get employees involved:** Employees play a critical role in helping to prevent cyberattacks, and should be educated on security best practices. Since small businesses have fewer resources, all employees should be vigilant and know how to spot phishing scams, ransomware attacks and be aware of which sites they can visit on their work devices. Small businesses should invest in educating employees so they become your best line of defence against cyberattacks, not your weakest link.
- **Use strong passwords:** Use unique passwords for all your devices and business accounts. Change your passwords every three months and never reuse your passwords. Additionally, consider encouraging staff to use Norton Identity Safe, to further protect your information and keep cybercriminals at bay. Wi-Fi networks should also be password protected to help ensure a safe working environment.
- **Get Wi-Fi savvy:** When connecting to public wi-fi or unsecured networks, make sure you use a virtual private network (VPN) such as Norton WiFi Privacy, so all data sent and received is encrypted. Norton WiFi Privacy helps to prevent hackers from eavesdropping on your online activity and intercepting confidential data. This is particularly important when working from locations away from your office, such as airports, hotels or cafes.

Norton by Symantec

... INTO SECURITY

PC PCMAG.COM EDITORS' CHOICE 39 TIME WINNER

iOS

Don't let a security breach ruin your hard work.

Norton Small Business combines enterprise-grade security with ease-of-use designed for you. A single subscription helps protect all of your business' devices; such as computers, smartphones, and tablets from viruses, malware and other online threats, helping safeguard sensitive company and customer data. With simple setup and ongoing support, Norton Small Business requires no specialist IT skills, so peace of mind comes easy.

9. Norton Small Business covers PCs, Macs, Androids, iPads and iPhones. Some features are not available on iPad and iPhone.

Auto-scan of apps on Google Play supported on Android 4.0.3 or later except for Samsung devices. Samsung devices running Android 4.2 or later are supported. For earlier versions of Android, the Google Play "Share" function must be used to scan apps on Google Play.

Norton by Symantec

NORTON™ SMALL BUSINESS

Protection built for big business.
Simplicity designed for yours.

Spam Blocking
Helps keep unwanted, dangerous, and fraudulent emails out of your employees' computer inboxes.

Download Insight
Helps prevent your employees from downloading files from questionable websites to help protect your business from being infected by malicious files.

Cybercrime Prevention
Helps secure your business against viruses, malware, spam, ransomware and targeted attacks.

Scalable and Flexible
Allows you to easily add protection to new devices, or move protection between devices as your business needs grow or change.

Multiple Devices
PCs, Macs, Android and iOS[10] devices. Norton helps keep data secure, no matter where it lives.[11]

Speed and Ease of Use
Helps you secure multiple devices in minutes with quick, centralised setup, easy-to-use email based on-boarding and a cloud-based management console.

App Scanning
Scans and checks the apps on Android mobile devices for malware and greyware and helps protect against potential privacy risks such as exporting your contacts, calendar and call logs.[12]

Always Up-to-Date
Helps you stay secure with automatic updates that download and install important product and feature updates when you or your employees are not using your computers.

Support Whenever you Need
Any of your employees can call to get help from a certified Norton technician. Lost or stolen devices can be reported and locked in the middle of the night.[12] Unlimited support is available 24x7 for anyone on your team.[13]

Protection Promise
We offer a 100% money-back guarantee with your subscription. A Norton expert will be able to help keep your devices virus-free or give you a refund.[14]

SECURE YOUR SMALL BUSINESS NOW ›

10. Some features not available on Mac, iPhone or iPad.
11. To check operating system requirements, visit https://nz.norton.com/small-business
12. Feature available on Android only.
13. English only.
14. Virus Protection Promise, conditions apply. Click here to view.

Norton™ by Symantec


Norton™
by Symantec