SECURITY FOR YOUR SMALL BUSINESS

Australia 2017

A guide to help keep your small business secure.

Norton by Symantec

RUNNING A BUSINESS IS NO SMALL FEAT

Small business operators have increasingly become aware of the prevalence of cyber security based attacks. The majority of businesses require Internet access in their daily operations, whether it be from an office location, travelling, or working remotely.

The growing need for cyber security to ensure the safety and security of your business' network, client information and vendor details are paramount to avoid the downtime and potential financial loss associated with many cyber attacks.

The recent 2017 Norton SMB Cyber Security Survey reveals that Australian small businesses are becoming more cyber security savvy as they prepare to future-proof their business.

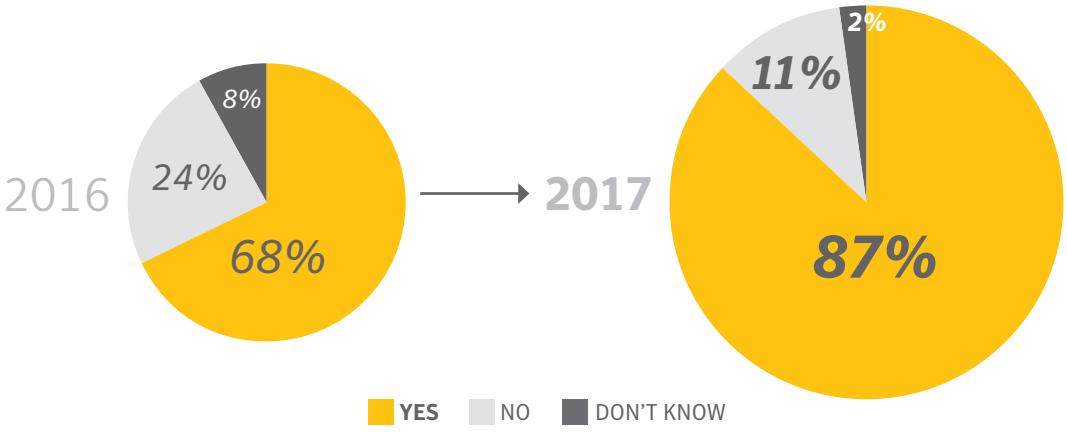
ALMOST 1 in 4 BUSINESSES (25%)
HAD BEEN AFFECTED BY A CYBER ATTACK
OR HACKING ATTEMPT
INCREASED FROM 19% IN 2016[1]

OVER 1/3 OF BUSINESSES

DON'T THINK THEY WOULD LAST A WEEK

WITHOUT CRITICAL BUSINESS INFORMATION

SMALL BUSINESSES THAT IMPLEMENT AN INTERNET SECURITY SOLUTION



2017: 13% of SMB have no internet security solution[2], thus not protected from cyber threats

Source
1. Norton Australian SMB Cyber Security Survey, 2016
2. Norton Australian SMB Cyber Security Survey, 2017

Norton by Symantec

HOW BUSINESSES HAVE BEEN IMPACTED

THE TYPES OF CYBER THREATS THAT HAVE IMPACTED THESE SMBs?	2017[2]	2016[1]
Email or phishing scam (an attempt to acquire sensitive information such as user names, passwords and credit card details)	**54%**	**52%**
Hacking attempt	**36%**	**35%**
Ransomware scam (a virus that encrypts your files and then requests a ransom payment to recover them)	**28%**	**28%**
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)	**12%**	**10%**
Privacy or data breach (unauthorised access to, or collection, use or disclosure of personal information either by an organisation or individual)	**11%**	**14%**
An accidental loss of a laptop or mobile device or well-meaning employee distributing confidential data unintentionally	**7%**	**7%**
An employee posting confidential information on a social networking site	**5%**	**12%**
An internal threat such as employee stealing data on USB key or leaking information to competitors	**4%**	**8%**
Other	**3%**	**3%**

OF THE BUSINESSES WHO HAD EXPERIENCED A CYBER ATTACK:

54% HAD FALLEN VICTIM TO AN EMAIL OR PHISHING SCAM[2]

↑ UP 2% FROM 2016 ↑

Source
1. Norton Australian SMB Cyber Security Survey, 2016
2. Norton Australian SMB Cyber Security Survey, 2017

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 cyber crime has evolved to adapt to changing online habits, and there are a whole host of cyber attacks and threats that could put your devices and business-critical data at risk. Below are the main types of cyber threats that you and your employees should be aware of.

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.[2] It also includes apps for mobile devices, such as those running Android and iOS operating systems.

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.[4] Ransomware can be particularly crippling for a small business that can't afford downtime without access to business-critical data.

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 information. 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.

PHISHING

Essentially phishers are nothing more than tech-savvy online 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.[3]

ONLINE SCAMS

Facebook and Twitter have collectively over 1 billion active monthly users - a haven for online 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 unknowingly downloaded spyware on to their device, potentially collecting personal or confidential information.[5] It's important that all employees in a small business are aware of these risks and what is considered acceptable social media and online usage when at when either at work, or on work devices.

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.

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

Norton by Symantec

CYBER THREATS BY NUMBERS

THE FINANCIAL COST OF CYBER CRIME TO AUSTRALIAN SMALL BUSINESSES IS HIGHER THAN EXPECTED

IN ONLY 12 MONTHS,
THE COST MORE THAN ***DOUBLED*** TO

$10,299 AUD

UP FROM
$3,708 AUD IN 2016

WITHIN THE ASIA PACIFIC AND JAPAN REGION, AUSTRALIA RANKS[6]:

2nd

HIGHEST TARGETED CYBER THREATS BY CRYPTOMINERS

5th

HIGHEST TARGETED FOR RANSOMWARE ATTACKS

ONLINE SCAMS

10% OF EMPLOYEES HAD FALLEN VICTIM TO ONLINE SCAMS

THE TYPE OF SCAM

- Online purchase scam 55%
- Online support scam 28%
- Fake charity 19%
- Other/Don't know 19%

THE COST OF ONLINE SCAMS TO BUSINESSES[7]:

ONLINE SCAMS COST 20% OF VICTIMS BETWEEN $1,000 - $5,000 AUD[7]

ONLINE SCAMS COST 6% OF VICTIMS OVER $5,000 AUD[7]

6. Symantec Internet Security Threat Report 23, 2017
7. Norton Australian SMB Cyber Security Survey 2017

Norton by Symantec

PREVENTATIVE MEASURES

The rise of cyber attacks has meant that there is an increasing requirement for small businesses to take preventative measures to help keep their business critical data secure.

In the event of loss of access to critical business information, small businesses would likely experience significant downtime, costing them loss of potential revenue as well as countless hours dedicated to retrieving the information.

FORMAL POLICY AND MANDATORY TRAINING[8]

Businesses surveyed had neither a formal security policy nor mandatory training in place	**55%**
Businesses with a formal policy	**33%**
Businesses have mandatory training in place	**20%**

BACKUP/RECOVERY[8]

20% of micro and small businesses backed up their business data no more than monthly (down from 24% in 2016). Almost one third (32%) were backing up continuously (improved from 26% in 2016).

WHERE IS DATA BACKED UP?[8]	2016	2017
External hard drive	**62%**	**67%**
In the cloud	**24%**	**32%**
Offsite server	**21%**	**17%**
Computer only	**25%**	**16%**

Wi-Fi[8]

40% of business have employees on the road or working remotely.

Half of the respondents surveyed were accessing public Wi-Fi from a mobile device, and most took security precautions in some form, but use of VPN was limited (only 18%).

Almost 2/3 of businesses have a router, and using the router supplied by the ISP provider was common. 45% had used a router purchased elsewhere (other than their ISP).
Less than half of the businesses surveyed were taking adequate security measures regarding their router. Only 48% had performed firmware updates on their router and 38% regularly change their router or Wi-Fi password.

8: Norton Australian SMB Cyber Security Survey, 2017

Norton by Symantec

RECOMMENDED BEST PRACTICES

Here are our recommended best practices to help keep your business safe from cyber criminals:

- **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 cyber attack 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 to understand 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 cyber attack, SMBs must implement comprehensive security software solutions for all their devices. Businesses should also backup regularly 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. This means every PC, laptop, tablet, mobile device or router that the business owns and that every employee uses to access work-related information.

- **Keep up-to-date:** Ensure all your company devices, routers, operating systems, software and applications are always kept up to date with the latest versions and patches. It's a common pitfall for many small businesses to delay software updates, however outdated software, operating systems and applications can have security vulnerabilities that can be exploited, leaving many small businesses open to potential cyber attacks.

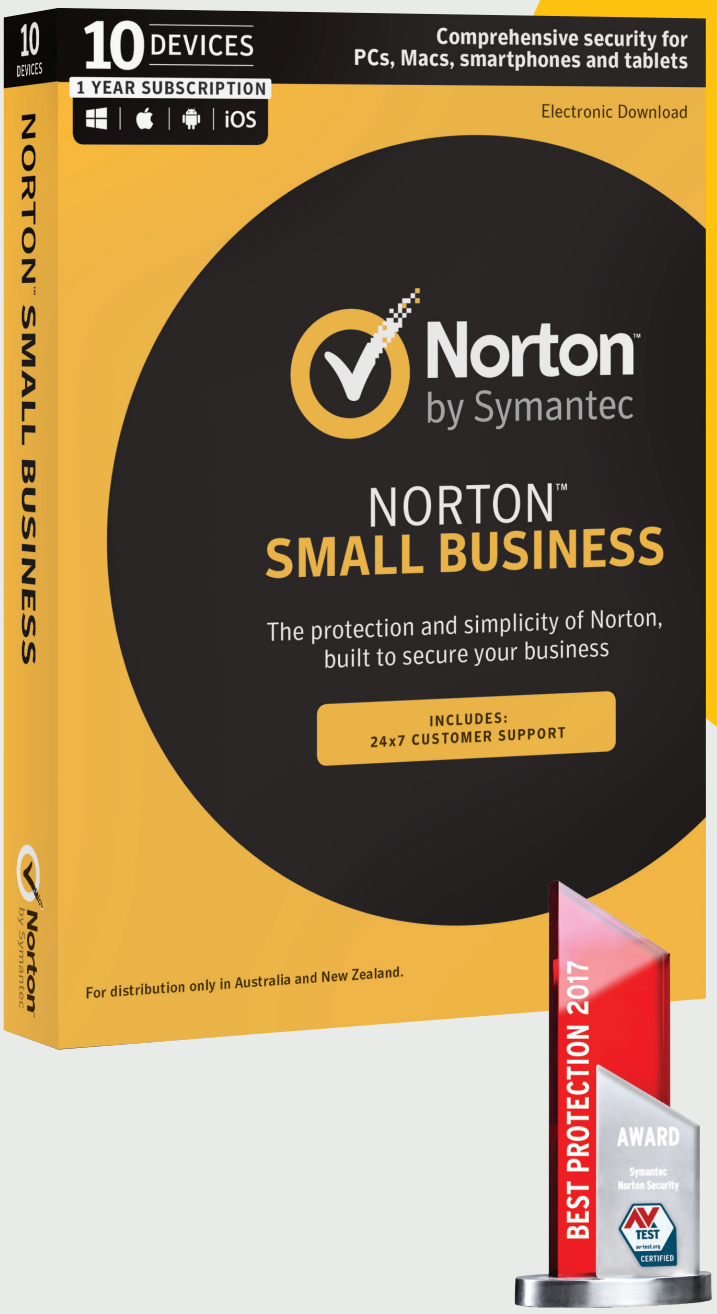
- **Get employees involved:** Employees play a critical role in helping to prevent cyber attacks, and should be educated on security best practices. Since small businesses have fewer resources, all employees should be vigilant and know how to spot phishing scams, ransomware attacks and be aware of which sites they can visit on their work devices. Small businesses should invest in the education of their employees via mandatory training sessions or implementing a formal policy so they become your best line of defence against cyber attacks, not your weakest link.

- **Use strong passwords:** Use unique passwords for all your devices, business accounts and routers too. Change your passwords every three months and never reuse your passwords. Wi-Fi networks and routers should also be password protected to help ensure a safe working environment. Using a password manager like Norton Identity Safe can help you and your employees secure all accounts.

- **Get Wi-Fi savvy:** When connecting to public Wi-Fi or unsecured networks, make sure you use a virtual private network (VPN), so all data sent and received is encrypted. A VPN 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

TURN UNCERTAINTY INTO SECURITY...



NORTON™ SMALL BUSINESS

PC PCMAG.COM EDITORS' CHOICE™

39 TIME WINNER

The Most Awarded Consumer Security Brand Ever

iOS

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

Norton Small Business[9] combines enterprise-grade security with ease-of-use designed for you. A single subscription helps protect 10 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.

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.

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

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

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]

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]

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

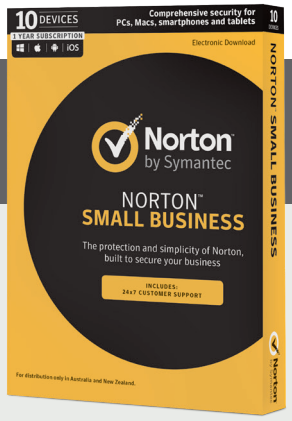
Scalable and Flexible
Allows you to easily add protection to new devices, or move protection between devices as your business needs grow or change.

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.

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.

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://au.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